IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 November 2023, accepted 15 January 2024, date of publication 24 January 2024, date of current version 2 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3357940

SURVEY

A Taxonomy of Challenges for Self-Sovereign Identity Systems

ABYLAY SATYBALDY[1], MD. SADEK FERDOUS[2], AND MARIUSZ NOWOSTAWSKI[1]
[1]Department of Computer Science, Norwegian University of Science and Technology, 2815 Gjøvik, Norway
[2]Department of Computer Science and Engineering, BRAC University, Dhaka 1212, Bangladesh

Corresponding author: Abylay Satybaldy (abylay.satybaldy@ntnu.no)

ABSTRACT Creating and utilizing digital identities are fundamental steps towards accessing online services. In order to facilitate the management of user identities, the concept of identity management has been introduced. Various systems and protocols have been developed to manage online identities. However, these systems are provider-centric, focusing on aiding providers in managing their user bases. As a result, users often have limited control over their identity data and remain unaware of how centralized identity providers use or potentially misuse their data. Self-Sovereign Identity (SSI) has emerged as a new paradigm in the digital identity management landscape, aiming to empower users by allowing them greater control over their identity data. Although SSI is a relatively new domain, there have been numerous efforts, primarily from the industry, to introduce SSI standards, protocols, and systems, with multiple options in each category. Researchers eager to contribute to the SSI domain might find it challenging to understand the interconnections among these components. Notably, the SSI domain faces several challenges, as highlighted in various research works. These challenges must be addressed before SSI can achieve widespread adoption. This article presents a comprehensive systematic literature review of SSI, offers a detailed taxonomy, and identifies and analyzes the open challenges in SSI.

INDEX TERMS Self-sovereign identity, digital identity, taxonomy.

I. INTRODUCTION

Self-Sovereign Identity (SSI) is a paradigm that puts individuals in full control of their own personal data, allowing them to determine when and how it is shared with others [1]. Unlike traditional identity systems, SSI eliminates the need for a central authority to hold and disseminate data upon request. Instead, individuals have the ability to independently present identity claims themselves. Identity claims and credentials can be verified with cryptographic certainty. This shift in identity management is facilitated by the use of cryptographic techniques and verifiable data registries. This enables individuals to share their data directly with chosen recipients in a secure and trusted manner without the need for central intermediaries.

The concept of SSI acknowledges the significance of privacy, consent, and individual agency in the digital realm [2]. SSI empowers individuals to act as custodians of their own data, ensuring that personal information remains under their control and is not subject to control or exploitation by centralized entities. Through SSI, individuals gain the ability to selectively disclose specific claims, data elements or attributes, allowing users to engage in digital interactions while maintaining authority over their identities. Within this model, the identity *holder* retains the ownership of their identity information and credentials, while *issuers* are responsible for issuing verifiable credentials to holders. *Verifiers*, in turn, rely on these credentials to authenticate and validate the presented identity. Such a model enables individuals to securely exchange credentials with verifiers, establishing trust and facilitating a wide range of digital interactions without the need for centralised intermediaries.

An SSI system minimizes trust in third parties and leverages cryptographic technologies, distributed ledgers, and standardized protocols to ensure the security, privacy, and interoperability of identity data. While the concept of SSI

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Guidi.

holds great promise, there are various challenges that need to be addressed. These challenges span multiple dimensions, including technical, legal, and social aspects.

In this research work we provide three contributions to the field of SSI. Firstly, we undertake a thorough systematic literature review, critically analyzing academic and grey literature sources. Through this comprehensive review and synthesis, we formulate an architectural framework that provides a structured overview of the SSI stack. Additionally, we define the development phases specific to SSI systems. Secondly, we identify and analyze the open challenges prevalent in the field. Lastly, we propose a taxonomy for these challenges, mapping them into the aforementioned architectural framework and classifying them based on their respective development phases and categories. This classification offers a structured and organized perspective on the diverse range of challenges, aiding researchers and practitioners in better understanding and addressing these obstacles. Overall, the contributions of this article advance the understanding of SSI systems, provide insights into open challenges, and offer directions for future research and development in this field with a structured and synthesized taxonomy.

The remainder of this article is structured as follows. In Section II, we provide an overview of the existing literature and discuss relevant studies that have contributed to the SSI development and the identification of open challenges. Section III outlines the methodology for conducting the study. Subsequent sections present the findings of the study, including the architectural framework for the SSI stack (Section IV), the identified development phases for SSI systems (Section V) and challenges (Section VI). In Section VII, we present a taxonomy categorizing the identified challenges. Lastly, in Section VIII, we summarize the key contributions of the article and discuss directions for future research.

II. RELATED WORK

In recent years, SSI has gained significant attention from researchers and practitioners, resulting in a growing body of research works that address various aspects of SSI. This section provides an overview of the existing literature and research efforts related to SSI systems.

Several studies have focused on conducting systematic reviews of the literature on SSI. Kuperberg [3] conducted a systematic survey of solutions and technologies in the SSI field, establishing an extensive structured set of evaluation criteria and evaluating existing SSI solutions. Čučko et al. [4] presented a systematic map of decentralized and self-sovereign identity solutions, classifying research papers based on predefined parameters such as contribution, application domain, IT field, research type, research method, and place of publication. Schmidt et al. [5] conducted a systematic grey literature review to structure the SSI ecosystem. They derived a four-dimensional taxonomy that portrays members of the SSI ecosystem and classified them into eight archetypes. Ahmed et al. [6] presented a literature review of state-of-the-art academic publications and commercial market offerings regarding the applicability of blockchain-based SSI solutions. The article suggested that authentication, integrity, privacy, trust, and simplicity are crucial for developing effective SSI solutions. Mühle et al. [7] examined the basic components of SSI, including identification, authentication, verifiable claims, and attribute storage. They discussed how different research studies and market offerings attempt to address each of these components.

There are limited research papers that have specifically explored and discussed open challenges for SSI systems. Schardong et al. [8] conducted a comprehensive systematic review of the literature, mapping theoretical and practical advances in SSI. They classified surveyed papers and discussed the practical problems introduced and solved in these papers. Bai et al. [9] reviewed works that use distributed ledgers to implement SSI. Based on their analysis and comparison of various blockchain-based SSI implementation schemes, they summarized the development difficulties and pointed out future development directions. Bartolemeu et al. [10] provided a review and discussion of the use cases, technologies, and challenges that SSI faces in the context of Industrial Internet of Things (IoT) applications. They discussed potential advantages and key challenges that needed to be addressed. Zhu and Badr [11] also reviewed papers that use blockchain to implement SSI in the context of IoT devices. Giannopoulou [12] provided an overview of current SSI solutions within the technological environment involving decentralized networks, analyzing challenges related to data protection and privacy laws.

In contrast to the aforementioned research efforts, the main goal of our systematic review of the literature was to identify open challenges and propose a taxonomy that classifies these challenges within a well-defined framework and easily understood categories. This facilitates synthesis and eases comparisons across the research of diverse initiatives. Furthermore, our approach goes beyond blockchain-based SSI solutions and does not focus on a specific use case or challenge, but instead seeks to provide a comprehensive understanding of the challenges in the SSI ecosystem. We acknowledge the valuable insights provided by previous works on systematic reviews and surveys, which have contributed to the development of the taxonomy of challenges for SSI systems in this paper.

III. RESEARCH METHODOLOGY

This section provides an overview of the research methodology for this study. The main research objectives are:

- Synthesis of the architectural framework based on the literature review in order to provide a comprehensive and consolidated description of the architecture for the SSI stack, offering a structured overview of its components and their interrelationships.
- Define a System Development Life Cycle (SDLC) specifically tailored for the development of SSI systems,

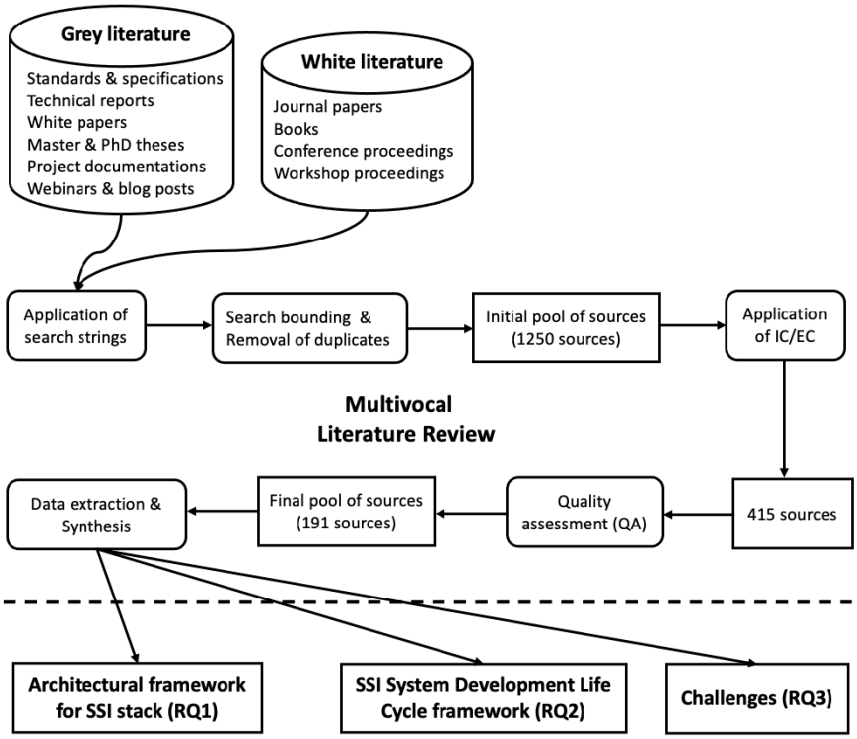

FIGURE 1. Research methodology.

taking into account their unique characteristics and requirements. The focus here is placed on decentralized and distributed systems, simplification and suitable for taxonomy and classification.

- Identify and classify the open challenges that exist in the field of SSI, providing a systematic understanding of the obstacles and potential areas for improvement, on the basis of the two previous points. Taking into account the synthesized architectural framework and SDLC from point 2.

Based on the objectives defined above, we formulate our research questions:

1) RQ1: What are the existing frameworks, components, and applications within the SSI ecosystem? This question explores the various architectural models, technical components, and real-world applications that are part of the SSI landscape.
2) RQ2: What are the defined system development phases, specifically for SSI systems, as outlined in the existing literature? This question explores the literature to identify and understand the different stages or phases that have been proposed or discussed for the development of SSI systems. By examining the existing literature, we seek to gain insights into the systematic approach taken in the design, implementation, and deployment of SSI systems, allowing us to build upon the established knowledge and practices in the field.
3) RQ3: What are the challenges faced in the design and implementation of SSI systems, and how can these challenges be effectively classified? This question focuses on identifying and categorizing the specific challenges that arise during the development and deployment of SSI systems, enabling a structured understanding of the obstacles encountered.

A. MULTIVOCAL LITERATURE REVIEW (MLR)

We conducted an MLR following the guidelines provided by Garousi et al. [13]. An MLR is a variant of the Systematic Literature Review (SLR) that encompasses both published (white) literature and grey literature. Our motivation for including grey literature stems from its potential to reveal additional challenges beyond those derived solely from white literature. Moreover, given the current limited availability of academic literature on SSI, the inclusion of grey literature is crucial for identifying a broader range of issues.

Following the guidelines for conducting an MLR formulated by Garousi et al., we present the source selection process, search strategy, quality assessment of sources, and the methodology for extracting relevant data from the selected sources. The review process for this study is described in the following sections and illustrated in Figure 1. To conduct the review, we followed the subsequent steps:

1) SOURCE SELECTION

Academic literature, also known as white literature, comprises peer-reviewed publications created by researchers, scholars, and experts. It encompasses various written works, including journal articles, books, conference papers, and

workshop proceedings that have undergone rigorous peer review. In our pursuit of white literature sources, we conducted searches on prominent academic online repositories, including the ACM Digital Library, IEEE Xplore, Springer Link, Science Direct Elsevier, and Google Scholar. Additionally, we incorporated Google's regular search engine to identify grey literature sources relevant to our research objective. Grey literature encompasses diverse literature that has not been published through conventional peer-review publishing channels. This category includes specifications, technical reports, theses, white papers, project documents, and industry reports.

2) SEARCH STRATEGY

The specific search strings were utilized for the selected online libraries (for the white literature search) and the Google search engine (for the grey literature search). Initially, we developed the search strings using a set of terms relevant to the RQ1 and RQ2 as shown below:

- (''self-sovereign identity'' OR ''decentralized identity'' OR SSI) AND (standard OR framework OR components OR application OR protocol OR architecture)
- (''decentralized system'' OR ''self-sovereign identity system'' OR ''self-sovereign identity'') AND (''development'' OR ''implementation'' OR ''design) AND (''principle'' OR ''process'' OR ''life cycle'' OR ''methodology'')

Subsequently, we formulated additional search strings to address the RQ3:

- (''self-sovereign identity'' OR ''decentralized identity'' OR SSI) AND (analysis OR evaluation OR review OR challenge OR issue OR problem OR limitation)

3) SEARCH BOUNDING AND REMOVAL OF DUPLICATES

To limit the search scope and exclude irrelevant grey literature, we implemented the Effort Bounded strategy [14] by focusing on the first 100 Google search results. Additionally, within our source pool, we ensure that only one instance of each source from multiple repositories is considered.

4) APPLICATION OF INCLUSION AND EXCLUSION CRITERIA

We established and applied specific criteria to determine which sources would be included or excluded from our analysis. These criteria were directly applied to the sources obtained from online repositories, based on the evaluations of the papers' titles, keywords, and abstracts. Our inclusion criteria (IC) and exclusion criteria (EC) were designed to gather sources that are relevant to our research goal:

- IC1: The identified sources directly relate to the topic of SSI and are highly relevant to our research objectives.
- IC2: The source is a peer-reviewed item of white literature or a credible item of grey literature.
- IC3: The literature item is written in English.

Conversely, the exclusion criteria we applied were as follows:

- EC1: The publication date is prior to January 2017.
- EC2: Claims made in grey literature cannot be verified.
- EC3: The source is inaccessible for reading or unavailable for download.

Any sources that did not meet the aforementioned inclusion criteria or met any of the exclusion criteria were excluded from our analysis.

5) QUALITY ASSESSMENT OF SOURCES

Every source in the pool was thoroughly read and evaluated in its entirety. Each author assessed the quality of the sources, considering various aspects recommended by Garousi's guidelines for conducting MLRs. These aspects included the authority of the source, methodology employed, objectivity of the content, reliability of the information presented, and relevance to our research questions.

We identified a total of 1250 sources by applying the designated search strings and removing any duplicates. We conducted a thorough review of the titles, abstracts, and keywords of these studies and applied our predefined inclusion and exclusion criteria. This process resulted in the approval of 415 sources for further analysis. Subsequently, we performed a comprehensive assessment of the quality of the selected sources based on their full-text content. Following the completion of all the aforementioned stages, as illustrated in Figure 1, our final pool consisted of 191 relevant sources. We identified 88 sources that are related to RQ1, 18 sources that are relevant to RQ2, and 85 sources that are applicable to RQ3.

6) DATA EXTRACTION AND SYNTHESIS

Once we compiled our final pool of sources, we proceeded with the data extraction and synthesis phase, which included both white and grey literature sources. During this phase, we carefully synthesized the information to formulate an architectural framework for the SSI stack (RQ1) and define the development life cycle for SSI systems (RQ2). Additionally, we systematically documented all the challenges and issues discussed in the literature (RQ3). In total, we identified 25 challenges.

IV. ARCHITECTURAL FRAMEWORK FOR SSI STACK

In our review for RQ1, we examined various sources identified from an MLR, including academic articles, standards, specifications, and technical documentations. Furthermore, we conducted an analysis of existing frameworks from Trust over IP Foundation [15], Sovrin Foundation [16], and Decentralized Identity Foundation [17]. We carefully synthesized our findings and present an architectural framework for the SSI stack that integrates technology with human accountability across legal and social layers, thereby forming a complete four-layer architecture (Layer 1, Layer 2, Layer 3, and Layer 4 as illustrated in Figure 2). Compared to existing frameworks, the proposed framework offers a more comprehensive and detailed representation of the SSI architecture. The framework is articulated through two stacks: the SSI technology stack and the SSI governance

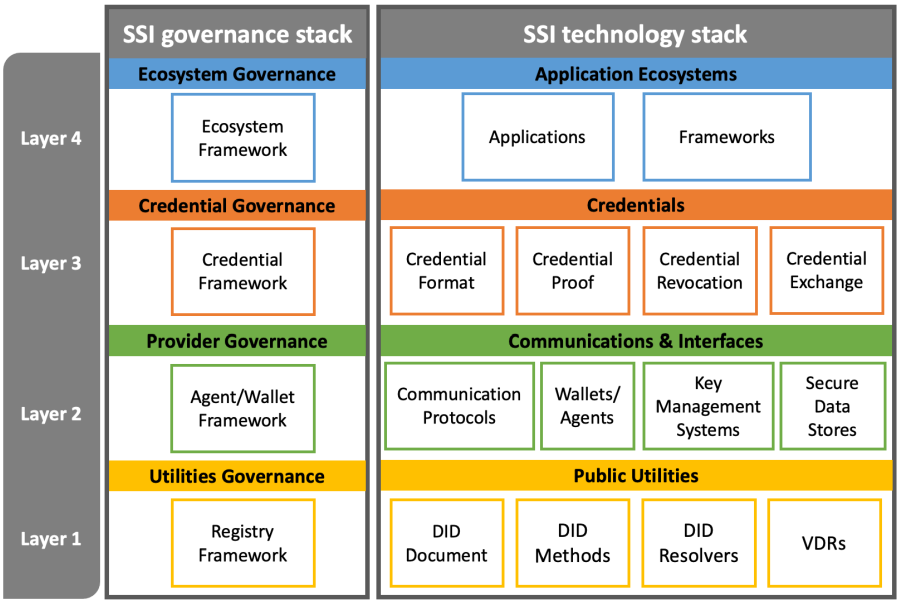

FIGURE 2. SSI stack includes both a governance and a technology.

stack. The former consists of numerous components, with multiple implementations available for each, providing a diverse array of choices to enable the required functionalities of self-sovereign identities. The latter refers to the set of frameworks that govern the operation and management of SSI systems, encompassing rules, policies, and mechanisms that enable individuals to maintain control over their identities and personal data. We will introduce and outline the components that constitute each layer within the SSI stack in the following sections.

