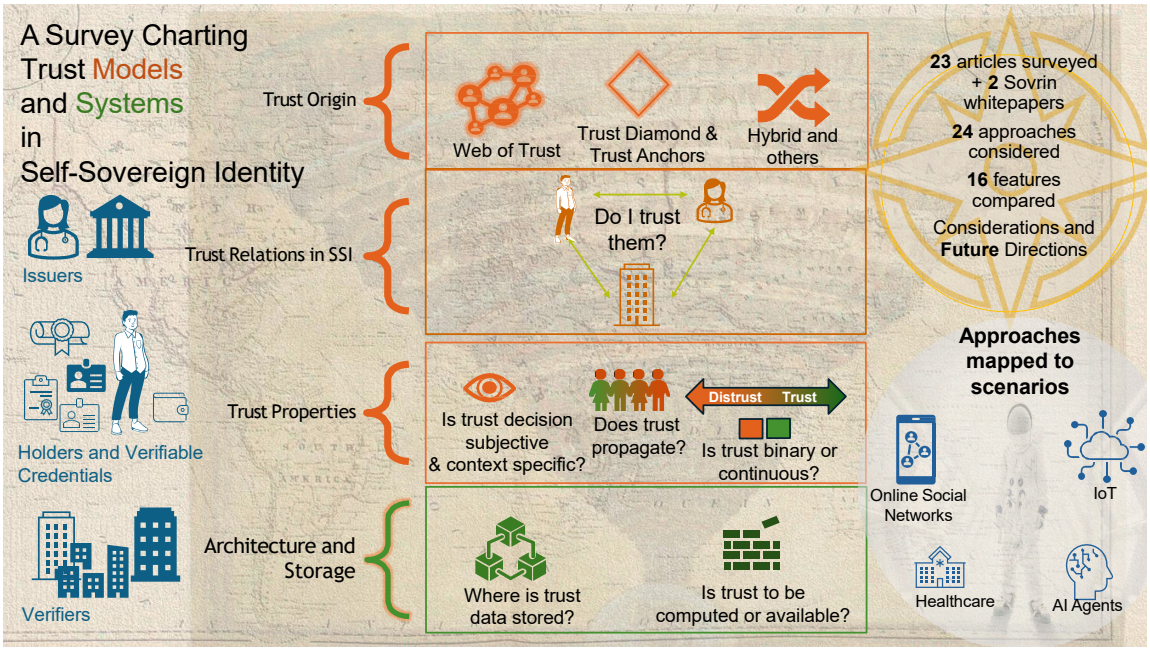
Graphical Abstract

A Survey Charting Trust Models and Systems in Self-Sovereign Identity*

Calogero Turco, Andrea De Salve, Damiano Di Francesco Maesa, Paolo Mori, Laura Ricci



Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Highlights

A Survey Charting Trust Models and Systems in Self-Sovereign Identity

Calogero Turco, Andrea De Salve, Damiano Di Francesco Maesa, Paolo Mori, Laura Ricci

- Surveys 26 sources on trust models in Self-Sovereign Identity
- Analyzes trust models and systems across trust directions, properties & architecture
- Benchmarks 12 features spanning trust relations in SSI and trust properties
- Benchmarks 4 features of Trust Management Systems Architecture & Storage
- Identifies 5 trust challenges in SSI, including AI and portability

Version of Record: **https://www.sciencedirect.com/science/article/pii/S1574013726001565**

DOI: **https://doi.org/10.1016/j.cosrev.2026.101048**

A Survey Charting Trust Models and Systems in Self-Sovereign Identity

Calogero Turco[a,*], Andrea De Salve[b], Damiano Di Francesco Maesa[a], Paolo Mori[c], Laura Ricci[a]

[a]*Department of Computer Science, University of Pisa, Largo Bruno Pontecorvo, 3, Pisa, 56127, PI, Italy*
[b]*ISASI, National Research Council (CNR), Via Amendola, 122/D, Lecce, 73100, LE, Italy*
[c]*IIT, National Research Council (CNR), Via G. Moruzzi, 1, Pisa, 56124, PI, Italy*

Abstract

Self-Sovereign Identity (SSI) is widely positioned as the decentralized future of digital identity. However, although traditional SSI literature emphasizes architecture and privacy, it largely overlooks a systematic analysis of how trust is formed, propagated, and managed. Trust is fundamental because, without it, the actions performed by key actors, including credential issuers, lose much of their practical value. In this landscape, trust is the ground on which SSI systems stand; when that ground is absent or unstable, any structure built on it crumbles. Against this backdrop, we chart the landscape of trust through a comprehensive survey of Trust Models (TMs) and Trust Management Systems (TMSs) in SSI. At the abstract level, we analyze TMs by examining the type of trust relationships among SSI actors and how trust is defined and represented. At the implementation level, we discuss TMSs in terms of how trust is represented, stored, and protected in the systems proposed in the literature. We analyzed 26 sources (24 peer-reviewed papers plus the Sovrin whitepaper and governance framework document), consolidated into 24 approaches, benchmarking 16 features across these dimensions. Based on this analysis, we identify

Official article: https://doi.org/10.1016/j.cosrev.2026.101048
*Corresponding author
Email addresses: calogero.turco@phd.unipi.it (Calogero Turco), andrea.desalve@isasi.cnr.it (Andrea De Salve), damiano.difrancesco@unipi.it (Damiano Di Francesco Maesa), paolo.mori@iit.cnr.it (Paolo Mori), laura.ricci@unipi.it (Laura Ricci)

five open challenges: enabling cross-chain trust portability; designing a hybrid TM that blends Web of Trust and hierarchies; supporting heterogeneous actors such as IoT devices and humans; implementing privacy-preserving feedback mechanisms; and TM and TMS interoperability in emerging settings, including delegated AI agents. Our analysis offers a compass to guide researchers and developers in selecting trust models and advancing SSI systems.

Keywords: Self-Sovereign Identity, Trust, Trust Models, Trust Management, Decentralized Identity

1. Introduction

If cryptocurrency and credit cards are the digital equivalent of paper money, why shouldn't paper IDs be transformed into digital credentials? The idea is alluring: just as cryptocurrencies enable peer-to-peer transactions without intermediaries, digital identity could achieve the same for proving who we are. Physical currencies and cryptocurrencies enable direct exchanges, i.e., transactions between mutually untrusted parties without intermediaries. Similarly, physical IDs are presented directly to those who request them, whereas digital IDs often require a third-party intermediary.

As society becomes increasingly digitized and digital identity becomes more prevalent [1], the need for a digital form of trust becomes even more urgent. Online, users cannot always rely on social cues or institutional assurances. Instead, they must be able to rely on technological systems and digital frameworks.

Today, digital identity largely relies on centralized authorities like Certificate Authorities (CAs) and Identity Providers (IdPs). CAs serve as trust roots, recognized as reliable by all within their ecosystem. A different role is played by IdPs, which act as trust brokers. Their presence makes digital identity a federated system. As such, they are integrated into login interfaces as "Log in with" options, allowing users to authenticate using accounts created on their platforms (such as Google or Meta), while also providing claims about the user, e.g., that a user is of a certain age or holds a given degree. Those federated systems are based on trust derived from already trusted entities. More institutional examples include government-regulated digital identity systems such as EU Digital Identity Wallets [2], BankID [3], and SingPass [4], among others. In these federated systems, trust ultimately stems from guarantees provided by public authorities acting as trust anchors.

Self-Sovereign Identity (SSI) challenges these traditional models by fundamentally rethinking how digital identities are created, managed, and verified. In SSI, an actor's identity is not created by a third party. Instead, the actors themselves, called holders, can create one or more Decentralized Identifiers (DIDs) to represent

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

themselves. Other actors, called issuers, issue Verifiable Credentials (VCs) to a DID, asserting claims about the DID's holder. Note that, since holders store the VCs that refer to them, they retain full control over them and decide to whom they wish to disclose them. Any other actor can verify VCs, independently of centralized control, without directly interacting with the VC issuer. This decentralization offers greater autonomy, but it also raises new trust challenges. How can verifiers distinguish trustworthy issuers from malicious or unreliable ones? What mechanisms help holders to decide whether to share data with a verifier? How can trust models be protected against collusive behavior among actors?

Ultimately, the SSI paradigm involves people, machines such as Internet of Things (IoT) devices [5], and web services making claims to one another and relying on their truthfulness. SSI technology can guarantee that a claim is correctly signed and has not been altered, but it cannot determine whether the claim should be trusted. This leaves us wondering who we should trust, and on what grounds.

Although a significant body of research on SSI exists, few works rigorously analyze trust across different levels: at the abstract level, through Trust Models (TMs), including trust properties, trust relationships among SSI actors, and whether trust propagates; and at the implementation level, through their realization as Trust Management Systems (TMSs). In particular, limited attention has been given to how trust is integrated into SSI solutions, how it interacts with core SSI technical mechanisms (such as DIDs), how trust-related data is structured and managed, and where it is stored within the ecosystem.

We aim to fill this gap by addressing the following research questions.

- **RQ1:** How do TMs for SSI proposed in the literature conceptualize **Trust relations** and **Trust Properties**, and how do they differ?
- **RQ2:** How can the concrete implementations of TMs within TMSs in the SSI literature be classified in terms of **Architecture** and **Storage**, and how do these approaches map to specific application scenarios?
- **RQ3:** What are the major gaps and limitations in current SSI trust solutions?

1.1. Motivation and Contributions

There is a striking absence of guidelines for selecting which TMs and TMSs are most suitable for different SSI scenarios. This gap in the literature leads many SSI solutions to default to Anchor-Based Trust Models (ABs), which require a predefined set of trusted actors, ultimately centralizing the system and contradicting the transparency, interoperability, and portability principles of SSI [6]. Even worse,

some proposals in SSI research omit trust modeling entirely without mentioning or justifying a specific TM.

The goal of this article is to serve as a compass, supporting researchers in choosing the TM that best suits their specific SSI-based systems. Although the literature contains many foundational works on SSI trust, they often mix academic contributions with industry solutions. Instead, we provide a comprehensive framework that classifies all academic trust approaches to SSI TMs and TMSs. Throughout this survey, we use the term *approach* to refer to a surveyed proposal, including both its conceptual TM and its concretization as a TMS. Our focus on academic work was dictated by the aim of capturing a broad design space of TMs and TMSs unconstrained by immediate deployment requirements and economic constraints.

Existing surveys have examined no more than five academic works on trust approaches in SSI. Thus, no prior survey has analyzed a body of work of comparable breadth with a similarly comprehensive selection of papers.

Contribution. Our key contributions are:

- **Corpus:** We searched the literature for peer-reviewed research papers on TMs in SSI, and we selected and analyzed **24** papers (2016–2025) along with **2** technical documents concerning the Sovrin SSI Technical Foundations and its Master Governance Framework.

- **Analytical Framework:** We introduce an analytical framework in the form of a comparative schema, structured around the following three focus areas to address **RQ1** and **RQ2**: *Trust relations*, which capture characteristics related to SSI-specific TMs, including who assesses trust scores between actors and toward whom; *Trust Properties*, which describe how trust is defined, scoped, and represented within a general TM; *TMS Architecture & Storage*, which examines how trust data is structured, managed, and stored within an SSI ecosystem. The analytical framework comprises 16 features that provide a basis for analyzing current and future TMs and TMSs in SSI research.

- **Comparative Analysis:** We leverage the 16 features of the analytical framework to assess the papers in the corpus, answering **RQ1** and **RQ2**. The results are summarized in three comparative tables.

- **Real-World Scenario Mapping:** We identify the scenarios for which each surveyed approach, considering both its TM and corresponding TMS, is best suited, either because it was originally designed for that context or because, in our assessment, it represents a good fit.

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

- **Gap Analysis:** Finally, we address **RQ3** by identifying gaps, limitations, and open challenges emerging from the surveyed literature. These are discussed for each focus area of the analytical framework and span architectural and governance issues, such as the blockchain oracle problem and data protection concerns (e.g., the right to be forgotten), as well as conceptual and computational gaps, including missing mechanisms for trust propagation and aggregation, limited interoperability among trust models, and the absence of trust-score fusion strategies.

This survey is intended to be useful to a wide range of readers, including researchers, developers, and industry professionals engaging with SSI technology, digital trust management, and governance. Significant effort was devoted to organizing the material into clear thematic areas, allowing readers to quickly identify relevant topics and distinguish between theoretical TMs (e.g., community-based trust propagation or anchor-based assumptions) and implementation details in TMSs (e.g., whether trust data are stored on blockchain infrastructure and, if so, on which blockchain). For ease of reading, the list of acronyms used in this work is provided in Table 1.

1.2. Outline

Figure 1 gives an illustrative overview of this document, which is organized as follows. Section 2 presents the core concepts of trust, reputation, and assurance, with a historical review of Web Public Key Infrastructures (PKIs), Pretty Good Privacy (PGP)'s Web of Trust (WoT) up to trust evolution with Web3. Furthermore, an excursus on digital identity is present, arriving at the introduction of W3C DIDs (§2.4.1)Section 3 provides an overview of SSI foundations, including core principles, the W3C VC Data Model specification (§3.1.1), blockchains as Verifiable Data Registries (VDRs) (§3.2) and SSI Wallets (§3.3), thereby establishing the technological background.Section 4 introduces our methodology for selecting the works to classify. Then, Section 5 describes the taxonomy we use to categorize the TMs while also introducing the first feature of our analytical lens, namely whether a TM relies on prescribed trust anchors. Building on this analytical framework, our work examines the literature across three focus areas. These are divided between TMs in Section 6, which describes the TMs at a high level of abstraction, and TMSs in Section 7, which address implementation-level concerns and map SSI trust approaches to scenarios. The reviewed papers are discussed within the corresponding sections through the specified analytical lenses. Each section is further organized into subsections that progress from abstract to concrete, within which we define the features and perform comparisons: (i) Subsection 6.1 examines trust relations in TMs between SSI actors (Table 7); and (ii) Subsection 6.2 summarizes Trust Properties and Measurements

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 1: List of acronyms.

Acronym	Acronym	Acronym
AB: Anchor-Based	**EB-B:** Experience-Based	**MAC:** Message Authentication Code
ABAC: Attribute-Based Access Control	**EWMA:** Exponentially Weighted Moving Average	**MAM:** Masked Authenticated Messaging
ABE: Attribute-Based Encryption	**FAHP:** Fuzzy Analytic Hierarchy Process	**NFT:** Non-Fungible Token
ATIB: Attribute Trust-enhancing Identity Broker	**GF:** Governance Framework	**NI-ZKPoKE:** Noninteractive Zero Knowledge Proof of Knowledge of Exponent
CA: Certificate Authority	**HL:** Hyperledger	**O:** Other
CB: Community-Based	**IdP:** Identity Provider	**OpenID4VP:** OpenID for Verifiable Presentation
CD: Credential Definition	**IMS:** Identity Management System	**OSN:** Online Social Network
CIA: Credential Issuing Authority	**IoT:** Internet of Things	**P2P:** Peer-to-peer
CID: Content Identifier	**IPFS:** InterPlanetary File System	**RL-B:** Rule-Based
CS: Credential Schema	**PGP:** Pretty Good Privacy	**PKI:** Public Key Infrastructure
DAO: Decentralized Autonomous Organization	**PTR:** POINTER	**PUF:** Physical Unclonable Function
DDoS: Distributed Denial of Service	**RA:** Root Authority	**RB-B:** Reputation-Based
DID: Decentralized Identifier	**RL:** Revocation List	**SC:** Supporting Credential
DLT: Distributed Ledger Technology	**SMPC:** Secure Multi-party Computation	**SSI:** Self-Sovereign Identity
DNSSEC: Domain Name System Security Extensions	**TLS:** Transport Layer Security	**TM:** Trust Model
TMB: Trust Manager and Broker	**TMS:** Trust Management System	**TP:** Trusted Party
URI: Uniform Resource Identifier	**V2X:** Vehicle-to-Everything	**VC:** Verifiable Credential
VDR: Verifiable Data Registry	**VP:** Verifiable Presentation	**WoT:** Web of Trust
ZK: Zero-Knowledge		

in TMs (Table 8) and then applies them to the surveyed SSI works. (iii) Section 7 analyzes TMS Architecture & Storage (Table 9). Then (iv) Section 8 maps trust approaches to scenarios (Table 10).(v) Section 9 positions our work among prior SSI surveys. We highlight those where trust-related aspects were considered. The analysis leads up to Section 10, which outlines open challenges related to trust in SSI, both in TMs and TMSs. These open challenges span themes including portability across ecosystems, hybrid WoT/Trust Anchor models, privacy-preserving feedback, IoT/agent settings, and interoperability with Agentic AI. Ultimately, Section 11 presents the conclusions, which distill the main messages of this work and frame

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

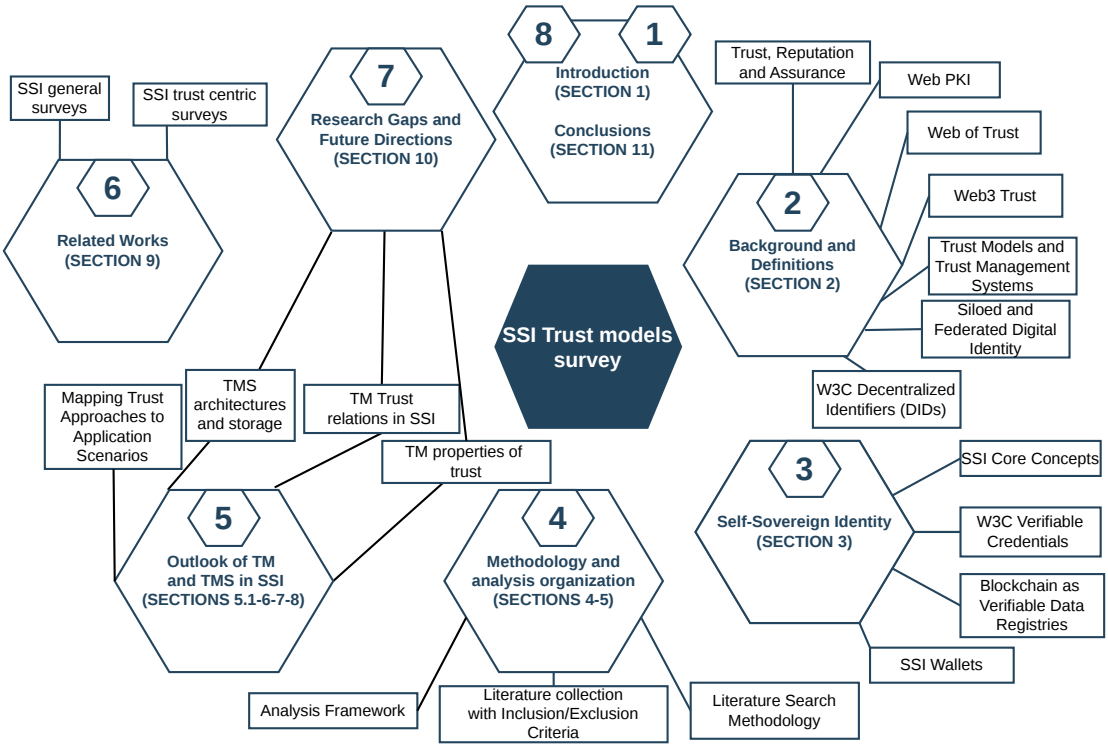


Figure 1: Clockwise-numbered visual outline of our survey.

them as prompts for reflection and action in future research.

2. Preliminary Concepts and Historical Overview

2.1. Conceptual Foundations: Trust, Reputation, and Assurance

Trust toward an entity is defined as the willingness to believe the claims made by that entity or to delegate action to it [7, 8]. Here, an entity may be a person, an organization, a system, or even a software agent. On the other hand, reputation refers to an entity's perceived reliability for being honest (also referred to as trustworthiness) [9]. Reputation is typically inferred from an entity's past behavior and the social feedback provided by the wider community. However, they differ in the perspective they capture. Considering the example of actor Alice, trust toward Alice differs from actor to actor and emerges from direct and personal interactions with each actor, such as Bob. By contrast, reputation is an aggregate evaluation formed from the experiences and opinions of many actors, such as the community

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565
DOI: https://doi.org/10.1016/j.cosrev.2026.101048

surrounding Alice. Both trust and reputation may strengthen or erode over time, depending on the consistency of an actor's actions and the quality of its interactions. The issue is further complicated by the challenges of computing trust and reputation for service providers [10] and other actors on the internet.

As observed by Jøsang et al. [10], the difference between trust and reputation can be illustrated by the following perfectly normal and plausible statements: (1) "I trust you because of your good reputation." (2) "I trust you despite your bad reputation." This illustrates that trust is personal and subjective. In contrast, reputation serves as an indirect source of trust information derived from others' experiences, which can be useful when direct interactions are lacking. Our explicit differentiation of trust and reputation follows Braga et al. [7], clearly defining trust as individual and subjective and reputation as collective and public.

It should be noted that trust is tied to a specific context, such as a thematic topic; accordingly, one entity may trust another only with respect to certain actions and statements, depending on the context [11].

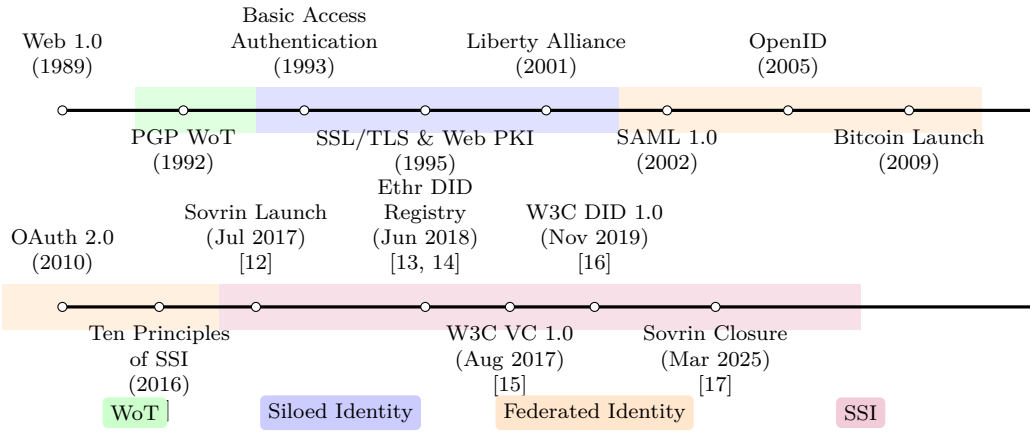


Figure 2: Evolution of digital identity paradigms: from siloed identity systems toward decentralized models, with blockchain technologies as a catalyst

Assurance represents policies and governance practices that reduce or mitigate the risks associated with trusting an entity. Trust enables social cooperation in environments where assurance is absent or insufficient, which is often the case in online interactions.

2.2. Trust Models and Trust Management Systems

A TM provides the conceptual foundation for how entities reason about trust. It defines the assumptions, rules, and evaluation procedures through which one party

evaluates whether, and how much, trust to place in another. This includes how trust is established, propagated, and verified. A TM also specifies the abstract structure of trust information defining what trust means in a given system, the actors involved, and the logic used to derive a trust-or-do-not-trust conclusion.

We consider a TMS as the set of concrete tools for expressing and enforcing trust decisions. In the words of Weeks [18], "trust management systems solve the subproblem by defining languages for expressing authorizations and access control policies, and by providing a trust management engine for determining when a particular request is authorized". In other words, a TMS implements the TM's abstract logic using actual registries, identifiers, and storage and verification mechanisms.

To clarify this distinction, consider a university admissions process: the TM corresponds to the admissions committee's philosophy and criteria. In this case: what counts as merit, how recommendations are weighed, and how exceptions are handled. The TMS is the admissions office itself: the forms applicants fill out, the file cabinet where the forms are stored, the procedures for verifying transcripts, and the staff who check whether each application meets the established criteria. The TM defines the logic of trust, whereas the TMS enacts and operationalizes that logic in practice.

2.3. Web3 foundations of Decentralized Trust

Early Web3 and NFT-based ecosystems played an important role in shaping the initial vision of decentralized trust by popularizing the idea that trust could be rooted in the technology itself, instead of relying on trusted intermediaries, an intuition that proved foundational to SSI. At the core of this transition lies blockchain technology, which enables decentralized ecosystems and interoperable web services. This evolution marks a paradigm shift from the web as a publishing medium to one that fosters interaction and participation [19], which is pivotal to SSI. As blockchain technology proposes to substitute the reliance on traditional trusted intermediaries, it offers shared ledgers, cryptographic verification, and programmable execution through smart contracts, paving the way for decentralized applications and identity.

