Trust Models for Blockchain-Based Self-Sovereign Identity Management: A Survey and Research Directions

Shu Yun Lim, Omar Bin Musa, Bander Ali Saleh Al-Rimy, and Abdullah Almasri

1 Introduction

Identity management (IDM) refers to the mechanism and standards for creation, maintenance, and de-provisioning of user accounts. It covers the administrative area that identifies and authenticates users and controlling the user's access to resources such as applications, systems, or online services. Identity management has evolved from centralized identity, where user credentials are owned and managed by a single entity, to federated identity that provides authentication and authorization capabilities across organizational and system boundaries.

In centralized identity system, users struggle to maintain different sets of credentials for different services. They lose control of their personal data when the information is duplicated across different providers. When federated identity is adopted, a privacy invasion issue arises because users are subject to profiling and analytics when their data resides with providers [1]. Identity providers, on the other hand, are facing constant security attacks on their centralized databases; therefore, high costs are incurred to build multifactor authentication and secure their perimeter network. Identity providers can also be held liable for data breaches under existing data protection acts [2]. The security, privacy, and usability challenges faced by

S. Y. Lim (✉) · O. B. Musa
Faculty of Business and Technology, UNITAR International University, Petaling Jaya, Malaysia
e-mail: lim_sy@unitar.my; omarm@unitar.my

B. A. S. Al-Rimy
School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Johor Bahru, Malaysia
e-mail: bander@utm.my

A. Almasri
School of Mathematical & Computer Sciences, Heriot-Watt University, Putrajaya, Malaysia
e-mail: a.almasri@hw.ac.uk

Y. Maleh et al. (eds.), *Advances in Blockchain Technology for Cyber Physical Systems*, Internet of Things, https://doi.org/10.1007/978-3-030-93646-4_13

both users and providers are expected to be resolved with the introduction of self-sovereign identity management (SSIDM) [3].

Self-sovereign identity is the concept that users should be able to control their own digital identity [4, 5]. Individual users or organizations can store their own identity data on their own devices and provide their identity to a verifier without relying on a central repository of identity data. Since this is independent from any individual silo, it gives the user full control, security, and full portability of their data [6]. Blockchain technology can be used to deliver this secure solution without the need for a trusted, central authority. It can be used for creating an identity on the blockchain, giving them greater control over who has their personal information and the way the information is being accessed [7].

One of the pioneers in blockchain-based SSIDM, Sovrin Foundation, describes self-sovereign identity as an Internet for identity where no one owns it, everyone can use it, and anyone can improve it [8]. By removing the need for a trusted third party, blockchain enables the creation of decentralized identity management without a central identity provider. In the light of this, decentralized IDM based on blockchain has different trust requirements compared to traditional IDM. There are various roles and objects that replace the centralized trusted third party; hence, trust must be managed in a dynamic and granular manner [7].

A SSIDM trust model should be able to assign a trust rating or trust score to every stakeholder based on observations from past transactions. The National Institute of Standards and Technology (NIST) presented in its cybersecurity white paper [9] a comprehensive list of entities and their roles in identity management. The stakeholders defined are requester, issuer, subjects and holders, verifier, and relying party. Every role in this ecosystem is involved in requesting credential, issuing credential, disclosing presentation, verifying presentation, and credential revocation (Fig. 1).

When a trust model is implemented on blockchain, a smart contract can be used for transparent, efficient, and secure calculation of trust rating. Automation using a smart contract should incur minimal overhead in terms of latency and throughput.

Trust is a pervasive and significant phenomenon in social societies with a diverse and manifold range of meanings and definitions [10]. Trust is also a fundamental for cooperation, conversation, and mutual interaction between entities. In recent decades, trust has been studied in many different disciplines and used as the basis for decision-making in different contexts [11].

Trust modeling uses the methodology of mathematics to obtain peers' trust intention and reliability information based on the definition of trust [12]. The trust engine, on the other hand, leverages multiple data sources to compute a risk score or credit score [13]. In mobile gaming, trust modeling is used to determine the authenticity of players' geo-position [14]. In wireless communication, trust refers to the relationship value computed based on the rate of successful transactions between network nodes [15]. There is much research on trust modeling, and most of them are in areas such as Internet of things, cybersecurity, social network, online services, and cloud computing, to name but a few [16–21].