A. LAYER 1: PUBLIC UTILITIES

Layer 1 of the SSI architecture serves as the foundational layer responsible for establishing the infrastructure and utilities necessary to create and manage decentralized identifiers (explained below) and cryptographic keys. The primary objective of this layer is to ensure a consensus among all stakeholders regarding the accurate interpretation of an identifier's reference and the cryptographic key required to verify control over that identifier.

The creation of trust revolves around decentralized identifiers that represent the SSI actors. The technical public utilities layer encompasses components related to decentralized identifiers, such as verifiable data registries for their storage and mechanisms for resolving them into documents containing relevant information. It is crucial to differentiate between technical trust through public utilities, which enables the establishment of trust among SSI actors through technologies like public-key cryptography, and legal trust, which empowers SSI actors to place trust in one another within a legally binding registry framework. Here, we focus on the technological aspect and will delve deeper into the discussion of Utilities Governance and registry framework in Section IV-E. Figure 4 presents different components of Layer 1.

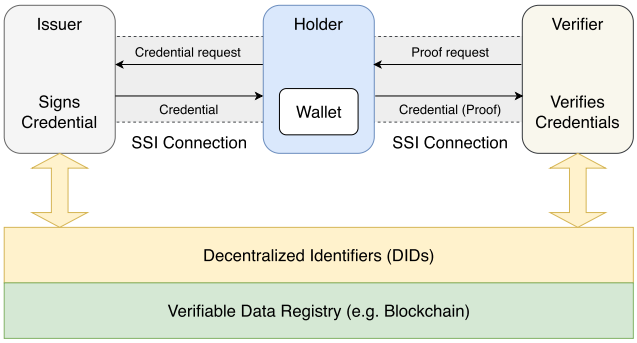

FIGURE 3. SSI actors.

1) ACTORS

SSI has three major actors: Issuer, Holder, and Verifier. An issuer is responsible for issuing a verifiable credential (VC, discussed in Section IV-C) to a user (holder) when it receives a credential request from the user. The user stores this VC in an SSI wallet. Next, in order to access a service, the verifier would request a proof, and the user releases this VC as proof to the verifier. The verifier can verify the validity of this VC in a decentralized way without relying on any third party, thereby facilitating decentralized verification within the SSI. In order to engage in these activities, SSI entities usually need to establish a pairwise SSI connection. This connection provides a secure private communication link between any two SSI entities. Figure 3 illustrates the different actors within SSI along with their interactions.

2) DECENTRALIZED IDENTIFIER

In the context of SSI, identifiers play a critical role in uniquely referencing SSI actors in a global context. Various identifier schemes exist, such as the International Standard

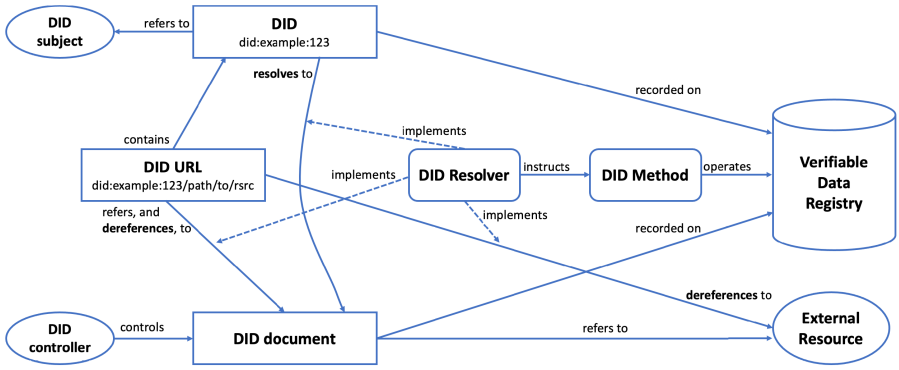

FIGURE 4. Detailed overview of Layer 1 architecture and the relationship of the basic components.

Book Number (ISBN), the Global Trade Item Number, and the Uniform Resource Identifier (URI). All of these examples require a central registry to issue and maintain the identifiers. SSI utilizes the emerging scheme called Decentralized Identifiers (DIDs) [18]. These DIDs are standardized by the World Wide Web Consortium (W3C) and offer a novel approach to identification in a decentralized way within the SSI framework. DID has the format of a URI scheme and is in the form `did:<DID method>:<method-specific identifier>`. A *DID URL* extends the syntax of a basic DID to incorporate additional standard URI components such as path, query, and fragment as shown in Figure 4. This extension allows for the location of specific resources, for instance, a cryptographic public key within a DID document or an external resource.

3) DID DOCUMENT

DIDs are resolvable to DID documents which contain additional information associated with a particular DID such as cryptographic public keys and authentication suites. Additionally, the document may include service endpoints that describe how to reach the DID subject and establish trusted communication channels. Organizations seeking public visibility can create public DIDs. The corresponding DID documents can be stored directly in a verifiable data registry (VDR), such as a distributed ledger. DID document includes the DID of the DID subject and, optionally, the DID of a DID controller, which is an entity that has the right to modify the document as authorized by the DID subject.

4) DID METHOD

A DID method serves as the mechanism through which a specific type of DID is created, resolved, updated, and revoked, along with its associated DID document. DID method-specific operations are:

- Create: This operation involves creating a new DID, configuring cryptographic keys, and defining a service endpoint.
- Resolve: The resolve operation is used to retrieve the DID document associated with a particular DID, which contains relevant information.
- Update: With the update operation, a DID can be modified by adding or extending cryptographic keys, defining additional service endpoints, or rotating cryptographic keys.
- Revoke: The revoke operation allows for the revocation of a DID, limiting its usage within the latest state of the VDR.

Currently, there exist numerous DID methods, each offering distinct features and capabilities [19]. Fdhila et al. [20] conducted an evaluation of various DID methods, examining their qualities and characteristics. Examples of some of the most popular DID methods are: did:ethr (Ethereum), did:btcr (Bitcoin), did:indy (Hyperledger Indy), did:sov (Sovrin Network), did:web (DID is resolved through the Domain Name System), and did:key (Ledger-independent DID method based on public/private key pairs).

5) DID RESOLVER

A DID resolver is a system component (software and/or hardware) that takes a DID as the input and produces a conforming DID document as its output. Its primary function is to execute read operations that enable the resolution of a DID to a corresponding DID document. Additionally, the DID resolver handles the dereferencing of DID URLs to retrieve associated resources. The steps for resolving a specific type of DID are defined by the relevant DID method specification. The Universal Resolver by Decentralized Identity Foundation (DIF) can be used to resolve DIDs across many different DID methods based on the W3C DID Core [18] and DID Resolution [21] specifications.

6) VERIFIABLE DATA REGISTRY

A VDR is a system designed to store DIDs and provide the necessary data to generate DID documents. VDRs can take various forms, including distributed ledgers, decentralized file systems, databases, peer-to-peer networks, and other

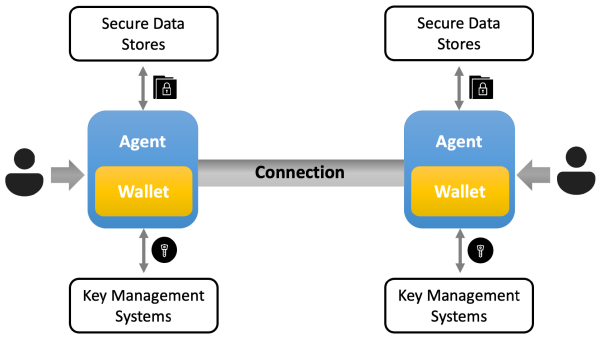

FIGURE 5. Layer 2: Communications and Interfaces.

trusted data storage solutions [2]. To establish technical trust and facilitate interactions between SSI actors, public DIDs and their corresponding DID documents need to be stored in a VDR. For example, the Ethereum blockchain network can be utilized to resolve DIDs using the *did:ethr* method. Distributed ledger technology offers desirable properties such as verifiability, availability, and immutability, which align with the requirements of public DIDs and DID documents, thereby contributing to the establishment of technical trust. Nevertheless, distributed ledgers are not the sole option for serving as DID anchors. Alternative approaches exist, including the Key Event Receipt Infrastructure (KERI) [22], web servers, the Interplanetary File System (IPFS), and even Public Key Infrastructures (PKIs). Depending on the context, trust may lie in the technology itself or the institution responsible for operating the instances.

B. LAYER 2: COMMUNICATIONS AND INTERFACES

Layer 1 focuses on establishing decentralized trust roots, whether publicly verifiable or peer-to-peer. Layer 2 is dedicated to establishing trusted communications among peers that rely on those trust roots. This layer encompasses communication protocols, digital agents, key management systems, and data stores, which facilitate secure DID-to-DID connections. Figure 5 illustrates different components of Layer 2.

1) COMMUNICATION PROTOCOLS

There are many existing robust mechanisms for secure communication. However, most rely on key registries, identity providers, certificate authorities, browsers or app vendors, or similar centralized entities. There needs to be a secure, private communication methodology built atop the decentralized design of DIDs. The DIDComm protocol [23] can fill this gap. It is a novel DID-based asynchronous end-to-end encrypted communication and messaging protocol maintained by the DIF. This protocol has various distinguishing characteristics that set it apart from other secure communication protocols. According to the specification, DIDComm is designed to be transport-agnostic, flexible, and interoperable [24]. It serves as the foundation for higher-level protocols to be implemented on top, inheriting the security and properties of DIDComm. For example, the presentation exchange protocol [25] allows a verifier to request credentials from a holder. DIDComm is widely adopted as the message envelope in the SSI technology stack. The DIDComm specification defines three message formats: DIDComm plaintext message, DIDComm signed message, and DIDComm encrypted message. These messages are typically encoded as JSON and follow the JSON Web Message (JWM) [26] specification. While plaintext messages do not guarantee any confidentiality or integrity, the DIDComm signed message ensures message integrity through a digital signature following the JSON Web Signature (JWS) [27] format. The DIDComm encrypted message, on the other hand, prevents unauthorized access by encrypting the content using the JSON Web Encryption (JWE) [28] format, providing both confidentiality and integrity guarantees.

2) WALLETS/AGENTS

A digital wallet refers to the software or hardware responsible for securely storing identity data and cryptographic contents. In the context of SSI solutions, this includes the storage of VCs, DIDs, and their associated cryptographic keys. An *agent*, acting on behalf of the user, interacts with other agents to perform various actions [2]. It typically accesses the digital wallet to store, retrieve, and perform cryptographic operations on identity data. The SSI agent is capable of signing, encrypting, and forwarding messages related to credentials and establishing agent-to-agent connections. These actions can be programmed to be executed automatically by the agent or manually by the user. As shown in Figure 5, an agent can be viewed as a digital guardian that wraps around the digital wallet, ensuring its protection and allowing only the identity owner, the individual responsible for verifiable credentials and cryptographic keys, to access and utilize them. Additionally, an agent can operate either on an edge device or in the cloud. Edge agents function at the network's edge, residing on the user's local devices, while cloud agents operate in the cloud, hosted by standard cloud computing platforms or specialized cloud service providers known as agencies. Cloud agents can also be designed to store and synchronize other data on behalf of an identity owner in secure data stores.

3) SECURE DATA STORES

Secure and encrypted storage, as well as privacy-preserving computation of data, are vital components of decentralized identity systems. Just as identifiers and names must be self-sovereign, meaning under the control of the owning entity, an individual's identity data must also remain private and accessible only to entities authorized by the individual. To address this, the DIF has established the Secure Data Storage working group [29], with the aim of developing specifications for secure data storage in SSI systems. The group is actively working on two key initiatives: Encrypted Data Vaults (EDV) [30] and Decentralized Web Node (DWN) [31]. The EDV specification is a collaborative effort between the

DIF and the W3C Credentials Community Group. It defines a privacy-respecting mechanism for securely storing, indexing, and retrieving encrypted data at a storage provider. It ensures that the storage provider cannot view, analyze, aggregate, or sell users' personal data. Additionally, this approach enables the portability of application data and safeguards it against data breaches by storage providers. The DWN, formerly known as the Identity Hub, serves as a data storage and message relay mechanism that enables entities to locate public or private permissioned data associated with a specific DID. DWNs operate as mesh-like data storage structures, allowing entities to manage and exchange their data with others without relying on location-specific infrastructure, provider-specific interfaces, or routing mechanisms. Through these initiatives, the DIF is working towards establishing secure and privacy-preserving data storage in SSI systems, promoting user control, data portability, and protection against unauthorized access or data breaches.

4) KEY MANAGEMENT SYSTEMS

In SSI systems, effective key management is a crucial aspect that encompasses the generation, storage, and safeguarding of cryptographic keys. In order to perform various operations within the system, such as creating message envelopes and establishing communication channels using DIDComm, agents must possess and control DIDs and their corresponding keys. Several organizations are already addressing the challenge of decentralized key management directly. One notable development is the emergence of the Decentralized Key Management System (DKMS), an open standard that outlines best practices for key usage, rotation, recovery methods, multi-device management, and key generation [32]. Additionally, the Wallet Security working group at the DIF [33] is dedicated to producing guidelines and defining security requirements applicable to identity wallet architectures. This includes key management, credential storage, credential exchange, backup and recovery mechanisms, as well as wallet portability.

In the traditional identity management models, key management relies on a trusted third party. However, in the SSI model, the responsibility of key management is shifted to the identity owners themselves. This is because there is no central authority that can restore user access in case of key or device loss. Therefore, a decentralized key backup and restore functionality is essential. Currently, there are two primary methods of key recovery in self-sovereign identity systems. The first method involves the creation of deterministic keys using a mnemonic code known as a seed phrase. This seed phrase is a human-readable encoding of the wallet's root private key, typically consisting of 12 to 24 mnemonic words. Users are required to back up the recovery mnemonics and ensure the set safekeeping. In the event of key loss, the mnemonics set can be used to regenerate the private key. This recovery option is widely used in cryptocurrency wallets and many existing identity wallets [34]. The second method is social recovery, where trusted entities known as ''trustees'' store recovery data on behalf of the identity owner. This data is typically stored in the trustees' own wallets. The Shamir Secret Sharing algorithm is commonly employed to split a private key into shares that are distributed among the trustees. In the event of key loss, the identity owner can retrieve the shares from the trustees to recover their private key [35].

The trust established between entities at this layer is limited to cryptographic trust. This means that there is trust in the control of a DID by another peer, the security of a DID-to-DID connection, and the authenticity of messages sent over the connection without tampering. While these conditions are necessary, they are not sufficient to establish human trust because they do not provide information about the person, organization, or entity associated with the DID. For instance, a DID-to-DID connection does not consider factors such as the ethics, honesty, or qualifications of the remote party. It only ensures that communication can occur in a tamper-proof and confidential manner. To address these aspects and establish trust in the actual entities involved, we need to move up to Layer 3.

C. LAYER 3: CREDENTIALS

Layer 3 focuses on credentials: its format, exchange, revocation, and other aspects. In the following, we explore these aspects involving credentials.

1) CREDENTIAL DATA FORMATS AND PROOF TYPES

In SSI, a credential is regarded as a collection of claims digitally signed by an issuer where each claim is a statement about the subject (a user). Verifiable Credentials (VCs) are tamper-proof credentials that can be verified cryptographically. VCs facilitate secure data transfer while ensuring data subjects maintain control over their information, making them increasingly relevant in both the private and public sectors. However, achieving interoperability and seamless implementation of digital credentials requires the establishment of a universal data format. Various credential formats, such as W3C VCs [36], AnonCreds [37], and ISO mDL standards [38], have emerged, each supporting different cryptographic proofs. Despite their differences, these formats share a common purpose: enabling issuers to package claims about an entity and seal the credential using cryptography. Through cryptographic signatures, verifiers can assess the integrity of the credential based on the issuer's public keys. The divergence lies in how issuers format claims within the credentials and utilize cryptographic signature suites for signing and sealing the credentials.