2.4. Evolution of Digital Identity Systems and Trust Assumptions

In this section, we trace the evolution of digital identity from its origins to the emergence of the SSI paradigm, setting the stage for its introduction in the next section. We briefly illustrate the evolution of digital identity in Figure 2, providing a historical overview that begins with the conceptualization of the World Wide Web. It is worth noting that the development of SSI predates its formal specification, with the launch of Sovrin preceding the subsequent W3C specifications for DIDs and VCs. This reflects the innovative yet still unsettled nature of the SSI paradigm.

Version of Record: **https://www.sciencedirect.com/science/article/pii/S1574013726001565**

DOI: **https://doi.org/10.1016/j.cosrev.2026.101048**

Web Public Key Infrastructure. The Web PKI is the system of CAs, X.509 certificates, and associated protocols that underpin secure communication on the web via the HTTPS protocol. PKI systems rely on the assumption that certification authorities are trustworthy, as their role in identity verification makes them central points of trust. X.509 certificates [20], issued by CAs, bind a public key to a real-world identity (such as a domain name). In the context of HTTPS, the certificate is used during the Transport Layer Security (TLS) protocol [21] handshake to authenticate the server to the client, proving the server's control over the domain. Root certificates, signed by the CA's private key, are pre-installed in browsers and operating systems as Trust Anchors. Intermediate certificates may be issued by root or other intermediates [22]. Any trusted CA can issue certificates for any domain, so the compromise of one CA can affect the entire ecosystem [23].

Web of Trust. The WoT is a social trust model introduced with PGP [24]. The WoT assumes that trust emerges from social relationships and their transitive closure, rather than from a single trusted third party. Users can act as introducers by signing one another's keys. These cryptographic signatures form a distributed network of trust in which each user maintains local decisions about whom to trust [25, 26].

Siloed Digital Identity and Federated Digital Identity. Siloed Digital Identity is the model in which each online Service Provider (SP) effectively acts as an IdP, managing its own user accounts and identity data independently. Unlike in the PKI model, where certification authorities are centralized services trusted by users across different organizations, users in this model place their trust in a single provider that manages their identities. As such, users must disclose their sensitive data to each SP they interact with. Each SP is responsible for independently verifying a user's identity. Given that responsibility, the user's identity is not accepted or recognized by other SPs whenever they do not recognize the user's IdP. This model evolved into Federated Digital Identity.

The federated model allows users to authenticate and exchange identity-related attributes across multiple SPs using an account created with an IdP trusted by the federation. This approach enables cross-domain authentication and attribute exchange, avoiding the need for separate passwords and accounts for every service [27]. Federated Identity represents a first step into a form of decentralization, allowing the bridging of digital identities across independent domains. In Federated Digital Identity, users still trust one or more IdPs to manage their identities. When a user requests a service, trust primarily flows from the SP to the IdP. Centralization and control over user data remain issues in this federated model, as a small number of

actors, often major IdPs such as Google or Meta (Facebook), manage users' identities and control their identity data.

A key protocol for Federated Digital Identity is the Security Assertion Markup Language (SAML) [28], an XML-based protocol in which the IdP sends assertions to the SP.

SAML is often deployed in circles of trust, where sets of SPs accept one or more trusted IdPs. In this sense, administrators of SPs plug in which IdPs are accepted for SSO. OpenID [29] and OpenID Connect [30] follow a similar goal, allowing interaction between an identity provider and a relying party, with mechanisms more suited to modern Web applications and cloud identity platforms such as Microsoft Entra ID [31, 32].

2.4.1. W3C Decentralized Identifiers (W3C DIDs): Foundations, Methods, and Usage

W3C DIDs [33] are a type of Uniform Resource Identifier (URI) that represent a digital identity and resolve to a so-called DID document. This document, typically expressed in JSON, contains metadata associated with the DID, including service endpoints and a reference to the cryptographic protocol for signature verification, possibly including public keys. These keys define how digital signatures can be verified, while the corresponding private key remains securely with the identity owner. It is important to note that DIDs, while being a fundamental ingredient of SSI systems, may also be found as technological components in other identity systems. The core concepts of SSI are discussed in detail in subsection 3.1. Here we discuss DIDs from a technical standpoint, and we anticipate their alignment with SSI. Generally, anyone can generate a DID and key pairs without the involvement of an IdP or CA. Nonetheless, there are some exceptions that we will see.

The creation and resolution of a DID depend on the DID method, which dictates how a DID can be created, resolved to a DID document, updated, or deactivated. There are multiple DID methods. One example is the DID method `did:web`, which leverages web pages to host the DID document and is resolved through the Domain Name System. While this alternative exists, most DID methods use a blockchain to provide hosting, tamper resistance, and global availability for DID documents. The format of a DID consists of three parts, each separated by a colon (:), i.e.:

```
did:<did-method>:<unique-id>
```

The first part, i.e., the string `"did"`, indicates that the URI is a DID; the second part, represented by `"<did-method>"`, specifies the DID method. The third part is the unique identifier in the domain of that DID method. Some examples of

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

DIDs are did:key, which is ledgerless, i.e., a self-contained DID that encodes a public key, allowing direct verification without external infrastructure; did:ethr, based on an Ethereum smart contract acting as a VDR for the DID document; and did:indy, tailored for consortium environments where a permissioned blockchain for SSI (Hyperledger (HL) Indy) serves as the VDR. Furthermore, many DID methods have been proposed, with a few collections of them recognized by the W3C consortium in their Known DID Methods group note [34]. However, some of the listed ones appear to be early proposals, solo projects, or slight variations over more popular approaches. Hopps et al. [35] categorized DIDs not only by their technical aspects, but also by whether they need the deployment of nodes in a network to function, whether they use a blockchain or distributed hash table, whether they are self-contained, or whether they can be stored on web services. In order to highlight the ubiquity of DIDs in adhering to decentralized SSI systems and their TMSs, but also in federated/centralized systems, we made a selection of DID methods, excluding individual hobby projects and methods whose specification cannot be found active online, and represented them according to their alignment with SSI. We show that alignment in Table 2. The methods were classified in accordance with these categories:

- SSI-aligned: DID methods whose identifiers are user-generated and based on a decentralized verifiable data registry with public or publicly grantable access, or where no registry is required at all. Note that this also includes ledgerless methods, where the public keys used for signature verification are inferred from the identifiers themselves, as in `did:key` [36]. In the same line, `did:peer` supports peer-to-peer identifiers that can be created without relying on a public registry [37]. Furthermore, `did:pkh` provides an example of a DID method that spans across multiple VDRs [38]. Rather than relying on a single registry, this method generates a DID Document from a blockchain account, with the target blockchain specified via a specific network identifier, namely `did:pkh:{network}`. It therefore supports network-specific verification methods. However, with some limitations, as it does not support key rotation, since the identifier is bound to the underlying blockchain account.

- Partially SSI-aligned: DID methods whose identifiers can still be created by their subjects, but whose resolution depends on Web-based infrastructure, such as DNS, HTTPS, and CA. For instance `did:web` [39] and `did:webvh` [40]

- Non SSI-aligned governmental: DID methods centered around governmental digital identity infrastructures. In contrast to SSI-aligned methods, the creation, assignment, or governance of identifiers is managed by public authorities. A striking example is `did:ebsi`[41], which operates on the European

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Blockchain Services Infrastructure (EBSI) blockchain and is connected to the European Digital Identity framework introduced by eIDAS 2.0 and the European Digital Identity (EUDI) Wallet architecture [42, 43]. Note that although `did:ebsi` uses a permissioned blockchain it is not perfectly aligned with the SSI decentralization principle. As only strictly authorized entities by the government-approved parties can participate in the network, and the blockchain node operators are chosen by the European Digital Infrastructure Consortium (EDIC)[44]. As such decentralization is limited and trust ultimately depends on the governing consortium.

- Non SSI-aligned enterprise/organization-controlled: DID methods targeting enterprise, institutional, or tightly governed consortium ecosystems. These methods may rely on centralized registries or private/permissioned blockchains, where access is mediated by a company, consortium, or organization, rather than being freely and publicly grantable. For instance, `did:plc` [45] is used in the Authenticated Transfer (AT) Protocol [46] access control to provide persistent account identifiers and support account portability; however, its current design relies on a central Public Ledger of Credentials (PLC) directory [45] service for distributing identity updates. Another example is `did:ccp` [47], maintained by Baidu, Inc., which can work on deployments of Quorum protocol [48] enterprise private permissioned blockchains [34].

Table 2: Representative DID methods clustered by SSI alignment.

Cluster	**Representative DID methods**
SSI-aligned	`3`, `bnb`, `bsv`, `btcr`, `ccd`, `celo`, `cheqd`, `ckb`, `cosmos`, `dht`, `dock`, `ens`, `eosio`, `erc725`, `ethr`, `factom`, `gns`, `hedera`, `hid`, `icon`, `iden3`, `indy`, `io`, `ion`, `iota`, `jolo`, `jwk`, `keri`, `key`, `kilt`, `klay`, `meta`, `near`, `nostr`, `onion`, `ont`, `orb`, `oyd`, `panacea`, `peaq`, `peer`, `pkh`, `polygon`, `polygonid`, `prism`, `safe`, `sov`, `trx`, `v1`, `yourd`
Partially SSI-aligned: web-hosted	`dns`, `ipid`, `jwks`, `ni`, `schema`, `web`, `webplus`, `webs`, `webvh`
Not SSI-aligned: governmental	`andorra`, `ebsi`, `kr`, `psi`, `tr`
Not SSI-aligned: enterprise / organization-controlled	`ala`, `bid`, `ccf`, `ccp`, `cn`, `cndid`, `corda`, `ctid`, `dotbit`, `dweb`, `elem`, `erat`, `evan`, `future`, `gatc`, `grg`, `gwm`, `hpass`, `ibmdc`, `id`, `iid`, `ishare`, `itn`, `iwt`, `kdid`, `kxtid`, `lac`, `ldid`, `mydata`, `nda`, `nuts`, `omn`, `plc`, `pml`, `san`, `snplab`, `ssw`, `tdid`, `ti`, `trustbloc`, `unitrust`, `vaa`, `wba`

As noted in the discussion on federation protocols, enterprise platforms such as Microsoft Entra ID exploit OAuth 2.0 and OpenID Connect to support digital identity, authentication, and authorization. Nonetheless, the Microsoft ecosystem incorporates DIDs and VCs in an enterprise setting, relying on the `did:web` method

for issuers and verifiers [49]. This shows that these technologies can be used beyond a strictly SSI setting. However, we observe that most DID methods still cater to SSI-compliant solutions.

For instance, Ceramic, a decentralized data network [50] allowing multiple blockchains to operate, uses DID technology. In their case, they exploit `did:pkh` to allow users to access Web3 apps over Ethereum with one-click sign-on. Furthermore, they support their own defined 3-ID authentication system to control their DID using blockchain accounts [51], which is capable of retrieving DID Documents over their data streams, which ultimately allows authentication to browser-based systems built using Ceramic.

3. Self-Sovereign Identity (SSI)

3.1. SSI Core Concepts

SSI is a paradigm shift in digital identity that empowers individuals to fully own and manage their digital identity. Instead of having their identity and all related data managed by an external organization and stored in its database, the identity subject stores their identity data either on their own device (i.e., in a wallet) or in a data space under their control, and discloses to external organizations only the data they choose to share when needed. Hence, in SSI, a subject has full control over their data, which enhances privacy and gives them substantial control over their digital identity and related information. Control is, in fact, one of the cardinal principles of SSI [6]. In SSI, a subject can have multiple identities created independently of any organization or context. At the same time, identities are portable, allowing the same identity to be used across multiple services and presented to different organizations.

SSI differs greatly from traditional digital identity, including federated identity. In Federated Digital Identity, some service providers acting as IdPs enable the portability of identities to another service (e.g., through "log in with external service" pages) [52]. However, the user lacks control over their identity because that identity is still stored and managed by an external organization, and the extent to which it is portable is determined by the organization managing it. In contrast, SSI technology allows the portability of digital certificates issued to an identity and the sharing of embedded information under the control of the individual to whom they refer. These digital certificates are called VCs, and they embed a set of claims related to the subject.

The main actors in the SSI scenario are the holder, to whom the VC refers; the issuer, which signs a VC with its private key; and the verifier, which verifies the VC signature with the issuer's public key [53]. When a holder presents one or more VCs to a verifier, they create a verifiable presentation, i.e., a structured collection of

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

credentials, and sign it using their DID private key. This signature proves that the holder is the one performing the presentation and makes it verifiable, which is why the signed presentation becomes what is called a Verifiable Presentation (VP). To enhance the privacy of the subject and strengthen their control over their identity data, several Selective Disclosure techniques, each with its own trade-offs and costs, can be used to disclose to the verifier only a selected subset of the claims embedded in a single VC [54]. Furthermore, other techniques, such as the one presented in [55] based on Zero-Knowledge Proofs (ZKPs) [56], allow a subject not to disclose their identity-related claims at all while still being able to prove certain conditions about them (e.g., being over 18).

The W3C DID [33] and VC Data Model [57] specifications underpin practical SSI deployments. The VC Data Model is illustrated in Figure 3, where a holder presents one or more VCs to a verifier that can verify their authenticity without having to contact the issuing institutions.

SSI has been proposed for a myriad of use cases, as surveyed by Costa and Cunha [58], such as healthcare and pandemics [59], supply chains, online social networks, IoT [5], automotive systems [60], government IDs and documents, and even DeFi know-your-customer scenarios [61].

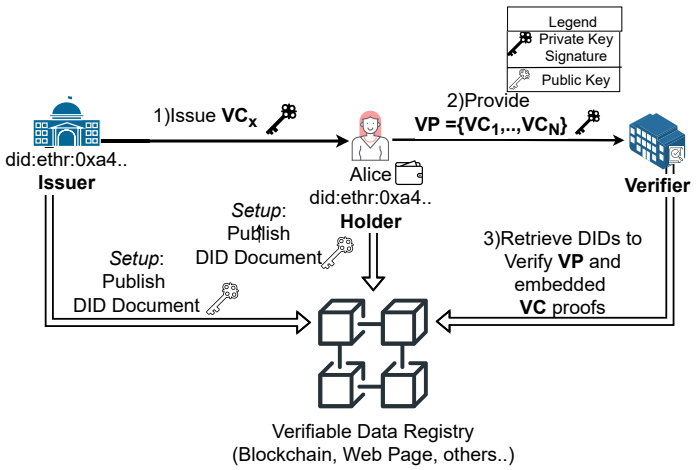


Figure 3: Issuing of VCs and Verification of VPs with embedded VCs.

3.1.1. Verifiable Credential (VC) Data Model v2.0

Verifiable Credentials, as defined by the W3C Data Model specification [57], are a type of digital certificate that holds a set of claims about a subject. VCs are generally JSON objects designed to be tamper-evident, privacy-preserving, and portable, as

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565
DOI: https://doi.org/10.1016/j.cosrev.2026.101048

they need not disclose the full name of the actor to whom they refer. They are issued by the issuer actor, who performs a digital signature using their DID private key. Each VC contains the DID of the issuer and of the holder to whom it refers, ensuring that there is a link to their identities. The issued VCs are stored by the designated holder in their digital wallet [62].

The holder of VCs can create VPs containing one or more of their VCs and send them to a verifier. The verifier checks the issuers' signatures by looking up their DIDs in a VDR specified by the issuer DID method and the holder DID method. VCs may have different cryptographic signatures and verification that are located in the 'proof' field of the VC. A possible signature for a VC is a JSON Web Signature [63], which results in a self-describing JSON Web Token representation; another is a Camenisch-Lysyanskaya (CL) signature [64].

The AnonCreds subtype of VC [65] used in HL Indy requires the creation of a Credential Schema (CS), which defines the structure and list of attributes of a VC. Afterward, an issuer that intends to create VCs with those attributes will publish a Credential Definition (CD). A CD includes the public key used to verify credentials issued under that schema. Notably, this key pair used for signing and verification is kept independent of the issuer's DID key pair. This separation allows specialized cryptographic schemes, enabling advanced features such as revocation [66], selective disclosure, and Zero-Knowledge (ZK) proofs.

A VP is used to provide a tamper-evident presentation of one or more VCs. It includes a proof field containing a signature that attests both to the holder's control of their DID and to the integrity of the VP itself. Furthermore, the VP may contain holder claims, as the holder can also act as an issuer, attesting information about themselves. In general, the signature formats for a VP are the same as those listed above for VCs.

3.2. Blockchain as VDR

A blockchain is a linked list of blocks containing signed transactions and replicated across a peer-to-peer network [67, p.195]. To ensure a consistent ordering of transactions, peers adopt a consensus algorithm. Blockchains provide tamper-evident registries but cannot guarantee the truthfulness of the original input data, a limitation known as the oracle problem [68, 69]. Several studies in the literature address the challenge of establishing trustworthy oracles [70, 71]. Additionally, blockchains exhibit different characteristics depending on the trade-off between decentralization, scalability, and security, defined as the blockchain trilemma by Nakai et al. [72].

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 3: Representative wallets and holder-agent frameworks with their deployment type, SSI alignment, and operational trust assumptions.

Name	**Category**	**Deployment type**	**SSI alignment**	**Operational trust assumption**
Veramo	Agent framework	Full local or full cloud	High	Depends on deployment, plugins, storage, and keys [73].
Credo	Agent framework	Full local or full cloud	High	Depends on agent configuration, storage, and keys [74].
ACA-Py	Cloud agent	Full cloud	High	Depends on backend operator, DB, and key storage [75].
Aries VCX	Agent library	Full local or hybrid	High	Depends on application, wallet backend, and keys [76].
SpruceKit	Wallet toolkit	Full local or full cloud	High	Depends on application design, storage, and keys [77].
Hyperledger Identus	Identity platform	Hybrid or full cloud	High / partial	Depends on platform deployment and storage model [78].
walt.id Community Stack	Wallet infrastructure	Full local, hybrid, or full cloud	Partial / high	Depends on self-managed or hosted deployment [79].
Sphereon Wallet Agent	Wallet agent	Full local or hybrid	Partial / high	Depends on wallet storage and key management [80].
Bifold / BC Wallet	Mobile wallet	Full local	Partial	Depends on device security and local keys [81].
Microsoft Authenticator / Entra Verified ID	Enterprise wallet	Hybrid	Weak / partial	Depends on device security and Entra services [49].
EUDI Wallet	Government wallet	Hybrid	Weak / partial	Depends on device security and certified services [43].

3.3. Wallets: Trust and Assurance

Over the years, many wallets, i.e., applications, libraries, and frameworks for storing VCs and the cryptographic material backing DID, have been defined and engineered. We list a set of popular wallets in Table 3, and we classify them based on their category, i.e., depending on how developers categorized them, on their deployment type, on their alignment with the SSI paradigm, and, ultimately, on the trust assumptions to consider when using them.In column "Category" of Table 3 we distinguish wallets as being:

i) Agent framework, which implements the functionalities of SSI wallets plus other functionalities; ii) Cloud Agents, which implement wallet functionalities over remote servers; iii) Wallet toolkit, representing libraries allowing the execution of wallet operations; iv) Mobile wallet and v) Wallet agent, fully functional applications with working wallet functionalities; vi) Enterprise wallet, clients/applications integrated within an enterprise identity ecosystem; vii) Government wallet, which refers to wallet applications or frameworks certified as compliant with public-sector digital identity requirements. Wallets can also be classified according to their de-

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

ployment type, as some may entirely operate locally or fully in the cloud, while some support both approaches, allowing users to choose the preferred deployment type. Furthermore, wallets may adopt a hybrid deployment model, with one local component and a remote one. The EUDI Wallet [82] and Microsoft Entra Verified ID [83] are examples of hybrid wallet deployment, where part of the wallet functionalities are executed locally, while other parts are hosted on the cloud. In the "Deployment type" column of Table 3, *Full local* denotes wallets or agents whose relevant functions are executed on the holder's device without relying on remote services for ordinary operation; *Full cloud* denotes agents whose core execution and storage are delegated to backend infrastructure; while *Hybrid* denotes architectures in which a local wallet or agent still relies on remote services, registries, governance frameworks, ledgers, trust lists, or resolvers.

Regardless of their category, the primary and critical functionality of a wallet is the protection of the holder's private keys and VCs. The storage of these assets depends on the deployment model: full-local wallets rely on the security of the holders' devices, whereas full-cloud ones delegate key custody to an external provider, reintroducing a trusted third party and thereby weakening alignment with SSI principles.

The choice of wallet deployment is independent of the trust model adopted by the ecosystem (see Subsection 5.1). An ecosystem's trust-origin class does not dictate how holders store their private keys and verifiable credentials. Yet, the kind of wallet adopted by an actor influences the trust relationship within the ecosystem. Any relationship rooted in the holder assumes that the holder retains control on their private keys and that the device hosting the wallet has not been compromised. However, it is worth noting that the trust approaches we survey abstract away from wallet-level security, putting the spotlight instead on the behavior of the SSI actors: how their trustworthiness is evaluated and how trust information is propagated throughout the ecosystem.

Concerning wallet risks, Grüner et al. analyzed in depth threats to wallets [84]. To assess how those threats affect actors in an SSI ecosystem, we distinguish two threat types and their associated risks:

- **Local attacks**: an attacker targets each wallet individually through cyberattacks or phishing [84, 85]. The risk remains local to each user, while the ecosystem of wallets remains more resilient, since the attacks operate on a per-user basis.

- **Cloud attacks**: an attacker may instead compromise a shared cloud infrastructure [86]. Because credential management is concentrated in the cloud

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

wallet provider [87], risk mitigation is only as strong as that provider, and a single compromise is correspondingly more consequential for the ecosystem.

4. Methodology: Literature Search and Inclusion Criteria

Our analysis of SSI TMs and TMSs is a comprehensive study of how they are structured and how they operate across multiple dimensions. The focus is on capturing how TMs have been proposed and classified, and how they have evolved in the academic literature. We examine their architectural choices, storage strategies, trust relations, and trust properties, including the representation of trust, distrust, and propagation, with the aim of guiding the design of SSI systems and paving the way for new TMs and improved TMSs.

We focus exclusively on research that proposes or implements mechanisms for trust formation, trust enforcement, and trust management. To identify relevant works, we conducted a two-stage database search. First, we looked into specific publisher-curated digital libraries: ScienceDirect (Elsevier), IEEE Xplore, ACM Digital Library, and SpringerLink. We then broadened the search scope using Google Scholar.

In order to provide a fully reproducible pipeline, in Table 4 we provide the search terms and the queries that may be used to reproduce our search. The search was carried out over the bibliographic metadata services OpenAlex [88] and Crossref [89]. Figure 4 summarises in a PRISMA flow the records processed in multiple stages. We started by removing duplicates from the results obtained by the previously mentioned services; from those, we obtained 73 possible records that we sought for retrieval. We screened 72 retrievable papers and decided on their inclusion based on our inclusion and exclusion criteria. We categorized each excluded work into a specific excluded category. Furthermore, we archived in a Zenodo repository the reference dataset produced after each step, together with the detailed per-paper exclusion reasons [90].

This survey covers an emerging field in which terminology is unstable and the relevant body of work is not yet consolidated. Given the scarcity of focused literature and the conceptual overlap between trust, trustworthiness, and reputation (see Subsection 2.1), we did not apply overly restrictive exclusion criteria. Instead, we conducted a manual full-text assessment of borderline works using the inclusion and the consequential exclusion categories we defined, so as to ensure coverage of diverse TMs, architectures, and perspectives across application domains. Furthermore, we ensured that the final corpus did not present any work targeting non-SSI decentralized identity or even more general blockchain reputation systems.