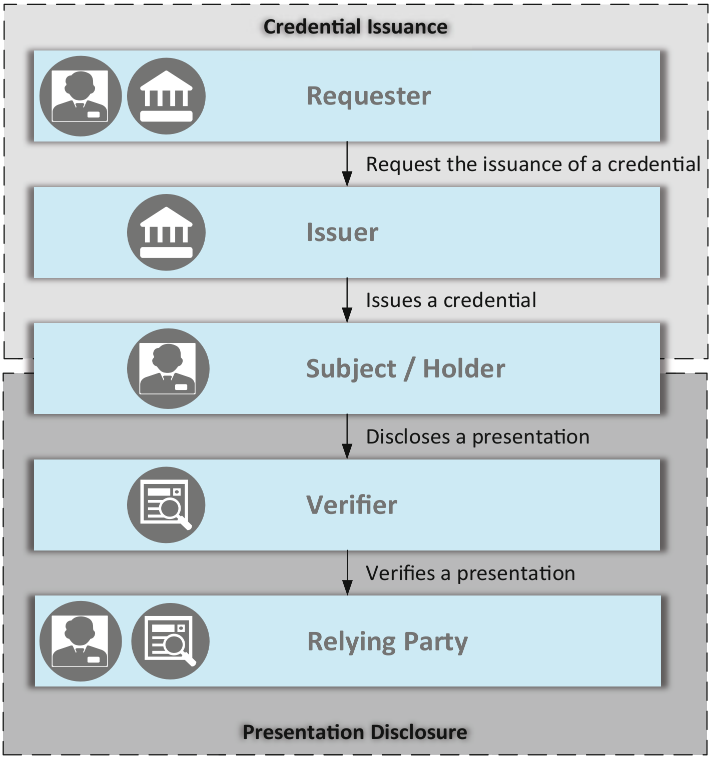


Fig. 1 Identity management roles defined by the NIST [9]

However, these solutions are not suitable when applied to Self-Sovereign IDM. With the introduction of blockchain-based Self-sovereign IDM, a different approach is needed for the computation of trust in digital identities. Self-sovereign IDM calls for specific requirements of trust not just for digital identities but also for claims and attestations made by entities. Existing blockchain-based IDM solutions can be further improved to determine the trustworthiness of claims and digital identities [22].

Many existing trust models use a static, preconfigured trust relationship to interact, such as the web of trust approach with pre-defined trust anchors in the Sovrin project [8]. The trust anchors' trustworthiness is assumed, rather than derived. However, trust can change dynamically according to actions and behaviors of entities [23].

Therefore, a distributed and dynamic approach for managing trust among identity management roles in Blockchain-based Self-sovereign IDM is needed. There are many parameters that could be considered for the trustworthiness of identities, claims, and attestations. A richer set of trust clues or parameters will lead to less fraud in identity transactions and management.

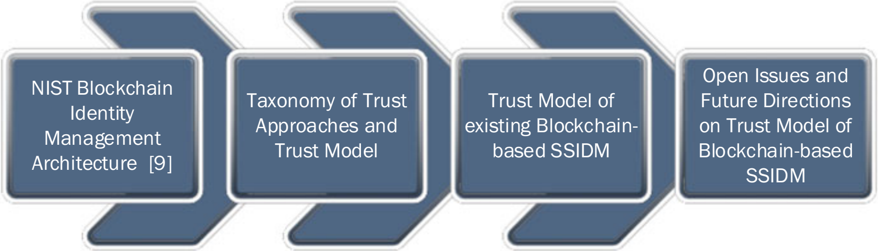

NIST Blockchain Identity Management Architecture [9]
Taxonomy of Trust Approaches and Trust Model
Trust Model of existing Blockchain-based SSIDM
Open Issues and Future Directions on Trust Model of Blockchain-based SSIDM

Fig. 2 Research methodology

We provide a survey of trust model in blockchain-based SSIDM with the methodology shown in Fig. 2. First of all, the NIST blockchain identity management system architecture is adopted and referenced for the baseline terms and definition. Next, a taxonomy of trust approaches and trust models were examined. In the third phase, related works were investigated with a focus on their trust model. Finally, we use input from the previous phases to derive the open issue and the future directions of trust modeling for blockchain-based SSIDM.

The paper starts by introducing the evolution of online identities and the concept of blockchain-based self-sovereign identity. In Sect. 2, the components of blockchain-based SSIDM are described. The components include verifiable credentials, verifiable presentations, digital wallet, decentralized identifiers, the underlying Blockchain network, and the Trust infrastructure of SSIDM. Section 3 presents a taxonomy of trust approaches and trust models. A summary of related SSIDM projects and respective trust models are presented in Sect. 4. The paper closes with research directions in Sect. 5 and a conclusion.

2 Architecture of Blockchain-Based SSIDM

Blockchain-based SSIDM consists of several components at different layers of the architecture. All identity data such as *claims*, *verifiable credentials*, and *verifiable presentations* are held in a *digital wallet* by an identity holder. The digital wallet is identified by a public key, facilitated by *decentralized identity (DID)* layer. A *smart contract* runs on top of the blockchain to implement the business logic. Beneath all components is the *distributed ledger*, a shared and tamper-proof record of transactions. The ledger on different nodes forms the heart of a *blockchain system* that empowers this self-sovereign identity ecosystem. The building blocks are discussed in detail in the following subsections.