The AnonCreds v1.0 (Anonymous Credentials) specification [37] is built upon the open-source verifiable credential implementation developed as part of the Hyperledger Indy project. It introduces essential privacy-enhancing features to the core assurances of VCs. AnonCreds utilizes Camenisch-Lysyanskaya signatures to encode individual claims, enabling selective disclosure and preserving privacy. This allows users to prove specific criteria about their claims without revealing

the entire content. Additionally, AnonCreds supports non-correlating identifiers, generating unique identifiers for each connection between a holder and a verifier. This approach mitigates the privacy risks associated with using a single identifier across multiple online services, preventing user profiling. It is important to note that AnonCreds predates the W3C Verifiable Credentials standard and does not fully align with its specifications.

The W3C has developed the Verifiable Credentials Data Model v1.1 [36], which is a widely adopted standard used in government and commercial applications. Within the W3C VC framework, there are two distinct types of verifiable credentials that differ in how they express the data model and associated cryptographic material. The first type is JSON-LD VCs using Linked Data Proofs [39] which provide semantic clarity and discernment for verifiers regarding the issuer's intended meaning for specific attributes in the credential. Recently, JSON-LD with BBS+ Signatures was introduced to provide support for selective disclosure of claims by enabling the use of zero-knowledge proofs (ZKPs) [40]. This allows users to prove specific claims without revealing the entire credential. The second type is JSON-JWT VCs, which are expressed in JSON format and utilize JWT (JSON Web Tokens) for proof formats. JSON-JWT VCs lack the means to support semantic disambiguation but are well-established and simpler to implement as an assertion format. The proof formats specified as JWT (IETF 7519 Proposed Standard) [41] or SD-JWT (IETF Internet Draft) [42] use JOSE cryptographic suites. The SD-JWT specification describes a format for signed JWTs that enables selective disclosure, allowing the sharing of only a subset of claims included in the original signed JWT, instead of disclosing all claims to every verifier.

The ISO mobile document specification, developed in ISO/IEC 18013-5 [38], primarily focuses on the mobile driving license (mDL) but can be used to specify various types of credentials. With the ISO mDL standard, the holder retains full control over the credential and has the authority to determine the extent of information provided, the timing of its provision, and the intended recipients. Selective disclosure of data elements, informed user consent and data minimization are supported by the standard. The credential proof format is specified as ISO 23220-2 Mobile Security Object (MSO) [43]. The MSO and all the claims of the mDL subject are signed using the issuing authority's private key. Public keys are associated with their corresponding identities through X.509 certificates, which must be compiled and maintained by a certification authority. While the standard mentions revocation methods, they are not defined and fall outside the scope of the standard.

2) CREDENTIAL EXCHANGE PROTOCOLS

Credential exchange is the process through which verifiable credentials are issued, held, presented, and verified. It involves the exchange of verifiable data between various parties. Several credential exchange protocols exist, such as the Aries Credential Exchange [44], DIF Credential Exchange [45], Credential Handler API [46], and OpenID for Verifiable Credentials [47].

The Aries Issue Credential Protocol 2.0 (RFC 0453) [44] is a standardized protocol designed for issuing credentials. It focuses on defining the messages exchanged between the issuer and the holder during the credential issuance process, aiming for interoperability regardless of the specific credential format or proof type. Another aspect of credential exchange is the verification of Verifiable Presentations (VPs). VP expresses data from one or more VCs, and is packaged in such a way that the authorship of the data is verifiable. The Hyperledger Aries project offers the Aries Present Proof Protocol 2.0 (Aries RFC 0454) [48], which enables seamless interactions between the prover and the verifier. Like the Issue Credential Protocol, it adopts a flexible approach that supports various proofs and credential formats. However, it is worth noting that these protocols currently have been implemented for the DIDComm v1 message envelope and are commonly used in AnonCreds-based systems.

The Presentation Exchange 2.0 specification [45], developed by the DIF, provides a data format called Presentation Definition that allows verifiers to express their proof requirements. It also introduces the Presentation Submission data format, which enables holders to describe and submit proofs that meet these requirements. This specification is designed to be independent of the specific claim format or transport envelope used. It can be used with various claim formats such as W3C JSON-LD, W3C JWT, or any other JSON format, and can be conveyed through different transport envelopes like OpenID4VC, DIDComm v2, CHAPI (Credential Handler API, discussed next), or others. Another specification from the DIF is the Credential Manifest 1.0 [49], which facilitates the interaction between an issuer and an identity holder. It defines a standard data format for capturing the necessary information from the identity holder in order to issue a verifiable credential.

The Credential Handler API (CHAPI) is an open protocol that facilitates the interaction between third-party web applications and users in managing credentials [46]. It allows web applications to request credentials from users and provides a secure interface for storing and managing those credentials for future use. CHAPI empowers users by giving them control over their wallets and the ability to choose service providers. This protocol is an extension of the Credential Handler API 1.0 draft specification [50], which is maintained by the W3C Credentials Community Group.

OpenID for Verifiable Credentials (OpenID4VC) is a protocol proposed by the OpenID Foundation, in collaboration with the DIF and working groups in ISO, to enable the exchange of verifiable credentials [47]. It builds upon the existing OpenID Connect (OIDC) protocol and offers support for various credential formats, identifiers, cryptography suites, and trust management mechanisms. OpenID4VC includes specifications for both credential issuance and

presentation. OpenID for Verifiable Credential Issuance (OpenID4VCI) [51] defines an API for issuing verifiable credentials, while OpenID for Verifiable Presentations (OID4VP) [52] outlines mechanisms for presenting claims in the form of verifiable credentials. These specifications are compatible with W3C Verifiable Credentials, ISO mobile driver's licenses (mDLs), and other credential formats. In an OpenID4VC credential exchange, the VDR can be a ledger or another decentralized data store if the presentation involves DIDs. Alternatively, the VDR can be obtained using Public Key Infrastructure (PKI) or web pages accessible under a domain name controlled by the issuer.

3) CREDENTIAL REVOCATION MECHANISMS

An issuer should possess the capability to revoke a verifiable credential in situations where the circumstances of the holder have changed, leading to inaccuracies in the credential. This could include scenarios such as the holder's authorization to use the credential being modified (e.g., loss of driver privileges), changes in the data contained within the credential (e.g., address change), or errors in the credential issuance process. Presently, there are various approaches to credential revocation for VCs.

The Verifiable Credentials Status List v2021 [53] specification proposes a mechanism for efficiently publishing status information, such as the suspension or revocation of verifiable credentials. This approach uses a binary representation to indicate the status of each credential issued by an issuer. The issuer maintains a bitstring list where each credential is associated with a position, and a binary value of 1 denotes revocation while 0 signifies that the credential is not revoked. This method allows for fast and scalable revocation status validation, with a 16KB bitstring capable of accommodating uncompressed 131,072 entries. However, one drawback of this approach is the lack of privacy, as the VP needs to include a unique identifier that points to the location in the bitstring, potentially revealing personally identifiable information with each presentation.

The AnonCreds v1.0 specification includes a revocation mechanism that ensures the validity and accuracy of credentials while maintaining privacy. This mechanism utilizes ZKPs to allow the holder to prove the non-revocation of their credential without revealing any identifying information. In the AnonCreds revocation mechanism, revocation is achieved through the use of cryptographic accumulators and tail files stored in the VDR. An accumulator is a cryptographic data structure that efficiently represents a set of revoked credentials. By incorporating the accumulator into the credential verification process, verifiers can efficiently check if a credential has been revoked without relying on a central authority or lengthy revocation lists. This approach provides a privacy-enhancing solution for credential revocation in the Hyperledger ecosystem. However, it is important to note that this mechanism has a limitation regarding the size of the tail files. Tail files can grow up to 1 GB while accommodating approximately 100,000 credentials [37]. This large size may present scalability challenges for the revocation mechanism.

Among traditional revocation mechanisms, the Certificate Revocation List (CRL) is widely used. A CRL is a timestamped list that contains entries identifying the revoked certificates. These lists can be signed by a Certificate Authority (CA) or a CRL issuer. The CRL is typically published in a public repository and is updated at regular intervals, which can range from a few hours to several weeks [54].

Summary: Table 1 summarizes different aspects of the existing credential formats that we discussed.

D. LAYER 4: APPLICATIONS ECOSYSTEMS

In this layer, we consider two different components: frameworks and applications. We will discuss each of them in the following sections.

1) FRAMEWORKS

A framework represents a concrete implementation of different components from other layers. It utilizes the components and services from the other layers, thereby creating a full technology stack that can be utilized to develop SSI applications (which will be discussed next). Currently, there are only a few such functional frameworks readily available for developing SSI applications. Next, we will discuss these frameworks along with their dependencies.

a: HYPERLEDGER ARIES

Hyperledger Aries [55] is currently one of the most prominent SSI frameworks, offering a comprehensive stack for developing SSI applications. This framework includes a toolkit that comprises infrastructure and protocols for blockchain-rooted peer-to-peer SSI interactions, as well as VC generation, sharing, and storage capabilities. To facilitate these SSI functionalities, Aries provides a set of libraries and APIs that applications can integrate within their ecosystem. Presently, Aries is primarily associated with an SSI-focused blockchain system known as Hyperledger Indy [56] (discussed later), but it aspires to be blockchain-agnostic with ongoing community efforts to achieve this goal. Aries has a number of implementations in different programming languages, e.g. Hyperledger Aries Cloud Agent Python (ACA-Py) written in Python [57] and Aries Framework JavaScript (AFJ) written in JavaScript [58]. Additionally, Hyperledger Aries relies on Hyperledger Ursa [59] for secure cryptographic operations and decentralized key management functionalities. Moreover, Aries makes use of another crucial SSI component, the SSI wallet (discussed later). Next, we delve into the details of two of its core components:

- *Hyperledger Indy:* Hyperledger Indy (or Indy, in short) is a purpose-built blockchain system for SSI [56]. It has built-in support for creating and resolving DIDs, storing DID documents and storing VC schemas. Sovrin is a special type of blockchain system that shares

TABLE 1. Verifiable credential format comparison.

Credential formats	Anoncreds	W3C JSON-LD	W3C JSON-JWT	ISO mDL
Proof types	CL-signatures	ECDSA, BBS+	JOSE	Mobile security object (MSO)
Standardization	Hyperledger Foundation	W3C Recommendation & IETF	W3C Recommendation & IETF	ISO/IEC 18013-5 & 23220-2
Exchange protocols	Aries Credential Exchange: DIDComm v1	DIF Credential Exchange: OpenID4VC, DIDComm v2, CHAPI	DIF Credential Exchange: OpenID4VC, DIDComm v2, CHAPI	ISO 23220-4 REST API: OpenID4VC, OIDC
Revocation mechanism	Anoncreds revocation v1.0	Status List v2021	Status List v2021	Certificate Revocation List (CRL)
Trust infrastructure	DLT	DLT & CA/PKI	DLT & CA/PKI	CA/PKI

the codebase of Hyperledger Indy and has similar support for storing the metadata for DIDs, the DID documents and VC schemas [60], [61]. It is a public-permissioned blockchain in the sense that anybody can submit transactions in this network, however, who can operate the network and become a validator is restricted. Sovrin is actually the first SSI-supporting blockchain and its codebase were open-sourced and released to the public under the Hyplerdger Indy project.

- *Wallets:* The Hyperledger Aries also has a community-driven open-source SSI wallet, called Aries Mobile Agent React Native or Aries Bifold [62]. It utilises the AFJ framework along with Indy SDK for its functionalities. In addition to these, there are other commercial SSI wallets such as Esatus [63], Lissi [64], Trinsic [65] and so on.

b: AFFINIDI

Affinidi is a framework that offers a range of APIs for developing SSI applications [66]. One of the key components utilized by Affinidi is the Sidetree protocol, a blockchain-agnostic protocol designed for creating and managing DIDs [67]. The Sidetree also supports a Content Addressable Storage (CAS) such as IPFS. In its present version, Affinidi leverages *Sidetree.js*, which is an implementation of the Sidetree protocol using MongoDB as the long-term cache and Ethereum as the underlying ledger. However, it remains unclear whether the current version of Affinidi can accommodate other blockchains as well.

c: VERAMO

Veramo is another API-based framework that exposes a number of APIs that can be used to carry out a number of SSI functionalities, e.g. creating DIDs, issuing VCs and so on [68]. These APIs could be used to develop SSI applications. Currently, it supports several DID methods such as Ethereum-based DIDs, Web DIDs and a light-weight self-certifying DID method (*did:key*). It aims to be ledger agnostic, however, Veramo is still in a public beta stage with many functionalities that are not properly implemented.

Apart from these frameworks, there are a few other SSI systems such as uPort [69], Jolocom [70], Civic [71], Veresone [72] and Remme [73]. All these utilise different blockchain systems to offer SSI identities, however, they do not have any comprehensive framework as Hyperledger Aries.

2) APPLICATIONS

In the application sub-layer, we examine various SSI applications across different application domains. Even though the concept of SSI is relatively new, numerous researchers have explored the possibility of integrating SSI into many domains. We will now highlight some of these research works on SSI applications, categorized according to their respective domains.

a: INTERNET OF THINGS (IoT)

We found a number of SSI-based research works within the IoT domain. For example, Fedrecheski et al. argued in [74] that the existing SSI approach assumed substantial computation and storage capabilities in IoT devices, which might not be practically feasible. To address this, they introduced a low-overhead SSI approach for IoT devices. Their main contribution was the proposal of a new extension and a concise serialization method for DIDs and their metadata, which could enable a native use of DIDs and DID-based secure communication on constrained devices. The proposal was tested in a simulated environment with a blockchain mock, meaning they did not implement their proposal in an actual blockchain system.

In [75], the authors proposed a scheme that utilized DIDs in IoT devices. According to their proposal, each IoT device is equipped with a secure key-pair during its initialization phase, which is stored in a Trusted Execution Environment (TEE) [76]. This key pair is used to create the respective DID for the device. A blockchain is used to store the required metadata and develop a registrar for recording device ownership information. The authors created a prototype based on Ethereum. However, they did not utilize any SSI framework such as Aries and did not consider the use of VCs within their system.

The authors in [77] presented a trustworthy SSI-based Identity Management framework for IoT devices. They argued that the current setup of SSI-based IoT devices would require the storage of VCs within the IoT devices, which might not be practical considering the limited storage and computational capability of many IoT devices. To mitigate this problem, the authors proposed a secret sharing-based solution that utilizes DID, DID documents, and VC

components of SSI and was implemented using an Ethereum simulator called Ganache [78]. However, their solution did not utilize any SSI framework.

In [79], Kulabukhova et al. presented an exploratory paper that compared different SSI platforms, such as Sovrin, Civic, uPort, Jolocom, Ontology, Veres One, and Remme, against a set of minimal criteria. It also explored a supply chain use case based on IoT and SSI. However, the authors did not present any architecture or discuss any implementation details.

Bartolomeu et al. explored different aspects, such as advantages, disadvantages, and challenges, involving SSI and industrial IoT [10]. This work compared several SSI systems such as Hyperledger Indy, uPort, Blockstack, Veres One, and Jolocom. Moreover, the authors identified a number of technical, standardization, organizational, and application-oriented challenges. However, this work did not present any architecture or its implementation within a specific use-case of industrial IoT.

In [80], the authors explored the requirements for integrating SSI to manage the identities of IoT devices, with a specific focus on Electric Vehicle (EV) Charging Networks. Based on these requirements, the authors presented an SSI-integrated architecture considering all entities involved in the EV charging networks. A Proof of Concept using Hyperledger Indy and Hyperledger Aries was also presented. The authors evaluated the requirements and the developed systems by gathering opinions from domain experts and concluded that the majority of the feedback was mostly positive. They argued that their proposed mechanism could be adapted to other IoT applications with minor modifications.

Terzi et al. [81] presented an architecture for a blockchain-based SSI system to ensure tamper-proof evidence of emission data from smart vehicles. Their proposal integrated a private consortium Hyperledger Fabric-based blockchain with an Indy blockchain. They utilized concepts such as VCs, DIDs, and Zero-knowledge Proof, but did not elaborate further on these. Additionally, they did not use any framework like Hyperledger Aries.

To verify the identity of nodes in a wireless Ad-Hoc Mesh network, the authors in [82] presented an approach for integrating SSI into IoT mesh networks, using LoRaWAN (Long Range Wide Area Network). They also presented a system based on their proposal, which utilized Hyperledger Aries and Indy, and evaluated its performance.

b: HEALTHCARE

There are not many research works in the healthcare domain. We discuss the relevant research works below.

Siqueira et al. [83] and Houtan et al. [84] have presented surveys of SSI in the healthcare sector. Given the scarcity of research works on SSI in the healthcare sectors, both of these works expanded their research scopes to include not only SSI-based healthcare research works but also blockchain-based research works that did not consider any SSI standards. Their main contributions were to analyze the current state-of-the-art and identify limitations and future research challenges.

In another work, Siqueira et al. explored a number of healthcare-related use-cases [85]. They also mapped the roles and respective interactions of different entities in these use cases to the respective roles and interactions of SSI entities. They then presented a representative architecture, consisting of the Hyperledger Aries framework and its related components, e.g., Indy, Ursa, and so on, which could be utilized for developing applications for these use cases. However, no implementation of the proposed architecture was reported.