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

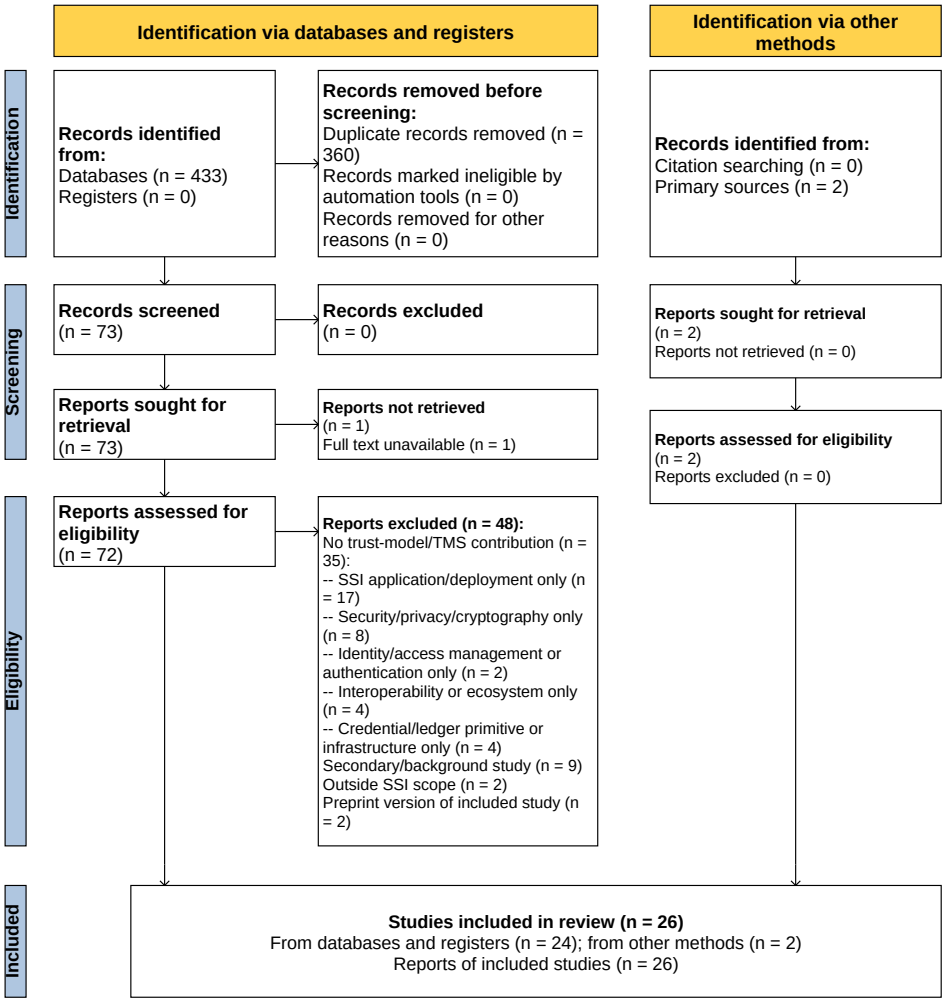


Figure 4: PRISMA 2020 flow diagram of the literature selection.

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 4: Search strategy with sources, terms, and query template to build the corpus.

Component	**Specification**
Metadata sources (main search)	OpenAlex, Crossref
Publication window	2016-01-01 to 2025-06-30
Identity anchor (≥ 1)	"self-sovereign identity", "self sovereign identity", "SSI", "decentralized identifier", "DID", "verifiable credential", "VC"
Trust-related term (≥ 1)	"trust", "trust model(s)", "trust management system(s)", "trust framework", "trust registry", "reputation", "trust propagation", issuer/holder/verifier trust, "trustworthy digital credentials", "privacy preserving trust management", "privacy preserving reputation", "trust governance"
Query template	Type-1: Boolean conjunction of one identity anchor and one trust-related term: $\langle$identity anchor$\rangle \wedge \langle$trust-related term$\rangle$. Type-2: DID/VC variants with explicit SSI anchor: $\langle$DID/VC term$\rangle \wedge \langle$trust-related term$\rangle \wedge$ SSI.

Ultimately, we selected 24 representative academic articles, along with two key documents from the Sovrin Foundation: the Technical Foundations and the Master Governance Framework [91, 92].

Our inclusion criteria guided both the formulation of the search queries reported in Table 4 and the definition of the exclusion criteria.

The inclusion criteria we defined through the query presented in Table 4 can be summarized as follows.

- It focuses on TMs and TMSs in a Self-Sovereign Identity context.
- It includes keywords such as *trust*, *reputation*, *trust model*, or *trustworthiness*, or explicitly discusses mechanisms for assessing, propagating, or enforcing trust between SSI actors, including cases in which holders evaluate verifiers before disclosure or verifiers evaluate issuers and holders before relying on credentials.
- It provides sufficient technical detail to enable comparison within our analytical framework.
- It provides a generalizable TM that can go beyond a single narrow application.

Conversely, we excluded works that fall into any of the categories in Table 5, whose labels correspond to the *Reports excluded* box of the PRISMA flow in Figure 4.

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565
DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 5: Exclusion criteria and rationale. Labels match the *Reports excluded* box of Figure 4.

Excluded category	**Rationale for exclusion**
SSI application/deployment only	Presents an SSI use case or deployment but proposes no TM or TMS, hence no mechanism for trust between SSI actors.
Security, privacy, or cryptography only	Targets security, privacy, or cryptographic primitives without affecting how trust is established between actors.
Identity/access management or authentication only	Focuses on access control or authentication with SSI credentials rather than on assessing trust.
Interoperability or ecosystem only	Addresses interoperability or ecosystem architecture without a mechanism for cross-domain trust.
Credential, ledger primitive, or infrastructure only	Contributes a credential format, ledger primitive, or infrastructure component, with no trust model layered on top.
Secondary/background study	Reviews existing approaches, e.g., prior surveys, rather than proposing a TM.
Preprint of an included study	Non-peer-reviewed preprint superseded by a peer-reviewed version already in the corpus.

To offer a complete discussion of trust in SSI, throughout this article, we also incorporate and cite a broad range of supplemental academic works, using them as conceptual groundwork for definitions, supporting claims, and, where relevant, brief discussions of their contributions. These include foundational texts in cryptography, blockchain, and application scenarios to contextualize and enrich our analysis. Our goal is to ensure comprehensive coverage of the major aspects of trust in SSI.

We summarize the reviewed articles in Table 6.

5. Anatomy of Trust Models and Management Systems in Self-Sovereign Identity

To the best of our knowledge, and based on an exhaustive examination of the existing literature we could conduct, this survey provides the most comprehensive

Table 6: Surveyed trust approaches

Paper	Publisher	Year
[93]	IEEE	2021
[94]	Elsevier	2024
[95, 96]	IEEE	2022, 2023
[97, 98]	Gesellschaft für Informatik e.V.	2021, 2022
[99]	Gesellschaft für Informatik e.V.	2023
[91, 92]	Sovrin Foundation	2016
[68]	IET	2023
[100]	IEEE	2021
[101]	Elsevier	2024
[102]	Elsevier	2023
[103]	Springer Nature	2023
[104]	Elsevier	2023
[105]	IEEE	2020
[106]	IEEE	2018
[107]	IEEE	2024
[108]	Springer Nature	2025
[109]	IEEE	2025
[110]	IEEE	2025
[111]	IEEE	2020
[112]	Springer Nature	2025
[113] (Merkle)	IEEE	2023
[113] (BBS)	IEEE	2023
[114]	Elsevier	2025
[115]	IEEE	2025

chart to date of academic research on TMs and their TMSs in SSI, filling a gap left by previous studies, which mainly focused on other aspects of SSI, often emphasizing production-grade SSI platforms and reviewing no more than five academic papers each. In particular, this paper stands out from earlier works because it formalizes and examines the concept of trust in SSI systems while taking into account TMs and TMSs with different characteristics.

Our analysis of TMs and TMSs follows a layered approach, spanning from conceptual trust abstractions at the top of the stack to their concrete implementation at the bottom. In application scenarios, trust is defined across all levels, encompassing both abstract conceptualizations and concrete implementations, as illustrated in Figure 5.

At the top of the stack depicted in Figure 5, we categorize the surveyed TMs into three distinct classes according to their Trust Origin, as shown in Figure 6 and detailed in Subsection 5.1, where we define those classes. This Trust Origin-based classification is then carried throughout the survey in order to categorize the proposed TMs according to this primary criterion.

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

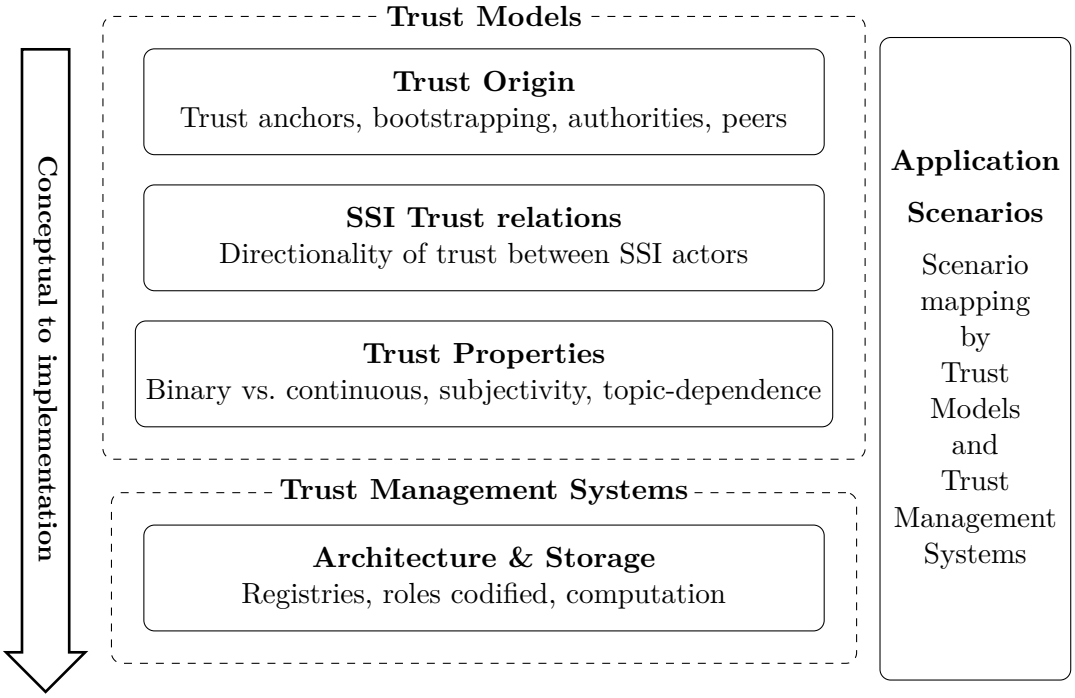


Figure 5: Analytical dimensions of trust in SSI, from conceptual trust models to their concrete realization through trust management systems and application scenarios.

5.1. Trust Model Classes Based on Trust Origin

Considering the trust assumptions and design choices adopted in the surveyed literature, we classify the proposed TMs into two primary classes according to Trust Origin, that is, the source from which trust is initially assumed or derived within the system. We introduce a third residual class for TMs that do not fit neatly into either category.

Trust does not arise spontaneously, nor can it be assumed to exist without some underlying basis. However, many computational systems implicitly assume its presence without explicitly modeling its foundations [116]. This calls for the explicit modeling of trust and its underlying sources. Trust may originate from different sources: it can emerge through direct interactions and accumulated experience among entities operating at the same level (Community-Based), or it can be bootstrapped from socially recognized roles, institutional affiliations, or legal and regulatory frameworks that act as external trust anchors (Anchor-Based), as detailed below.

ABs. ABs, illustrated in Figure 8 through the SSI trust diamond, rely on a set of authoritative actors, such as governments, that are explicitly trusted, while all other

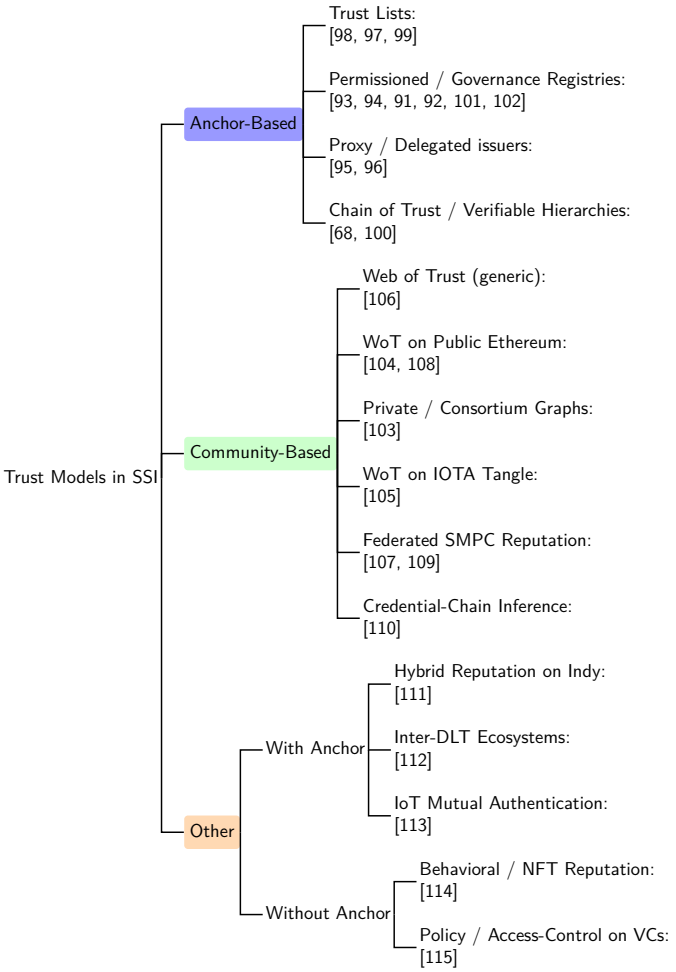


Figure 6: Complete taxonomy of SSI trust models with all surveyed papers.

participants establish trust transitively through endorsements issued by them. Exemplified by Sovrin, these models provide structure and a clear Governance Framework (GF). A GF comprises the policies, roles, and trust rules that govern how participants issue, manage, and verify credentials within an SSI ecosystem, thereby ensuring accountability and interoperability beyond pure cryptography [92]. More generally, the presence of an anchor in a TM indicates that it relies on a predefined set of trusted entities acting as roots of trust. In such a setting, the TM functions like an organizational hierarchy, whereas without an anchor it resembles a self-organizing Peer-to-peer (P2P) network. Certain entities are inherently designated as trusted authorities, and all other participants derive their credibility from them. This de-

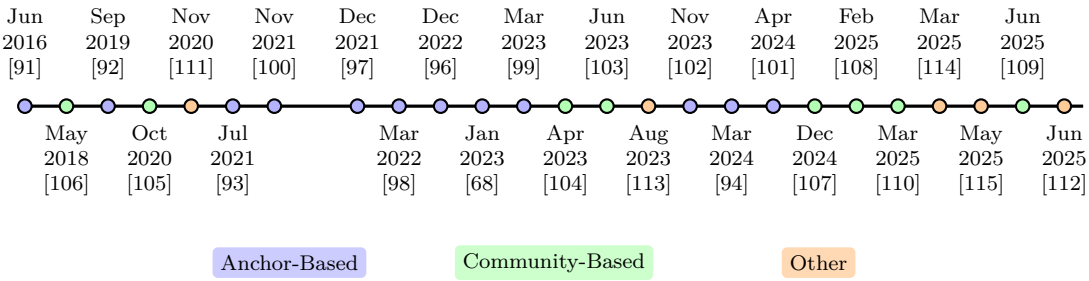


Figure 7: Timeline of surveyed TM papers (2016–2025), each representing an individual publication, with color codes for the type of TM.

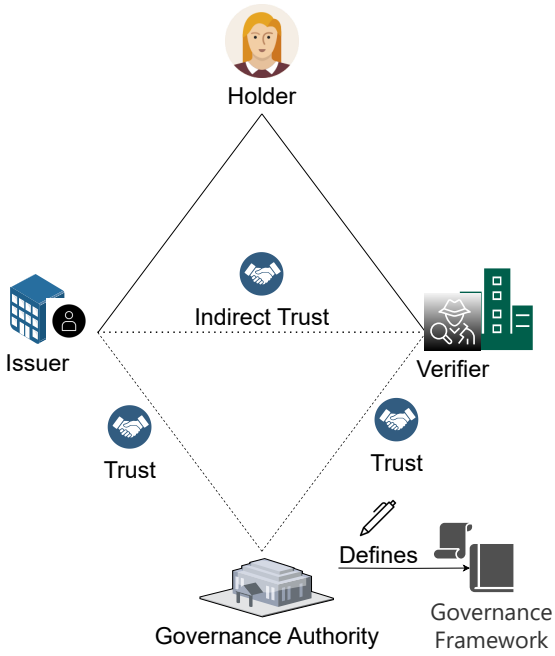


Figure 8: The Anchor-Based SSI "trust diamond": holder and verifier to issuer trust with the Governance Authority defining the Governance Framework and inducing indirect trust.

sign simplifies verification and enables efficient bootstrapping of trust. As shown in Figure 8, a verifier only needs to recognize the anchor as a source of trust and can then determine the level of trust to assign to issuers accordingly, thereby indirectly extending trust to those endorsed by the anchor. From a trust perspective, ABs align more closely with traditional centralized systems, since they concentrate trust in a limited set of accredited entities.

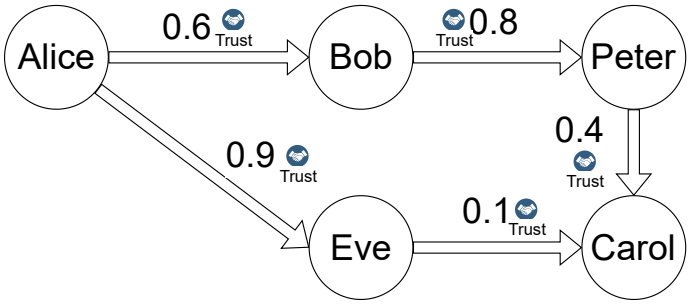


Figure 9: Community-Based SSI with Web of Trust graph. Peers endorse others with trust scores as edge weights, enabling propagation and aggregation of trust.

Community-Based Trust Models (CBs). CBs are generally based on P2P relationships among actors, typically represented through a WoT graph in which trust propagates, as illustrated in Figure 9. Historically, these models are rooted in the PGP WoT, where community members publicly endorse one another or assign trust ratings. In the absence of anchor entities, participants must collaborate, exchange information, and build trust in a decentralized manner. Although these models offer greater flexibility, they are also more fragile and demanding, since entities must actively engage in trust assessment and adapt to the evolving behavior of other community members. By allowing trust to emerge and spread through peer endorsements, CBs avoid single points of failure and foster a decentralized TM [8].

Other Trust Models (Os). Lastly, we categorize as O those works that do not fit neatly into the two categories because they merge AB and CB elements or adopt fundamentally different TMs tailored to closed ecosystems or multi-ecosystem interoperability.

While all AB TMs rely on one or more predefined trust anchors, some of the models that we classify as O also exploit anchoring mechanisms, yet without making them the central organizing principle of the trust model, often in combination with CB functionalities. For this reason, the O class captures TMs that cannot be cleanly classified as either AB or CB, despite exhibiting features of one or both.

First, [111] extends the HL Indy model by incorporating features typical of CB TMs while remaining grounded in Indy, which relies on a set of trust anchors responsible for appointing authorized VC issuers. However, trust in this work is not derived exclusively from the anchor hierarchy, as peer-derived reputation signals also contribute to trust assessment. Consequently, anchoring does not constitute the sole organizing principle of the model, preventing a strict classification as AB.

Second, in [112], the proposed Trust Manager and Broker (TMB) acts as a cross-

system intermediary and effectively becomes a trust anchor mediating interoperability between independent SSI ecosystems. In this case, however, the anchor role is confined to cross-domain trust translation and does not represent a system-wide root of trust within any single ecosystem. Trust, therefore, remains distributed across domains rather than hierarchically anchored in a limited set of roots of trust. Consequently, we place this TM outside the AB class.

Moreover, [113] (Merkle and BBS variants) explicitly introduces a Trusted Party that functions as a trust anchor, since it publishes either a signed list of Merkle roots or a signed revocation list for group keys. However, this anchor is limited to anchoring state information on-chain and does not encode governance rules, trust delegation, or endorsement semantics. As such, it does not constitute the central organizing authority typical of AB TMs.

Conversely, [114] and [115] are classified as O even though they do not require trust anchors. In [114], any actor in the SSI ecosystem can mint Non-Fungible Token (NFT) trust scores on Ethereum smart contracts based on behavioral characteristics. However, unlike CBs, no aggregation mechanism or coordinating authority for those trust scores is specified. Finally, [115] provides a mechanism through which issuers declare which verifiers they trust to access certain claims within a VC, but without a governance framework defining trust anchors as ABs. On top of that, it does not exhibit peer-to-peer trust relationships as in a WoT characterizing CBs.

6. A Guide to Trust Models

The focus of the survey is primarily on how the concept of trust is addressed within the context of SSI, particularly with respect to the trust relationships among the various actors in the SSI model, as required by different frameworks (see Section 6.1). However, these trust relationships are grounded in underlying models that define how such relationships are established, how trust is measured, and other characteristics of trust management (see Section 6.2). Although these trust characteristics are not unique to SSI, our analysis focuses specifically on the 24 TMs we collected from the SSI literature. This section therefore provides a conceptual compass, in terms of features and analysis of the 24 TMs, to navigate the surveyed TMs for SSI at an abstract level before moving to their concrete realization as TMSs. Building on the previously introduced trust-origin classes, we analyze trust models through two complementary levels. Throughout this section, we retain the AB/CB/O class division of TM (defined in Subsection 5.1) in order to group and compare the models consistently. In issuer–holder–verifier interactions, a VDR may serve as the source from which trust-related information is retrieved when such information is

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

recorded there. How this information is stored, accessed, and used is discussed at the TMS level in Section 7.

6.1. Trust Relations in SSI

Rather than concentrating on the foundations of trust, this section focuses on how trust relationships are established and directed among actors, capturing the model's strategy for defining who trusts whom in SSI. Table 7 highlights the trust directions we observed in the literature. We discuss those directions below.

H $\rightarrow$ ***V***. This feature denotes whether the holder evaluates their trust in the verifier when deciding whether to grant access to the sensitive data embedded in their VCs. For instance, the holder may need to check whether the verifier is trusted to store their personal data securely and not reuse it without their consent.

H $\rightarrow$ ***I***. This feature denotes whether the holder assesses their trust in the issuer from whom they receive VCs, since the holder may want to deal only with reputable issuers. For example, before accepting a VC from an issuer, the holder may want to trust that (i) the issuer is legitimate (e.g., a university issuing degree VCs of that type) and (ii) the issuer can be trusted to manage its cryptographic keys and issuance infrastructure securely, thereby reducing the risk of fraud, mis-issuance, forgery, or signing-key compromise.

V $\rightarrow$ ***I***. This feature denotes TMs in which verifiers assess their trust in the issuers of the VCs they receive from holders. For instance, when verifying a diploma, verifiers may check whether the issuing university is recognized and reputable for issuing such a credential.

V $\rightarrow$ ***H***. This feature denotes whether the verifier performs checks on the holder besides checking their VCs before granting them access to services or data. This occurs when the verifier evaluates a trust score for the holder in order to decide whether to grant them access to a service, in addition to verifying the holder's VCs. Thus, depending on that trust score and the attributes in the VC, the verifier accepts or rejects service requests from the holder. Consider cases in which the verifier may need to assign some degree of trust to the holder, since it must assume that the holder securely manages their private keys and that their device has not been compromised.

I $\rightarrow$ ***V***. This feature indicates whether an issuer, in some way, assesses whether a verifier can be trusted, since the latter will access the VCs issued by the former. Issuers do this with the aim of protecting the holders to whom they issue VCs. As such, issuers may add protection mechanisms to their VCs to prevent holders

from presenting sensitive data to sketchy, untrusted, or malicious verifiers. One motivation is to prevent potential misuse of the holder's sensitive data by certain verifiers. Accordingly, issuers apply safeguards to protect claims involving sensitive data, as presented in [115]. Note that, in accordance with the W3C VC Data Model [57], no direct interaction can occur between the verifier and the issuer for this purpose. For instance, in governance frameworks, an issuer may want only verifiers that comply with agreed standards to access or accept some or all claims within credentials released to holders. This concept aligns with the relying-party model of the European Digital Identity Wallet ecosystem, where relying parties, which are similar to SSI verifiers, are required to register under governance rules before they can request and rely on wallet-presented credentials [117].

I $\rightarrow$ ***I***. This feature denotes whether issuers specify trust relationships among themselves. This may happen when issuers are part of a WoT, or when they endorse peer issuers. This feature is worth noting because, in governance settings, issuers often act as maintainers and de facto trust anchors: it is therefore natural to expect them to endorse other trust anchors (e.g., a university endorsing another university), for instance to support credential recognition and cross-domain interoperability. Our past work [118] models these relations as attributes of VC issued toward a holder, dependent on other VCs presented by that holder and on the issuer's trust in the issuers of those latter VCs.

Interestingly, holder-to-issuer trust (H $\rightarrow$ I) remains largely underexplored in the surveyed literature, appearing in only one surveyed TM. This highlights a gap in current SSI TMs, where holders are often assumed to accept issuers' VCs without explicitly evaluating their trustworthiness and thus do not fully adhere to the SSI principle of consent [6]. Furthermore, in the surveyed papers we observed that Trust Directionality is independent of the Trust Origin classification. However, we note that some patterns are apparent in the surveyed works. For instance, I $\rightarrow$ I relationships are not present in the approaches adopting AB TMs. This is because I $\rightarrow$ I relationships are used in those approaches where trust relations are defined between peers at the same level, which is the case in CB TMs. In fact, there are no TMs in the surveyed literature where a trust anchor is used by issuers to evaluate trust towards other issuers.