A. Stakeholders

The technical paper presented by the NIST [9] provides an overview of stakeholders that interact in a blockchain-based SSIDM. *Subjects or holders* request for

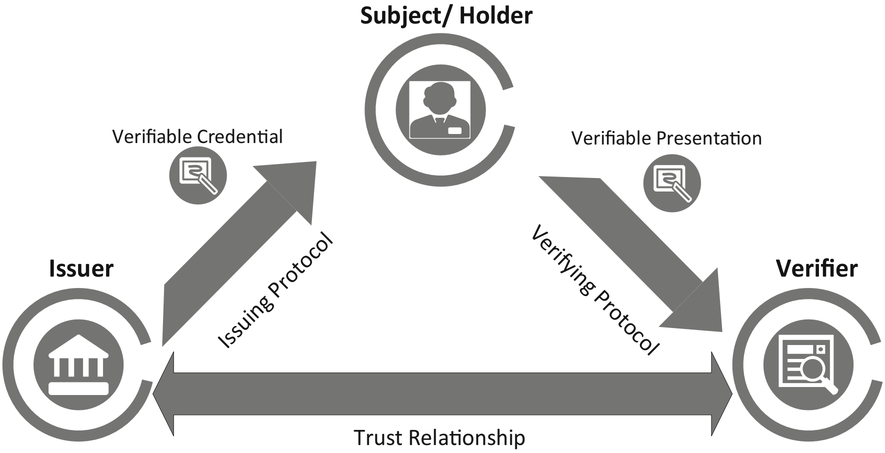


Fig. 3 Stakeholders of blockchain-based SSIDM

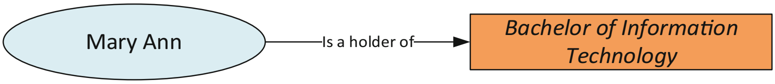


Fig. 4 Subject-property-value relationship [24]

the issuance of a credential. The *issuer* issues a credential to *subjects or holders* based on the request. The credential can later be presented to a *verifier*. The *verifier* will verify the presentation to a *Relying Party*. These roles are not exclusive because both *subject* and *issuer* can play the role of requester and a *subject* and *verifier* can both be a *Relying Party* (Fig. 3).

B. Claim

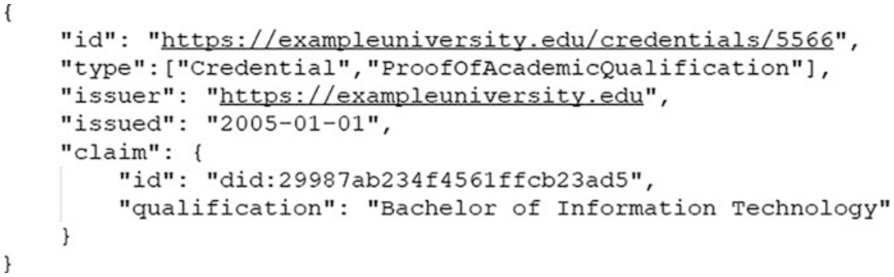
A claim is an identifier, or a statement made about an entity. An entity in this case can be a distinct person, organization, or device. For example, “Mary Ann is a holder of a bachelor’s degree in IT” is described as a subject-property-value relationship in Fig. 4 [24].

The verifiable claims have a specific data model that can be expressed in data representation languages such as JSON (Fig. 5), JSON-LD, WebIDL, and XML [24].

C. Verifiable Credential

On the other hand, credential is more formal than a claim. It can be a set of one or more claims made by an entity. Verifiable credentials (Fig. 6) are digital certifications such as academic degree (Fig. 7), proof of employment (Fig. 8), and proof of income (Fig. 9). Every stakeholder could issue, hold, or verify credentials.

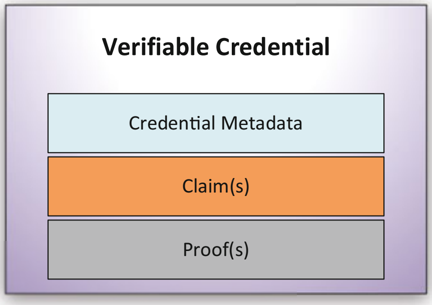
A verifiable credential may contain at least one or a set of claims in the form of metadata that describes the properties of the credential, such as a credential



```
{
    "id": "https://exampleuniversity.edu/credentials/5566",
    "type":["Credential","ProofOfAcademicQualification"],
    "issuer": "https://exampleuniversity.edu",
    "issued": "2005-01-01",
    "claim": {
        "id": "did:29987ab234f4561ffcb23ad5",
        "qualification": "Bachelor of Information Technology"
    }
}
```

Fig. 5 Example of verifiable claim in JSON

Fig. 6 Verifiable credential [25]



identifier, a public key of the issuer, or a timestamp. These metadata may be signed by the issuer. The issuer will attach a cryptographical signature such as an RSA signature, a nonce, a signature value, a creation timestamp, and an issuer's public key. These parameters are required for a third party to verify a credential.

D. Verifiable Presentation

Verifiable presentations are created out of claims and verifiable credentials. They serve to present personal identity information in a trusted way to third parties, revealing only as much information as required, to preserve the identity owner's privacy. Presentation is based on one or multiple credentials. The relationship between a claim, credential, and presentation is depicted in Fig. 10.