Similarly, Shuaib et al. explored the applicability of SSI in the healthcare domain [86]. Specifically, they presented a number of requirements and discussed the advantages of adopting SSI in the healthcare sector.

The prevalence of COVID-19 since 2020 motivated several works to explore how privacy-preserving contact tracing can be facilitated using SSI [87], [88]. Song et al. presented an SSI-based contact tracing solution that utilized Hyperledger Aries and Indy [87]. Similarly, Bandara et al. proposed another SSI-based contact tracing platform without using the existing SSI frameworks [88]. Instead, a custom solution was developed and utilized.

c: TRUST MANAGEMENT

There are a few research works that have explored the issues of trust within SSI. We briefly review these works next.

In [89], the authors highlighted the need to include personal issuers within the SSI model and argued that a model of trust involving the personal issuers needed to be considered. They also discussed a use-case to support delegation and create a chain of verification to enable trust in this delegated scenario. However, this was an exploratory work and no practical implementation was reported.

Gruner et al. proposed a brokered identity aggregation framework that could integrate different identity management modules, including SSI [90]. This framework would enable the aggregation of attributes from multiple attribute providers (identity providers) and establish trust according to different trust models. They outlined the architecture of the framework, presented a number of corresponding challenges and requirements to mitigate these challenges, and discussed its implementation. Their implementation could integrate attributes from different SSI-based solutions such as Jolocom, uPort, and Aries, as well as non-SSI systems such as OpenID [91] and SAML (Security Assertion Markup Language) [92].

In [93], the authors highlighted two important issues with respect to managing trust in SSI: i) the lack of a trust anchor and ii) the difficulty in establishing automated trust. They presented a trust management infrastructure for SSI, but did not provide implementation details regarding the infrastructure.

In [94], the authors presented an approach for writing a trust policy for SSI based on an existing framework called the Trust Policy Language (TPL). The discussion in this work mainly focused on how to transform the existing TPL to make it suitable for any SSI system.

d: AUTHENTICATION AND AUTHORISATION

In this category, we explore research works that have used SSI for authentication and/or authorisation in different systems.

A framework for using SSI to authenticate users in various services is presented in [95]. In the proposed system, the Service Provider (SP) acts both as the Issuer and Verifier. The SP issues a VC to the user, which is then stored in their wallet. During service access, the user presents the VC to the SP. Upon successful verification of the VC, the user is authenticated. The authors used Hyperledger Aries, Hyperledger Indy, and the Aries Bifold wallet to develop a prototype of their application.

In [96], the author presented a prototype of an SSI agent for authentication and authorisation in different applications. They used Hyperledger Aries and Hyperledger Indy and discussed issues such as trust.

The authors in [97] presented an SSI-integrated authorisation system that combines SSI with traditional Role-Based Access Control (RBAC) [98] and Attribute-Based Access Control (ABAC) [99]. They used Hyperledger Aries, Hyperledger Indy, and an unspecified RBAC/ABAC framework, and analysed its performance. One issue with their approach is the use of a centralized access control server, a requirement in any RBAC/ABAC framework. This creates a single point of failure in their otherwise decentralised system.

One of the earliest works on SSI and authentication is found in [100], where the authors presented a biometric authentication system that uses an Android mobile phone's fingerprint service to authenticate a user. They envisioned their work as a key building block for an SSI component.

e: MISCELLANEOUS

In this category, we explore a variety of application domains with minimal research works.

- *Data Sharing:* Alsayed et al. presented a personal data sharing protocol using SSI in [101]. They did not use the Hyperledger Aries framework, opting for Ethereum as the backbone instead. However, the creation of the DID was not elaborated upon.
- *Client Onboarding:* In [102], Soltani et al. proposed an SSI-based KYC (Know Your Customer) mechanism. The proposal is well-formulated, but no implementation details are provided.
- *Money Transfer:* Bandara et al. presented a blockchain-based P2P money exchange system as an alternative to ATMs in [103]. Users would use their wallets to create their respective DIDs for use with another user. Each DID relies on the Rahasak blockchain platform [104]. The authors also presented a performance analysis of their system. Notably, they did not use any SSI framework, nor did they employ any VCs within their system.
- *Banking:* In [105], Ahmed et al. explored how SSI could be leveraged for banking functionalities. The authors proposed a framework for carrying out banking functionalities using Chip and Pin based banking cards. They implemented their system with Veramo as the SSI framework and Ethereum as the underlying blockchain. The system's performance was also evaluated.
- *Document Verification:* [106] presents an SSI framework for document verification, focusing on a specific use-case involving online loan processing. The proposed solution eliminates the need for intermediaries during the document verification process. The authors presented an architecture implemented using the Affinidi SSI framework with Ethereum as the underlying blockchain, utilising W3C DIDs and VCs.
- *Mobile to Mobile (M2M) Communications:* Enge et al. presented a system for establishing SSI connections between two mobile devices, even without internet connection, in [107]. They used Bluetooth Low Energy (BLE) as the data transmission medium and the DIDComm protocol to establish the SSI communication between two devices. The authors implemented their proposal using the Veramo framework and evaluated its performance.
- *Business Process Management:* In [108], the authors presented a novel privacy-preserving SSI-based mechanism for managing inter-organisational business processes. The Veramo framework was used to implement the proposal, with Ethereum serving as the underlying Blockchain. The performance and cost of the implementation were also evaluated.

Summary: We present a summary of the comparative analysis of existing works against a few properties in Table 2. It is to be noted that review and exploratory research works which did not have any concrete architecture or implementation have not been considered in the table. The explanation for the symbols used in the table can be found in its caption. This table shows that many research studies did not use SSI frameworks like Aries and instead opted for custom implementations. Without using a standardized SSI framework, the development and deployment of an SSI-based application might be challenging. We also investigated if the implemented research works have adhered to standards such as those provided by the W3C, DIF, or Hyperledger Foundation. Although most of the research utilized these SSI standards, some works did not follow any standard. Without adhering to a common standard, authors might be inclined to propose and utilize entirely different and incompatible formats of decentralized identifiers and credentials. These works utilized various types of blockchain systems, with Indy being the predominant one. Furthermore, many research works did not provide any implementation of their proposal, making it challenging to evaluate the applicability of a proposal.

TABLE 2. Comparison of existing research works.

Application Domain	Research Work	SSI Framework	SSI Standards	VDR	Architecture	Implementation
IoT	Fedrecheski et al. [74]	○	○	○ (Mock Blockchain)	●	●
	Weingaertner et al [75]	○	● (W3C)	● (Ethereum)	○	●
	Samir et al [77]	○	● (W3C)	● (Ethereum Simulator)	●	●
	Capela et al. [80]	● (Aries)	● (W3C)	● (Indy)	●	●
	Terzi et al. [81]	○	● (W3C)	● (Fabric & Indy)	●	●
	Grabatin et al. [82]	● (Aries)	● (W3C)	● (Indy)	●	●
Healthcare	Song et al. [87]	● (Aries)	● (Hyperledger)	● (Indy)	○	●
	Bandara et al. [88]	○	○	○	●	●
Trust Management.	Mukta et al. [89]	○	○	○	●	○
	Gruner et al. [90]	● (Aries)	○	● (Indy)	●	●
	Kubach et al. [93]	○	● (W3C)	○	●	○
	Alber et al. [94]	○	○	● (Ethereum)	○	○
Authn. & Authz.	Ferdous et al. [95]	● (Aries)	● (W3C)	● (Indy Dev Network)	●	●
	Gerard et al. [96]	○	● (W3C)	● (Indy)	●	●
	Belchior et al. [97]	● (Aries)	● (W3C)	● (Indy)	●	●
	Hammudoglu [100]	○	○	○	○	○
Data Sharing	Kassem et al. [101]	○	○	● (Ethereum)	●	●
Client onboarding	Soltani et al. [102]	○	○	● (Indy)	●	○
Money transfer	Bandara et al. [103]	○	○	● (Rahasak)	●	●
Banking	Ahmed et al. [105]	● (Veramo)	● (W3C)	● (Ethereum)	●	●
Document verification	Satybaldy et al. [106]	● (Affindi)	● (W3C)	● (Ethereum)	●	●
M2M Communication	Enge et al. [107]	● (Veramo)	● (W3C, DIF)	○	●	●
Business Process Mgmt.	Abid et al. [108]	● (Veramo)	● (W3C)	● (Ethereum)	●	●

'●' denotes that a certain work satisfies the respective property, '○' indicates the opposite (not satisfied).

E. GOVERNANCE LAYER

The governance stack is where the focus shifts primarily from machines and technology to humans and policies. Governance frameworks play a pivotal role in the SSI stack, serving as a bridge between the technical aspects of the SSI stack and the practical considerations of business, legal, and social requirements in SSI solutions.

Similar to the technical stack, the governance stack is also divided into four layers: Layer 1, Layer 2, Layer 3, and Layer 4. In the following sections, we explore each of these layers in detail.

1) LAYER 1 – UTILITY GOVERNANCE

Governance in Layer 1 of SSI systems predominantly pertains to operating a public utility that provides verifiable data registry (VDR) services. The VDR, which can be implemented using various technologies like blockchain, distributed ledger, or peer-to-peer protocols, serves as a decentralized datastore.

The governance of Layer 1 depends on the specific architecture of the VDR. Different governance models are employed based on the type of VDR:

1) Public permissionless proof-of-work blockchains, like Bitcoin [109], rely on open-source projects and the decision-making power of miners to govern the network.
2) Public permissionless proof-of-stake blockchains, such as Ethereum [110], Stellar [111], and Cosmos [112], utilize voting algorithms tied to token holdings for governance.
3) Public permissioned blockchains, like Sovrin [61] and Hyperledger Indy [56], employ formal governance frameworks developed through an open public process.
4) Hybrid blockchains, for example, Veres One [72] and Hedera [113], combine elements of permissioned and permissionless models, with community groups and boards of governors overseeing network changes.
5) Private blockchains, like Hyperledger Fabric [114] and Quorum [115], are operated by their members for internal purposes, and their governance frameworks may or may not be publicly accessible.

It is worth noting that Layer 1 can also include alternative options for VDRs, such as distributed file systems (e.g., IPFS) [116], key event logs (e.g., KERI) [22], and distributed hash tables (DHTs). Some trust communities within the SSI landscape find centralized registries, directory systems, or certificate authorities acceptable for their VDR needs.

Key governance roles at Layer 1 include maintainers (developers of the blockchain code), miners/stakers (operators of permissionless nodes), stewards (operators of permissioned nodes), transaction authors (initiators of transactions), and transaction endorsers (parties authorizing transactions to a permissioned blockchain).

A proposed draft standard, ISO 23257 [117], introduces the concept of a blockchain governance authority, referred to as a DLT governor. This authority plays a crucial role in governing the entire DLT system, developing policies, communicating with stakeholders, resolving conflicts, defining consensus mechanisms and node participation policies, collaborating with DLT providers, and enforcing monitoring and governance with node operators.

2) LAYER 2 – PROVIDER GOVERNANCE

The Layer 2 governance in SSI systems is distinct from Layer 1 governance as it pertains to the management of digital wallets, agents, and agencies rather than public utilities. The primary focus is on establishing baseline requirements for security, privacy, and data protection, as well as implementing interoperability testing and certification programs for the following key roles:

- Hardware developers: These individuals or entities provide compliant hardware components such as secure enclaves, trusted execution environments, and hardware security modules (HSMs).
- Software developers: Their responsibility is to develop compliant wallets, agents, secure data stores, and other related software functionalities.
- Agencies: In the context of Layer 2 governance, agencies refer to service providers that host cloud wallets and agents on behalf of individuals, organizations, and guardians.

While security and privacy requirements for hardware and software are relatively well-understood, hosting wallets and agents in the cloud introduces the need for agencies as a new type of service provider. These agencies facilitate agent-to-agent message routing, queuing, wallet backup, synchronization, and recovery services.

Layer 2 governance frameworks must encompass the security, privacy, and data protection requirements associated with agency services, as these functions are closely tied to the activities of wallet holders. Additionally, specialized agency services are necessary to support digital guardianship, where guardians manage cloud wallets on behalf of individuals who are unable to do so themselves (e.g., refugees, homeless individuals, minors, or the infirm). To ensure proper fiduciary responsibilities, a Layer 2 governance framework needs to outline the legal duties and obligations of digital guardians.

3) LAYER 3 – CREDENTIAL GOVERNANCE

The Layer 3 governance in SSI systems focuses on the transition from technical trust to human trust, incorporating governance frameworks that resemble those used for physical credentials. Many existing policy frameworks for governing physical credentials, such as credit cards, driver's licenses, passports, and health insurance cards, can be adapted with minimal modifications to apply to digital credentials. Therefore, Layer 3 governance in SSI systems focuses on human trust and incorporates governance frameworks similar to those used for physical credentials. Credential registries play a vital role in enabling decentralized trust infrastructure, while insurers offer additional protection by mitigating risks associated with VCs.

Standard roles and policy types in Layer 3 governance frameworks include issuers, holders, verifiers, credential registries, insurers, and their corresponding policy types, such as qualification and enrollment, security, privacy, data protection, verification procedures, level of assurance, credential revocation requirements, business rules, and technical requirements.

One key aspect of Layer 3 governance is the concept of credential registries. These registries serve as verifiable directories of verifiable credentials (VCs), enabling decentralized digital trust infrastructure. By publishing VCs in a registry, they can be searched, discovered, and verified by qualified verifiers. Credential registries are particularly useful for public information, such as business registrations and licenses that are required by legislation to be publicly available. An example is the OrgBook service provided by the British Columbia government [118], which publishes the business registrations and licenses of all businesses in the province.

It's important to note that the same VC can be issued to different holders, with the data in the claims describing the credential subject remaining identical. In the case of credential registries, the holder is the registry itself, which is responsible for publishing the credential for public search and verification purposes. Credential registries utilize unique cryptographic identifiers (DIDs or link secrets for Zero-Knowledge Proof credentials) to ensure authenticity and prevent impersonation.

Another role in Layer 3 governance frameworks is insurers. Insurers come into play when there is a risk associated with VCs. Higher-value VCs increase liability for issuers, who may offset this risk by providing insurance coverage. This insurance serves as recourse for verifiers in the event of relying on falsified, hacked, or erroneous credentials, making VCs from insured issuers more attractive.

4) LAYER 4 – ECOSYSTEM GOVERNANCE

The Layer 4 governance operates at the application layer, establishing the foundation for digital trust ecosystems. They address interoperability, delegation and guardianship, transitive trust, usability, and trust marks. Ecosystem governance frameworks encompass general roles such as member directories, certification authorities, auditors, and auditor accreditors, ensuring the effective operation of the ecosystem's governance and trust mechanisms.

Layer 4 ecosystem governance framework has the broadest scope and can specify requirements that apply to all other layers of the stack. For instance, it may define security and privacy requirements for Layer 3 credentials, Layer 2 wallets and agents, and Layer 1 utilities operating within the ecosystem. Additionally, it may involve multiple governance authorities since digital ecosystems are typically composed of constituent trust communities, each having its own governance authorities and frameworks. Thus, an ecosystem governance framework represents cooperation across these diverse governance entities.

Ecosystem governance frameworks govern the elements that directly interact with individuals and organizations operating within the ecosystem. The main objectives of these frameworks include:

- Interoperability: Facilitating applications within the ecosystem to communicate and securely share user data. While technical challenges are being addressed, ecosystem governance frameworks focus on resolving legal, business, and social barriers to interoperability.
- Delegation and guardianship: Establishing legal, technical, and business rules for easily and securely delegating data management responsibilities to trusted professionals or service providers. This accommodates individuals who prefer not to manage their own data or

lack the capacity to directly handle SSI digital wallets and agents.
- Transitive trust: Leveraging SSI technology and governance frameworks to enable trust developed in one context to be recognized and applied in another context. This allows for the establishment of transitive trust between applications and websites within the ecosystem, similar to how physical credentials are recognized across different contexts.
- Usability: Ensuring that SSI systems are user-friendly and safe for individuals with varying levels of technical knowledge. Ecosystem governance frameworks may define usability guidelines, incentivize adherence, and offer certification programs to verify compliance.
- Trust marks: Defining trust marks and the rules for earning and utilizing them. Trust marks serve as recognizable symbols of trust, similar to well-known brands in the physical world. Ecosystem governance frameworks play a visible role in defining these trust marks and consolidating the necessary components for individuals to make informed digital trust decisions.

Standard roles within ecosystem governance frameworks are more general compared to lower layers and may include:
- Member directories (trust registries): These confirm an entity's membership within the ecosystem, ensuring compliance with the governance framework's terms and accountability requirements. Member directory services can be implemented through centralized, federated, or decentralized approaches, serving as credential registries as well.
- Certification authorities: Responsible for certifying entities in various roles within the ecosystem based on criteria defined by the governance framework. Certification authorities oversee assessments and publish results using verifiable credentials.
- Auditors: Conduct audits to review an entity's policies, practices, and procedures, assessing compliance with the governance framework's requirements and qualification for certification.
- Auditor accreditors: Approve auditors to perform their role. As ecosystems scale, there is a need to outsource this function to accredited auditor organizations, similar to how WebTrust and the Kantara Initiative operate in other digital trust frameworks.