Nonetheless, such a relationship could still be viable in future work, provided that a TM presents a trust anchor governing issuer-to-issuer trust in a reasonable and justifiable way.

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 7: Trust directions across surveyed SSI trust models.

TM Class	Paper	H → V	H → I	V → I	V → H	I → V	I → I
AB	[93]	×	×	✓	×	×	×
	[94]	✓	×	×	×	×	×
	[95, 96]	×	×	✓	×	×	×
	[97, 98]	×	×	✓	×	×	×
	[99]	✓	×	×	×	×	×
	[91, 92]	×	×	✓	×	×	×
	[68]	×	×	✓	×	×	×
	[100]	×	×	✓	×	×	×
	[101]	✓	×	✓	×	×	×
	[102]	×	×	✓	✓	×	×
CB	[103]	×	×	✓	×	×	✓
	[104]	×	×	✓	×	×	✓
	[105]	×	×	✓	×	×	✓
	[106]	×	×	✓	×	×	✓
	[107]	×	×	✓	×	×	✓
	[108]	✓	×	×	×	×	×
	[109]	×	×	×	✓	×	×
	[110]	×	×	×	✓	×	×
O	[111]	✓	×	✓	×	×	✓
	[112]	×	×	×	✓	×	×
	[113] (Merkle)	×	×	×	✓	×	×
	[113] (BBS)	×	×	×	✓	×	×
	[114]	✓	✓	✓	✓	×	×
	[115]	×	×	×	×	✓	×

Legend: AB = Anchor-Based, CB = Community-Based, O = Other
H → V = holder evaluates verifier, H → I = holder evaluates issuer, V → I = verifier evaluates issuer, V → H = verifier evaluates holder, I → V = issuer evaluates verifier, I → I = issuer evaluates issuer
✓= Present, × = Not Present

6.1.1. Trust Relations in the literature

This subsection analyzes the trust-relation features introduced above across all 24 surveyed TMs. Note that the verifier-to-issuer direction, while the most straightforward aspect, since a verifier must trust an issuer to accept a credential, is not the core of every proposed TM, as it is generally taken for granted.

For each TM, we describe which of the previously defined features are present and how trust is exercised among SSI actors. The full comparison is summarized in Table 7, which provides a consolidated view of the trust-relation features exhibited by each TM, while Figure 10 presents a bar plot highlighting the number of TMs identified in the surveyed papers that address a specific trust direction.

To facilitate comparison, the discussion is organized according to the TM classes defined in Section 5.1, namely ABs, CBs, and Os. This structure aims to highlight

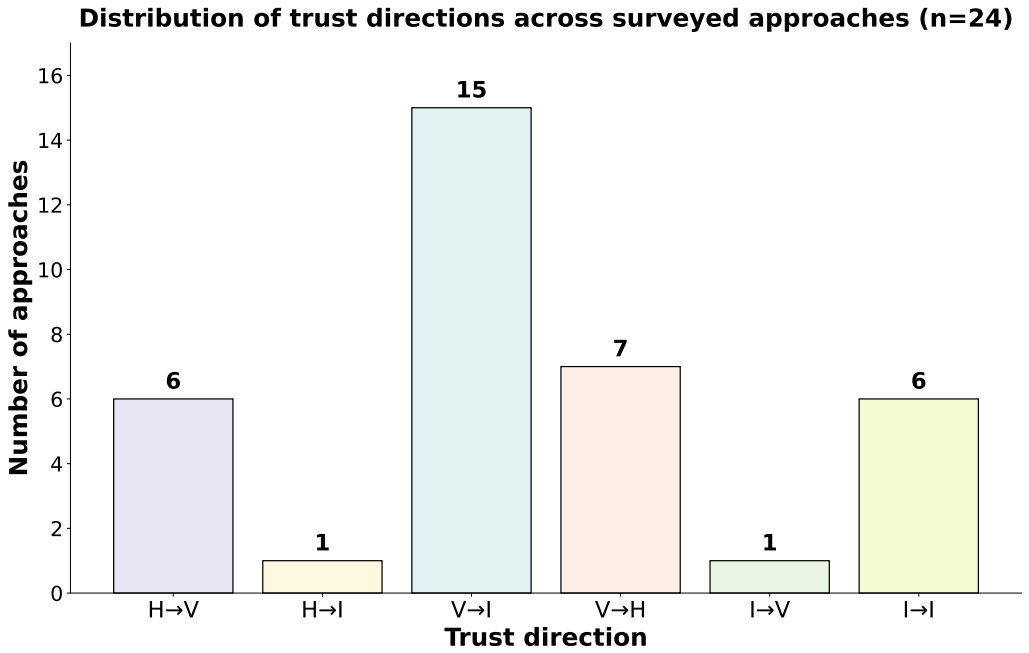


Figure 10: Overview of trust directions across surveyed TMs.

recurring patterns and notable differences in how trust relations are realized within each class.

Anchor-Based Models. **Lauinger et al.** [93] define a verifier-to-issuer trust dynamic: a verifier (or any relying party) evaluates whether a Credential Issuing Authority (CIA) was authorized by a Root Authority (RA) via a ZK proof showing membership in an on-chain RSA accumulator.

Buccafurri et al. [94] define a holder-to-verifier trust dynamic: holders selectively encrypt VC attributes using keys issued to verifiers based on their roles. Trust is expressed through encrypted policies that determine whether a verifier may access attributes.

Mukta et al. [95, 96] define a verifier-to-issuer trust dynamic: the verifier checks whether the issuer possesses valid Supporting Credential (SC)s issued by a Governance Authority.

Grüner et al. [100] define a verifier-to-issuer trust dynamic mediated by the Attribute Trust-enhancing Identity Broker (ATIB). As such, the verifier relies on the ATIB to calculate the trustworthiness of claims issued by Attribute Providers. Internally, the ATIB relies on its own trust model to make decisions about claims from Attribute Providers.

The **TRAIN framework** [**97, 98**] supports verifier-to-issuer trust relations, where verifiers assess issuer trustworthiness by resolving Domain Name System Security Extensions (DNSSEC)-based Trust Schemes. **Chadwick et al.** [**99**] extend TRAIN with a holder-to-verifier trust dynamic, in which holders examine the verifier's domain and trust metadata via OpenID for Verifiable Presentations (OpenID4VPs) and its *"vp token"* mechanism before disclosing VCs.

TrustChain [**68**] defines a verifier-to-issuer trust dynamic: verifiers walk a chain of DID attestations from the issuer up to a Root DID, validating signatures at each step to verify transitive trust.

Ling and Butakov [**101**] support a holder-to-verifier trust dynamic, where holders grant consent-based access only to verifiers they trust. Simultaneously, verifier-to-issuer trust is expressed by auditing whether issuers are registered in a VDR, as required by local authorities.

Pujari et al. [102] introduce a governance framework for the digital-health ecosystem for which they define a verifier-to-issuer and verifier-to-holder trust dynamics. The framework maps SSI actors to healthcare stakeholders and aligns their roles and accreditations with the UK digital identity and attribute trust framework.

Community-Based Models. In **Eer et al.** [**103**], issuers declare issuer-to-issuer trust relationships. Verifiers traverse the graph by paying tokens to issuers along the trust path and may challenge suspicious issuers via a voting mechanism. If trust is found to be misplaced, the involved issuers are penalized.

De Salve et al. [**104**] define a verifier-to-issuer trust dynamic in which verifiers traverse a graph of social attestations published on Ethereum.

Luecking et al. [**105**], building on **Grüner et al.** [**106**], define verifier-to-issuer trust in a WoT model in which each IoT agent maintains its own list of trusted identities.

Yin et al. [**107**] implement a verifier-to-issuer trust dynamic based on feedback aggregated by distributed computation parties (CPs). Data Parties submit issuer-specific feedback, which CPs aggregate using secret sharing into trust scores. Verifiers consult these final scores stored on-chain to assess issuer trustworthiness.

Chung et al. [**108**] define a holder-to-verifier trust dynamic. After an interaction, the holder anonymously provides feedback using blind-signed tokens. These are submitted to a Reputation System that aggregates the trust scores of the community of holders. The Reputation System publishes verifier scores on-chain.

Borges et al. [109] define a verifier-to-holder trust dynamic for the Internet of Vehicles. Vehicles authenticate one another through VCs and then assess a sender's trustworthiness with a distributed *proof of reputation*: a reputation score in the range $[0, 5]$ is aggregated from the positive and negative feedback of neighbouring vehicles

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

by means of multi-party computation, so that trust toward a peer emerges from the collective judgement of the surrounding community rather than from a central authority.

Papaioannou and Ritas [110] define a verifier-to-holder trust dynamic in which the verifier estimates whether a holder can be trusted for properties not explicitly present in its VCs. The paper models this as a credential-discovery problem: GSP-X, CAM, and LPwE derive additional properties from the holder's existing VC and from VC relations observed across a population of entities.

Other models. **Bhattacharya et al. [111]** compute a "confidence" score by combining trust and reputation, extending the graph-based WoT model introduced by Grüner et al. [106]. The trust component originates from attestations between peers. Simultaneously, the reputation of an issuer is calculated locally by the verifier based on the number of VCs the issuer has issued over time. To normalize the reputation, a Exponentially Weighted Moving Average (EWMA) of VC issuance across all issuers is computed. The individual issuer's reputation is then evaluated relative to this EWMA baseline and merged with the trust score to derive a continuous confidence score. This choice captures an important intuition: in institutional scenarios, trust is inversely proportional to the sheer volume of issued VCs. Imagine, for instance, a university with notoriously lax standards that issues hundreds of diplomas in a matter of months. On paper, such productivity might look like prestige; in practice, it betrays a lack of rigor. The EWMA mechanism penalizes these bursts of over-issuance, damping inflated activity and ensuring that credibility is earned through consistent, meaningful issuing. These safeguards prevent institutions from being too careless and prevent automated bots masquerading as institutions from gaming the system by flooding it with credentials. The computation is entirely verifier-local; holders do not participate in this flow.

Frutos et al. [112] define a model in which centralized TMBs manage trust within and across domains. Each TMB assigns trust scores to IoT agents or entities, and these scores are recorded via smart contracts. Multiple TMBs can monitor or interoperate with one another, enabling cross-domain trust propagation. Scores are computed centrally by each TMB, following experience-based (Experience-Based (EB-B)) rules defined per domain. Trust propagates from centralized TMBs and verifiers in their domain to external domains, enabling dynamic inter-domain trust evaluation.

Pino et al. [113] describe two static verifier-to-holder trust relations for mutual authentication in IoT. In the Merkle approach, a verifier checks whether an IoT node belongs to a Merkle tree signed by a Trusted Party (TP) by verifying a Merkle proof. In the BBS approach, the verifier checks whether the node possesses a valid group

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

key (BBS signature) that is not listed in the revocation list. In both cases, trust is binary, fixed at issuance time, and computed solely by the verifier through inclusion verification.

Song et al. [**114**] define an any-to-any trust dynamic in which any SSI actor may act as an evaluator and assign behavioral trust scores to any other actor. Evaluators assess others through features such as trustworthiness, reliability, and security, organized in a hierarchical Fuzzy Analytic Hierarchy Process (FAHP)-based model and compared pairwise. The weighted scores are aggregated into a final reputation score, embedded into a non-transferable NFT via a smart contract.

Bistarelli et al. [**115**] define an issuer-to-verifier trust dynamic: issuers embed access control policies in VCs using smart contracts. During the presentation, verifiers must satisfy the policy conditions specified by the issuer, proving that they meet pre-specified trust criteria before being granted access to a VC's claim.

6.2. Properties of Trust in SSI Trust Models

This subsection analyzes the properties of trust in general TMs and applies them to SSI across all 24 surveyed TMs. While the previous subsection focused on identifying who trusts whom and how trust propagates among SSI actors, this subsection instead examines the intrinsic characteristics that trust can assume within a model, drawing on established dimensions from computational trust and reputation systems [11, 116, 119, 10, 120] and extending them where necessary to reflect SSI-specific design choices. In particular, we examine the intrinsic characteristics that define the type of trust supported by each model, considering how trust is defined, measured, and scoped, and whether privacy aspects are integrated.

For each surveyed TM, we identify which trust properties are supported and how. The resulting comparison is summarized in Table 8. To facilitate comparison and highlight systematic differences, the table is organized by TM class, as defined in Subsection 5.1.

Trust Formation. This feature characterizes the methods for defining trust, i.e., the mechanisms by which a system decides that one actor (or entity) can be considered trustworthy. At a high level, trust can be represented by three broad families: rule-based [121], reputation-based [10], or experience-based [116, 119]. Rule-based trust applies whenever the governors of a GF specify the rules and policies that designate which actors are to be trusted. Reputation-based trust is characterized by trust emerging from P2P trust relationships, where evaluations provided by actors accumulate into a reputation that propagates across the network. Lastly, experience-based trust emerges from direct interactions and other available information sources about an actor, including VCs and general claims, data, and information available

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 8: Trust properties in SSI TMs.

TM Class	Paper	Trust Formation	Propagation	Granularity	Distrust	Context Awareness	Subjectivity
AB	[93]	RL-B	×	Bin	×	×	×
	[94]	RL-B	×	Bin	×	✓	×
	[95, 96]	RL-B	×	Bin	×	✓	×
	[97, 98]	RL-B	×	Bin	×	×	✓
	[99]	RL-B	×	Bin	×	×	✓
	[91, 92]	RL-B	×	Bin	×	×	×
	[68]	RL-B	×	Bin	×	✓	✓
	[100]	RL-B	×	Num	×	✓	×
	[101]	RL-B	×	Bin	×	✓	×
	[102]	RL-B	×	Num	×	✓	×
CB	[103]	RB-B	✓	Num	×	✓	×
	[104]	RB-B	✓	Num	✓	✓	✓
	[105]	EB-B	✓	Num	×	✓	✓
	[106]	EB-B	✓	Num	×	✓	✓
	[107]	EB-B	×	Num	✓	✓	×
	[108]	RB-B	×	Num	✓	✓	×
	[109]	RB-B	×	Num	✓	✓	×
	[110]	EB-B	✓	Num	×	✓	×
O	[111]	EB-B	✓	Num	×	✓	×
	[112]	EB-B	×	Num	×	✓	×
	[113] (Merkle)	RL-B	×	Bin	×	×	×
	[113] (BBS)	EB-B	×	Bin	×	×	×
	[114]	RB-B	×	Num	✓	✓	×
	[115]	RL-B	×	Bin	×	✓	×

Legend:
AB = Anchor-Based, CB = Community-Based, O = Other, RL-B = Rule-Based, RB-B = Reputation-Based, EB-B = Experience-Based, Bin = Binary, Num = Numerical
✓= Present, × = Not Present

on the Internet [119]. Figure 11 shows the prominence of **rule-based** TMs among the 24 surveyed TMs. Read against the Trust Origin classes in Subsection 5.1, the surveyed ABs are rule-based, whereas the surveyed CBs use reputation-based or experience-based formation.

Granularity. This feature, inspired by prior work on the computational representation of trust values [119], discerns whether trust is modeled as a binary yes/no choice or as a numerical range representing shades of gray.Granularity therefore follows the Trust Origin and Trust Formation pattern as a tendency: AB and rule-based models tend toward binary trust, while CB and reputation- or experience-based models tend toward numerical values.

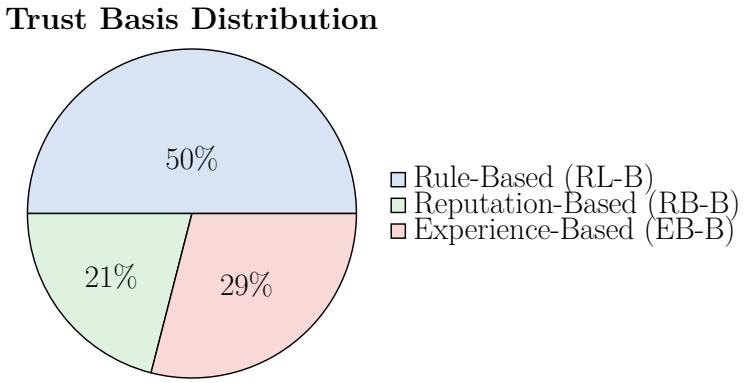


Figure 11: Distribution of trust basis among surveyed SSI trust models.

Propagation. A TM exhibits propagation whenever, considering Alice, trust in her is derived from the trust that other actors place in her through chains of relationships. For instance, if Bob has not interacted directly with Alice but trusts Carol, and Carol trusts Alice, then Bob may derive a trust score for Alice through the propagation of trust along the path Bob $\rightarrow$ Carol $\rightarrow$ Alice. This feature, inspired by trust-score propagation mechanisms studied in networked systems [120, 122, 119], denotes whether trust, expressed as a trust score (binary or continuous), is inferred through P2P relationships between actors placed at the same level, with no trust-score aggregation performed beforehand. Thus, this feature is not present when there is a community-aggregated trust score. By contrast, it is present when an actor needs to reconstruct trust-score chains from their peers. Among the methods for propagating trust, we highlight trust derived from VCs. Accordingly, a VC may encode information that is processed during trust-score assessment by an actor. For instance, [106, 105] derive an actor's trust score from trust in the issuers of VCs about that actor, propagated through the possession of those VCs. For the purpose of Table 8, we also mark propagation when a paper explicitly uses credential chains or graph/label-propagation mechanisms over VCs to infer trustworthiness for properties that are not directly attested by a holder's credentials. In the surveyed TMs, propagation appears mainly among non-rule-based models. Note that it is not a strict consequence of the trust-formation category; however, when propagation is present, the propagated trust is represented numerically.

Distrust Modeling. By contrast, this feature considers whether negative feedback or negative trust scoring is factored into the TM design. This feature was drawn from [123] and is inspired by non-monotonic trust models and adversarial settings [121, 124]. Across the surveyed TMs, distrust appears mainly where feedback or

reputation contributes to trust formation, and the cases that model distrust represent it with numerical trust values.

Context Awareness. This feature indicates that trust can be limited to particular domains; for example, a hospital may be trusted for issuing medical certificates, but not for driving licenses. We drew this feature from models emphasizing context-dependent trust [125]. Looking at the corpus TMs, context awareness is systematic among CBs, while ABs and Os exhibit it unevenly.

Trust Subjectivity. Finally, this feature looks at the differences in point of view between the actors. We highlight the inherently subjective nature of trust from prior trust literature [116, 10, 119]. When trust is assessed subjectively, the same entity may obtain different judgments depending on the assessing actor. Otherwise, trust is absolute if it is the same for all actors within the TM. In other words, different trust scores may be obtained for a given actor.

A broad comparison of how the different TM categories support trust-related properties detailed below is shown in the radar chart in Figure 12, highlighting how CBs encompass the widest range of trust features.

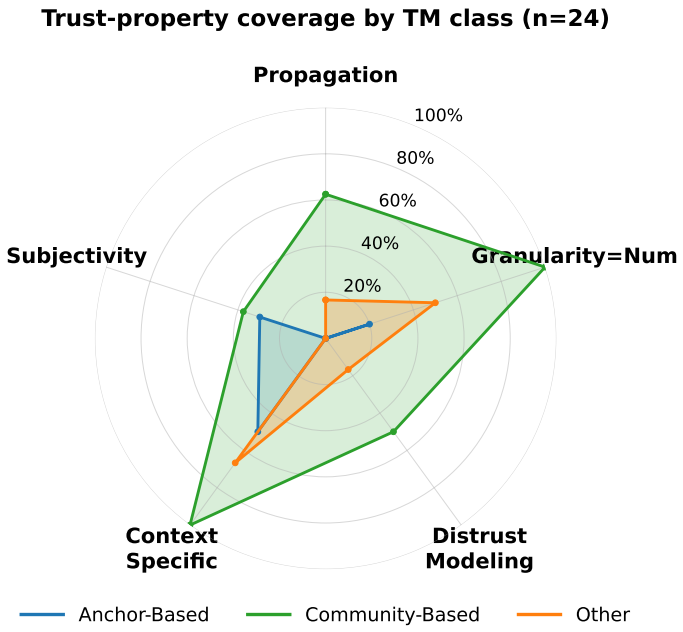


Figure 12: Distribution of trust property support across AB, CB, and O models. Values represent the percentage of models in each category supporting each property.

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565
DOI: https://doi.org/10.1016/j.cosrev.2026.101048

6.2.1. A Chart of Trust Properties in SSI Literature

This subsection analyzes the trust properties introduced above across all 24 surveyed TMs. For each TM, we describe which of the previously defined features are present. The full comparison is summarized in Table 8, which provides a consolidated view of the trust property features exhibited by each TM. To facilitate comparison, the discussion is organized by TM class as defined in Section 5.1, aiming to highlight recurring patterns and notable differences in how trust properties are realized within each class.

Anchor-Based Models. All AB systems adopt a Rule-Based (RL-B) trust-definition paradigm: a governing actor (Trustee, Steward, Root Authority, TSO, consensus provider, ...) issues a binary "trusted / not trusted" judgment that verifiers check. Consequently, trust is almost always static. There can be updates to the set of trusted entities when the anchor revokes the trust placed in an issuer or endorses a new issuer, as in Sovrin [91, 92], TRAIN [97, 98, 99], and Lauinger et al. [93].

Because the output is Boolean, authors rarely use granular metrics. The work of **Grüner et al. [100]** is an outlier, since the broker returns a continuous confidence value regarding an issuer's ability to issue certain attributes. VCs are used to embed the anchor's decision in **Mukta et al. [95, 96]**, which use SCs to authorize the issuance of VCs within a given topic, thereby showing context awareness. Trust is evaluated by following a credential chain up to a governance anchor.

Lauinger et al. [93] define trust in a rule-based manner: a CIA is trusted as an authorized issuer only if it satisfies the governance rules established by the RA. More precisely, trust depends on whether the CIA can prove membership in the set of entities authorized by the RA. As such, trust is binary, since the outcome is simply whether the issuer is authorized or not. No trust propagation mechanism is provided, as trust is not inferred through chains of peer relations but directly from the RA's authorization. Likewise, no distrust model is introduced, and trust is not subjective, since the authorization outcome does not depend on the evaluator's personal perspective. The corresponding TMS also includes a privacy-preserving mechanism through which a CIA can prove membership in the authorized set without disclosing its identity.

Buccafurri et al. [94] preserve the privacy of the VC holder by implementing the trust model through access control over specific VC attributes. Trust is expressed through VDR records on smart contracts; no distrust mechanism is provided, and trust is binary with respect to capabilities, i.e., trust for a topic.

In **TRAIN [97, 98, 99]**, trust is subjective because it depends on the DNS operators' governance rules that decide who is trusted for evaluator actors. In **TrustChain**

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

[68], by contrast, trust assessment depends on the upstream DID trusted in the chain of trust.

Community-Based Models. In community-based models, instead of relying on hard rules through which trust anchors designate trusted issuers, users provide feedback on others to build reputation scores based on collected evidence. Trust is therefore **dynamic** and is generally represented as a continuous value. Trust scores flow through a web of issuers, with verifiers incentivizing propagation as paying customers and policing it as the jury when the trust extended by issuers is misplaced.

Grüner et al. [106] and Luecking et al. [105] propose the same trust model, with the latter providing an implementation over IOTA. In both works, trust is evaluated by the verifier through a recursive traversal of the trust graph from the perspective of the actor assessing trust, weighted by the number and depth of attestations on context-specific claims. Trust scores are updated round by round as new claims and attestations are incorporated. In this TM, verifiers first evaluate direct attestations of VCs issued by them toward the actor being evaluated and, if these are unavailable, follow multi-hop attestations through the WoT. A personalized trust function aggregates trust along the path, reducing weight as depth increases.

In **Eer et al.** [103], trust relationships are publicly declared by issuers in the private HL Besu deployment. Trust is a continuous value involving the Besu graph state and is expressed in a context-specific manner. Issuers that assign a wrong or malicious trust score to others in a path can be challenged and punished by a verifier, causing them to lose the coins they staked.

In **Yin et al.** [107], the Secure Multi-party Computation (SMPC)-based feedback mechanism allows users to submit context-specific ratings, positive or negative, encrypted with additive secret sharing. Computation parties collaboratively compute statistics (min, max, median) without learning individual scores. Trust can change dynamically over time. In this case, there is no trust propagation, as the computation of the trust score does not require traversal over a WoT, but instead relies on aggregated values derived by CPs from anonymous feedback.

De Salve et al. [104] use Ethereum smart contracts to represent trust graphs among OSN users. Trust is derived from subjective social relationships, so the resulting trust score differs for each actor depending on the WoT graph and is computed contextually. The system allows the expression of continuous trust scores in a given context, and trust can change dynamically with updates. Trust propagates along friendship links with weighted scores, and the verifier computes a custom trust function to obtain trust from their node in the WoT up to the issuer.