E. Digital Wallet

A subject or holder stores credentials in a personal device and software such as digital wallet, as in the real world where people keep their IDs in their physical wallet [27, 28]. A digital wallet serves as an agent in SSIDM ecosystem [7]. The wallet is used to perform authentication and prove ownership using the public and private key pairs generated. Since credentials are issued off-chain, the wallet contains all the self-attested information and credentials regarding the identity

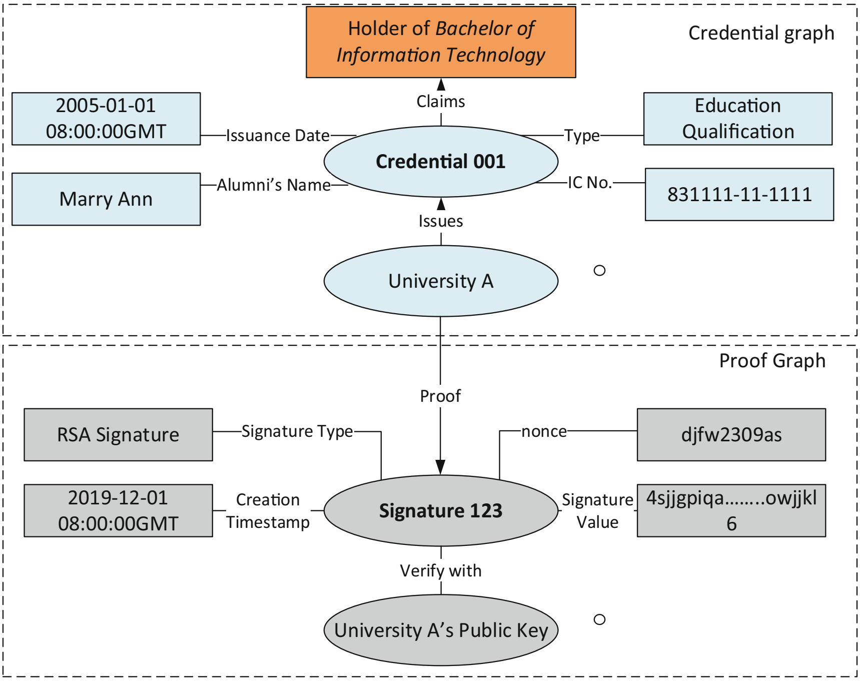


Fig. 7 Credential graph showing credential metadata and proof graph for credential presentation. University A is the issuer of credential as a degree awarding institution. This is a proof of academic qualification

owner. The credential can be presented to a third party for authentication or authorization to use a service. A holder could present entire credentials, parts of them, or combinations of multiple credentials in the form of proofs to verifiers. Thus, the holder has full control over which data is shared and how it is used.

F. Decentralized Identity

The decentralized identity (DID) layer allows an entity to be publicly identified in SSIDM solutions. DID methods allow users to request or issue verifiable credentials by providing the operations to create, read, update, and delete credentials in a decentralized way without the need of a central authority. There are emerging standards for recording credential metadata such as decentralized identifiers (DIDs) from W3C [26], DID Auth from the Rebooting the Web-of-Trust (RWOT) working group [29], Universal Resolver and Identity Hubs from the Decentralized Identity Foundation (DIF) [30], and Open Badges from Mozilla and IMS Global [31]. A DID standard will decide what credential metadata is recorded on the distributed ledger. Instead of storing credential metadata directly into the ledger, an identifier is used because the underlying blockchain is immutable.

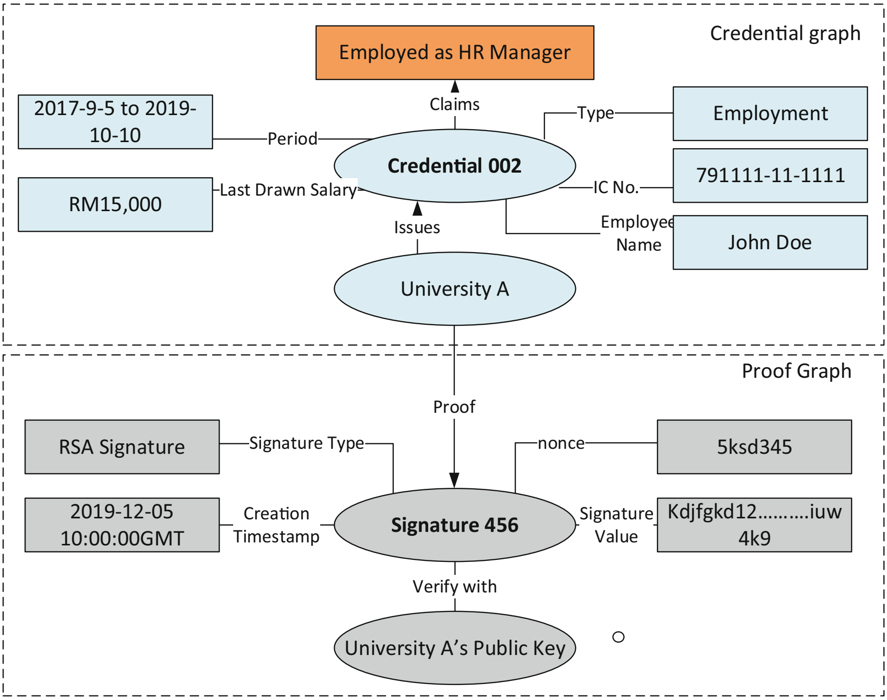


Fig. 8 Credential graph showing credential metadata and proof graph for credential presentation. University A is the issuer of the credential as an employer. This is a proof of employment

G. Smart Contract

A smart contract [32] defines the interactions between transacting parties and implements logic agreed by all nodes in a blockchain network. It is sometimes referred to as chaincode, but a smart contract is in fact defined within a chaincode. Multiple smart contracts for related business processes can be deployed in the same chaincode.