5) GOVERNANCE AUTHORITY

The governance authority, a standard role in all governance frameworks, is responsible for developing, maintaining, and enforcing the given governance framework. Potential governance authorities include governments at all levels, industry consortia, NGOs, corporations and enterprises, universities and school systems, religious organizations, and online communities. With SSI governance frameworks, anyone in any community of any size and jurisdiction can facilitate digital trust. Governance of the governance authority varies depending on the trust community's preferences. Transparent publication of the governance authority's own governance structure and policies is a key best practice.

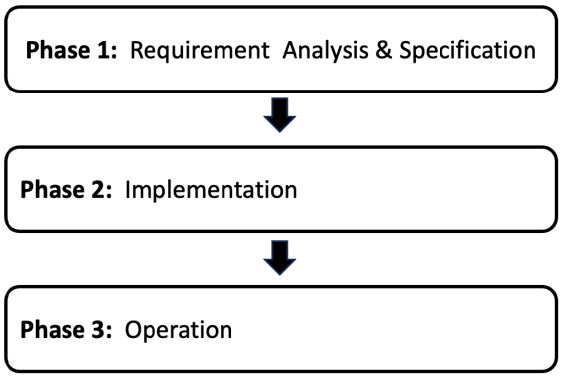

FIGURE 6. SSI system development life cycle framework.

V. SSI SYSTEM DEVELOPMENT LIFE CYCLE FRAMEWORK

We conducted an MLR with the objective of addressing research question RQ2. This comprehensive review allowed us to identify a wide range of academic sources that extensively discuss the development processes and methodologies employed in various contexts, including traditional software systems [119], [120], [121], decentralized systems [122], [123], [124], and self-sovereign identity systems [125], [126]. Additionally, we conducted an analysis of relevant gray literature, specifically studying the extensive technical documentation and standards from reputable organizations such as the DIF [23], [29], [33], W3C [18], [19], [36], and European blockchain service infrastructure (EBSI) [127]. Furthermore, we conducted an investigation into implementation frameworks, including Hyperledger Aries [55] and Veramo [68], which are widely used in the development of self-sovereign identity systems. We also examined deployed applications, such as digital identity wallets [34], to gain practical insights into the implementation and utilization of self-sovereign identity in real-world scenarios. Through careful synthesis of these findings, we have formulated an SSI System Development Life Cycle (SSI-SDLC) framework. This framework is derived from the literature and has been adapted to cater to the unique characteristics and requirements of SSI. The SSI-SDLC encompasses three sequential and iterative phases: requirement analysis and specification, implementation, and operation, as illustrated in Figure 6.

The first phase, *requirement analysis and specification* (RAS), is dedicated to understanding and documenting the requirements of the SSI system. The primary objective is to identify the essential features, functionalities, and conduct a comprehensive analysis of security considerations and privacy requirements. During this phase, data models, protocol designs, and interoperability standards are defined and created. The RAS phase serves as the foundation for the subsequent development phases and culminates in the creation of technical specifications and standards that serve as guidelines for the implementation process.

The second phase, *implementation*, focuses on designing and developing the SSI system based on the requirements and specifications defined in the previous stage. It encompasses designing the system architecture, developing software components, and integrating various modules to create a functional system. Rigorous testing and quality assurance practices ensure the correctness and reliability of the implementation.

The third phase, *operation*, centers around deploying and maintaining the SSI system in a production environment. It includes activities such as system deployment, configuration management, performance optimization, governance, and ongoing support. User accessibility, system availability, and reliability are key considerations during this stage. Continuous evaluation and improvement processes drive enhancements to the system's performance and alignment with evolving user needs.

The SSI-SDLC provides a structured approach for the development and lifecycle management of self-sovereign identity systems. It ensures that these systems are designed, implemented, and maintained in a systematic and controlled manner, aligning with the principles of self-sovereign identity.

VI. CHALLENGES

To ensure wide-scale adoption of SSI, it is imperative to identify the current challenges and then implement appropriate measures to mitigate them. In the course of our study, particularly in response to RQ3, we have identified numerous challenges across various layers of both technical and governance stacks. This section offers a summary of the open challenges that emerged during our investigation.

A. CHALLENGES IN PUBLIC UTILITIES LAYER

1) VULNERABILITIES IN BLOCKCHAIN NETWORKS

Many existing SSI systems leverage different blockchain networks, including Bitcoin, Ethereum, and Hyperledger Indy, to facilitate a VDR. While blockchain technology offers decentralized and transparent services for digital identity management, it is crucial to address the security risks and challenges associated with this innovative approach. Ahmed et al. [6] highlighted the significance of potential vulnerabilities within the underlying blockchain network, which could lead to unforeseen attacks and compromise the overall security and privacy of SSI systems. Therefore, it is essential to conduct a systematic investigation into adversarial methods that can undermine the blockchain network and, subsequently, the SSI system. In the academic literature, researchers extensively discuss various attacks, such as majority attacks, sybil attacks, replay attacks, and collusion attacks, that have the potential to undermine the integrity and security of blockchain networks in general [128].

2) SCALABILITY OF SSI NETWORK

Scalability is a critical aspect to consider in the design and implementation of SSI systems. As the adoption and usage of SSI systems continue to grow, the ability to handle increased user demand and accommodate a larger network of participants becomes crucial. According to [129], scalability plays a crucial role in the success of SSI systems by directly influencing the system's capacity to provide timely and efficient identity management services. Many SSI systems leverage blockchain technology as a foundation for a new trust model that establishes immutable records linking decentralized identifiers and their owners. However, for blockchain-based SSI to become widely accepted as a digital identity management system, the underlying blockchain infrastructure must exhibit scalability, especially in terms of transaction throughput. The scalability challenge becomes apparent when considering public permissionless blockchains like Ethereum, which are commonly used in many SSI systems. These blockchain systems employ complex consensus mechanisms, making it challenging to accommodate a large user base and a high number of transactions [130], [131], at least for the time being. Private blockchains, which are typically more centralized, can handle larger numbers of users and transactions more easily, but they may sacrifice security in order to achieve this scalability.

3) COMPLIANCE WITH PRIVACY LAWS

The characteristics of blockchain, such as data immutability and public ledger storage, give rise to concerns regarding compliance with data protection and privacy laws, including the General Data Protection Regulation (GDPR) of the European Union. One of the most challenging aspects for blockchain-based systems in terms of compliance is the right to erasure or right to be forgotten (Art. 17 GDPR) [132]. When the data subject is also the controller, a person or other body which decides the purposes and methods of processing personal data, the right to erasure may not apply. Similarly, the right to erasure may not apply if the controller has a valid justification for retaining the personal data. Data related solely to credential issuing institutions typically do not fall under the category of personal data. However, in cases where DIDs, credential hashes, or revocation hashes are stored on a blockchain, a case-by-case analysis is necessary to determine if any specific entry still qualifies as personal data. For example, a hash value that was previously considered personal data may no longer be considered as such if the hashed object has been securely deleted [12], [133]. It is crucial to conduct thorough assessments and evaluations to ensure compliance with privacy laws while leveraging the benefits of blockchain technology in SSI systems.

4) DID DOCUMENT CORRELATION RISKS

As DID documents contain information associated with a DID, they can potentially be used for correlation, raising privacy concerns. The Decentralized Identifiers v1.0 specification points out this issue and recommends to use pairwise DIDs, where each DID acts as a pseudonym, reducing the risk of correlation [18]. However, the effectiveness of pairwise

DIDs is limited if the metadata in the DID documents remains correlatable. For example, using the same cryptographic public key across different DID documents carries the same correlation information as using the same DID. Additionally, bespoke service endpoints in multiple DID documents can also lead to correlation risks. This poses a dataveillance problem, where a verification agency can deduce personal information through the service endpoint properties in the DID document. The issue arises from the fact that service property data in the DID document is often written in plain text, the service endpoints are presented as URLs that can be easily accessed, and there is a lack of control over how verification agencies approach these endpoints. A study conducted by Kim et al. [134] highlighted the anonymity issue with endpoint URLs in DID documents, claiming that URLs could expose personal information such as country of origin and affiliations.

5) LIMITATIONS OF LEDGER-BASED DID METHODS

All DID methods rely on a root of trust starting point for proving the chain of trust based on a public/private key pair [135]. Although the key pair is usually generated in secure hardware using a long random number, most DID methods do not rely on this root of trust alone (they are not self-certifying). They require a second step: using the private key to digitally sign a transaction in a distributed ledger or blockchain to "record" the DID and the initial associated public key [136]. Once that record is created, the ledger becomes the algorithmic root of trust for the DID. This means verifiers must check with the ledger to verify the current public key and any other contents of the DID document associated with the DID. For early 2023, 95% of the over 150 DID methods registered in the W3C DID Specification Registry [19] use ledger-based DID methods. However, these DID methods have certain challenges and open issues:

- Dependency on another party or network: Although the ultimate root of trust is still the key pair used to generate the DID and update the DID document on the ledger, a ledger-based DID method requires a DID controller to depend on a distributed ledger and its associated governance mechanisms to be trustworthy [137].
- Non-portability: Ledger-based DIDs are "locked" to a specific ledger and cannot be moved if problems develop with the ledger or its governance or if the DID controller desires to use other DID methods [138].

B. CHALLENGES IN COMMUNICATIONS AND INTERFACES LAYER

1) DIFFERENT MESSAGE ENVELOPES

There are two versions of DIDComm: DIDComm v1, incubated in the Hyperledger Aries community [139], and DIDComm v2, described in the specification brought forward by the DIF [23]. These versions differ in several aspects, including message structures, the handling of DIDs, and underlying cryptographic primitives [140]. In addition to DIDComm, another message envelope is proposed in the OpenID for Verifiable Credentials (OIDC4VCs) specification [47]. This protocol extends OpenID Connect (OIDC) with the concept of a Self-Issued OpenID Provider (SIOP v2) [141], which supports DIDs and enables the creation of a secure envelope between agents. The public key is shared as a JSON Web Key, and the OIDC extension supports the DID method for resolving key material. The choice of message envelope significantly affects technical interoperability. For instance, the message structure differs between DIDComm v1, DIDComm v2, and SIOP v2 to the extent that they are incompatible with each other [142], [143]. This means that agents using different technology stacks must support each other's message envelope to achieve interoperability on the agent layer. It is crucial for the same message envelope to be supported in order to exchange information effectively between agents.

2) DID EXCHANGE

The DIDComm protocol enables the transmission of messages through various transport protocols such as HTTP, Bluetooth, NFC, as well as out-of-band (OOB) channels like QR codes and email. However, before entities can communicate, they need to exchange DIDs. Agents must establish relationships and securely exchange information using keys and endpoints defined in DID Documents. To facilitate this, a clear protocol for DID exchange is necessary. The Aries RFC 0023: DID Exchange Protocol 1.0 [144] specifies the process of exchanging DIDs between agents when establishing a DID-based relationship. It should be noted that the specification is primarily intended for Aries agent developers and may require modifications for other implementations. The DID exchange protocol can be initiated either through knowledge of a resolvable DID (implicit invitation) or through an out-of-band invitation message from OOB protocols. It is crucial to consider security threats such as Man-in-the-Middle (MITM) attacks during the DID exchange process. Measures must be taken to prevent data tampering attacks and ensure the security of the exchange process [107].

3) DID ROTATION

A DID rotation involves switching from one DID to another DID. Regularly rotating the keys is recommended to mitigate risks in case of a key compromise. The key rotation challenge has been addressed in [145]. One of the challenges is to ensure that only the DID creator, i.e., the person who knows the secret seed, can rotate to the next key pair. DID rotation is also necessary when using the DIDComm messaging protocol. In the initial stages of a DIDComm connection, it is common for the first message to be in the form of an unencrypted Out of Band (OOB) message. This message can be observed by third parties or transmitted through insecure channels like QR codes or URLs in emails or webpages. The DID used in the OOB message should be treated as a temporary DID

solely for initiating the conversation. However, it is highly recommended to rotate the DID after the initial exchange to enhance privacy and security [107], [146].

4) KEY RECOVERY

Traditional identity management models typically rely on trusted third parties for key management protocols, whereas in the context of SSI, the responsibility of key management is delegated to identity owners themselves. Addressing the key management requirements within the SSI architecture is a crucial step towards its widespread adoption. The development of practical and privacy-preserving key management protocols plays a vital role in the adoption of digital identity wallets, which enable individuals to manage secret keys, credentials, and personal information securely. One significant concern in SSI systems is the ability to restore a private key in case of device loss or inaccessibility [35], [147]. Failure to recover private keys can result in the loss of previously issued verifiable credentials and DID documents, necessitating identity re-verification with previous service providers. There have been instances where users lost their cryptographic keys, leading to the irretrievable loss of valuable information and funds. Therefore, there is a pressing need for a practical key backup and recovery protocol. Kim et al. [148] emphasized the lack of research in effectively restoring private keys based on self-sovereign identity principles.

5) OFFLINE COMMUNICATION

One fundamental principle of SSI is to allow individuals to engage in digital interactions with the same trust and freedom they experience in the physical world. There are numerous situations where proving our identity is necessary without internet access. As a result, SSI solutions must be capable of functioning offline or with intermittent connectivity. This presents a significant engineering challenge for SSI architects, and it remains an unsolved issue. The domain of offline communication within SSI remains largely unexplored [2]. Most current SSI implementations depend on an Internet connection for operations and message transmission between parties. There's limited research on how SSI technology can function in an offline setting without external infrastructure. A secure and interoperable solution for offline communication, based on the DIDComm protocol among agents from different vendors, is acknowledged as essential [149], [150].

6) PORTABILITY OF IDENTITY

It is one of the key requirements for an SSI system [7], [151]. It refers to the ability of individuals to have control over the storage and mobility of their identity information and credentials, allowing them to switch providers without being locked into a specific vendor. Data portability plays a crucial role in achieving self-sovereignty by enabling the migration of self-sovereign identities, keys, and related data to another agent or wallet within the user's domain. Within the Hyperledger Aries ecosystem, the export of issued credentials to another wallet is facilitated. This export includes the credentials themselves, along with the associated DIDs, keys, and binding information, utilizing the import/export functionality of the Indy-SDK and following the BIP-39 Standard [152]. Currently, wallet portability has been implemented among three vendors, namely the Trinsic wallet, the Lissi wallet, and the Esatus wallet, all of which are based on the Aries framework. However, there is a need for a universal method that allows wallet portability with various providers outside the Hyperledger ecosystem. To address this, a specification is required to define wallet portability and establish a data model encompassing different wallet types and functionalities related to SSI. This would enable various wallet providers to translate and import wallet data into their respective architectures. It is important to consider regulatory requirements, such as those outlined in the European Digital Identity Wallet Architecture framework [153], which may restrict the portability of certain credentials, like eID. A hybrid approach could be adopted, allowing data portability for credentials with a lower level of assurance while disabling it for credentials with a higher level of assurance, offering a balanced solution.

C. CHALLENGES IN CREDENTIALS LAYER

1) DIFFERENT CREDENTIAL FORMATS AND PROOFS

We discussed various credential formats and proof types in Section IV-C. W3C VCs, AnonCreds, and ISO mdoc standards define different credential formats, each supporting a range of cryptographic proofs. While it is important to have a universal data format for VCs that enables interoperable implementation of digital credentials, currently these standards do not support each other's formats, resulting in a lack of interoperability [154]. For instance, AnonCreds do not adhere to the standardization of verifiable credentials as defined by the W3C. In addition to different credential formats, interacting agents must also support the same proof types to effectively issue, store, and validate self-sovereign identities. There are multiple proof types available as illustrated in Table 1, reflecting diverse objectives and business requirements. The SSI community has been discussing the possibility of finding a single proof type to unify solutions, but due to the variety of business requirements, achieving consensus on a single proof type may be challenging [142]. To achieve technical interoperability, it is essential to either align on a common proof type or support a wide range of proof types. In either case, implementing them with defined and standardized signature suites is crucial.

2) IDENTITY DERIVATION

SSI systems currently lack privacy-preserving mechanisms for decentralized identity derivation, which would allow the importation of qualified electronic identification (eID) data from existing eID systems. This process entails not

only converting data between different formats and protocols but also ensuring the integrity and trustworthiness of the data. While recent progress has been made in the field of eID derivation and its integration into SSI systems, these approaches fall short in addressing user privacy concerns [8], [155]. Centralized intermediaries involved in the process may have access to users' eID attributes in plaintext, posing a risk to privacy. Additionally, during authentication with service providers, users may be required to disclose more information than necessary. One promising decentralized approach for eID derivation in SSI systems has been proposed by Abraham et al. [156], but further research is still needed in this area.