Chung et al. [108] introduce a privacy-preserving holder-to-verifier feedback system. Verifiers issue blind-signed tokens during interactions. Holders later sub-

mit anonymous feedback about the verifiers in a specific context, with the review authenticated through those tokens. Feedback is published on-chain, and the average trust score is provided in a VC issued to the verifier. In this TM, there is no trust score propagation because the computation of the trust score does not require traversal over a WoT. Verifiers may subsequently receive VCs reflecting their accumulated reputation. These VCs are described as being issued by the on-chain reputation system. However, the paper does not specify the technical details of the issuance process. Borges et al. [109] define a reputation-based, numerical, and context-aware trust score for IoV entities, where positive and negative feedback are aggregated through MPC rather than propagated along trust paths. Papaioannou and Ritas [110] define three algorithms for deriving implied credentials from VCs. In their model, trust toward a holder is inferred by estimating whether the holder possesses properties not directly attested by its presented credentials, using credential chains and graph/label-propagation patterns observed across entities with related credential sets.

Other models. The models in this category leverage trust representations not covered in AB or CB schemes.

Bhattacharya et al. [111] combine the Grüner et al. WoT model [106] with local issuer reputation based on the number of issued credentials. Verifiers compute a continuous "confidence" score by normalizing issuance statistics using EWMA and merging them with the WoT-derived trust. Trust is context-specific, computed locally, and represented as a continuous measure. Distrust and privacy-preserving mechanisms are not supported. Trust propagates through WoT peer attestations made by multiple verifiers, and each verifier integrates this propagated trust with reputation to assess final trust toward issuers. In **Frutos et al. [112]**, a TMB decides trust or distrust based on EB-B rules to assign context-specific trust scores. Furthermore, these scores are stored on-chain via smart contracts. In **Pino et al. [113]**, the authors propose two authentication schemes which we refer to as **(A)** and **(B)**. In both cases, trust is represented as a yes or no answer to belonging to a trusted entity set.

Song et al. [114] compute trust scores locally using FAHP on behavioral features such as trustworthiness and reliability. The resulting continuous, context-specific score is embedded in an NFT, with metadata stored off-chain. Trust evolves dynamically based on updated evidence. Each evaluator performs trust computation independently, without WoT propagation.

In **Bistarelli et al. [115]**, trust is binary toward verifiers that must satisfy policy conditions on a context to be trusted.

7. Trust Management Systems

In this section, we move from abstract TMs to their realization as TMSs and analyze how the surveyed works implement their TMs in concrete systems. We focus on architectural and storage design choices, highlighting the actors involved, how their roles are encoded for trust management, and how trust information is stored, retrieved, and used. These aspects are evaluated through four features, which are summarized in Table 9 and discussed in the following paragraphs.

DID Method Dependence. This feature captures whether a TMS operates independently of any specific DID method or is designed to support a particular one. This distinction reflects two alternative TMS design strategies: an agnostic TMS enables broader interoperability, while a method-specific TMS allows tighter integration with its features, albeit at the cost of reduced flexibility and potential lock-in. In the surveyed TMSs, DID-method-specific designs may co-vary with storage choices when the method is tied to a particular VDR or registry, but this relation is not universal.

Storage. The Storage feature identifies which registry is used to store trust-related data, such as credentials, relationships, or past interactions, thus indicating whether its availability is explicitly guaranteed. The choice of registry dictates the design of the entire solution, as ABs generally rely on permissioned blockchains or other registries such as DNS. In contrast, CBs target a public blockchain to ensure maximum decentralization. In an SSI TMS, availability plays a decisive role, and blockchain-based registries are a strong guarantee of it whenever the data are fully stored and retrievable on-chain. Indeed, a blockchain guarantees persistence, tamper freeness and accessibility by design; by contrast, alternative registries are generally less costly and more flexible with respect to modification and redaction, but lack the built-in guarantees of persistence, integrity, and availability offered by blockchain systems.

Privacy Preservation. This feature poses the question of whether the TMS ensures that trust-related information (e.g., trust scores, feedback, endorsements, or trust-graph edges bound to a DID) is protected from unrestricted disclosure. We distinguish between TMSs in which trust-related data are publicly accessible through the underlying registry and TMSs that limit their visibility to authorized parties by means of additional Access Protection mechanisms (e.g., access-control policies, authentication, membership in a permissioned network, encryption/key management, anonymization or aggregation of feedback, or selective disclosure). In this sense, Access Protection concerns whether trust-related data can be obtained by any actor once the underlying registry or platform is reached, or whether access to such data is gated by platform-level control mechanisms, preventing actors from obtaining

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

the trust data in the first place unless specific access conditions are satisfied. These mechanisms can provide stronger security controls, finer-grained access management, and potential compliance guarantees (e.g., GDPR, by limiting the public exposure of trust and identity-related information). However, they also introduce drawbacks, since they must be managed and may render trust opaque to actors that are not authorized to access the data. We introduce this feature as it is fundamental to the SSI paradigm and a unique feature that is part of its core principles.

Trust Computation Mode. This feature specifies whether trust data are provided in a pre-assembled form and directly stored (S), or instead computed dynamically at runtime ($F, Fresh$). In the first case, (S), trust is represented explicitly, meaning that the registry contains a directly retrievable trust assertion. For example, this may take the form of an explicit trust score for actor X, such as "this entity is trusted with this trust score," with a binary or numerical trust score, associated with an entity, that can be read directly from the registry without further computation. In contrast, in the second case, (F), no explicit trust assertion is stored; rather, trust is dynamically computed at runtime by the TMS during interaction from the raw information available in the registry. For example, this may involve calculating paths in a trust graph to evaluate actor X's final trust score, where "actor U in the path states that they trust actor X with a trust score," and aggregating multiple pieces of evidence, i.e., trust scores relevant to actor X under evaluation.

7.1. Charting TMS Architectures and Storage

This subsection examines how the surveyed works implement their TMs as concrete TMSs. Specifically, we analyze the architectural and storage design choices captured by the four features detailed above in Table 9: the assumed DID method, where trust-related data reside, which external dependencies protect access to such data, whether trust is stored explicitly or computed at runtime and if there are privacy protection mechanisms involved. The discussion is organized by TM class (AB, CB, and O) to facilitate comparison.

Anchor-Based Models. All anchor-based TMSs embed explicit trust anchors at their core. For instance, in **Sovrin** [91, 92] (a HL Indy deployment), "Trustees," a role built directly into HL Indy's role system, designate the actors who serve as primary trust anchors. They have the authority to approve policies, ratify governance decisions, run validator nodes, and ultimately define the Sovrin GF. "Trustees" can appoint "Stewards," who abide by the Sovrin governance framework and are capable of running validator nodes. In turn, "Trustees" and "Stewards" can nominate

Table 9: Architecture & storage properties of TMS in SSI.

Type	Paper	DID Method Dep.	Storage	Privacy Preservation	Computation Mode
AB	[93]	did:indy	Any	✓	S
	[94]	Any	IPFS + Ethereum	✓	S
	[95, 96]	Any	HL Fabric	×	F
	[97, 98]	Any	DNSSEC	×	S
	[99]	Any	DNSSEC	✓	S
	[91, 92]	did:sov	Sovrin	×	S
	[68]	did:ion	IPFS + Bitcoin	×	S
	[100]	Any	PostgreSQL	×	S
	[101]	Any	local VDR	×	S
	[102]	did:indy	HL Indy + HL Fabric	✓	F
CB	[103]	Any	Besu + Ethereum	✓	F
	[104]	did:ethr	Ethereum	×	F
	[105]	did:iota	IOTA Tangle	×	S
	[106]	Any	Trust Graph	×	F
	[107]	Any	FISCO BCOS	✓	S
	[108]	Any	Ethereum	✓	S
	[109]	Any	Any DLT	✓	F
	[110]	Any	Any DLT	×	F
O	[111]	did:indy	HL Indy	×	F
	[112]	Any	Inter consortium DLTs	×	S
	[113] (Merkle)	Any	Any DLT	×	F
	[113] (BBS)	Any	Any DLT	×	F
	[114]	Any	Ethereum + IPFS	✓	F
	[115]	Any	VDR with Smart Contracts	×	F

Legend: ✓= Present, × = Not Present, F = on the Fly (runtime), S = Stored persistently

"Endorsers," who act as issuers of VCs. Accordingly, both "Trustees" and "Stewards" place direct trust in "Endorsers." Given the need to make such endorsement information explicitly available, trust data are stored on Sovrin and can likewise be stored in any other HL Indy deployment. To appoint an "Endorser," a "Trustee" executes an HL Indy NYM transaction that assigns the "Endorser" role to the corresponding DID. These NYM transactions are publicly visible on the permissioned network and are not protected by any access-control mechanism. The stored NYM records are sufficient to assess the trust status of an identity. Notably, in Sovrin and, more generally, in any HL Indy deployment, the DID methods did:sov and did:indy are not merely supportive components but central elements of the TM. Indeed, the DID document itself is derived from NYM transactions, which record the actor's role

directly on the ledger.

Lauinger et al. [93] enrich the HL Indy-based TMS by defining two new trust-anchor roles: the RA and the CIA. The RA actors have the authority to publish a CS on HL Indy. Those RAs can then appoint CIAs actors, which can publish a CD derived from that CS on HL Indy; thus, CIAs can issue VCs based on the RA schema. Those endorsements are stored on-chain through transactions and can be checked statically without the need for trust score aggregations. A CS is created through a SCHEMA transaction containing a key-value map and is identified by its transaction sequence number and transaction ID, which includes the issuer DID, protocol version, schema name, and schema version. The schema structure is immutable, so any change requires creating a new version, and multiple issuers can reuse the same schema to issue credentials with identical attribute sets. The RAs are predefined as actors allowed to publish transactions on the permissioned blockchain and act as accumulator managers. To establish authorization, the RA associates an RSA-based cryptographic accumulator with each published CS. Then, those RAs can authorize CIAs by adding them to the accumulator, granting them the ability to publish a CD referencing that CS. A CD is derived from a specific CS and represents a public declaration by an issuer that it will issue credentials under that schema. It contains the cryptographic material needed for verification, including a public key that allows verifiers to check the issuer's credentials. The issuer keeps the corresponding private key in their wallet for signing. At the same time, the public part is published to the ledger through a CRED_DEF transaction. The RA keeps a private tails file that maintains a mapping between authorized CIAs and their accumulator elements. In contrast, the current accumulator value is stored on-chain in the verifiable registry. CIAs can also write to the permissioned blockchain: to join, a CIA generates a unique prime element, which the RA adds to the accumulator and for which it returns a witness to the CIA. Consequently, this TMS includes privacy-preserving mechanisms through which CIA actors can prove membership in the group of actors authorized by the RA without disclosing their identity. This is achieved by having the RA insert the unique prime element representing the CIA actor into the RSA-accumulator and provide a corresponding witness, which the CIA actor can later use to prove membership.

Buccafurri et al. [**94**] define a Consensus Provider as a trusted anchor entity that manages encrypted VCs and updates access policies through Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE). This ensures a notarized track record of policy changes on the Ethereum blockchain. The storage of trust information for access to VC content is split: the entire encrypted VC files are stored on InterPlanetary File System (IPFS), while the access policies and the re-encryption

symmetric keys needed to open them (as VCs can be encrypted multiple times when access policies change) are immutably logged and mediated via Ethereum. Thus, trust information is stored both on IPFS and Ethereum without any access protection on that information and without any additional computation required to assess trust. In practice, the holder encrypts each VC with a symmetric key, and this key is then re-encrypted under attribute-based policies by the Consensus Provider. Only verifiers satisfying the policy can obtain the corresponding re-encrypted key and decrypt the VC. Confidentiality is maintained by expressing trust in the verifier since there are no public records of trust towards verifiers, since trust towards a verifier is expressed in giving them keys to decrypt holder attributes under access control policies. The availability of retrieving a VC, which, as said, is stored with encrypted attributes as prescribed by the model, depends on IPFS, which does not guarantee 100% availability.

Mukta et al. propose a blockchain-agnostic governance framework, the **SC model** [**95**], later extended into the **VCTP protocol** [**96**]. In this model, VCs are issued by a recognized governance authority that establishes a GF. The SC is itself a special VC that authorizes an entity to issue other VCs in a specific context. On HL Fabric, the permission to publish the associated CS and CD is recorded on-chain, anchoring the attributes of the SC and the definitions required for issuance. Trust, however, is ultimately evaluated at verification time, when the verifier validates the SC. In this setup, the governance authorities are explicitly recorded on a permissioned HL Fabric blockchain deployment, granting them the authority to create the corresponding CS and CD needed for credential issuance.

The TRAIN framework [**97, 98**] leverages DNSSEC trust schemes to publish Trust Lists via POINTER (PTR) records by DNS operators acting as anchors, later extended by **Chadwick et al.** [**99**] to enforce verifier trust via OpenID4VP [126] and DNS PTR cross-certification [127]. The OpenID4VP protocol extends OAuth2 by allowing a verifier to request a dedicated so-called "*vp token*" that carries holder VPs. The wallet then checks the verifier's trust metadata anchored in DNS through TRAIN before releasing the requested credentials, ensuring that only recognized verifiers can obtain selectively disclosed information. In this way, OpenID4VP operationalizes the trust anchors provided by TRAIN and makes verifier trust explicit at runtime for specific attributes accessible to verifiers. All trust data are stored persistently in the DNS, and availability depends on DNS operators hosting a trust list.

TrustChain [**68**] mirrors real-world hierarchies through a chain of DIDs anchored in a timestamped Root DID. The DID method used is the ION method, which combines Bitcoin and IPFS as the VDR. The Root DID, published to IPFS, is anchored via its Content Identifier (CID) in a Bitcoin transaction, providing inde-

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

pendently verifiable timestamping. DID documents are persistently stored in IPFS and referenced through on-chain CIDs. Endorsements between entities are encoded within the DID documents themselves, where upstream entities sign and attest to the validity of downstream identifiers. Availability thus depends on the non-guaranteed nature of IPFS for documents, whereas Bitcoin poses no availability concerns.

Grüner et al. [100] present an ATIB that acts as an intermediary trust broker, evaluating attributes by assigning per-attribute confidence scores through probabilistic aggregation of claims from multiple Attribute Providers. A claim type (e.g., email, name) is accepted if its aggregated trust score exceeds a configurable threshold in the ATIB trust engine. Trust data, including AP trust scores and thresholds, are stored in a PostgreSQL database managed by the ATIB broker. Consequently, the availability of trust data depends on the broker's operation, and the data can only be accessed through the ATIB itself.

Finally, **Ling and Butakov** [101] describe an ecosystem in which a *local license verifier* anchors healthcare interactions in the metaverse. In this model, the *verifier* confirms the accreditation of *healthcare providers*, enabling online-verified *doctors* to act as credential *issuers*, while *patients* remain the ultimate holders and gatekeepers of their VCs. In fact, VCs are logged persistently in a local VDR. However, the authors do not specify a particular solution; instead, they discuss a blockchain-based one (e.g., HL Aries) to ensure immutability. Trust derives from the local license verifier's license checks stored on the VDR. As such, the availability of trust information relies on both the local VDR network and its supporting storage infrastructure. Crucially, access is gated by patient consent, which in this setting reflects trust in the healthcare provider. There is therefore a kind of double lock: the verifier must confirm that the healthcare provider is properly licensed, and the patient must actively grant consent through one-time keys. Only when both locks are opened can data be retrieved. These patient-issued keys define exactly which dataset is shared, with which provider, and for how long. The VDR enforces these rules, recording every attempt and releasing information only when both conditions are satisfied.

Pujari et al. [102] implement this framework with separate SSI identity and healthcare-data ledgers. Identity credentials, schemas, and revocation data are managed on HL Indy, while medical-data access transactions are recorded on HL Fabric. They state that VCs are signed with ED25519 and they propose to keep them on an Aries-Askar wallet [128] or through Aries Cloud Agent [76]. At runtime, the TMS computes an entity trust score from VCs by aggregating context-level scores over credential claims, accreditation weights, and VC significance. Smart contracts then use roles, attributes, owner consent, and context-aware policies to control access to medical data, while selective disclosure and predicate ZK proofs protect exposed

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

attributes.

Community-Based Models. Community-based models avoid fixed anchors, relying instead on decentralized WoTs.

Eer et al. [103] store trust information on a private HL Besu network, on top of which a smart contract is used to construct a WoT trust graph. Issuers need to stake tokens to join and access the private HL Besu network. The graph state is anchored to a Merkle root hash of state updates on Ethereum, giving an additional guarantee. Moreover, there is privacy protection for the general public i.e. external actors to the TMS. As trust score information is shared only among issuers within the Besu network. There is, in fact, an access protection mechanism in the form of barring access to the private network. As a matter of fact, Verifiers, in order to access the Besu private network for trust assessment, must stake a set amount of coins. The availability of trust information depends on the HL Besu deployment, while Ethereum guarantees the availability for the retrieval of the Merkle root hash stored over it.

Luecking et al. [105] build a quantifiable IoT WoT on the IOTA Tangle using Masked Authenticated Messaging (MAM) streams, where claims, attestations, and each identity's list of trusted peers, together with the corresponding trust scores, are published as transactions within the respective identity's MAM stream on the Tangle and are used to compute trust. The availability of trust information depends on the IOTA network used.

De Salve et al. [104] derive trust from friendship relations declared on a WoT trust graph deployed on Ethereum, where trust relationships are explicitly modeled as weighted and directed edges among issuers and verifiers. Each edge is represented as a tuple (u, w, v, c), consisting of the source identity DID u, the target identity DID v, a weight $w \in [0, 1]$, and a bitstring c encoding the trust context. Users update trust edges through smart contract calls, which persist trust relations on-chain within a multi-layer graph architecture (issuers, contexts, and entry-point layers). Smart contracts are used solely to verify the existence of graph elements and paths. During verification, the trust graph is reconstructed at runtime by traversing on-chain data via smart contract queries. Trust evaluation is therefore performed on the fly by computing trust paths over the multi-layer graph, filtering edges by exact context matching, and aggregating edge weights along each path. Privacy is not preserved, as trust scores for peer relationships are explicitly stored in the Smart Contract over the Ethereum block. Furthermore, the trust score is bound to user identities and is publicly accessible to anyone, as it is on the public blockchain. While this entails a loss of privacy, it ensures strong availability of information related to trust. **Yin et al. [107]** also propose a federated SMPC protocol [129, 130] on the FISCO BCOS

Blockchain [131] over which privacy-preserving trust feedback is derived from actors' shares and aggregated. FISCO BCOS is an open-source, enterprise-grade permissioned consortium blockchain that supports authenticated participation and secure data sharing. The authors promote it as providing stronger data privacy by enabling selective access restricted to authorized participants. FISCO BCOS achieves high throughput through Block Level Pipelining for inter-block parallelism and Deterministic Multi-Contract for intra-block smart contract concurrency. It has been deployed in hundreds of industrial applications. In this setting, trust data becomes available once all shares have been collected by selected actors, with commitments stored persistently on-chain and their availability ensured by the FISCO BCOS consortium infrastructure.

Chung et al. [108] issue ERC20 Ethereum review tokens via blind signatures to authenticate holder feedback and establish the reputation of verifiers (service providers), with the underlying Ethereum network guaranteeing the availability of these tokens and thus embedding the associated trust records.

Borges et al. [109] store DIDs and per-application reputation scores in a verifiable data registry (instantiable as a blockchain or a DAG) accessible across the network's radio-access nodes, and compute trust on the fly through a multi-party proof of reputation; ZK proofs and selective disclosure preserve the privacy of both identities and individual feedback.

Papaioannou and Ritas [110] realize their trust assessment through a credential-chain inference using a blockchain smart-contract as trust broker. This smart contract derives trust at runtime from the VCs held across a population of entities, without relying on a fixed trust anchor.

Other models. Other TMSs adopt hybrid strategies, where certain entities are appointed as predefined trust anchors, but trust is further extended through trust chaining or cross-consortium federation.

Bhattacharya et al. [111] extend the WoT-based model of Grüner et al. by introducing reputation scores for issuers in HL Indy. Issuers are formally onboarded by the GF as trust anchors, receiving an initial reputation value at entry. This reputation is then continuously adjusted through an EWMA of credential-issuance activity recorded on-chain. At runtime, the final confidence score results from combining the persistent attestation-derived trust score from the WoT with the dynamically evolving reputation of the anchor. The outcome is a hybrid model, where trust scores flow through attestations. Still, entities are also appointed as anchors whose trust is not static, instead shaped by issuance-dependent reputation scoring.

Frutos et al. [112], in the context of the European Union ERATOSTHENES project [132], deploy a multi-domain Trust Manager, called TMB, writing to interop-

erable permissioned Distributed Ledger Technology (DLT)s managed by other TMBs and communicating trust scores to IoT devices. Trust scores are computed off-chain and summarized via Merkle roots, which are anchored on a shared public ledger. Availability depends on both the permissioned DLTs and the public blockchain.

Pino et al. [**113**] propose two lightweight mutual authentication methods for IoT. **The first, Merkle,** uses a Merkle-root anchor: each node builds a Merkle tree of its DIDs, and a TP publishes the root hashes on a DLT. Authentication occurs via Merkle proofs. In this case, only root hashes are stored on-chain; full lists remain off-chain, with availability tied to the TP, and proof verification is computed dynamically. **The second, BBS,** employs BBS group signatures: the TP assigns key shares to nodes and maintains a Revocation List (RL) on-chain. Nodes authenticate by signing with their group private key, proving both DID ownership and group membership, with revocation requiring group key updates. Group public keys and RL entries are stored persistently on-chain. Trust evaluation at runtime requires revocation lookups.

Song et al. [**114**] propose a system where trust is expressed as trust scores that are issued as NFTs to actors. The goal of each actor is to collect them as rewards, incentivizing them to strive for higher scores. These NFTs are minted via Ethereum smart contracts. Each NFT includes a pointer (called tokenURI) to the corresponding metadata stored off-chain on IPFS. The off-chain metadata contains the trust score itself. This TMS allows third parties to verify the issued score and its evaluation basis without relying on a centralized trust source or storage. The metadata, including the evaluated trust score, is stored off-chain on IPFS, while the scores are published via Ethereum smart contracts. The availability of trust scores depends on the IPFS nodes hosting the NFTs metadata.

Bistarelli et al. [**115**] propose the use of smart contracts on any supporting blockchain, governed by access control policies that verifiers must satisfy. In their TMS, the VC leverages the TermsOfUse field of the VC Data Model to embed a link to the corresponding smart contract. The actual availability and enforcement of these terms thus depend on the underlying blockchain infrastructure.

8. Mapping Trust Approaches to Application Scenarios

In Table 10, we map a number of relevant application scenarios to trust approaches from the surveyed literature. The table now prioritizes scenarios that are directly stated or exemplified by the papers themselves. This mapping also reflects our own assessment: not all the listed works explicitly target the corresponding scenario, but we include them when their design characteristics make them particularly

Table 10: Mapping of trust approaches to specific SSI application scenarios.

Scenario	**Suitable Approaches**
Online Social Network (OSN)	[104] [111, 103]
Sensitive Holder Data (e.g., Healthcare / Digital Health)	[94][115][102][101]
First-time Peer-to-Peer Service Interactions / Sharing Platforms (e.g., Car Sharing)	[108]
Constrained IoT Devices	[113, 112, 105]
Automotive / Software Update Ecosystems / Internet of Vehicles	[93] [109]
Delegation / Local Trust Zones / Dynamic Role Switching (e.g., Hospitals, Doctors, Patients)	[96, 95]
Anonymous Peers	[107]
Institutions	[115, 94, 91, 92, 93, 95, 100]
Cross-domain Trust	[98, 97, 99, 112] [110]
Open Systems / Microservices	[110]
Crowdsourced Systems	[103]

suitable for it. More precisely, the table associates each scenario with representative approaches that either explicitly address it or exhibit properties that, in our view, make them especially well suited to it. The table is intended to be illustrative rather than exhaustive: it pins each scenario to the approaches that most sharply exemplify it, and, as discussed at the end of this section, a few surveyed approaches are deliberately left unpinned because their trust models are scenario-agnostic building blocks rather than designs targeted at a single setting.