A smart contract comprises trigger conditions and response rules. Input to the smart contract can be time, event, transaction, action, etc. It performs evaluation of contract clauses and auto-executes contract statements once triggered. Upon completion, the output based on conditions and response rules will be written on a new block (Fig. 11).

H. Blockchain and Distributed Ledger Technology (DLT)

Blockchain is one of the main pillars of SSIDM, alongside verifiable credentials, verifiable presentations, decentralized identifiers, and smart contract. Underneath smart contract is the blockchain network and distributed ledger where the immutable and transparent records reside. The characteristics of blockchain make it a good fit

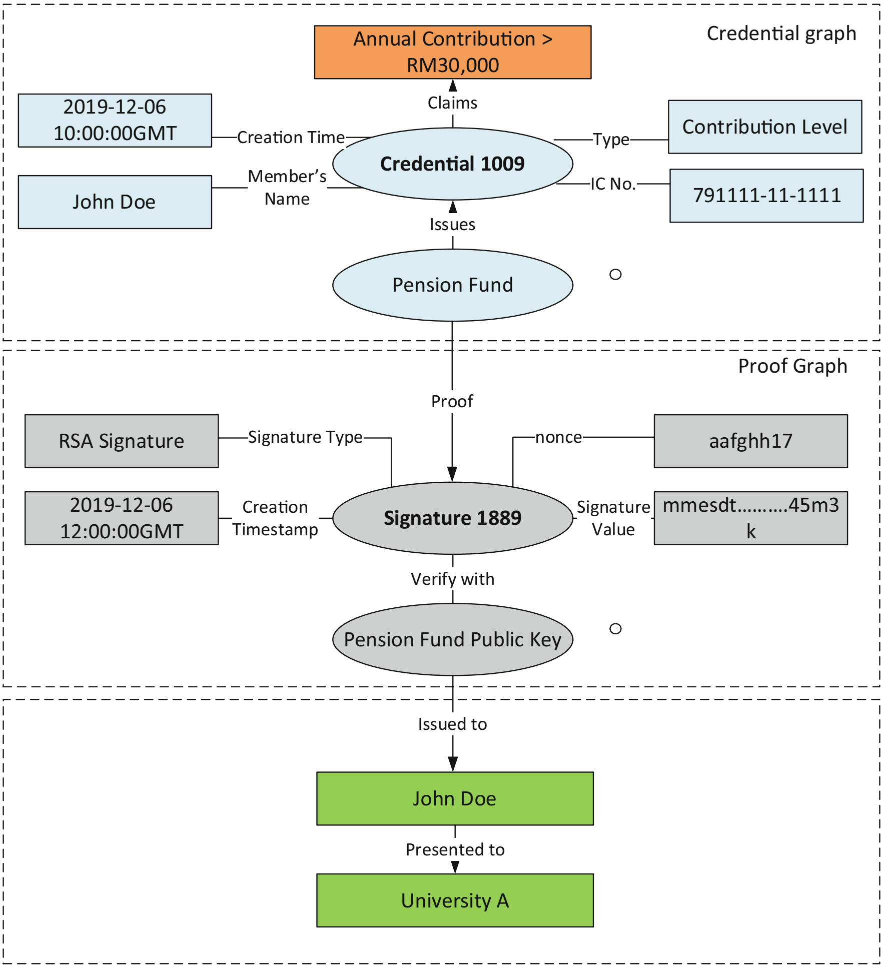


Fig. 9 University A, a potential employer for John Doe, is the verifier of a credential issued by pension fund to determine annual remuneration of John Doe. This is a proof of income level.

for creating an advanced identity management ecosystem in a decentralized manner which satisfies the principles of self-sovereign identity (Fig. 12).

The consensus layer is critical for any blockchain network. Consensus ensures that all nodes in blockchain agree to the truth. For a blockchain with cryptocurrency like Ethereum, consensus also rewards the nodes for validating the transactions and maintaining the blockchain network. Proof of work (PoW), proof of stake (PoS), and Practical Byzantine Fault Tolerance (pBFT) are excellent consensus algorithms for nodes to agree on the records on blocks. Hyperledger Fabric, Indy, and Iroha implemented voting-based consensus. For instance, Hyperledger Fabric uses RAFT algorithm for the log replication process [34]. Once a leader is elected, all messages