3) DATA MINIMIZATION

The design of SSI systems must consider the privacy concerns associated with the collection and storage of VCs. One issue with revealing a credential in its entirety, including the hash or the DID, is that it enables easy and strong correlation of the credential holder across all verifiers with whom the credential is shared. The Verifiable Credentials Data Model v1.1 specification [36] acknowledges the significant privacy risks associated with this approach. To mitigate these privacy risks, data minimization techniques can be employed to limit the collection, processing, and storage of sensitive personal data. The literature describes three types of techniques:

- Selective disclosure [40], [42], [157]: This technique allows users to selectively share VCs with specific attributes revealed, giving them control over the information they disclose.
- Predicates [37], [158]: Predicates involve using boolean assertions over data, providing a way to make statements based on specific conditions or attributes.
- Arbitrary statements over attributes [159], [160], [161]: This technique allows for the creation of custom statements about attributes, enabling more flexible and fine-grained control over the disclosure of information.

By employing these data minimization techniques, SSI systems can enhance privacy protection and mitigate the risks associated with correlating holders' identities across different verifiers. Continued efforts in this area will contribute to the development of robust and privacy-preserving solutions for the secure and responsible management of verifiable credentials.

4) CREDENTIAL REVOCATION

The revocation verification of VCs in a decentralized and privacy-preserving manner is an active area of research in SSI. Revocation mechanisms for SSI system should not rely on any centralised infrastructure, and should provide offline verification capabilities. SSI systems enable users to authenticate and share information with verifiers using verifiable credentials from issuers. Verifiers need to determine the validity of presented credentials and whether they have been revoked. However, direct communication between verifiers and issuers contradicts the principles of SSI, which emphasize the protection of identity data creation and verification from third-party observation or interference. Preserving the confidentiality, integrity, and availability of revoked credentials is crucial to uphold SSI principles. As we discussed in Section IV-C, existing implementations, such as Status List v2021 and Anoncreds revocation mechanisms, have drawbacks like privacy and scalability issues. Additionally, offline scenarios where the user and verifier lack internet access pose another challenge in verifying the revocation status of a presented credential. Several works in academic literature propose new approaches to address offline revocation of credentials [157], [162], [163], but there are still open questions and the need for further research in this area. Resolving these issues is essential for advancing the state of revocation mechanisms in SSI systems while maintaining privacy, scalability, and offline verification capabilities.

5) INTEGRATION WITH TRADITIONAL IDENTITY SYSTEMS

Another area of study in SSI is the integration with legacy identity systems. Currently, traditional identity and access management protocols are not sufficiently addressed, and there is a lack of infrastructure to enable the issuance of verifiable credentials within these systems. Failure to successfully address this challenge may jeopardize the adoption of SSI, as billions of users have electronic identities in Identity Providers (IdPs) that can only communicate using traditional identity protocols. This challenge has been highlighted as the driving problem in several research papers [8], [164], [165]. Although there are initiatives to integrate SSI with federated identity management protocols such as OpenID Connect [47], [137], [166], FIDO [167], [168], SAML [169], and national eID solutions [106], [170], notable challenges remain, and further research is needed to address them.

D. CHALLENGES APPLICATION ECOSYSTEMS LAYER

1) USABILITY OF APPS AND FRAMEWORKS

SSI systems should be designed to address the challenges faced by end users. However, it has been noted by several researchers that usability still poses significant concerns in current SSI solutions [4], [171]. A number of studies have been conducted to examine the usability issues associated with SSI apps. The authors of [34] and [172] analyzed the usability of widely used SSI digital identity wallets and identified various usability issues in existing wallet applications.

2) USER INTERACTION

We have observed that existing SSI implementations primarily focus on the underlying technology and often neglect user interaction aspects [8], [151], [173]. The usability of interfaces and the privacy implications for users have not been adequately addressed. Multiple research papers have focused on exploring the usability and human perception challenges associated with SSI systems. In a particular study [174], the authors conducted a comprehensive analysis of the

SSI interface layer and identified that current interactions within SSI systems demand considerable internalized representations, prior knowledge, and participant responsibility. They argued that these elements present significant obstacles and act as barriers to achieving sustainable adoption. Consequently, this research emphasizes the importance of collective standardization, strategic planning, and design thinking to enhance the likelihood of sustainable adoption. Shanmugarasa et al. [175] conducted a research study that focused on addressing the challenge of users effectively managing verifiable credentials. They recognized that non-technically proficient users may inadvertently disclose more information than necessary when interacting with verifiers. To tackle this issue, the authors proposed a privacy preference recommendation system designed to assist users. This system provides suggestions to users, recommending which attributes can be safely shared, thereby helping users make informed decisions and protect their privacy.

3) TECHNOLOGY ADOPTION

To ensure the success of SSI as a new identity model, it is essential to make several modifications to existing system architectures. A crucial aspect in this journey is engaging in discussions about the appropriate technology stacks, deployment practices, and operational procedures. Special consideration needs to be given to user support, including the user interactions from the operator's perspective [176]. It is important to take proper design steps to prevent a fate similar to other valuable innovations like Pretty Good Privacy (PGP) [177], which, despite being a useful technology, did not achieve the anticipated widespread adoption.

4) LACK OF TOOLS

The problem of searching for metadata in blockchain-based SSI systems has been highlighted by several researchers [178], [179]. The unstructured nature of data storage on the blockchain presents a challenge when it comes to locating credential metadata. Therefore, there is a demand for innovative tools that facilitate searching information on identity ledger.

5) LACK OF FRAMEWORKS

Hyperledger Aries is currently the most matured SSI framework with other frameworks are still in development. The lack of frameworks forces to develop a solution based on only one framework which might create a vendor lock-in issue. As discussed earlier, Hyperledger Aries currently supports only Hyperledger Indy as the VDR. The support for other blockchain based VDR and for other traditional databases is not readily available. These issues must be addressed for any wide-scale adoption of SSI applications.

E. CHALLENGES IN GOVERNANCE LAYER

1) LEGAL CHALLENGES

The literature highlights legal challenges related to aligning SSI systems with existing regulations, such as eIDAS [180]. From an ideological perspective, SSI is in line with these regulations, as it emphasizes user privacy, explicit consent for data sharing, and interoperability of identities across countries. However, establishing a legal framework for decentralized technologies in the public sector is currently challenging given the existing legal landscape [133]. To overcome this, sustainable cooperation among multiple stakeholders is essential. While various entities are actively developing SSI solutions, the maturity of SSI depends on the unification of efforts to ensure its widespread adoption. Otherwise, there is a risk of having isolated SSI ecosystems that cannot effectively interconnect. Moreover, a trust framework is needed to legally ensure that organizations follow specific processes or are registered in recognized public registers. The promotion of SSI relies on the recognition of the legal value of elements such as blockchain networks, DIDs, VCs, and digital wallets [9].

2) ACCOUNTABILITY

It is crucial to establish clear policies and procedures for identifying and addressing malicious behavior and dishonest entities within the context of SSI governance. Additionally, it is important to determine the appropriate level of decentralization required to support the vision and requirements of SSI. Certain identity management operations, such as identity claim issuance, identity lookup, and secure data storage, may rely on a certain degree of centralization and trusted intermediaries. However, relying too heavily on a small group of trusted entities can create vulnerabilities within the SSI network. On the other hand, more decentralized and programmable governance frameworks have also exhibited flaws in the past [181]. Therefore, finding the right balance between centralization and decentralization is a critical area of investigation.

3) AUDITABILITY OF CREDENTIALS

When compared to other identity models, SSI offers enhanced privacy. However, there are certain use cases where the auditability of credentials or presentations becomes necessary. Lemieux et al. [182] highlight that there are specific scenarios where evidence collection is required to verify that a VC was issued and delivered to its holder, or that a VP was performed, in order to adhere to legal, audit, and accountability standards.

VII. TAXONOMY

To develop a taxonomy for categorizing the identified challenges, we employed a three-step method as described below.

1) **Mapping challenges to the architectural framework**. We mapped the open challenges identified in the study onto the formulated architectural framework for SSI stack (Section IV). This mapping helped us gain a clear understanding of the areas where these challenges arise within the SSI ecosystem.
2) **Classifying challenges into development stages**. To effectively address the challenges throughout the

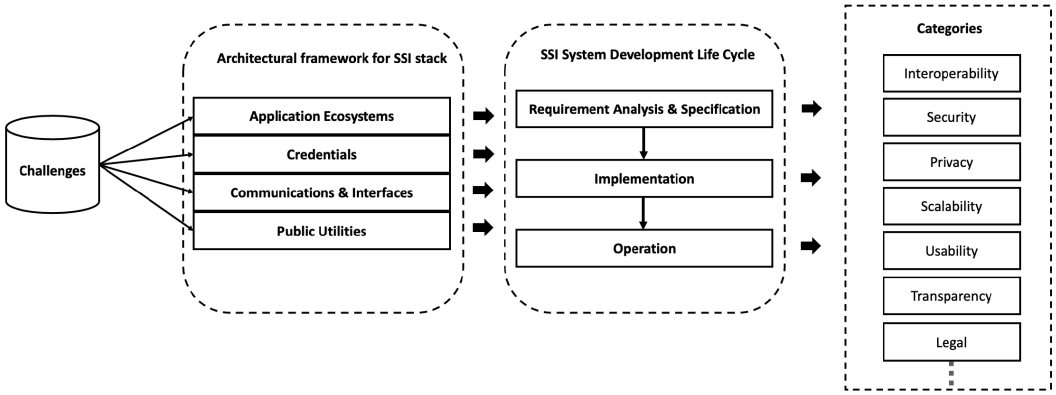

FIGURE 7. Taxonomy of challenges for SSI systems.

TABLE 3. A taxonomy of open challenges.

SSI Stack	Component	Challenge	Development Stage	Category
Layer 1:	Verifiable data registry	Vulnerabilities in blokchain network	Implementation	Security
	Verifiable data registry	Scalability of SSI network	Implementation	Scalability
Public	Verifiable data registry	Compliance with privacy laws	RAS*	Privacy
Utilities	DID document	DID document correlation risks	Implementation	Privacy
	DID method	Limitations of ledger-based DID methods	Implementation	Portability
Layer 2:	Communication protocols	Different message envelopes	RAS	Interoperability
	Communication protocols	DID exchange	RAS	Interoperability & Security
Communications	Communication protocols	Offline communication	Implementation	Interoperability & Security
& Interfaces	Key management systems	DID rotation	Implementation	Security & Privacy
	Key management systems	Key recovery	Implementation	Security & Privacy
	Wallets/Agents	Portability of identity	RAS	Portability
Layer 3:	Credential format & Credential proof	Different credential formats and proofs	RAS	Interoperability
	Credential proof	Data minimization	RAS	Privacy
Credentials	Credential exchange	Identity derivation	Implementation	Privacy
	Credential exchange	Integration with traditional identity systems	Implementation	Interoperability
	Credential revocation	Revocation verification of VCs	RAS	Privacy & Scalability
Layer 4:	Applications & Frameworks	Usability of apps and frameworks	Operation	Usability
Application	Applications & Frameworks	Technology adoption	Operation	Management
Ecosystems	Applications	User interaction	RAS	Usability
	Frameworks	Lack of tools and frameworks	Operation	Management
Governance	Trust framework	Legal challenges	Operation	Legal
Layer	Trust framework	Accountability	Operation	Management
	Credential framework	Auditability of credentials	Operation	Transparency

*RAS: Requirement Analysis & Specification

development life cycle, we categorized them into specific development stages defined within the SSI System Development Life Cycle (SSI-SDLC) framework (Section V). This categorization allows for a systematic approach to addressing the challenges at each stage of the SSI system development process.

3) **Classifying challenges into specific categories**. We classified the challenges into specific categories such as interoperability, security, privacy, scalability, and others, as depicted in Figure 7.

A taxonomy of open challenges is presented in Table 3. The taxonomy interconnects each discussed challenge with its respective SSI component, layer, and the SSI development stage. Additionally, the taxonomy introduces nine different categories and highlights which challenges belong to which category. The following paragraphs provide a discussion regarding this table.

- **Interconnected challenges:** Many challenges span multiple categories, such as interoperability and security or privacy and scalability. This interconnectedness implies that addressing one challenge might impact or even exacerbate another. For instance, enhancing privacy within a credential revocation mechanism could compromise scalability, while ensuring data minimization might impact the system's interoperability with traditional identity systems.
- **Privacy as a recurring theme:** Privacy-related challenges, such as compliance with privacy laws, DID document correlation risks, and data minimization, recur across different layers. This emphasis on privacy underscores its importance in the SSI domain, especially given the increasing global focus on data protection and user rights.
- **The balance between usability and security:** Challenges like key recovery, user interaction, and the usability of apps and frameworks highlight the tension between creating a secure SSI system and ensuring it is user-friendly. Striking the right balance is crucial for the

widespread adoption of SSI systems. Overly complex systems might deter users, while weak security measures could compromise the system's integrity.

- **Legal and governance implications:** The inclusion of challenges such as legal issues, accountability, and the auditability of credentials suggests that the development and adoption of SSI systems are not merely technical endeavors. They carry significant legal and governance implications, necessitating collaboration between technologists, legal experts, and policymakers.
- **The need for standardization:** Challenges like varying credential formats and proofs, integration with traditional identity systems, and different message envelopes for DID exchange underscore the need for future work in standardization. Without standardized protocols and formats, there is an increased risk of fragmentation, which could potentially hinder the system's interoperability and widespread adoption.

In summary, the taxonomy paints a picture of an SSI ecosystem that is rich in potential but also fraught with challenges. These challenges span technical, operational, and even legal domains. Addressing them would require adopting a holistic approach, one that considers not just the technical aspects but also the human, legal, and societal dimensions of the system.

VIII. CONCLUSION AND FUTURE WORK

The emergence of SSI represents a promising paradigm shift in the digital identity landscape, aiming to return control and autonomy to the users. This research has delved deep into the SSI ecosystem, offering a comprehensive review of the literature, an architectural framework, and a taxonomy that classifies the challenges faced in the domain.

Based on the insights derived from this study, the following future research directions are proposed:

- Deepening the understanding of SSI systems: While this research has provided a foundational understanding of SSI systems, there is a need for further studies that delve into the technical and operational nuances of these systems. This could involve exploring the underlying protocols, standards, and mechanisms that drive SSI.
- Addressing open challenges: Our taxonomy of challenges provides a roadmap for researchers. Delving deeper into each challenge and devising innovative solutions will be vital for the widespread adoption and success of SSI.

In closing, while the journey towards establishing a universally accepted and adopted SSI system is still underway, the strides made thus far are commendable. Through continued research, collaboration, and innovation, the vision of a truly self-sovereign digital identity landscape can become a reality.

REFERENCES

[1] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103059–103079, 2019.

[2] A. Preukschat and D. Reed, *Self-Sovereign Identity*. Shelter Island, NY, USA: Manning, 2021.

[3] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020.

[4] Š. Cucko and M. Turkanovic, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE Access*, vol. 9, pp. 139009–139027, 2021.

[5] K. Schmidt, A. Mühle, A. Grüner, and C. Meinel, "Clear the fog: Towards a taxonomy of self-sovereign identity ecosystem members," in *Proc. 18th Int. Conf. Privacy, Secur. Trust (PST)*, Dec. 2021, pp. 1–7.

[6] Md. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey," *IEEE Access*, vol. 10, pp. 113436–113481, 2022.

[7] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Comput. Sci. Rev.*, vol. 30, pp. 80–86, Nov. 2018.

[8] F. Schardong and R. Custódio, "Self-sovereign identity: A systematic review, mapping and taxonomy," *Sensors*, vol. 22, no. 15, p. 5641, Jul. 2022.

[9] Y. Bai, H. Lei, S. Li, H. Gao, J. Li, and L. Li, "Decentralized and self-sovereign identity in the era of blockchain: A survey," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Aug. 2022, pp. 500–507.

[10] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, and J. Ferreira, "Self-sovereign identity: Use-cases, technologies, and challenges for industrial IoT," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2019, pp. 1173–1180.

[11] X. Zhu and Y. Badr, "Identity management systems for the Internet of Things: A survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, 2018.

[12] A. Giannopoulou, "Data protection compliance challenges for self-sovereign identity," in *Proc. 2nd Int. Congr. Blockchain Appl.* Cham, Switzerland: Springer, 2020, pp. 91–100.

[13] V. Garousi, M. Felderer, and M. V. Mäntylä, "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering," *Inf. Softw. Technol.*, vol. 106, pp. 101–121, Feb. 2019.

[14] V. Garousi and M. V. Mäntylä, "When and what to automate in software testing? A multi-vocal literature review," *Inf. Softw. Technol.*, vol. 76, pp. 92–117, Aug. 2016.

[15] Trust Over IP Found. (2022). *Trust Over IP (ToIP) Technology Architecture Specification*. [Online]. Available: https://trustoverip.org/wp-content/uploads/ToIP-Technical-Architecture-Specification-V1.0-PR1-2022-11-14.pdf

[16] P. Windley. (2020). *The Sovrin SSI Stack*. Accessed: Jun. 23, 2023. [Online]. Available: https://www.windley.com/archives/2020/03/the_sovrin_ssi_stack.shtml

[17] J. Caballero, H. van Cann, and S. L. von Gohren Edwin. (2023). *Decentralized Identity FAQ*. [Online]. Available: https://identity.foundation/faq/

[18] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen. (2022). *Decentralized Identifiers (DIDs) V1.0. W3C Recommendation*. World Wide Web Consortium. [Online]. Available: https://www.w3.org/TR/did-core/

[19] O. Steele and M. Sporny. (2023). *DID Specification Registries*. Accessed: May 7, 2023. [Online]. Available: https://www.w3.org/TR/did-spec-registries/

[20] W. Fdhila, N. Stifter, K. Kostal, C. Saglam, and M. Sabadello, "Methods for decentralized identities: Evaluation and insights," in *Proc. Int. Conf. Bus. Process Manage.* Cham, Switzerland: Springer, 2021, pp. 119–135.