The selected scenarios were drawn from at least one surveyed work. They were then related to other approaches whose characteristics, architecture, or trust assumptions make them applicable to the same setting. The reasoning behind these choices is discussed below, clarifying which scenarios are explicitly motivated by the literature and which ones instead reflect our own broader interpretation. Crucially, the criterion used for each scenario is not introduced ad hoc here but is expressed in terms of the analytical lens built earlier in the survey: the trust-origin classes AB, CB, and O of Section 5.1, the trust properties charted in our properties table (Trust Formation, i.e., rule-, reputation-, or experience-based; Propagation; Granularity; Distrust; Context Awareness; Subjectivity), the trust-relation directions ($H \to V$, $H \to I$, $V \to I$, $V \to H$, $I \to V$, $I \to I$), and the Architecture & Storage features

(notably Privacy Preservation / Access Protection). Each criterion below therefore carries, in parentheses, the class and feature profile it selects for.

The following list consolidates, for each scenario together with the requirement references to justify the mapping:

- **Online Social Network (OSN).** *Scenario requirement:* OSNs require trust mechanisms able to infer reliability from social relations, repeated interactions, community feedback, and reputation signals, especially when direct experience between two users is missing [133, 134]. *Mapping criterion:* an approach is mapped to this scenario when it treats trust as a social and contextual relation that can be inferred from interaction graphs, propagated attestations, or community reputation, rather than trust coming from institutional authorities. In our taxonomy: Community-Based models whose properties-table profile combines reputation- or experience-based Trust Formation, numerical Granularity, Propagation, Subjectivity, and Context Awareness, typically exercising $V \rightarrow I$ but also including P2P $I \rightarrow I$ relations.

- **Sensitive holder data (e.g., healthcare / digital health).** *Scenario requirement:* healthcare and digital-health systems require privacy protection mechanisms that determine who can access patient data and how to minimize its dissemination. Plus, they require support for trustworthy interoperability between different service providers while accounting for diverse privacy requirements of healthcare stakeholders [135]. *Mapping criterion:* an approach is mapped to this scenario when trust is used to regulate the disclosure or use of sensitive holder data, either by helping the holder assess verifier entitlement or by helping the verifier assess whether the issuer can be trusted. In our taxonomy: Anchor-Based or Other models with Context Awareness and platform-level Access Protection, exercising holder-to-verifier ($H \rightarrow V$) and issuer/verifier-to-issuer ($I \rightarrow V$, $V \rightarrow I$) relations.

- **First-time peer-to-peer service interactions / sharing platforms.** *Scenario requirement:* sharing platforms and peer-to-peer services require mechanisms to estimate the trustworthiness of a provider before the first interaction, when the requester has no direct experience and must rely on reputation or feedback from others [136]. *Mapping criterion:* an approach is mapped to this scenario when it supports a holder's decision to interact with, or disclose credentials to, a previously unknown service provider by replacing direct experience with reputation or feedback evidence. In our taxonomy: Community-Based models with reputation-based Trust Formation and a holder-to-verifier

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

$(H \to V)$ relation that substitutes community feedback for absent direct experience.

- **Constrained IoT devices.** *Scenario requirement:* IoT and Social-IoT environments require lightweight trust establishment, mutual authentication, dynamic trust updates, cross-domain device management, and resilience against malicious or compromised devices [124, 137]. *Mapping criterion:* an approach is mapped to this scenario when it enables constrained or heterogeneous devices to establish and update trust with limited computational, storage, or interaction assumptions. In our taxonomy: lightweight Anchor-Based/Other binary schemes, or Community-Based models whose Propagation runs over a constrained verifiable data registry.

- **Automotive / software-update ecosystems / Internet of Vehicles.** *Scenario requirement:* automotive and Internet-of-Vehicles environments require strong authorization of software-update sources, verification of credential chains, and reputation mechanisms for vehicles or infrastructure actors whose behavior affects safety-critical decisions [138]. *Mapping criterion:* an approach is mapped to this scenario when the trust decision protects a safety-sensitive interaction, such as accepting a software update, relying on an infrastructure actor, or evaluating another vehicle. In our taxonomy: Anchor-Based rule-based authorization for update sources. Also considering Community-Based reputation, with Distrust, among vehicles $(V \to H)$.

- **Delegation / local trust zones / dynamic role switching.** *Scenario requirement:* local trust zones require mechanisms for proving authority in a specific context, delegating that authority to another actor, and limiting the validity of that delegation according to role, place, time, or purpose [139]. *Mapping criterion:* an approach is mapped to this scenario when it allows authority to be transferred, constrained, or validated within a bounded context, rather than treating issuer authority as static and globally valid. In our taxonomy: Anchor-Based, rule-based models with Context Awareness, where per-topic supporting credentials carry delegable, role-scoped authority.

- **Anonymous peers.** *Scenario requirement:* anonymous peer environments require trust or reputation to be computed without revealing the identity of the actors who provide feedback, because exposing feedback sources may undermine privacy or discourage honest negative evaluations [140, 141]. *Mapping criterion:* an approach is mapped to this scenario when peer feedback can influence trust or reputation while the identity or individual contribution of feed-

back providers remains protected. In our taxonomy: Community-Based models in which the Privacy Preservation / Access Protection feature anonymizes or aggregates individual feedback.

- **Institutions.** *Scenario requirement:* institutional digital services require trust in the public or organizational bodies that provide them, together with confidence in the technical, procedural, and risk-management conditions under which those services operate [142]. In SSI settings, this translates to having those procedures and bodies be well defined in GFs. *Mapping criterion:* an approach is mapped to this scenario when trust is derived from a governance framework, which defines institutional governance with defined roles such as issuer authorization to issue a credential over a topic. In our taxonomy: Anchor-Based models with rule-based Trust Formation derived from a governance framework.

- **Cross-domain trust.** *Scenario requirement:* cross-domain SSI requires mechanisms to decide whether credentials, issuers, trust lists, or governance schemes from another administrative domain should be accepted in the local domain [143]. *Mapping criterion:* an approach is mapped to this scenario when it enables trust decisions to cross administrative, organizational, or ecosystem boundaries by making external trust information discoverable, verifiable, or translatable in the local domain. In our taxonomy: Anchor-Based or Other models that translate trust across boundaries, exercising $V \rightarrow I$ and $H \rightarrow V$ relations.

- **Open systems / microservices.** *Scenario requirement:* open systems and autonomous microservice ecosystems require trust decisions over entities whose relevant properties cannot always be verified directly and where trust cannot be certain as it is through seen through cryptographic validity alone [136]. *Mapping criterion:* an approach is mapped to this scenario when it supports context-specific trust inference of entities' properties beyond their single VCs. In our taxonomy: CB, experience-based inference with Propagation over verifiable credentials, exercising a $V \rightarrow H$ relation that reaches properties beyond a single VC.

- **Crowdsourced systems.** *Scenario requirement:* crowdsourced systems require trust mechanisms that aggregate the behavior and feedback of a distributed crowd to then discourage malicious, low-quality, or collusive contributions [144]. *Mapping criterion:* an approach is mapped to this scenario when trust is assessed and evaluated through collective participation rather than

assigned by a single authority. In our taxonomy: Community-Based models with reputation-based Trust Formation and Distrust realized through staking, challenges, and penalties.

Read together, these criteria align the scenarios with the trust-origin classes and properties established earlier in the survey, so that Section 8 reuses rather than restates our analytical lens. Peer-driven scenarios (Online Social Network (OSN), first-time P2P, anonymous peers, crowdsourced) select CB models with reputation- or experience-based Trust Formation, numerical Granularity, and Context Awareness, plus Propagation and Subjectivity where social trust is multi-hop and Distrust where negative feedback matters. Authority-structured scenarios (institutions, delegation / role switching, and the authorization side of automotive updates) select AB, rule-based models. Scenarios that need both an authoritative backbone and emergent or cross-boundary trust (sensitive holder data, constrained IoT, cross-domain, open systems / microservices) select O or hybrid models that retain an anchor while adding propagation, reputation, or runtime inference. Orthogonally to the class, the trust-relation directions and the Privacy Preservation feature decide fit within a class: holder-to-verifier and issuer-to-verifier relations together with Access Protection are what make an approach suitable for sensitive-data and anonymous-peer settings, whereas verifier-to-issuer and issuer-to-issuer endorsement underpin the reputation-driven ones.

De Salve [104] explicitly targets OSN environments. [111] and [103] were previously included because their community-based characteristics fit social settings well: both rely on peer interactions, endorsements, or community-derived trust signals, which naturally align with environments in which trust emerges from repeated user interactions and social relations.

In scenarios where sensitive holder data must be shared with verifiers, approaches centered on controlled disclosure and regulated access are especially relevant. In particular, [94] explicitly motivates this problem through a healthcare example involving medical information. [115] was previously included because it focuses on issuer-driven restrictions on verifier access, a characteristic appropriate for healthcare-like contexts in which sensitive attributes should only be disclosed under tightly controlled conditions. Pujari et al. [102] explicitly target the digital-health ecosystem and healthcare stakeholders, including patients, doctors, hospitals, research institutes, and insurers. Ling and Butakov [101] likewise explicitly address healthcare, proposing a trust framework for self-sovereign identity in metaverse healthcare applications.

A further scenario explicitly discussed in the literature is that of first-time peer-to-peer service interactions and sharing platforms. In particular, [108] highlights situations in which the user and the service provider interact for the first time,

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

explicitly mentioning peer-to-peer services such as Uber, Airbnb, and eBay, and also presenting a car-sharing example. This makes it a natural fit for settings in which trust toward the verifier or service provider is especially relevant before disclosure.

The works [113, 112, 105] are suitable for ecosystems involving IoT devices. All three explicitly address IoT: [113] targets mutual authentication in IoT networks, [112] targets IoT device-lifecycle management, and [105] proposes a trust-management framework for the IoT instantiated over the IOTA Tangle.

The automotive domain is also explicitly present in the surveyed literature. In particular, [93] motivates its approach through a software-update scenario in which a vehicle manufacturer authorizes software providers to issue credentials used in automotive update validation. Borges et al. [109] explicitly target Internet-of-Vehicles scenarios in which vehicles assess trust between each other via sender reputation for their C-V2X/ADAS communications. This makes these approaches relevant to automotive, software-update, and IoV ecosystems in which authorization or reputation chains must be tightly controlled.

The works [96, 95] are suitable for local trust zones and dynamic role switching. In particular, these works motivate their proposals through delegation-oriented and healthcare-related examples, making them especially relevant to settings in which authority or role must be demonstrated in context. More generally, both approaches allow trust to be expressed and verified through VCs, which makes them well-suited to settings in which the same entity may need to prove different roles in different contexts, such as doctor, patient, employee, or service provider. This is explicit in [96], which presents a hospital emergency scenario in which a patient issues a letter of authority so that another person may act on their behalf, thereby framing trust propagation for personal issuers in a healthcare business process.

The case in which peer anonymity must be preserved is explicitly addressed by [107], which is specifically designed to support trust establishment while protecting the privacy of participants' individual feedback.

Institutional settings with hierarchical structures were previously associated with works such as [115, 94, 91, 92, 93, 95, 100]. These approaches were considered suitable because they rely on governance frameworks, predefined trusted roles, organizational trust anchors, or brokered trust decisions, all of which fit contexts in which trust is structured by institutional authority rather than emerging purely from peer interaction. Within this row, we synthesized the trust approaches that, to our judgment, allow us to model and manage closed hierarchical institutions.

The approaches [98, 97, 112] are suitable for cross-domain trust. The TRAIN line [97, 98], together with its verifier-side extension [99], explicitly addresses cross-domain trust through DNS-published trust schemes designed to be recognized across

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

organizational boundaries, while [112] explicitly manages trust both within and across domains.

Papaioannou and Ritas [110] explicitly motivate open-system microservices: their algorithms infer trustworthiness for properties such as availability, latency, accuracy, and security vulnerability from credentials observed in a microservice population.

Finally, [103] was previously associated with a crowdsourced setting, since its design relies on token-based staking, challenges, punishments, and incentives, all of which are especially relevant in environments where trust must emerge from the contributions and monitoring of a distributed crowd. As with the institution scenario, this association should be understood as part of our analytical mapping rather than as an application scenario explicitly identified as such in the paper.

It may also be possible to combine approaches. For instance, IoT device agents may interact within WoT architectures that, given limited storage capabilities, may require claim and attestation storage on a VDR such as IOTA. In such a case, the WoT may support communication among devices within the same domain while still operating alongside that domain's governance framework.

We also note that an agent within an OSN may rely on a WoT architecture with a public reputation score, while an anonymous peer network may instead adopt Secure Multi-Party Computation (SMPC) to aggregate trust information without revealing individual inputs. Furthermore, the same actor may interact with anchor-based architectures in institutional settings and with other trust approaches in different scenarios while still using the same DID.

9. Related Work

Table 11 compares major SSI surveys and systematization efforts that either fall outside the scope of this work or partially overlap with it. The rationale behind each classification is discussed below, with trust-specific surveys analyzed in more detail in Subsection 9.1. Notably, very few studies have addressed TMs in SSI in depth. None of them considers the full range of features we define for TMs in Section 6 and for TMSs in Section 7, nor does any prior survey cover as many academic papers on trust approaches as this one.

The following discussion presents general SSI surveys in chronological order.

The first wave of surveys from 2018 to 2020 provided a systematic overview of the foundational aspects of SSI, focusing mainly on architecture and basic ecosystem considerations. From 2018, Mühle et al. [145] provided early foundational insights into SSI architecture but offered limited detail on TMs architectures, storage, and trust directions. In 2020, Fedrecheski et al. [5] discussed the integration of SSI and

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 11: Comparison of key SSI review works.

Year	Reference	Type	SSI Foundations	Trust Dir. and Prop	TMS Properties	TMS Arch. & Storage	Num. Trust Approaches
2018	Mühle et al. [145]	LR	●	○	○	○	0
2020	Fedrecheski et al. [5]	LR	●	○	○	○	0
2020	Kaneriya et al. [146]	LR	●	◔	○	◔	0
2021	Nokhbeh Zaeem et al. [147]	CF	●	◔	◔	◔	0
2021	Čučko et al. [148]	SMS	●	○	◔	◔	1
2021	Soltani et al. [149]	LR	●	○	○	◔	0
2022	Bai et al. [150]	IMP	●	○	○	○	0
2022	Čučko et al. [151]	LR	●	○	◔	○	0
2022	Lim et al. [152]	LR	●	●	●	●	1
2024	Krul et al. [87]	SoK	●	◓	◓	◓	5
2024	Tan et al. [153]	LR	●	○	○	◔	0
2024	Satybaldy et al. [154]	LR	●	○	○	◔	0
2025	Mazzocca et al. [53]	LR	●	○	◔	◔	0
2025	da Silva Costa et al. [58]	LR	●	◔	◔	◔	2
2025	Biele et al. [155]	CF	◓	◓	◔	◓	1
2025	Manimaran et al. [156]	IMP	●	◔	◔	◓	1
2025	Lee et al. [66]	LR	●	○	○	○	0
2026	Fathalla et al. [157]	LR	●	○	○	○	0
2026	Ours	LR	●	●	●	●	24

Legend: ○ = Not covered; ◔ = Mentioned; ◓ = Partially analyzed; ● = Systematically covered.
Type classifications: LR = Literature Review; SoK = Systematization of Knowledge; SMS = Systematic Mapping Study; CF = Conceptual Framework; IMP = Implementation comparison.

IoT, but did not assess trust management, while Kaneriya et al. [146] presented a comparative analysis of SSI systems focusing on flow and architectural models, but did not evaluate TMs or trust-scoring mechanisms.

In the second wave, spanning 2021 to 2023, surveys expanded their scope to include governance, mapping studies, and implementation aspects. The 2021 contributions include [147], [148], and [149]. Nokhbeh Zaeem et al. [147] described SSI architecture and governance ecosystems broadly but lacked a focused discussion on trust or security mechanisms. Čučko et al. [148] conducted a systematic mapping study but only mentioned trust at a conceptual level without modeling or computational detail. Soltani et al. [149] surveyed the broader SSI ecosystem and described

architecture at a high level, but did not analyze trust computation or representation. In 2022, Bai et al. [150] examined the architecture and implementation of DID and VC of different methods and types, respectively, omitting discussion of trust or trust-related flows. Also in 2022, Čučko et al. [151] evaluated usability, security, and foundational traits of SSI systems through expert validation, but did not analyze TM computation or flow propagation. The 2022 paper by Lim et al. [152] and the work by Krul et al. [87] focus specifically on trust in SSI. We therefore dedicate Subsection 9.1 to them.

The most recent wave of surveys, from 2024 to 2025, shows a shift toward governance, security, and cross-ecosystem perspectives. The surveys in 2024 begin with Tan et al. [153], which provides a governance-centric overview of SSI challenges without explicitly modeling or scoring trust. Satybaldy et al. [154] offered a taxonomy of architectural and governance issues but omitted TM and trust-computation aspects. Lastly, in 2025, Mazzocca et al. [53] reviewed DID/VC protocols and briefly mentioned Vehicle-to-Everything (V2X) trust transfer, but did not analyze trust scoring systems or computation models.

Da Silva Costa et al. [58] performed a comprehensive systematic literature review of blockchain-based SSI, organizing the results thematically and by sector, but mentioned TMs and trust mechanisms only at a high level. Biele et al. [155] emphasized governance metadata and registries but omitted the modeling, propagation, and computation of trust through web-of-trust or reputation-based systems. Manimaran et al. [156] compare, across multiple aspects, the Identity Management Systems (IMSs) of Federated Digital Identity, represented by eIDAS, with SSI, represented by HL Indy and IOTA Identity. They highlight that, in eIDAS, the reference model is federated, with well-defined, trusted issuers, whereas in SSI each verifier must adapt its own trust policy and decide whom to trust. Lee et al. [66] focus on revocation techniques and touch on governance-aware revocation methods in SSI. Finally, the most recent work by Fathalla et al. [157] reviews fundamental SSI concepts and discusses usability in application scenarios, scalability challenges, and quantum-computing threats with corresponding mitigation strategies, while also addressing governance aspects; however, it does not survey or compare TMs/TMSs from either the research literature or industry.

9.1. Trust-Centric Perspectives in Prior SSI Surveys

This section examines previous survey and review works that address trust in SSI, positioning them with respect to the features covered and the approaches studied. Lim et al. [152] introduced the first structured taxonomy of TMs regarding blockchain-based SSI, classifying models based on control (centralized, decen-

tralized, distributed), trust relations (e.g., issuer-to-verifier), and trust basis (rule-, reputation-, or experience-based). The paper also highlights concepts such as quantifiable trust, the WoT, and centralized trust registries. However, the analysis is limited to two academic works: one mainly focused on SSI [106], and one more general work on blockchain-based trust [158], plus five industry deployments, including Sovrin. While foundational, their coverage is narrow and does not address many of the trust dimensions considered in our work. Krul et al. [87] focus on numerous security threats in SSI, proposing mitigation strategies across system layers. We identified a section acknowledging trust relationships, particularly between holders and verifiers, but it does not address how trust is modeled, quantified, or propagated. They present a compelling categorization of SSI trust environments as trustful (where no trust mechanisms are needed), intermediate (partial trust with risk-sensitive data), and zero-trust (where no entity is inherently trusted). Brunner et al. [159] point out that neither DID nor W3C VC standards prescribe binding to a real-world identity, a gap they address by suggesting the use of WoT-style certification or hybrid approaches that integrate CA-based trust anchors, similar to Web PKI, to provide a guarantee from a trustworthy institution. Biele et al. [155] explore trust governance, highlighting the limitations of current SSI frameworks in handling interoperability. They differentiate trust relations (e.g., verifier-to-issuer vs. holder-to-verifier) and propose that trust decisions should be supported by machine-readable, standardized metadata. Their proposed conceptual model outlines four segments—organizational trust, governance, authoritative data, and technical components—supported by the Trust VDR Query Protocol (TRQP) for cross-ecosystem queries.

Overall, while prior studies address important aspects of trust, most focus on specific systems or governance frameworks rather than generalizing across architectures and representations. In contrast, our work consolidates the academic literature into a comprehensive framework, offering the first taxonomy of SSI TMs together with a multi-dimensional classification framework for TMs and TMSs.

10. Future Directions: Open Challenges in SSI Trust

This section presents Tables 12–15, which summarize the main limitations and challenges we identified when applying existing TMs and TMSs to real-world scenarios. A tabular format was adopted to convey this information in a more immediate and systematic manner.

Tables 12 and 13 highlight architectural, storage, governance, and privacy shortcomings that remain to be addressed in current SSI systems with particular emphasis on the limited role of DIDs in trust computation, the challenges of storing reputa-

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 12: Future directions in SSI trust: architectural and storage challenges.

Topic	Limitation	Resolution / Research Direction
DID in trust frameworks	DIDs are insufficiently integrated into trust frameworks: the DID document is rarely used as a trust anchor and lacks standardized metadata for trust computation, even though identity is shaped by social and trust relations [149, 160, 68].	Trust-Equipped and Composite DID resolvers, where multiple DIDs (possibly across VDRs) are assessed collectively, and trust-related metadata is made tamper-evident through blockchain-backed resolution.
On-chain reputation vs GDPR; off-chain VC persistence	Storing reputation or trust scores on-chain (e.g., in WoT) conflicts with GDPR due to immutability, the right to be forgotten, and data minimization. Moving trust off-chain into VCs shifts persistence and security responsibilities to holders. Existing secret-sharing and SMPC-based storage schemes also raise problems when they ignore the trustworthiness of storage nodes, exposing collusion and availability issues [161, 162].	Distributed VC storage via secret sharing and SMPC, such as Shamir's Secret Sharing [163] and encrypted credential fragments stored via smart contracts [164], can improve availability and resilience against single points of failure.
Limits of Blockchain as VDR: oracle problem	Blockchain-based VDRs provide integrity and persistence but cannot guarantee the truthfulness of off-chain data. Trust assignments, issuer accreditation, and governance decisions rely on unverifiable external assertions, inheriting the oracle problem [68, 69, 70, 71].	Oracle-based mechanisms (e.g., optimistic oracles and voting schemes such as UMA [165, 166]) to validate off-chain claims, leading to oracle-driven trust inputs.

tion and credential data, the constraints imposed by blockchain-based VDRs, and the limitations of off-chain, document-based governance frameworks.

The lack of DID support in trust frameworks, together with the oracle problem, represents a cross-cutting challenge across SSI ecosystems. Addressing these issues would enable broader adoption of DID capabilities in a wide range of SSI use cases.

The oracle problem is an issue that afflicts all SSI TMSs using blockchains as VDR. Instead, in the OSN case, the CB TMs, leveraging WoT, would benefit from some form of off-chain VC trust sharing instead of keeping trust information available on chain. A concrete example of transitioning from **governance documents in PDF format** to **on-chain machine-readable governance** is provided by SSI systems deployed in high-stakes economic settings, such as investment-oriented DAOs,

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 13: Future directions in SSI trust: governance and privacy challenges.

Topic	Limitation	Resolution / Research Direction
From governance PDFs to on-chain DAOs	Current SSI governance frameworks are expressed as static, off-chain documents (e.g., Sovrin [92]), making policy evolution opaque, enforcement weak, and incentives for participation and accountability poorly aligned.	Model governance frameworks as on-chain Decentralized Autonomous Organizations (DAOs), embedding rules, evidence requirements, and trust translation policies in smart contracts; avoid off-chain voting [167]; integrate smart-contract trust expression [104] and incentive mechanisms [103].
Privacy in trust lists	In anchor-based TMs, publishing public lists of trusted issuers or anchors may leak sensitive trust relationships and undermine the privacy of governance structures.	Use cryptographic accumulators and vector commitments [168] to construct **trust lists** that allow verifiable proof of issuer or anchor membership without revealing the full list.

Table 14: Future directions in SSI trust: interoperability and propagation challenges.

Topic	Limitation	Resolution / Research Direction
Limitations in storing and porting trust data	Most SSI trust models operate within isolated, single-blockchain ecosystems. DID specifications lack native support for cross-chain identities and trust portability, while on-chain trust immutability hinders retractability, update, and cross-ecosystem reuse of trust evaluations [169].	Cross-chain interoperability infrastructures (e.g., Cosmos [170], HL Cacti [171]); retractable blockchain models for mutable trust data [169]; open challenge: formal trust translation and governance across heterogeneous ledgers.
Missing trust propagation relations and AI integration	Many works do not specify how to compute trust when direct trust evidence is absent. Trust propagation models rarely capture temporal, contextual, or system-level dynamics, and do not account for the increasing role of agentic AI operating autonomously on behalf of identity holders [172].	ML-based estimation of indirect trust [173]; AI agent workflows acting under SSI; context-aware and role-dependent signatures for delegated actions [174]; open issue: aligning AI decision-making with governance-defined trust semantics.

where governance decisions are made collectively [179]. VCs could be issued to delegates, auditors, or proposal authors to attest to and support their actions in the name of the DAO. Since DAO governance already provides functionalities to define and manage governance on-chain, and given that governance opacity could be an issue,

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565
DOI: https://doi.org/10.1016/j.cosrev.2026.101048

Table 15: Future directions in SSI trust: measurement and issuer-evaluation challenges.