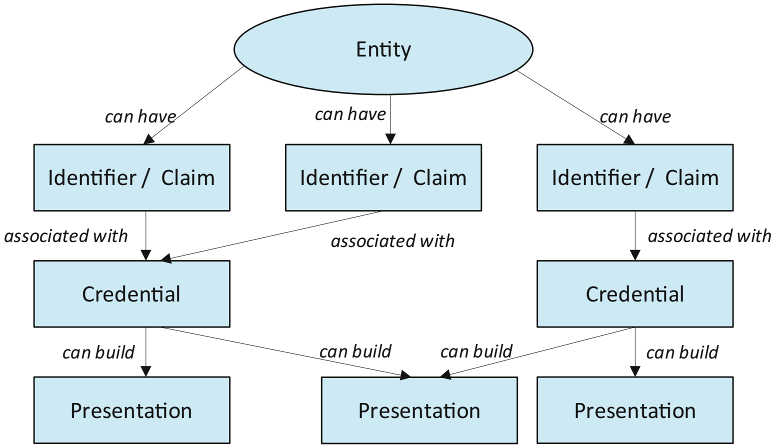


Fig. 10 Relationship between verifiable claim, verifiable credential, and verifiable presentation [26]

are sent via the leader. The leader will propagate the messages to all nodes, and the nodes then validate and write the messages. The nodes will also send a response to inform the leader that the message has been validated and written. Hyperledger Indy uses plenum [35] algorithm, which is an improved version of Redundant Byzantine Fault Tolerance. The consensus algorithm uses three-phase commit on the request to ensure that the ledger contains entries that are ordered and validated.

Network layer is used for information dissemination between participating peers [36]. *Data layer* consists of Merkle tree, a binary tree of hashes to offer integrity and non-repudiation for blockchain. Transactions are digitally signed in data layer using asymmetric cryptography.

Infrastructure layer is where all peer nodes reside. Organization uses certificate authority to assign X.509 digital certificates to all participating nodes recognized by the blockchain network. The nodes with virtualization using virtual machines or containers can support messaging services and storage of data [37].

Many blockchain networks have been developed for identity management. Notable works on identity management have been primarily conducted on the Hyperledger blockchain. Hyperledger Indy [38] is specifically created for self-sovereign identity management. This blockchain provides tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers so that they are interoperable with other blockchains. Indy provides built-in support for zero-knowledge proofs to avoid unwanted disclosure of identity attributes. When a verifiable claim is not considered true, zero-knowledge proofs enable identity owners to authenticate the possession of a credential without displaying the credential itself with the help of anonymous credential scheme [39].

Hyperledger Aries [40] is a spin-off of Hyperledger Indy, to realize interoperable self-sovereign identity which covers more on the client side components such as

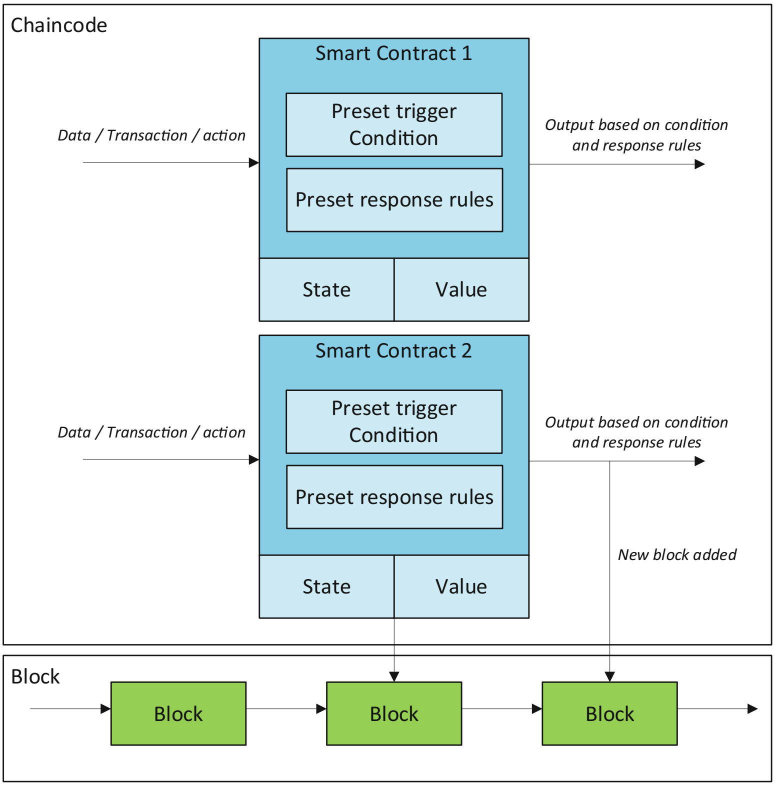
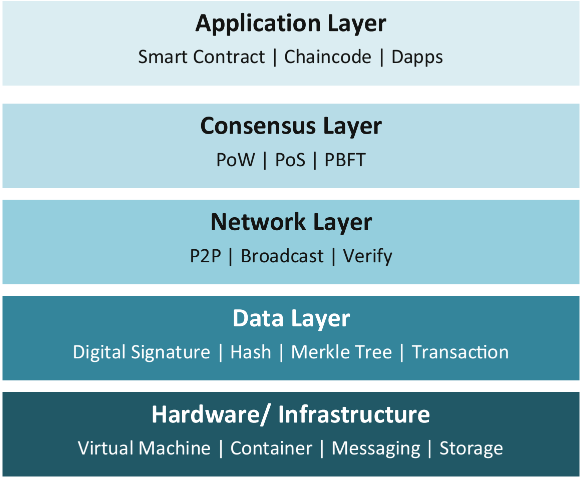