[21] M. Sabadello and D. Zagidulin. (2023). *Decentralized Identifier Resolution (DID Resolution) V0.3*. [Online]. Available: https://w3c-ccg.github.io/did-resolution/

[22] S. Smith. (2021). *Key Event Receipt Infrastructure (KERI) Design V2.6*. [Online]. Available: https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

[23] DIF DID Commun. WG. (2023). *DIDComm Messaging V2.1 Editor's Draft*. Accessed: Jun. 28, 2023. [Online]. Available: https://identity.foundation/didcomm-messaging/spec/v2.1/

[24] G. Laatikainen, T. Kolehmainen, and P. Abrahamsson, "Self-sovereign identity ecosystems: Benefits and challenges," in *Proc. 12th Scand. Conf. Inf. Syst.*, 2021, ch. 10. [Online]. Available: https://aisel.aisnet.org/scis2021/10

[25] DIF Claims & Credentials WG. (2023). *Presentation Exchange 2.0.0*. Accessed: Jun. 18, 2023. [Online]. Available: Https://identity.foundation/presentation-exchange/spec/v2.0.0/

[26] Internet Eng. Task Force (IETF). *JSON Web Message*. Accessed: Mar. 4, 2023. [Online]. Available: https://tools.ietf.org/id/draft-looker-jwm-01.html
[27] *JSON Web Signature*. Accessed: Mar. 4, 2023. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7515
[28] IETF. *JSON Web Encryption*. Accessed: Mar. 4, 2023. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7516
[29] DIF Secure Data Storage Work. Group. (2023). *Secure Data Storage*. Accessed: Mar. 6, 2023. [Online]. Available: https://identity.foundation/working-groups/secure-data-storage.html
[30] DIF & W3C. (2022). *Encrypted Data Vaults V0.1*. Accessed: Mar. 6, 2023. [Online]. Available: https://identity.foundation/edv-spec/
[31] DIF. (2023). *Decentralized Web Node*. Accessed: Mar. 6, 2023. [Online]. Available: https://identity.foundation/decentralized-web-node/spec/
[32] D. Reed, J. Law, D. Hardman, and M. Lodder. (2019). *DKMS (Decentralized Key Management System) Design and Architecture V4*. Accessed: May 20, 2023. [Online]. Available: https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0051-dkms/dkms-v4.md
[33] DIF. (2023). *Wallet Security Group*. Accessed: May 27, 2023. [Online]. Available: https://identity.foundation/working-groups/wallet-security.html
[34] A. Satybaldy, "Usability evaluation of SSI digital wallets," in *Proc. IFIP Int. Summer School Privacy Identity Manag.*, 2022, pp. 101–117.
[35] H. P. Singh, K. Stefanidis, and F. Kirstein, "A private key recovery scheme using partial knowledge," in *Proc. 11th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Apr. 2021, pp. 1–5.
[36] M. Sporny, D. Longley, and D. Chadwick. (2022). *Verifiable Credentials Data Model V1. 1. W3C Recommendation*. World Wide Web Consortium. [Online]. Available: https://www.w3.org/TR/vc-data-model/
[37] S. Curran, A. Phillip, H. Yildiz, S. Curren, and V. M. Jurado. (2023). *Anoncreds V1.0 Specification*. [Online]. Available: https://github.com/hyperledger/anoncreds-spec
[38] *Personal identification—ISO-Compliant Driving Licence—Part 5: Mobile Driving Licence (mDL) Application*, ISO/IEC Standard 18013-5:2021, International Organization for Standardization, Geneva, Switzerland, 2021. [Online]. Available: https://www.iso.org/standard/69084.html
[39] D. Longley and M. Sporny. (2023). *Verifiable Credential Data Integrity 1.0*. [Online]. Available: https://w3c.github.io/vc-data-integrity/
[40] T. Looker, V. Kalos, A. Whitehead, and M. Lodder. (2023). *The BBS Signature Scheme*. [Online]. Available: https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html
[41] Internet Eng. Task Force (IETF). *JSON Web Token*. Accessed: Mar. 4, 2023. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7519
[42] D. Fett and K. Yasuda. (2022). *Selective Disclosure JWT (SD-JWT)*. [Online]. Available: https://www.ietf.org/archive/id/draft-fett-oauth-selective-disclosure-jwt-02.html
[43] *Cards and Security Devices for Personal Identification—Building Blocks for Identity Management via Mobile Devices—Part 2: Data Objects and Encoding Rules for Generic eID Systems*, ISO/IEC Standard CD TS 23220-2, International Organization for Standardization, Geneva, Switzerlands, 2023. [Online]. Available: https://www.iso.org/standard/86782.html
[44] N. Khateev, S. Klump, and S. Curran. (2021). *Aries RFC 0453: Issue Credential Protocol 2.0*. [Online]. Available: https://github.com/hyperledger/aries-rfcs/tree/main/features/0453-issue-credential-v2
[45] DIF Work. Group. (2023). *Presentation Exchange 2.0.0*. [Online]. Available: https://identity.foundation/presentation-exchange/spec/v2.0.0/
[46] (2023). *CHAPI is the Credential Handler API*. Accessed: Jul. 4, 2023. [Online]. Available: https://chapi.io/
[47] K. Yasuda, T. Lodderstedt, and D. Chadwick. (2022). *OpenID for Verifiable Credentials*. Accessed: Jun. 25, 2023. [Online]. Available: https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf
[48] N. Khateev and S. Curran. (2021). *Aries RFC 0454: Present Proof Protocol 2.0*. [Online]. Available: https://github.com/hyperledger/aries-rfcs/blob/main/features/0454-present-proof-v2/README.md
[49] DIF Working Group. (2023). *Credential Manifest 1.0 Editor's Draft*. [Online]. Available: https://identity.foundation/credential-manifest/
[50] D. Longley and M. Sporny. (2021). *Credential Handler API 1.0*. [Online]. Available: https://w3c-ccg.github.io/credential-handler-api/
[51] T. Lodderstedt, K. Yasuda, and T. Looker. (2023). *OpenID for Verifiable Credential Issuance*. Accessed: Jun. 25, 2023. [Online]. Available: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
[52] O. Terbu, T. Lodderstedt, K. Yasuda, and T. Looker. (2023). *OpenID for Verifiable Presentations—Draft 18*. Accessed: Jun. 25, 2023. [Online]. Available: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
[53] D. Longley and M. Sporny. (2023). *Verifiable Credentials Status List V2021*. Accessed: Jun. 25, 2023. [Online]. Available: https://www.w3.org/TR/vc-status-list/
[54] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," NIST, Gaithersburg, MD, USA, Tech. Rep. RFC 5280, 2008.
[55] Hyperledger Foundation. (2023). *Hyperledger Aries*. Accessed: Apr. 28, 2023. [Online]. Available: https://www.hyperledger.org/use/aries
[56] (2023). *Hyperledger Indy*. Accessed: Apr. 28, 2023. [Online]. Available: https://www.hyperledger.org/use/hyperledger-indy
[57] Hyperledger Aries. (2023). *Hyperledger Aries Cloud Agent—Python*. Accessed: Apr. 28, 2023. [Online]. Available: https://github.com/hyperledger/aries-cloudagent-python
[58] (2023). *Aries Framework JavaScript*. Accessed: Apr. 28, 2023. [Online]. Available: https://github.com/hyperledger/aries-framework-javascript
[59] Hyperledger Foundation. (2023). *Hyperledger Ursa*. Accessed: Apr. 28, 2023. [Online]. Available: https://www.hyperledger.org/use/ursa
[60] D. Khovratovich and J. Law, "Sovrin: Digital identities in the blockchain era," *Github Commit*, vol. 17, pp. 38–99, Oct. 2017.
[61] Sovrin Foundation. (2020). *Sovrin Glossary V2*. Accessed: Feb. 23, 2023. [Online]. Available: https://sovrin.org/library/glossary/
[62] Hyperledger. (2023). *Aries Mobile Agent React Native*. Accessed: Apr. 28, 2023. [Online]. Available: Https://github.com/hyperledger/aries-mobile-agent-react-native
[63] Esatus. (2023). *Esatus Wallet*. Accessed: Apr. 28, 2023. [Online]. Available: https://esatus.com/index.html
[64] Neosfer GmbH. (2023). *Lissi Wallet*. Accessed: Apr. 28, 2023. [Online]. Available: https://www.lissi.id/
[65] Trinsic Technologies Inc. (2023). *Trinsic Wallet*. Accessed: Apr. 28, 2023. [Online]. Available: https://trinsic.id/trinsic-wallet/
[66] Affinidi. (2023). *Affinidi Solution*. Accessed: Jul. 2, 2023. [Online]. Available: Https://www.affinidi.com/
[67] H. A. Tsai, D. Mudassir, C. Guillaume, L. Isaac, H. Christian, K. Den, and T. Looker. (2023). *Sidetree v1.0.1*. Accessed: Jul. 2, 2023. [Online]. Available: https://identity.foundation/sidetree/spec/
[68] Veramo. (2023). *Veramo*. Accessed: Jul. 2, 2023. [Online]. Available: Https://veramo.io/
[69] uPort. (2023). *UPort Solution*. Accessed: May 3, 2023. [Online]. Available: Https://www.uport.me/
[70] Jolocom. (2023). *Jolocom—Decentralized Identity & Access Management*. Accessed: May 3, 2023. [Online]. Available: Https://jolocom.io/
[71] Civic. (2023). *Civic Pass—identity Management Tools for Web3*. Accessed: May 3, 2023. [Online]. Available: Https://www.civic.com/
[72] Veres One. (2023). *Veres One—A Globally Interoperable Network for Identity*. Accessed: May 3, 2023. [Online]. Available: Https://veres.one/
[73] Remme. (2023). *Distributed PKI and Apps for the Modern Web*. Accessed: May 3, 2023. [Online]. Available: Https://remme.io/
[74] G. Fedrecheski, L. C. Costa, S. Afzal, J. M. Rabaey, R. D. Lopes, and M. K. Zuffo, "A low-overhead approach for self-sovereign identity in IoT," in *Proc. 5th The Global IoT Summit (GIoTS)*, Dublin, Ireland. Cham, Switzerland: Springer, Jun. 2023, pp. 265–276.
[75] T. Weingärtner, "Identity of things: Applying concepts from self sovereign identity to IoT devices," *J. Brit. Blockchain Assoc.*, vol. 4, no. 1, pp. 1–7, Apr. 2021.
[76] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 57–64.
[77] E. Samir, H. Wu, M. Azab, C. Xin, and Q. Zhang, "DT-SSIM: A decentralized trustworthy self-sovereign identity management framework," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 7972–7988, Jun. 2022.
[78] Truffle Framework. (2023). *Ganache*. Accessed: May 1, 2023. [Online]. Available: Https://trufflesuite.com/ganache/

[79] N. Kulabukhova, A. Ivashchenko, I. Tipikin, and I. Minin, "Self-sovereign identity for IoT devices," in *Proc. 19th Int. Conf. Comput. Sci. Appl. (ICCSA)*, Saint Petersburg, Russia. Cham, Switzerland: Springer, 2019, pp. 472–484.

[80] F. Capela, "Self-sovereign identity for the Internet of Things: A case study on verifiable electric vehicle charging," M.S. thesis, Dept. Comput. Sci., Univ. Groningen, Groningen, The Netherlands, 2021.

[81] S. Terzi, C. Savvaidis, K. Votis, D. Tzovaras, and I. Stamelos, "Securing emission data of smart vehicles with blockchain and self-sovereign identities," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 462–469.

[82] M. Grabatin and W. Hommel, "Self-sovereign identity management in wireless ad hoc mesh networks," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2021, pp. 480–486.

[83] A. Siqueira, A. F. Da Conceição, and V. Rocha, "Blockchains and self-sovereign identities applied to healthcare solutions: A systematic review," 2021, *arXiv:2104.12298*.

[84] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90478–90494, 2020.

[85] A. Siqueira, A. F. da Conceição, and V. Rocha, "User-centric health data using self-sovereign identities," 2021, *arXiv:2107.13986*.

[86] M. Shuaib, S. Alam, M. S. Alam, and M. S. Nasir, "Self-sovereign identity for healthcare using blockchain," *Mater. Today, Proc.*, vol. 81, pp. 203–207, Jan. 2023.

[87] W. Song, R. N. Zaeem, D. Liau, K. C. Chang, M. R. Lamison, M. M. Khalil, and K. S. Barber, "Self-sovereign identity and user control for privacy-preserving contact tracing," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell.*, Dec. 2021, pp. 438–445.

[88] E. Bandara, X. Liang, P. Foytik, S. Shetty, and K. D. Zoysa, "A blockchain and self-sovereign identity empowered digital identity platform," in *Proc. Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2021, pp. 208–223.

[89] R. Mukta, H. Paik, Q. Lu, and S. Kanhere. (2021). *Credential-Based Trust Management in Self Sovereign Identity*. Accessed: May 3, 2023. [Online]. Available: https://womencourage.acm.org/2021/wp-content/uploads/2021/07/87_extendedabstract.pdf

[90] A. Grüner, A. Mühle, and C. Meinel, "ATIB: Design and evaluation of an architecture for brokered self-sovereign identity integration and trust-enhancing attribute aggregation for service provider," *IEEE Access*, vol. 9, pp. 138553–138570, 2021.

[91] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in *Proc. 2nd ACM Workshop Digit. Identity Manage.*, Nov. 2006, pp. 11–16.

[92] J. Hughes and E. Maler, "Security assertion markup language (SAML) v2. 0 technical overview," OASIS SSTC Work. Draft, Tech. Rep. 13, Sep. 2005. [Online]. Available: https://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf

[93] M. Kubach and H. Roßnagel, "A lightweight trust management infrastructure for self-sovereign identity," in *Proc. Open Identity Summit*, 2021, pp. 155–165.

[94] L. Alber, S. More, S. Mödersheim, and A. Schlichtkrull, "Adapting the TPL trust policy language for a self-sovereign identity world," in *Proc. Open Identity Summit*, 2021, pp. 107–118.

[95] M. S. Ferdous, A. Ionita, and W. Prinz, "SSI4Web: A self-sovereign identity (SSI) framework for the web," in *Proc. 4th Int. Congr. Blockchain Appl.* Cham, Switzerland: Springer, 2023, pp. 366–379.

[96] V. Gerard, "Designing the future identity: Authentication and authorization through self-sovereign identity," M.S. thesis, Dept. Elect. Eng., Math. Comput. Sci., TU Delft Univ., Delft, The Netherlands, 2019.

[97] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, "SSIBAC: Self-sovereign identity based access control," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1935–1943.

[98] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[99] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, Feb. 2015.

[100] J. S. Hammudoglu, J. Sparreboom, J. I. Rauhamaa, J. K. Faber, L. C. Guerchi, I. P. Samiotis, S. P. Rao, and J. A. Pouwelse, "Portable trust: Biometric-based authentication and blockchain storage for self-sovereign identity systems," 2017, *arXiv:1706.03744*.

[101] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, "DNS-IdM: A blockchain identity management system to secure personal data sharing in a network," *Appl. Sci.*, vol. 9, no. 15, p. 2953, Jul. 2019.

[102] R. Soltani, U. T. Nguyen, and A. An, "A new approach to client onboarding using self-sovereign identity and distributed ledger," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1129–1136.

[103] E. Bandara, X. Liang, P. Foytik, S. Shetty, N. Ranasinghe, K. De Zoysa, and W. K. Ng, "Promize—Blockchain and self sovereign identity empowered mobile ATM platform," in *Proc. Comput. Conf. Intell. Comput.*, vol. 2, 2021, pp. 891–911.

[104] Rahasak Labs. (2023). *Rahasak Blockchain*. Accessed: May 3, 2023. [Online]. Available: Https://rahasak.com/

[105] K. A. M. Ahmed, S. F. Saraya, J. F. Wanis, and A. M. T. Ali-Eldin, "A blockchain self-sovereign identity for open banking secured by the customer's banking cards," *Future Internet*, vol. 15, no. 6, p. 208, Jun. 2023.

[106] A. Satybaldy, A. Subedi, and M. Nowostawski, "A framework for online document verification using self-sovereign identity technology," *Sensors*, vol. 22, no. 21, p. 8408, Nov. 2022.

[107] A. Enge, A. Satybaldy, and M. Nowostawski, "An offline mobile access control system based on self-sovereign identity standards," *Comput. Netw.*, vol. 219, Dec. 2022, Art. no. 109434.

[108] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "A blockchain-based self-sovereign identity approach for inter-organizational business processes," in *Proc. 17th Conf. Comput. Sci. Intell. Syst. (FedCSIS)*, Sep. 2022, pp. 685–694.