Topic	**Limitation**	**Resolution / Research Direction**
Missing holder-to-issuer trust	None of the surveyed TMs model holder-to-issuer trust explicitly. Holders implicitly accept credentials from issuers without any TMS that allows them to evaluate trust toward issuers.	Implement mechanisms enabling holders to provide feedback on issuers and to explicitly accept or reject VCs at issuance time. For example, prior work on rejectable Soulbound token (SBT) credentials allows holders to accept or refuse credentials and associated terms at issuance time [175]. This would support holder–issuer negotiation mechanisms and embed issuer evaluation into the credential lifecycle.
Trust measurement and WoT aggregation	Heterogeneous trust representations (binary vs. continuous) complicate interoperability. WoT-based models face unresolved challenges in trust score fusion, participation incentives, and trust data storage. Distributed trust evaluation is further distorted by cognitive biases such as anchoring [176].	Trust score translation via cutoff functions; fuzzy logic-based direct trust computation and reinforcement learning-based indirect trust estimation [177, 178]; OWA-based trust fusion to balance conflicting trust paths [122].

DAOs represent a promising use case for replacing off-chain governance documents with machine-readable rules. Such rules, collectively defined through democratic decisions, could improve transparency and foster active engagement of the ecosystem [179].

Relating to **privacy in trust lists**, (in anchor-based TMs publishing trusted issuers or anchors may compromise governance privacy), we identified the use case of journalism accreditation through SSI. Today, gatekeeper organizations [180, 181] could serve as trusted issuers of press-accreditation VCs in SSI ecosystems. However, whenever a verifier checks a journalist's accreditation by consulting the trust list associated with the VC, the journalist's affiliation may be disclosed. Privacy-preserving trust lists are therefore fundamental in such SSI deployments.

Tables 14 and 15 focus on unresolved interoperability, trust propagation, issuer-evaluation, and trust measurement challenges across heterogeneous and interoperable SSI ecosystems. In particular, they highlight the lack of mechanisms for cross-domain and cross-chain trust portability and collective trust representation, the omission of trust relationships from trust calculation when direct trust is unavailable, the limited

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

consideration of holder-to-issuer trust, and open challenges in trust measurement and aggregation within WoT-based models, as well as in settings involving AI integrations. Indeed, **interoperability** among SSI ecosystems and strong **AI integration** remain insufficiently addressed especially for Agentic AI use cases. These issues become particularly important in Agentic AI scenarios, where autonomous agents are expected to evaluate trust, exchange verifiable credentials, and interact across multiple SSI ecosystems. As a survey on Agentic AI states [172], the goal of this technology is to aid humans in the automation of tasks that would otherwise require high involvement. Pfeiffer and Bugeja propose a compelling case in [174], where agents are linked to an identity holder and use different kinds of digital signatures to sign the operations they perform depending on the task being performed. Thus, TMSs must be able to recognize agents' actions and assess the corresponding trust based on the identity holder that delegated the task. Consider, for instance, agents operating in scenarios where they first rely on a CB TM deployed over a public blockchain to identify suitable workers, and then need to verify that the selected candidate complies with an external governance framework over an AB TM, i.e., a professional licensing authority. In this case, the agent must rely on trusted sources from different domains with diverse TMs within the same workflow. This makes the interoperability gap concrete, as realistic SSI deployments require agents to move across heterogeneous trust domains.

While largely overlooked by existing trust approaches, **Holder-to-issuer trust relationships** are particularly relevant, for instance in educational credential and micro-credential ecosystems. In such scenarios, students (holders) may choose to enroll in courses offered by the most trusted issuers. By obtaining credentials from reputable educational institutions, holders can strengthen the value of their certifications, as organizations often consider the reputation of the issuers when evaluating educational credentials [182].

Finally, Agentic AI introduces new trust requirements arising from agent-to-agent interactions and the monitoring of autonomous agent behavior [183]. In these scenarios, both binary and continuous trust become relevant, and trust measurement with WoT aggregation becomes fundamental. This may occur in ecosystems where agents have delegated authority, which can provide binary authorization evidence, while they may also advertise their capabilities, requiring a trust assessment related to those capabilities. In such cases, ways to assess both the delegation from one agent to another and the trust in their advertised capabilities would be compelling.

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

11. Conclusions

In this paper, we charted the landscape of research on TMs and TMSs in SSI to help researchers and practitioners identify the most suitable approaches for their systems and to map prior research while highlighting the remaining gaps. Through this analysis, we addressed the three research questions guiding this study.

We identified and collected a body of works on trust in SSI involving TMs, grouping them on the basis of shared characteristics into ABs, in which some actors act as trust anchors; CBs, which typically feature WoT relationships; and Os, which may combine both or fall outside this categorization but are included for completeness. Each work has its own intricacies and distinctive characteristics that must be considered when answering **RQ1**, **RQ2**, and **RQ3**, as presented in the introduction (Section 1).

We addressed **RQ1** by examining how trust is defined and structured across abstract TMs, emphasizing its subjective and context-dependent nature in assessing other actors' reliability. Furthermore, trust may be represented either as a binary value or as a numerical range, illustrating the variety of trust representations in SSI.

Our study highlighted that trust requires different levels of bootstrapping effort depending on the TM and the entities involved. For instance, in CBs, actors must set up and expand WoT, leveraging peer data as trust propagates to derive a trust score. We also highlighted how trust is assessed across different actors within the issuer–holder–verifier triad by analyzing trust relations in terms of directionality and possible composition. Trust assessments may be oriented toward different actors and may or may not be propagated along a chain. The surveyed literature exhibits a rich spectrum of trust relations, with verifier-to-issuer assessment being dominant (15 out of 24 approaches), alongside holder-to-verifier assessment for deciding whether to disclose VC attributes (6 approaches). More complex configurations also emerge, including combined verifier-to-issuer and holder-to-verifier patterns, particularly in other models.We have also observed that trust may be assessed in various ways: computed locally by the verifier, delegated to intermediaries, computed through SMPC, or derived from multi-hop endorsements with decaying weights.

As digital identity becomes increasingly integrated into society, it is closely tied to trust-anchor solutions, and the governments that manage them will remain prominent. However, we have seen that WoT networks can facilitate trust between peers and create even broader opportunities in online interactions. CBs demonstrate how peer endorsements, token-based traversal, and personalized trust functions enable trust to emerge without authoritative anchors, while other models combine reputation, issuer-activity metrics such as EWMA-normalized issuance, and on-chain social attestations. In answering **RQ2**, we found that TMs are concretely realized and op-

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

erationalized within diverse TMSs through heterogeneous architectural and storage choices. These include public and permissioned blockchains, as well as other registries such as DNSSEC, used as VDRs for trust data, governance-controlled trust lists, smart contracts, and hybrid on-chain/off-chain data structures. Such design decisions directly influence how trust information is anchored, updated, verified, and propagated, as well as its availability, mutability, scalability, and compliance with data-protection requirements. Thus, we conclude that the representation of trust information in SSI systems varies according to different requirements in terms of tamper-proofness, transparency, availability, and cost.

The most prominent challenge today is making SSI TMs scalable, self-sufficient, and easy to access and use. This will also require bridging different SSI ecosystems and enabling seamless translation of trust relationships from one ecosystem to another. These limitations and open challenges directly answer **RQ3** by exposing where current SSI TMs and TMSs fall short. Looking ahead, the goal is to build upon the SSI paradigm to mediate trust between people, communities, devices, and software services. What we presented here outlines the foundation of an SSIs system, with TMs serving as an initial structural layer on which more capable and interoperable trust mechanisms can be assembled.

We believe that future work will refine this layer, moving toward a digital ecosystem where identity is no longer constrained and controlled by IdPs, but is instead decentralized and privacy-preserving. In such a landscape, the web can evolve toward a Web3 paradigm. This would empower individuals, rather than relying on a few large actors, such as organizations or governments, to control digital identities and impose predetermined trust anchors.

Declaration of generative AI use

We acknowledge the use of AI-based tools, such as *Grammarly* and *ChatGPT*, to refine the writing. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Funding

This research was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union

Version of Record: https://www.sciencedirect.com/science/article/pii/S1574013726001565

DOI: https://doi.org/10.1016/j.cosrev.2026.101048

- NextGenerationEU and PON MI_1301 Secure Ubiquitous Networks and Services (SUNS).

Data availability

No data was used for the research described in the article.

References

[1] European Commission, About the initiative: EU Digital Identity Wallet, accessed: 2025-06-19 (2025).
URL https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/About+the+initiative

[2] European Commission, EU Digital Identity Wallet Home, accessed: 2026-02-23 (Jan. 2026).
URL https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU+Digital+Identity+Wallet+Home+

[3] BankID, Bankid introduction, developer documentation. Accessed: 2026-02-23 (2026).
URL https://developers.bankid.com/getting-started/introduction

[4] Singpass Developer Docs, Singpass apis documentation, accessed: 2026-02-23 (Feb. 2026).
URL https://docs.developer.singpass.gov.sg/docs

[5] G. Fedrecheski, J. M. Rabaey, L. C. P. Costa, P. C. Calcina Ccori, W. T. Pereira, M. K. Zuffo, Self-sovereign identity for iot environments: A perspective, in: 2020 Global Internet of Things Summit (GIoTS), 2020, pp. 1–6. doi:10.1109/GIOTS49054.2020.9119664.

[6] C. Allen, The path to self-sovereign identity, accessed: 2025-06-17 (2016).
URL https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/

[7] D. D. S. Braga, M. Niemann, B. Hellingrath, F. B. D. L. Neto, Survey on computational trust and reputation models, ACM Comput. Surv. 51 (5) (Nov. 2018). doi:10.1145/3236008.

[8] A. J. Mathew, Can security be decentralised? the case of the pgp web of trust, in: Socio-Technical Aspects in Security: 11th International Workshop, STAST 2021, Virtual Event, October 8, 2021, Revised Selected Papers, Springer-Verlag, Berlin, Heidelberg, 2021, p. 67–85. doi:10.1007/978-3-031-10183-0_4.

[9] R. Hardin, Trust and Trustworthiness, The Russell Sage Foundation series on trust, Russell Sage Foundation, 2002.
URL http://www.jstor.org/stable/10.7758/9781610442718

[10] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decision Support Systems 43 (2) (2007) 618–644, emerging Issues in Collaborative Commerce. doi:10.1016/j.dss.2005.05.019.

[11] C. Castelfranchi, R. Falcone, Trust Theory: A Socio-Cognitive and Computational Model, John Wiley & Sons, Ltd, 2010. doi:10.1002/9780470519851.

[12] Sovrin Foundation, Sovrin launch ceremony, published July 31, 2017; Accessed: 2025-11-03 (Jul. 2017).
URL https://blog.sovrin.org/sovrin-launch-ceremony-21a7d8141ba3

[13] uPort Project, ethr-did-registry – ethereum did registry (github repository), accessed: 2025-11-03 (2025).
URL https://github.com/uport-project/ethr-did-registry

[14] Etherscan, Address: 0xdca7ef03e98e0dc2b855be647c39abe984fcf21b — analytics, accessed: 2025-11-03 (2025).
URL https://etherscan.io/address/0xdca7ef03e98e0dc2b855be647c39abe984fcf21b#analytics

[15] M. Sporny, D. Longlay, D. Chadwick, Verifiable credentials data model v1.1 — publication history, accessed: 2025-11-03 (2022).
URL https://www.w3.org/standards/history/vc-data-model-1.1/

[16] W. W. W. Consortium, Decentralized identifiers (dids) v1.0 — publication history, accessed: 2025-11-03 (2022).
URL https://www.w3.org/standards/history/did-1.0/

[17] Sovrin Foundation, Sovrin shutdown, published: 2025-02-08. Accessed: 2025-11-03 (Feb. 2025).
URL https://sovrin.org/sovrin-foundation-mainnet-ledger-shutdown-likely-on-or-before-march-31-2025

[18] S. Weeks, Understanding trust management systems, in: Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001, 2001, pp. 94–105. doi:10.1109/SECPRI.2001.924290.

[19] S. Wan, H. Lin, W. Gan, J. Chen, P. S. Yu, Web3: The next internet revolution, IEEE Internet of Things Journal 11 (21) (2024) 34811–34825. doi:10.1109/JIOT.2024.3432116.

[20] S. Farrell, R. Housley, S. Turner, Internet x.509 public key infrastructure: Certification path building, RFC 4158 (Sep. 2005). doi:10.17487/RFC4158.
URL https://www.rfc-editor.org/info/rfc4158

[21] E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, standard (Aug. 2018).
URL https://datatracker.ietf.org/doc/html/rfc8446

[22] D. G. Berbecaru, A. Lioy, An evaluation of x.509 certificate revocation and related privacy issues in the web pki ecosystem, IEEE Access 11 (2023) 79156–79175. doi:10.1109/ACCESS.2023.3299357.

[23] R. Holz, L. Braun, N. Kammenhuber, G. Carle, The ssl landscape: a thorough analysis of the x.509 pki using active and passive measurements, in: Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, IMC '11, Association for Computing Machinery, New York, NY, USA, 2011, p. 427–444. doi:10.1145/2068816.2068856.

[24] P. R. Zimmermann, The Official PGP User's Guide, MIT Press, 1995.

[25] D. Shaw, B. Laurie, P. Zimmermann, OpenPGP Message Format, RFC 9580 (2024).
URL https://www.rfc-editor.org/rfc/rfc9580.html

[26] A. Oram, J. Viega, Beautiful Security: Leading Security Experts Explain How They Think, O'Reilly Media, Sebastopol, CA, 2009, ebook ISBN: 978-0-596-80205-9.
URL http://shop.oreilly.com/product/9780596527488.do

[27] J. Camenisch, B. Pfitzmann, Federated Identity Management, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007, pp. 213–238. doi:10.1007/978-3-540-69861-6_15.

[28] OASIS Security Services Technical Committee, Security Assertion Markup Language (SAML) V2.0 Technical Overview, Committee draft 02, OASIS (Mar. 2008).
URL https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

[29] OpenID Foundation, OpenID Authentication 2.0, final specification, 2007-12-05. Accessed: 2026-06-28 (2007).
URL https://openid.net/specs/openid-authentication-2_0.html

[30] OpenID Foundation, OpenID Connect Core 1.0, final specification. Accessed: 2026-06-28 (2014).
URL https://openid.net/specs/openid-connect-core-1_0.html

[31] E. Maler, D. Reed, The venn of identity: Options and issues in federated identity management, IEEE Security & Privacy 6 (2) (2008) 16–23. doi:10.1109/MSP.2008.50.

[32] B. Khaund, Oauth 2.0 and openid connect integration with azure entra id, Sarcouncil Journal of Engineering and Computer Sciences 4 (6) (2025) 17–24. doi:10.5281/zenodo.15732825.

[33] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, C. Allen, Decentralized identifiers (dids) v1.1, W3C Recommendation REC-did-1.1-20230817, World Wide Web Consortium (W3C) (08 2023).
URL https://www.w3.org/TR/did-1.1/

[34] W3C Decentralized Identifier Working Group, DID Methods: Known DID Methods in the Decentralized Identifier Ecosystem, W3C Group Note, World Wide Web Consortium (2026).

[35] F. Hoops, A. Mühle, F. Matthes, C. Meinel, A taxonomy of decentralized identifier methods for practitioners, in: 2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 2023, pp. 57–65. doi:10.1109/DAPPS57946.2023.00017.

[36] Did method specification: did:key (2024).
URL https://w3c-ccg.github.io/did-method-key/

[37] Did method specification: did:peer (2023).
URL https://identity.foundation/peer-did-method-spec/

[38] W. Chang, C. Lehner, J. Caballero, J. Thorstensson, did:pkh Method Specification, draft specification. Accessed: 2026-06-15 (2026).
URL https://github.com/w3c-ccg/did-pkh/blob/main/did-pkh-method-draft.md

[39] Did method specification: did:web (2022).
URL https://w3c-ccg.github.io/did-method-web/

[40] Decentralized Identity Foundation, The did:webvh DID Method Specification, live specification. Accessed: 2026-06-15 (2026).
URL https://didwebvh.info/latest/specification/

[41] E. Union, European blockchain services infrastructure (ebsi) did method (2024).
URL https://hub.ebsi.eu/vc-framework/did

[42] European Parliament and Council of the European Union, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, Official Journal of the European Union, accessed: 2026-06-13 (2024).
URL https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

[43] European Commission, The European Digital Identity Wallet Architecture and Reference Framework, architecture and Reference Framework for the European Digital Identity Wallet ecosystem. Accessed: 2026-06-13 (2025).
URL https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/

[44] European Commission, What is EBSI?, european Blockchain Services Infrastructure (EBSI). Last updated: 2026-02-02. Accessed: 2026-07-02 (2026).
URL https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/590447955/What%2Bis%2BEBSI

[45] Bluesky Social PBC, DID PLC Method Specification, accessed: 2026-06-14 (2025).
URL https://github.com/did-method-plc/did-method-plc

[46] Bluesky Social PBC, AT Protocol, specification for the Authenticated Transfer Protocol. Accessed: 2026-06-29 (2026).
URL https://atproto.com/specs/atp

[47] Baidu, DID Developer Center, baidu implementation of DID. Accessed: 2026-06-14 (2026).
URL https://did.baidu.com/

[48] ConsenSys, GoQuorum Documentation, accessed: 2026-06-15 (2019).
URL https://goquorum.readthedocs.io/

[49] Microsoft, Introduction to microsoft entra verified id, last updated: 2026-03-16; Accessed: 2026-06-14 (2026).
URL https://learn.microsoft.com/en-us/entra/verified-id/decentralized-identifier-overview

[50] 3Box Labs, Ceramic Documentation, accessed: 2026-06-15 (2025).
URL https://developers.ceramic.network/

[51] 0xPottery, What is 3ID Connect?, ceramic Blog. Accessed: 2026-06-28 (Nov. 2020).
URL https://blog.ceramic.network/what-is-3id-connect/

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

[53] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, M. Conti, A survey on decentralized identifiers and verifiable credentials, IEEE Communications Surveys & Tutorials (2025). doi:10.1109/comst.2025.3543197.

[54] A. De Salve, A. Lisi, M. Cascino, P. Mori, L. Ricci, Selective disclosure approaches in self-sovereign identity: An experimental comparison, IEEE Access 14 (2026) 1152–1181. doi:10.1109/ACCESS.2025.3649167.

[55] D. Di Francesco Maesa, A. Lisi, P. Mori, L. Ricci, G. Boschi, Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge, Journal of Network and Computer Applications 212 (2023) 103577. doi:10.1016/j.jnca.2022.103577.

[56] M. Dieye, P. Valiorgue, J.-P. Gelas, E.-H. Diallo, P. Ghodous, F. Biennier, É. Peyrol, A self-sovereign identity based on zero-knowledge proof and blockchain, IEEE Access 11 (2023) 49445–49455. doi:10.1109/ACCESS.2023.3268768.

[57] M. Sporny, D. Longley, D. Chadwick, I. Herman, Verifiable Credentials Data Model v2.0, W3C Recommendation REC-vc-data-model-2.0-20250515, World Wide Web Consortium (W3C) (05 2025).
URL https://www.w3.org/TR/vc-data-model-2.0/

[58] R. da Silva Costa, P. Rupino Da Cunha, Self-Sovereign Identities: Brief History and Survey of the Field, Springer Nature Switzerland, Cham, 2025, pp. 43–62. doi:10.1007/978-3-031-87880-0_3.

[59] R. B. Gans, J. Ubacht, M. Janssen, Self-sovereign identities for fighting the impact of covid-19 pandemic, Digit. Gov.: Res. Pract. 2 (2) (Dec. 2020). doi:10.1145/3429629.

[60] S. Terzi, C. Savvaidis, K. Votis, D. Tzovaras, I. Stamelos, Securing emission data of smart vehicles with blockchain and self-sovereign identities, in: 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 462–469. doi:10.1109/Blockchain50366.2020.00067.

[61] Togggle, Decentralized finance & self-sovereign identity, accessed: 2025-06-19 (Mar. 2024).
URL https://www.togggle.io/blog/decentralized-finance-self-sovereign-identity

[62] B. Podgorelec, L. Alber, T. Zefferer, What is a (digital) identity wallet? a systematic literature review, in: 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), 2022, pp. 809–818. doi:10.1109/COMPSAC54236.2022.00131.

[63] M. Jones, J. Bradley, N. Sakimura, JSON Web Signature (JWS), RFC 7515 (May 2015).
URL https://datatracker.ietf.org/doc/html/rfc7515

[64] J. Camenisch, A. Lysyanskaya, An efficient system for non-transferable anonymous credentials with optional anonymity revocation, in: B. Pfitzmann (Ed.), Advances in Cryptology — EUROCRYPT 2001, Springer Berlin Heidelberg, Berlin, Heidelberg, 2001, pp. 93–118.

[65] H. A. W. Group, Anoncreds specification, accessed: 2025-06-22 (2023).
URL https://hyperledger.github.io/anoncreds-spec/

[66] Y. Lee, H. Shin, D. Choi, A survey on credential revocation and did deactivation in self-sovereign identity systems, IEEE Access 14 (2026) 16089–16115. doi:10.1109/ACCESS.2025.3649792.

[67] A. M. Antonopoulos, Mastering Bitcoin: unlocking digital cryptocurrencies, second ed Edition, "O'Reilly Media, Inc.", 2017.

[68] T. Hobson, L. France, S. Greenbury, L. Hare, P. Wochner, Trustchain – trustworthy decentralised public key infrastructure for digital credentials, in: International Conference on AI and the Digital Economy (CADE 2023), Vol. 2023, 2023, pp. 31–40. doi:10.1049/icp.2023.2561.

[69] M. V. Nguyen, N. T. Le, D. Duong, Y. Li, M. Mukherjee, Blockchain oracles: Implications for smart contracts in legal reasoning and addressing the oracle problem, in: Proceedings of the 12th International Symposium on Information and Communication Technology, SOICT '23, Association for Computing Machinery, New York, NY, USA, 2023, p. 296–303. doi:10.1145/3628797.3628870.

[70] S. K. Ezzat, Y. N. M. Saleh, A. A. Abdel-Hamid, Blockchain oracles: State-of-the-art and research directions, IEEE Access 10 (2022) 67551–67572. doi:10.1109/ACCESS.2022.3184726.

[71] A. A. Alhussayen, K. Jambi, M. Khemakhem, F. E. Eassa, A blockchain oracle interoperability technique for permissioned blockchain, IEEE Access 12 (2024) 68130–68148. doi:10.1109/ACCESS.2024.3400672.

[72] J. Xu, C. Wang, X. Jia, A survey of blockchain consensus protocols, ACM Comput. Surv. 55 (13s) (Jul. 2023). doi:10.1145/3579845.

[73] Veramo, Veramo: A JavaScript Framework for Verifiable Data and SSI, accessed: 2026-06-15 (2026).
URL https://veramo.io/

[74] OpenWallet Foundation, Credo, accessed: 2026-06-15 (2026).
URL https://openwallet.foundation/projects/credo/

[75] OpenWallet Foundation, ACA-Py: Adaptive Cloud Agent Python, accessed: 2026-06-15 (2026).
URL https://aca-py.org/

[76] OpenWallet Foundation, Aries VCX, accessed: 2026-06-15 (2026).
URL https://github.com/openwallet-foundation/vcx

[77] SpruceID, DIDKit: A Cross-Platform Toolkit for Decentralized Identity, archived GitHub repository. Accessed: 2026-06-15 (2025).
URL https://github.com/spruceid/didkit

[78] Linux Foundation Decentralized Trust, Hyperledger Identus, accessed: 2026-06-15 (2026).
URL https://www.lfdecentralizedtrust.org/projects/identus

[79] walt.id, walt.id: Digital Identity and Wallet Infrastructure, accessed: 2026-06-15 (2026).
URL https://walt.id/

[80] Sphereon Open Source, Sphereon Mobile Wallet, accessed: 2026-06-15 (2026).
URL https://github.com/Sphereon-Opensource/mobile-wallet

[81] OpenWallet Foundation, Bifold Wallet, previously known as Hyperledger Aries Bifold. Accessed: 2026-06-15 (2026).
URL https://openwallet.foundation/projects/bifold/

[82] European Commission, The European Digital Identity Wallet architecture and reference framework. version 1.4.0, section 4.3 (architecture types), eIDAS Expert Group, Architecture and Reference Framework (ARF), v1.4.0, accessed: 2026-06-21 (2024).
URL https://eudi.dev/1.4.0/arf/#43-architecture-types

[83] Microsoft, Advanced Microsoft Entra Verified ID setup, Microsoft Learn, Microsoft Entra Verified ID documentation, last updated 2026-03-25. Accessed: 2026-06-21 (2025).
URL https://learn.microsoft.com/en-us/entra/verified-id/verifiable-credentials-configure-tenant

[84] A. Grüner, A. Mühle, N. Lockenvitz, C. Meinel, Analyzing and comparing the security of self-sovereign identity management systems through threat modeling, International Journal of Information Security 22 (2023) 1231–1248. doi:10.1007/s10207-023-00688-w.