Fig. 11 Structure of smart contract and chaincode [32]

Fig. 12 Architecture of blockchain DLT [33]


Application Layer
Smart Contract | Chaincode | Dapps
Consensus Layer
PoW | PoS | PBFT
Network Layer
P2P | Broadcast | Verify
Data Layer
Digital Signature | Hash | Merkle Tree | Transaction
Hardware/ Infrastructure
Virtual Machine | Container | Messaging | Storage

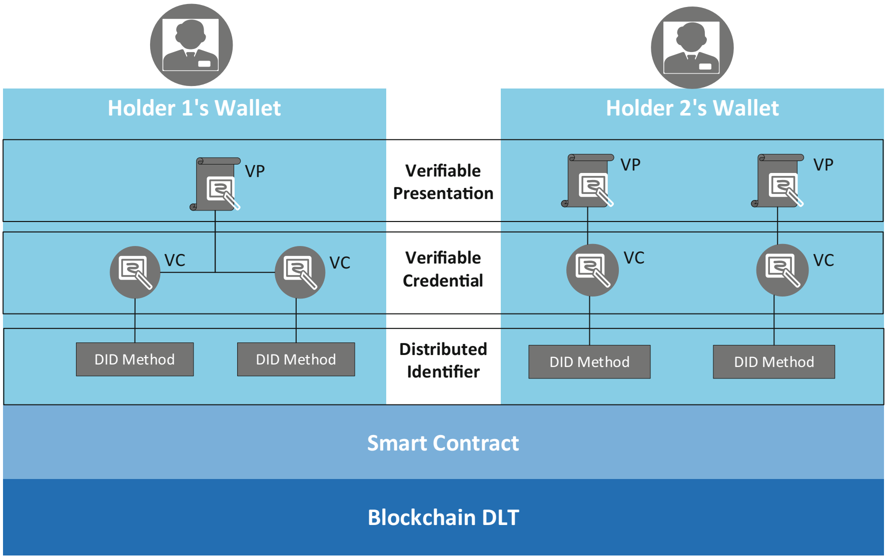


Fig. 13 Building blocks for blockchain-based self-sovereign identity management

wallet services and agent protocols. The blockchain focuses on providing tools and features to create, transmit, and store verifiable credentials in a wallet. This project utilizes cryptographic libraries and key management schemes provided by Hyperledger Ursa [41].

Another project under the Hyperledger project umbrella is Hyperledger Fabric [42, 43] which supports digital assets, distributed logic through chaincode, and the use of custom consensus through endorsement policies. Initially Fabric still lacked a key component for a decentralized identity, but TrustID was later incorporated in Hyperledger Fabric to simplify identity management in blockchain networks.

The trust framework is not shown in the architecture (Fig. 13) because trust can be implemented at all layers. The blockchain DLT serves as a root of trust in the architecture. Trust can also come from the decentralized identity layer and is managed depending on adopted DID standard. Verifiable credentials and verifiable presentations can have their own trust features implemented at a higher layer.

3 Types of Trust Model in Identity Management

One of the most cited definitions of trust is by Mayer et al. [44] "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party." Trust is determined by the trustor's

Table 1 Type of trust models based on flow of control

Type of trust model	Description
Centralized trust model	Top-down. Entities report trust rating to a trusted party
Decentralized trust model	Bottom-up. A peer-to-peer system for entities to determine trust rating
Distributed trust model	Bottom-up. Trust rating is shared among entities

Table 2 Types of trust models based on control of transaction

Type of trust model	Description
Static trust model	Rules pertaining to trust are defined by trust administration system
Dynamic trust model	Defines trust rating based on changing parameters

propensity to trust, ability, benevolence, and integrity of the trustee in their proposed model of trust.

Propensity to trust is the willingness to trust others across a broad spectrum of situations and trust targets. This suggests that every individual has some baseline level of trust that will influence that willingness to trust. *Ability* is also referred to as the competence of the trustee to do a given task. *Benevolence* is the disposition of goodwill toward the trusting party. And lastly, *integrity* is the trustor's perception that the trustee adheres to a set of principles that are acceptable to the trustors.

The goal of trust is to determine what course of action, if any, the trusting party is willing to take in relation to the trusted party. Based on the level of trust and the perceived risk, the trusting party may decide to take some action that involves some degree of risk taking. Trust level has a corresponding risk rating; a lower risk translates to higher level of trust.

Trust models are classified based on how they are controlled [20] as shown in Table 1. The NIST [25] defined the two main approaches as top-down and bottom-up, with the latter frequently associated with SSIDM principles. Top-down approaches to trust lead to centralization of information, control, and loss of individual privacy. The bottom-up approach to trust is taken to avoid these pitfalls.

These two approaches form a spectrum of trust models, i.e., centralized, decentralized, and distributed models which can support different types of governance structures and power delegation mechanisms. In a centralized system, trust level is exerted by just one entity (i.e., trust anchor, CA, board of trustees). In a decentralized system, there is no single controlling entity, and every entity makes their own decision on trust level. In distributed approach, the trust level is shared among entities, and trust computation is distributed across nodes. Nodes interact with each other to determine trust level.