[109] S. Squarepants, "Bitcoin: A peer-to-peer electronic cash system," *SSRN Electron. J.*, vol. 4, no. 2, p. 15, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[110] C. Dannen, *Introducing Ethereum and Solidity*, vol. 1. Berkeley, CA, USA: Springer, 2017.

[111] M. Lokhava, G. Losa, D. Mazières, G. Hoare, N. Barry, E. Gafni, J. Jove, R. Malinowsky, and J. McCaleb, "Fast and secure global payments with stellar," in *Proc. 27th ACM Symp. Oper. Syst. Principles*, 2019, pp. 80–96.

[112] J. Kwon and E. Buchman, "Cosmos whitepaper," *Netw. Distrib. Ledgers*, vol. 27, no. 1, pp. 4–7, Dec. 2019.

[113] L. Baird, M. Harmon, and P. Madsen, "Hedera: A public hashgraph network & governing council," *White Paper*, vol. 1, no. 1, pp. 9–10, Aug. 2019.

[114] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.

[115] A. Baliga, I. Subhod, P. Kamat, and S. Chatterjee, "Performance evaluation of the quorum blockchain platform," 2018, *arXiv:1809.03421*.

[116] J. Benet, "IPFS—Content addressed, versioned, P2P file system," 2014, *arXiv:1407.3561*.

[117] *Blockchain and Distributed Ledger Technologies—Reference Architecture*, ISO Standard 23257:2022, 2022. [Online]. Available: https://www.iso.org/standard/75093.html

[118] BC Government's Ministry of Citizens' Services. (2023). *OrgBook BC*. Accessed: Jul. 4, 2023. [Online]. Available: https://www.orgbook.gov.bc.ca/about

[119] O. E. Olorunshola and F. N. Ogwueleka, "Review of system development life cycle (SDLC) models for effective application delivery," in *Information and Communication Technology for Competitive Strategies (ICTCS)*. Singapore: Springer, 2022, pp. 281–289.

[120] K.-K. Lau and S. D. Cola, *An Introduction To Component-Based Software Developement*. Cleveland, OH, USA: World Scientific, 2018.

[121] A. Kossiakoff, S. M. Biemer, S. J. Seymour, and D. A. Flanigan, *Systems Engineering Principles and Practice*. Hoboken, NJ, USA: Wiley, 2020.

[122] M. J. H. Faruk, S. Subramanian, H. Shahriar, M. Valero, X. Li, and M. Tasnim, "Software engineering process and methodology in blockchain-oriented software development: A systematic study," in *Proc. IEEE/ACIS 20th Int. Conf. Softw. Eng. Res., Manage. Appl. (SERA)*, May 2022, pp. 120–127.

[123] S. Reddivari, J. Orr, and R. Reddy, "Blockchain-oriented software testing: A preliminary literature review," in *Proc. IEEE 47th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jun. 2023, pp. 48–57.

[124] S. Demi, "Blockchain-oriented requirements engineering: A framework," in *Proc. IEEE 28th Int. Requirements Eng. Conf. (RE)*, Aug. 2020, pp. 428–433.
[125] Š. Čučko, Š. Bećirović, A. Kamišalić, S. Mrdović, and M. Turkanović, "Towards the classification of SSI properties," *IEEE Access*, vol. 10, pp. 88306–88329, 2022.
[126] S. A. Mansoori and P. Maheshwari, "HEI-BCT: A framework to implement blockchain-based self-sovereign identity solution in higher education institutions," in *Proc. 8th Int. Conf. Inf. Technol. Trends (ITT)*, May 2022, pp. 6–10.
[127] EBSI. (2023). *European Blockchain Services Infrastructure Developers Hub*. Accessed: Jul. 4, 2023. [Online]. Available: https://api-pilot.ebsi.eu/docs
[128] M. R. Islam, M. M. Rahman, M. Mahmud, M. A. Rahman, M. H. S. Mohamad, and A. H. Embong, "A review on blockchain security issues and challenges," in *Proc. IEEE 12th Control Syst. Graduate Res. Colloq. (ICSGRC)*, Aug. 2021, pp. 227–232.
[129] D. Pöhn and W. Hommel, "An overview of limitations and approaches in identity management," in *Proc. 15th Int. Conf. Availability, Rel. Secur.*, Aug. 2020, pp. 1–10.
[130] J. Mišic, V. B. Mišic, and X. Chang, "Scalable self-sovereign identity architecture," *IEEE Netw.*, vol. 36, no. 3, pp. 114–121, May 2022.
[131] Y. Liu, Q. Lu, H.-Y. Paik, and X. Xu, "Design patterns for blockchain-based self-sovereign identity," in *Proc. Eur. Conf. Pattern Lang. Programs*, Jul. 2020, pp. 1–14.
[132] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR," in *Proc. 35th Annu. ACM Symp. Appl. Comput.*, Mar. 2020, pp. 342–345.
[133] S. Mahula, E. Tan, and J. Crompvoets, "With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case," in *Proc. 22nd Annu. Int. Conf. Digit. Government Res.*, Jun. 2021, pp. 495–504.
[134] K.-H. Kim, S. Lim, D.-Y. Hwang, and K.-H. Kim, "Analysis on the privacy of DID service properties in the DID document," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2021, pp. 745–748.
[135] P. Dunphy, "A note on the blockchain trilemma for decentralized identity: Learning from experiments with hyperledger indy," 2022, *arXiv:2204.05784*.
[136] O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, E. Maler, D. Reed, and M. Sporny, "Decentralized identity: Where did it come from and where is it going?" *IEEE Commun. Standards Mag.*, vol. 3, no. 4, pp. 10–13, Dec. 2019.
[137] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 71–78.
[138] M. Kubach, C. H. Schunck, R. Sellung, and H. Roßnagel, "Self-sovereign and decentralized identity as the future of identity management?" in *Proc. Open Identity Summit*, 2020, pp. 35–47.
[139] D. Hardman. (2019). *Aries RFC 0005: DID Communication*. [Online]. Available: https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0005-didcomm/README.md
[140] DIDComm User Group. (2023). *DIDComm V2. What's New?*. [Online]. Available: https://didcomm.org/book/v2/whatsnew
[141] K. Yasuda, M. Jones, and T. Lodderstedt. (2023). *Self-Issued OpenID Provider V2*. Accessed: Jun. 25, 2023. [Online]. Available: https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
[142] H. Yildiz, A. Küpper, D. Thatmann, S. Göndör, and P. Herbke, "A tutorial on the interoperability of self-sovereign identities," 2022, *arXiv:2208.04692*.
[143] S. Curren, "Basic message," Tech. Rep., 2021. [Online]. Available: https://didcomm.org/basicmessage/2.0/
[144] R. West, D. Bluhm, M. Hailstone, S. Curran, S. Curren, and G. Aristy. (2021). *Aries RFC 0023: DID Exchange Protocol 1.0*. [Online]. Available: https://github.com/hyperledger/aries-rfcs/blob/main/features/0023-did-exchange/README.md
[145] C.-S. Park and H.-M. Nam, "A new approach to constructing decentralized identifier for secure and flexible key rotation," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10610–10624, Jul. 2022.
[146] DIDComm User Group. (2023). *DIDComm V2 Guidebook: DID Rotation*. [Online]. Available: https://didcomm.org/book/v2/didrotation
[147] R. Soltani, U. T. Nguyen, and A. An, "Practical key recovery model for self-sovereign identity based digital wallets," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, pp. 320–325.
[148] M.-H. Kim, T. Anh Nguyen, and D. Min, "An efficient personal key recovery in self-sovereign identity environments," in *Proc. 15th Int. Conf. Adv. Comput. Intell. (ICACI)*, May 2023, pp. 1–8.
[149] D. WG. (2021). *Didcomm Over Bluetooth*. [Online]. Available: https://github.com/decentralized-identity/didcomm-bluetooth/blob/main/spec.md
[150] A. Heireth Enge, A. Satybaldy, and M. Nowostawski, "An architectural framework for enabling secure decentralized P2P messaging using DIDComm and Bluetooth low energy," in *Proc. IEEE 46th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jun. 2022, pp. 1579–1586.
[151] A. Satybaldy, M. Nowostawski, and J. Ellingsen, "Self-sovereign identity systems: Evaluation framework," in *Proc. 14th Privacy Identity Manag*, Windisch, Switzerland, Aug. 2020, pp. 447–461.
[152] Sovrin Foundation. (2020). *Interoperability Series: Sovrin Stewards Achieve Breakthrough in Wallet Portability*. Accessed: Jun. 30, 2023. [Online]. Available: https://sovrin.org/sovrin-stewards-wallet-portability/
[153] DIF DID Communication WG. (2023). *The European Digital Identity Wallet Architecture and Reference Framework V1.0.0*. Accessed: Jun. 28, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework
[154] A. Kudra, T. Lodderstedt, P. Bastian, M. Mollik, M. Leuken, and C. Roelofs. (2022). *A Credential Profile Comparison Matrix To Facilitate Technical and Non-Technical Decision Making*. Accessed: Jun. 28, 2023. [Online]. Available: https://github.com/WebOfTrustInfo/rwot11-the-hague/blob/master/final-documents/credential-profile-comparison.pdf
[155] A. Abraham, K. Theuermann, and E. Kirchengast, "Qualified eID derivation into a distributed ledger based IdM system," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1406–1412.
[156] A. Abraham, F. Hörandner, O. Omolola, and S. Ramacher, "Privacy-preserving eID derivation for self-sovereign identity systems," in *Proc. Int. Conf. Inf. Commun. Secur.* Cham, Switzerland: Springer, 2020, pp. 307–323.
[157] A. Abraham, S. More, C. Rabensteiner, and F. Hörandner, "Revocable and offline-verifiable self-sovereign identities," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1020–1027.
[158] J. Bobolz, F. Eidens, S. Krenn, S. Ramacher, and K. Samelin, "Issuer-hiding attribute-based credentials," in *Proc. 20th Int. Conf. Cryptol. Netw. Secur. CANS*, Vienna, Austria. Cham, Switzerland: Springer, Dec. 2021, pp. 158–178.
[159] J. Lee, J. Hwang, J. Choi, H. Oh, and J. Kim, "SIMS: Self sovereign identity management system with preserving privacy in blockchain," *Cryptol. ePrint Arch.*, vol. 2019, p. 1241, Oct. 2019.
[160] J. Lee, J. Choi, H. Oh, and J. Kim, "Privacy-preserving identity management system," *Cryptol. ePrint Arch.*, vol. 2021, p. 1459, Nov. 2021.
[161] M. Schanzenbach, T. Kilian, J. Schütte, and C. Banse, "ZKlaims: Privacy-preserving attribute-based credentials using non-interactive zero-knowledge techniques," 2019, *arXiv:1907.09579*.
[162] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1336–1342.
[163] R. Chotkan, J. Decouchant, and J. Pouwelse, "Distributed attestation revocation in self-sovereign identity," in *Proc. IEEE 47th Conf. Local Comput. Netw. (LCN)*, Sep. 2022, pp. 414–421.
[164] V. M. Jurado, X. Vila, M. Kubach, I. H. J. Jeyakumar, A. Solana, and M. Marangoni, "Applying assurance levels when issuing and verifying credentials using trust frameworks," in *Proc. Open Identity Summit*, 2021, pp. 168–178.
[165] D. Pöhn, M. Grabatin, and W. Hommel, "EID and self-sovereign identity usage: An overview," *Electronics*, vol. 10, no. 22, p. 2811, Nov. 2021.

[166] A. Grüner, A. Mühle, and C. Meinel, "An integration architecture to enable service providers for self-sovereign identity," in *Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA)*, Sep. 2019, pp. 1–5.
[167] R. Laborde, A. Oglaza, S. Wazan, F. Barrere, A. Benzekri, D. W. Chadwick, and R. Venant, "A user-centric identity management framework based on the W3C verifiable credentials and the FIDO universal authentication framework," in *Proc. 2020 IEEE 17th Annu. Consumer Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–8.
[168] D. W. Chadwick, R. Laborde, A. Oglaza, R. Venant, S. Wazan, and M. Nijjar, "Improved identity management with verifiable credentials and FIDO," *IEEE Commun. Standards Mag.*, vol. 3, no. 4, pp. 14–20, Dec. 2019.
[169] H. Yildiz, C. Ritter, L. T. Nguyen, B. Frech, M. M. Martinez, and A. Küpper, "Connecting self-sovereign identity with federated and user-centric identities via SAML integration," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Sep. 2021, pp. 1–7.
[170] S. M. Nóbrega Gonçalves, A. Tomasi, A. Bisegna, G. Pellizzari, and S. Ranise, "Verifiable contracting: A use case for onboarding and contract offering in financial services with eIDAS and verifiable credentials," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2020, pp. 133–144.
[171] Q. Stokkink, G. Ishmaev, D. Epema, and J. Pouwelse, "A truly SSI system," in *Proc. IEEE 46th Conf. Local Comput. Netw. (LCN)*, Oct. 2021, pp. 1–8.
[172] R. N. Zaeem, M. M. Khalil, M. R. Lamison, S. Pandey, and K. S. Barber. (2021). *On the Usability of SSI Solutions*. [Online]. Available: https://bit.ly/3ivOzCt
[173] K. C. Toth and A. Anderson-Priddy, "Self-sovereign digital identity: A paradigm shift for identity," *IEEE Secur. Privacy*, vol. 17, no. 3, pp. 17–27, May 2019.
[174] M. Lockwood, "An accessible interface layer for self-sovereign identity," *Frontiers Blockchain*, vol. 3, Mar. 2021, Art. no. 609101.
[175] Y. Shanmugarasa, H.-Y. Paik, S. S. Kanhere, and L. Zhu, "Towards automated data sharing in personal data stores," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops Affiliated Events (PerCom Workshops)*, Mar. 2021, pp. 328–331.
[176] R. Soltani, U. T. Nguyen, and A. An, "A survey of self-sovereign identity ecosystem," *Secur. Commun. Netw.*, vol. 2021, pp. 1–26, Jul. 2021.
[177] S. Garfinkel, *PGP: Pretty Good Privacy*. Sebastopol, CA, USA: O'Reilly Media, 1995.
[178] F. Schardong, R. Custódio, L. Pioli, and J. Meyer, "Matching metadata on blockchain for self-sovereign identity," in *Proc. Int. Conf. Bus. Process Manage.* Cham, Switzerland: Springer, 2021, pp. 421–433.
[179] Z. A. Lux, F. Beierle, S. Zickau, and S. Göndör, "Full-text search for verifiable credential metadata on distributed ledgers," in *Proc. 6th Int. Conf. Internet Things, Syst., Manage. Secur. (IOTSMS)*, Oct. 2019, pp. 519–528.
[180] *eIDAS Regulation (EU)*, document 910/2014, The European Parliament and the Council, Washington, DC, USA, 2014. Accessed: Jul. 4, 2023. [Online]. Available: https://www.eid.as/regulation
[181] U. W. Chohan, "The decentralized autonomous organization and governance issues," *SSRN Electron. J.*, vol. 1, pp. 1–17, Dec. 2017.
[182] V. Lemieux, A. Voskobojnikov, and M. Kang, "Addressing audit and accountability issues in self-sovereign identity blockchain systems using archival science principles," in *Proc. IEEE 45th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jul. 2021, pp. 1210–1216.

ABYLAY SATYBALDY received the master's degree in computer science from the Ulsan National Institute of Science and Technology, South Korea, advancing his knowledge in network theories and applications. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Norwegian University of Science and Technology, Norway. He is a dedicated Researcher with a focus on decentralized systems and blockchain technology. His career began as a Research Assistant with the Ulsan National Institute of Science and Technology, where his work on network design and resource allocation earned him the Best Paper Award at GameNets 2018. He investigates the use cases of blockchain, with a particular emphasis on decentralized identity systems with the Norwegian University of Science and Technology. He has made significant contributions to research and published academic articles on self-sovereign identity and privacy-enhancing technologies. Additionally, he guided graduate students through their thesis projects, demonstrating his commitment to education and mentorship.

MD. SADEK FERDOUS received the Ph.D. degree from the School of Computing Science, University of Glasgow. He is currently an Associate Professor with the Department of Computer Science and Engineering, BRAC University, Dhaka, Bangladesh. He is also an affiliated Research Associate with the Imperial College Business School, working in a project involving identity and blockchain technology. He is very research oriented and love to face new challenges and develop novel mechanisms based on his research. His current research interests include blockchain, self-sovereign identity, identity management, security usability, trust management, Petname systems, trusted computing, and privacy enhancement technologies.

MARIUSZ NOWOSTAWSKI received the M.Sc. degree in AI and machine learning, and the Ph.D. degree in autonomous systems and computational modeling of the biological process of life. He is currently an Associate Professor with the Norwegian University of Science and Technology. Previously, he was an Academic Lecturer with the University of Otago, New Zealand. He is passionate about self-organizing systems, adaptive, and autonomous computation. He has worked on high-end networking applications on GPUs and multicore systems with Sun Microsystems and Oracle. He is also involved in forensics research with Europol, Bitcoin anonymity, and Cryptocurrencies.