[85] MITRE ATT&CK, Phishing, Technique T1566, version 2.7; last modified: 2026-05-12. Accessed: 2026-06-28 (2026).
URL https://attack.mitre.org/techniques/T1566/

[86] MITRE ATT&CK, Valid Accounts: Cloud Accounts, Sub-technique T1078.004, version 2.0; last modified: 2026-05-12. Accessed: 2026-06-28 (2026).
URL https://attack.mitre.org/techniques/T1078/004/

[87] E. Krul, H.-y. Paik, S. Ruj, S. Kanhere, Sok: Trusting self-sovereign identity, Proceedings on Privacy Enhancing Technologies 2024 (2024) 297–313. doi:10.56553/popets-2024-0079.

[88] J. Priem, H. Piwowar, R. Orr, Openalex: A fully-open index of scholarly works, authors, venues, institutions, and concepts, arXiv preprint arXiv:2205.01833 [cs.DL] (2022).
URL https://arxiv.org/abs/2205.01833

[89] Crossref, Rest api, accessed: 2026-06-20 (2026).
URL https://www.crossref.org/documentation/retrieve-metadata/rest-api/

[90] C. Turco, Dataset a survey charting trust models and systems in self-sovereign identity, Zenodo (Jun. 2026). doi:10.5281/zenodo.20689788.
URL https://doi.org/10.5281/zenodo.20689788

[91] D. Reed, J. Law, D. Hardman, The technical foundations of sovrin, The Technical Foundations of Sovrin (2016).
URL https://sovrin.org/wp-content/uploads/2018/03/The-Technical-Foundations-of-Sovrin.pdf

[92] Sovrin Foundation, Sovrin governance framework v2 (master document v1), Sovrin Foundation, white Paper (Apr. 2019).
URL https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Document-V1.pdf

[93] J. Lauinger, J. Ernstberger, E. Regnath, M. Hamad, S. Steinhorst, A-poa: Anonymous proof of authorization for decentralized identity management, in: 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2021, pp. 1–9. doi:10.1109/ICBC51069.2021.9461082.

[94] F. Buccafurri, V. De Angelis, R. Nardone, How can the holder trust the verifier? a cp-abpre-based solution to control the access to claims in a self-sovereign-identity scenario, Blockchain: Research and Applications 5 (3) (2024) 100196. doi:10.1016/j.bcra.2024.100196.

[95] R. Mukta, H.-Y. Paik, Q. Lu, S. S. Kanhere, Credtrust: Credential based issuer management for trust in self-sovereign identity, in: 2022 IEEE International Conference on Blockchain (Blockchain), 2022, pp. 334–339. doi:10.1109/Blockchain55522.2022.00053.

[96] R. Mukta, R. C. Teh, H.-Y. Paik, Q. Lu, S. S. Kanhere, Vctp: A verifiable credential-based trust propagation protocol for personal issuers in self-sovereign identity platforms, in: 2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 2023, pp. 109–118. doi:10.1109/DAPPS57946.2023.00023.

[97] M. Kubach, H. Roßnagel, A lightweight trust management infrastructure for self-sovereign identity, in: Open Identity Summit 2021, Gesellschaft für Informatik e.V., Bonn, 2021, pp. 155–166.

[98] I. H. Johnson Jeyakumar, D. W. Chadwick, M. Kubach, A novel approach to establish trust in verifiable credential issuers in self-sovereign identity ecosystems using train, in: Open Identity Summit 2022, Gesellschaft für Informatik e.V., Bonn, 2022, pp. 27–38. doi:10.18420/OID2022_02.

[99] D. W. Chadwick, M. Kubach, I. Sette, I. H. Johnson Jeyakumar, Establishing trust in ssi verifiers, in: Open Identity Summit 2023, Gesellschaft für Informatik e.V., Bonn, 2023, pp. 15–26. doi:10.18420/OID2023_01.

[100] A. Grüner, A. Mühle, 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 9 (2021) 138553–138570. doi:10.1109/ACCESS.2021.3116095.

[101] A. Ling, S. Butakov, Trust framework for self-sovereign identity in metaverse healthcare applications, Data Science and Management 7 (4) (2024) 304–313. doi:10.1016/j.dsm.2024.04.003.

[102] C. Pujari, B. Muniyal, C. B. Chandrakala, A. Rao, V. Sadiname, M. Rajarajan, Identity resilience in the digital health ecosystem: A key recovery-enabled framework, Computers in Biology and Medicine 167 (2023) 107702. doi:10.1016/j.compbiomed.2023.107702.

[103] K. J. Eer, J. Diaz, M. Kohlweiss, Bottom-up trust registry in self sovereign identity, in: J. Prieto, F. L. Benítez Martínez, S. Ferretti, D. Arroyo Guardeño,

P. Tomás Nevado-Batalla (Eds.), Blockchain and Applications, 4th International Congress, Springer International Publishing, Cham, 2023, pp. 423–433. doi:doi.org/10.1007/978-3-031-21229-1_39.

[104] A. De Salve, D. Di Francesco Maesa, P. Mori, L. Ricci, A. Puccia, A multilayer trust framework for self sovereign identity on blockchain, Online Social Networks and Media 37-38 (2023) 100265. doi:10.1016/j.osnem.2023.100265.

[105] M. Luecking, C. Fries, R. Lamberti, W. Stork, Decentralized identity and trust management framework for internet of things, in: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1–9. doi:10.1109/ICBC48266.2020.9169411.

[106] A. Grüner, A. Mühle, T. Gayvoronskaya, C. Meinel, A quantifiable trust model for blockchain-based identity management, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1475–1482. doi:10.1109/Cybermatics_2018.2018.00250.

[107] J. Yin, Y. Xiao, J. Feng, M. Yang, Q. Pei, X. Yi, Didtrust: Privacy-preserving trust management for decentralized identity, IEEE Transactions on Dependable and Secure Computing 22 (3) (2025) 3105–3120. doi:10.1109/TDSC.2024.3524760.

[108] Y. Y. M. Chung, E. Krul, H.-Y. Paik, Privacy preserving reputation system for self-sovereign identity, in: S. Kanhere, R. Jurdak, J. Parkinson, B. Sridharan, S. Pal, K. Biswas (Eds.), Distributed Ledger Technology, Springer Nature Singapore, Singapore, 2025, pp. 55–70. doi:10.1007/978-981-96-4442-1_4.

[109] V. E. F. d. C. Borges, Á. Sobrinho, D. F. S. Santos, A. Perkusich, A self-sovereign identity-based authentication and reputation protocol for IoV applications, IEEE Access 13 (2025) 105693–105711. doi:10.1109/ACCESS.2025.3579929.

[110] T. G. Papaioannou, V. Ritas, VChain: Establishing trust based on verifiable credential chains, in: 2025 28th Conference on Innovation in Clouds, Internet and Networks (ICIN), IEEE, 2025, pp. 41–48. doi:10.1109/ICIN64016.2025.10943065.

[111] M. P. Bhattacharya, P. Zavarsky, S. Butakov, Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain, in: 2020 International Symposium on Networks, Computers and Communications (ISNCC), 2020, pp. 1–7. doi:10.1109/ISNCC49221.2020.9297357.

[112] A. Marín Frutos, J. García Rodríguez, A. Skarmeta, K. Loupos, S. Vavilis, Identity and trust architecture for device lifecycle management, in: M. Presser, A. Skarmeta, S. Krco, A. González Vidal (Eds.), Global Internet of Things and Edge Computing Summit, Springer Nature Switzerland, Cham, 2025, pp. 63–72. doi:10.1007/978-3-031-78572-6_4.

[113] A. Pino, D. Margaria, A. Vesco, Combining decentralized identifiers with proof of membership to enable trust in iot networks, in: 2023 33rd International Telecommunication Networks and Applications Conference, 2023, pp. 310–317. doi:10.1109/ITNAC59571.2023.10368540.

[114] X. Song, G. Xu, Y. Huang, A fuzzy ahp-based trust management mechanism for self-sovereign identity in the metaverse, Applied Soft Computing 174 (2025) 112994. doi:10.1016/j.asoc.2025.112994.

[115] S. Bistarelli, C. Luchini, F. Santini, Ssi policies implementing terms of use to control vc disclosure, in: 2025 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 2025, pp. 25–30. doi:10.1109/PerComWorkshops65533.2025.00036.

[116] S. Marsh, Formalising trust as a computational concept, Ph.D. thesis, Department of Computing Science and Mathematics University of Stirling (07 1999).

[117] European Digital Identity, Topic x – relying party registration, version 0.4, updated 25 April 2025. Accessed: 2026-02-23 (Apr. 2025).
URL https://eudi.dev/latest/discussion-topics/x-relying-party-registration/

[118] C. Turco, A. D. Salve, D. D. F. Maesa, P. Mori, L. Ricci, An aid to mitigate online misinformation with self-sovereign identity and artificial intelligence, in: 2025 7th International Conference on Blockchain Computing and Applications (BCCA), 2025, pp. 169–177. doi:10.1109/BCCA66705.2025.11229690.

[119] J. Sabater, C. Sierra, Review on computational trust and reputation models, Artificial Intelligence Review 24 (1) (2005) 33–60. doi:10.1007/s10462-004-0041-5.

[120] R. Guha, R. Kumar, P. Raghavan, A. Tomkins, Propagation of trust and distrust, in: Proceedings of the 13th International Conference on World Wide Web, WWW '04, Association for Computing Machinery, New York, NY, USA, 2004, p. 403–412. doi:10.1145/988672.988727.

[121] C. Dong, N. Dulay, Shinren: Non-monotonic trust management for distributed systems, in: M. Nishigaki, A. Jøsang, Y. Murayama, S. Marsh (Eds.), Trust Management IV, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 125–140.

[122] R. Ureña, G. Kou, Y. Dong, F. Chiclana, E. Herrera-Viedma, A review on trust propagation and opinion dynamics in social networks and group decision making frameworks, Information Sciences 478 (2019) 461–475. doi:https://doi.org/10.1016/j.ins.2018.11.037.

[123] C. Castelfranchi, R. Falcone, The Negative Side: Lack of Trust, Implicit Trust, Mistrust, Doubts and Diffidence, John Wiley & Sons, Ltd, 2010, Ch. 4, pp. 117–131. arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470519851.ch4, doi:https://doi.org/10.1002/9780470519851.ch4.

[124] C. Marche, M. Nitti, Trust-related attacks and their detection: A trust management model for the social iot, IEEE Transactions on Network and Service Management 18 (3) (2021) 3297–3308. doi:10.1109/TNSM.2020.3046906.

[125] C. Castelfranchi, R. Falcone, Socio-Cognitive Model of Trust: Basic Ingredients, John Wiley & Sons, Ltd, 2010, Ch. 2, pp. 35–94. arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470519851.ch2, doi:https://doi.org/10.1002/9780470519851.ch2.

[126] O. Terbu, T. Lodderstedt, K. Yasuda, D. Fett, J. Heenan, Openid for verifiable presentations 1.0, published 9 July 2025; Accessed: 2025-10-27 (2025).
URL https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[127] P. Mockapetris, Domain names - implementation and specification, RFC 1035 (Nov. 1987). doi:10.17487/RFC1035.
URL https://www.rfc-editor.org/info/rfc1035

[128] OpenWallet Foundation, Askar, accessed: 2026-06-21 (2026).
URL https://github.com/openwallet-foundation/askar

[129] A. C. Yao, Protocols for secure computations, in: 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), 1982, pp. 160–164. doi:10.1109/SFCS.1982.38.

[130] I. Damgård, V. Pastro, N. Smart, S. Zakarias, Multiparty computation from somewhat homomorphic encryption, in: R. Safavi-Naini, R. Canetti (Eds.), Advances in Cryptology – CRYPTO 2012, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 643–662. doi:10.1007/978-3-642-32009-5_38.

[131] H. Li, Y. Chen, X. Shi, X. Bai, N. Mo, W. Li, R. Guo, Z. Wang, Y. Sun, Fisco-bcos: An enterprise-grade permissioned blockchain system with high-performance, in: Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis, SC '23, Association for Computing Machinery, New York, NY, USA, 2023, p. 17. doi:10.1145/3581784.3607053.

[132] Eratosthenes: Iot trust and identity management framework, European Union, Horizon 2020 (2023).
URL https://eratosthenes-project.eu/

[133] Y. Ruan, A. Durresi, A survey of trust management systems for online social communities – trust modeling, trust inference and attacks, Knowledge-Based Systems 106 (2016) 150–163. doi:10.1016/j.knosys.2016.05.042.

[134] W. Sherchan, S. Nepal, C. Paris, A survey of trust in social networks, ACM Computing Surveys 45 (4) (2013) 1–33. doi:10.1145/2501654.2501661.

[135] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, S. Ghouzali, Trust and reputation management in healthcare systems: Taxonomy, requirements and open issues, IEEE Access 6 (2018) 17246–17263. doi:10.1109/ACCESS.2018.2810337.

[136] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decision Support Systems 43 (2) (2007) 618–644. doi:10.1016/j.dss.2005.05.019.

[137] S. Alam, S. Zardari, S. Noor, S. Ahmed, H. Mouratidis, Trust management in social internet of things (siot): A survey, IEEE Access 10 (2022) 108924–108954. doi:10.1109/ACCESS.2022.3213699.

[138] H. Hasrouny, A. E. Samhat, C. Bassil, A. Laouiti, Vanet security challenges and solutions: A survey, Vehicular Communications 7 (2017) 7–20. doi:10.1016/j.vehcom.2017.01.002.

[139] M. Blaze, J. Feigenbaum, J. Lacy, Decentralized trust management, in: Proceedings of the 1996 IEEE Symposium on Security and Privacy, IEEE Computer Society, 1996, pp. 164–173. doi:10.1109/SECPRI.1996.502679.

[140] O. Hasan, L. Brunie, E. Bertino, Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey, ACM Comput. Surv. 55 (2) (Jan. 2022). doi:10.1145/3490236.

[141] S. Gurtler, I. Goldberg, SoK: Privacy-preserving reputation systems, Proceedings on Privacy Enhancing Technologies 2021 (1) (2021) 107–127. doi:10.2478/popets-2021-0007.

[142] L. Alzahrani, W. Al-Karaghouli, V. Weerakkody, Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework, International Business Review 26 (1) (2017) 164–175. doi:https://doi.org/10.1016/j.ibusrev.2016.06.004.

[143] I. H. J. Jeyakumar, M. Kubach, A trust implementation model for cross-domain decentralized identity ecosystems: architecture, use case, and implementation, Procedia Computer Science 254 (2025) 10–19, international Conference on Digital Sovereignty (ICDS). doi:10.1016/j.procs.2025.02.059.

[144] A. Doan, R. Ramakrishnan, A. Y. Halevy, Crowdsourcing systems on the world-wide web, Communications of the ACM 54 (4) (2011) 86–96. doi:10.1145/1924421.1924442.

[145] A. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel, A survey on essential components of a self-sovereign identity, Computer Science Review 30 (2018) 80–86. doi:10.1016/j.cosrev.2018.10.002.

[146] J. Kaneriya, H. Patel, A comparative survey on blockchain based self sovereign identity system, in: 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 1150–1155. doi:10.1109/iciss49785.2020.9315899.

[147] R. Nokhbeh Zaeem, et al., Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study, in: IEEE/WIC/ACM International Conference on Web Intelligence, 2021, pp. 128–135. doi:10.1145/3486622.3493917.

[148] S. Cucko, M. Turkanovic, Decentralized and self-sovereign identity: Systematic mapping study, IEEE Access 9 (2021) 139009–139027. doi:10.1109/access.2021.3117588.

[149] R. Soltani, U. T. Nguyen, A. An, C. Galdi, A survey of self-sovereign identity ecosystem, Sec. and Commun. Netw. 2021 (Jan. 2021). doi:10.1155/2021/8873429.

[150] Y. Bai, H. Lei, S. Li, H. Gao, J. Li, L. Li, Decentralized and self-sovereign identity in the era of blockchain: A survey, in: 2022 IEEE International Conference on Blockchain (Blockchain), 2022, pp. 500–507. doi:10.1109/Blockchain55522.2022.00077.

[151] Š. Čučko, Š. Bećirović, A. Kamišalić, S. Mrdović, M. Turkanović, Towards the classification of self-sovereign identity properties, IEEE Access 10 (2022) 88306–88329. doi:10.1109/ACCESS.2022.3199414.

[152] S. Y. Lim, O. B. Musa, B. A. S. Al-Rimy, A. Almasri, Trust models for blockchain-based self-sovereign identity management: A survey and research directions, in: Y. Maleh, L. Tawalbeh, S. Motahhir, A. S. Hafid (Eds.), Advances in Blockchain Technology for Cyber Physical Systems, Springer International Publishing, Cham, 2022, pp. 277–302. doi:10.1007/978-3-030-93646-4_13.

[153] K. L. Tan, C.-H. Chi, K.-Y. Lam, Survey on digital sovereignty and identity: From digitization to digitalization, ACM Comput. Surv. 56 (3) (Oct. 2023). doi:10.1145/3616400.

[154] A. Satybaldy, M. S. Ferdous, M. Nowostawski, A taxonomy of challenges for self-sovereign identity systems, IEEE Access 12 (2024) 16151–16177. doi:10.1109/access.2024.3357940.

[155] E. Biele, D. Richter, R. Bochnia, J. Anke, Supporting trust decisions of holders and verifiers: a unified model of trust management in ssi, in: Open Identity Summit 2025, Gesellschaft für Informatik e.V., Bonn, 2025, pp. 113–126. doi:10.18420/oid2025_08.

[156] P. Manimaran, T. Garrett, L. Jehl, R. Vitenberg, Decentralization trends in identity management: From federated to self-sovereign identity management systems, Computer Science Review 58 (2025) 100776. doi:10.1016/j.cosrev.2025.100776.

[157] E. Fathalla, M. Azab, C. Xin, H. Wu, Self-sovereign identity as a secure and trustworthy approach to digital identity management: A comprehensive survey, ACM Comput. Surv. 58 (7) (Feb. 2026). doi:10.1145/3785466.

[158] K. Bendiab, N. Kolokotronis, S. Shiaeles, S. Boucherkha, Wip: A novel blockchain-based trust model for cloud identity management, in: 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2018, pp. 724–729. doi:10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00126.

[159] C. Brunner, U. Gallersdörfer, F. Knirsch, D. Engel, F. Matthes, Did and vc:untangling decentralized identifiers and verifiable credentials for the web of trust, in: Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications, ICBTA '20, Association for Computing Machinery, New York, NY, USA, 2021, p. 61–66. doi:10.1145/3446983.3446992.

[160] D. G. W. Birch, Identity is the New Money, Perspectives, London Publishing Partnership, London, 2014.

[161] I. Gamiz, C. Regueiro, O. Lage, et al., Challenges and future research directions in secure multi-party computation for resource-constrained devices and large-scale computations, International Journal of Information Security 24 (27) (2025). doi:10.1007/s10207-024-00939-4.

[162] M. Bellare, P. Rogaway, Robust computational secret sharing and a unified account of classical secret-sharing goals, Cryptology ePrint Archive, Paper 2006/449 (2006).
URL https://eprint.iacr.org/2006/449

[163] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613. doi:10.1145/359168.359176.

[164] E. Samir, H. Wu, M. Azab, C. Xin, Q. Zhang, Dt-ssim: A decentralized trustworthy self-sovereign identity management framework, IEEE Internet of Things Journal 9 (11) (2022) 7972–7988. doi:10.1109/JIOT.2021.3112537.

[165] S. Eskandari, M. Salehi, W. C. Gu, J. Clark, Sok: oracles from the ground truth to market manipulation, in: Proceedings of the 3rd ACM Conference on Advances in Financial Technologies, AFT '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 127–141. doi:10.1145/3479722.3480994.

[166] UMA Protocol, Uma: Universal market access whitepaper, Whitepaper, UMA Protocol, accessed: 2025-09-15 (2020).
URL https://github.com/UMAprotocol/whitepaper/blob/master/UMA-whitepaper.pdf

[167] O. Rikken, M. Janssen, Z. Kwee, The ins and outs of decentralized autonomous organizations (daos) unraveling the definitions, characteristics, and emerging developments of daos, Blockchain: Research and Applications 4 (3) (2023) 100143. doi:doi.org/10.1016/j.bcra.2023.100143.

[168] Dignifiedquire, Cryptographic accumulators and vector commitments in rust, accessed: 2025-08-09 (2020).
URL https://cambrian.github.io/accumulator/

[169] T. Ye, M. Luo, Y. Yang, K.-K. R. Choo, D. He, A survey on redactable blockchain: Challenges and opportunities, IEEE Transactions on Network Science and Engineering 10 (3) (2023) 1669–1683. doi:10.1109/TNSE.2022.3233448.

[170] J. Kwon, E. Buchman, Cosmos whitepaper, accessed: 2025-07-04 (2019).
URL https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md

[171] Hyperledger Foundation, Hyperledger cacti, accessed: 2025-07-04 (2024).
URL https://github.com/hyperledger-cacti/cacti

[172] D. B. Acharya, K. Kuppan, B. Divya, Agentic ai: Autonomous intelligence for complex goals—a comprehensive survey, IEEE Access 13 (2025) 18912–18936. doi:10.1109/ACCESS.2025.3532853.

[173] H. Bangui, E. Cioroaica, M. Ge, B. Buhnova, Deep-learning based trust management with self-adaptation in the internet of behavior, in: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, SAC '23, Association for Computing Machinery, New York, NY, USA, 2023, p. 874–881. doi:10.1145/3555776.3577694.

[174] A. Pfeiffer, M. Bugeja, Introducing the concept of "digital-agent signature-sagent signature": How ssi can be expanded for the needs of industry 4.0., in: A. Dingli, F. Haddod, C. Klüver (Eds.), Artificial Intelligence in Industry 4.0: A Collection of Innovative Research Case-studies that are Reworking the Way We Look at Industry 4.0 Thanks to Artificial Intelligence, Springer International Publishing, Cham, 2021, pp. 213–233. doi:10.1007/978-3-030-61045-6_15.

[175] R. Pericàs-Gornals, M. Mut-Puigserver, M. M. Payeras-Capellà, M. À. Cabot-Nadal, J. Ramis-Bibiloni, Rejectable soulbound tokens for credentials assignment and acceptance of terms, in: 2023 7th Cyber Security in Networking Conference (CSNet), 2023, pp. 212–218. doi:10.1109/CSNet59123.2023.10339728.

[176] A. Tversky, D. Kahneman, Judgment under uncertainty: Heuristics and biases, Science 185 (4157) (1974) 1124–1131.
URL http://www.jstor.org/stable/1738360

[177] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, Y. Ji, Decentralized trust evaluation in vehicular internet of things, IEEE Access 7 (2019) 15980–15988. doi:10.1109/ACCESS.2019.2893262.

[178] D. Zhang, F. R. Yu, R. Yang, H. Tang, A deep reinforcement learning-based trust management scheme for software-defined vehicular networks, in: Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, DIVANet'18, Association for Computing Machinery, New York, NY, USA, 2018, p. 1–7. doi:10.1145/3272036.3272037.

[179] T. Sharma, Y. Potter, K. Pongmala, H. Wang, A. Miller, D. Song, Y. Wang, Future of algorithmic organization: Large scale analysis of decentralized autonomous organizations (daos), ACM Trans. WebJust Accepted (Feb. 2026). doi:10.1145/3796547.

[180] United Kingdom Press Card Authority, United Kingdom Press Card Authority: UK Official Press Card, accessed: 2026-06-26 (2026).
URL https://presscards.co.uk/

[181] International Federation of Journalists, IFJ International Press Card, accessed: 2026-06-26 (2026).
URL https://www.ifj.org/press-card

[182] S. Varadarajan, J. H. L. Koh, B. K. Daniel, A Systematic Review of the Opportunities and Challenges of Micro-Credentials for Multiple Stakeholders: Learners, Employers, Higher Education Institutions and Government, International Journal of Educational Technology in Higher Education 20 (1) (2023) 13. doi:10.1186/s41239-023-00381-x.

[183] S. Raza, R. Sapkota, M. Karkee, C. Emmanouilidis, Trism for agentic ai: A review of trust, risk, and security management in llm-based agentic multi-agent systems, AI Open 7 (2026) 71–95. doi:https://doi.org/10.1016/j.aiopen.2026.02.006.