A trust model can also be categorized based on control of transactions (Table 2). The static model follows pre-defined rules, but the dynamic model adjusts with different parameters and progress based on the previous cached data stored in a data store.

Table 3 Types of trust approach

Type of trust approach	Description	Advantages	Disadvantages
Reputation based	Reputation of an entity is the collected estimation of public's trust	Public trust is ingrained in all communities	Reputation of an entity is assumed, not earned
Policy based	Formal trust methodologies which play a main role in PKI	Highly scalable and manageable	Rogue certificates issued by CA
Evidence based	Performance of entities from previous transactions determines the trust level	Higher accuracy since trustworthiness is dynamically deduced from past behaviors	Higher computation cost and performance issues

The types of trust approach are categorized as reputation-based trust, policy-based trust, and evidence-based trust [20]. In reputation-based trust, the reputation of an entity is the collected estimation of the public's trust toward that entity. Generally, many entities in a community trust an entity that has a high reputation; an entity, which is required to build trust decision on a trustee, uses the reputation to compute or approximate the trust level of the trustee [45]. However, Forrester Research [46] introduced the concept of a zero-trust model which states that no trust should be assumed but instead trust should be continually validated. This concept has been adopted widely in the design and implementation of IT systems.

In policy-based trust, formal trust methodologies are used to support key certification, digital signature, and validation. For instance, in PKI model, a certificate authority (CA) supports data attribute certification and validation. Certificate policies play a main role in PKI trust which has been introduced since the introduction of PGP [47]. In evidence-based trust, performance of entities from previous transactions determines the trust level. Trust level is deduced from past behavior in terms of accuracy and honesty [48].

A summary of the trust approaches is presented in Table 3 with respective advantages and disadvantages.

4 Related Works on Blockchain-Based SSIDM Trust Models

This new approach to manage identity has many opportunities going forward. Initiatives to research and explore the possibilities of this technology come from individuals and companies as well as governments. There are several trust models that have been introduced by various researchers and organizations incorporating their best parameters and efficiency. Limitation and summary of related works are exhibited in Tables 4 and 5.

Table 4 Limitation of existing trust models

Solution	Trust model	Limitations
Sovrin [8]	Trustees and trust anchors play a role in building the Sovrin web of trust. This framework uses delegation of trust from pre-defined trust anchor	Not efficient because every new node in the network will add to the existing long chain. It is costly to maintain the trust chain, and a mesh of cross-certifying nodes does not scale well
uPort [51]	Trust management platform where enterprises can assign trust rating for digital identities using the tools that come with the product suite	Static, top-down approach of trust assignment, which is assumed, not earned
Evernym [53]	Operating as a trust management platform with a verifiable credential trust triangle between issuer, holder, and verifier	The trust control is static, but trust level can change dynamically according to actions and behaviors of entities. Entities should not be trusted by default
Jolocom [54]	Static trust management platform	No mechanism to compute trust in a decentralized manner
Quantifiable trust model [56]	Aggregated trust into attestation issuers. Uses calculated numerical trust metric instead of dedicated evaluation of a trusted third party	Security assumption of the trust model is based on preconfigured trust of identities
WiP [57]	Dynamic trust control which does not require entities' preconfigured trust relationships. Trustworthiness is computed based on their behavior over time	The proposed credibility value is a preset range which lacks tests and experiments to ensure its accuracy and usability in the environment
SCPKI [58]	Gradually builds a web of trust where users vouch for each other's identity attributes	It does not provide the trustworthiness of verifiable claims. Cost incurred to process transactions on Ethereum blockchain. Actions may be delayed by transaction processing time
Centralized trust registry [59]	Decentralized exchange of data but a centralized issuance of trustworthiness by having a trust registry	Trust management is centralized, hence inheriting all problems of a centralized trust model

Table 5 Summary of blockchain-based SSIDM and trust models

Solution	Description	Project type	Blockchain	Network	Trust flow	Trust control	Trust approach
Sovrin [8]	Decentralized global public utility for self-sovereign identity	Nonprofitfoundation	Hyperledger Indy	Public permissioned	Decentralized	Static	Policy based, reputation based
uPort [51]	Ethereum-based identity management platform	Company	Ethereum	Public/private	Decentralized	Static	Policy based, reputation based
Evernym [53]	Identity and trust management platform	Company	Hyperledger Indy	Public/private	Decentralized	Static	Policy based, reputation based
Jolocom [54]	Open-source protocols for decentralized identity management	Open source	Generic	Public/private	Decentralized	Static	Policy based, reputation based
Quantifiable trust model [56]	Qualitative assurance levels based on preset intervals	Academic	Generic	Not specified	Distributed	Dynamic	Evidence based
WiP [57]	Trustworthiness of entities and verifiable claims	Academic	Generic	Not specified	Distributed	Dynamic	Evidence based

SCPKI [58]	A smart contract-based PKI and identity system	Academic	Ethereum	Public/private	Decentralized	Static	Policy based
Centralized trust registry [59]	Blockchain-based SSIDM with decentralized exchange of data and centralized trust registry	Academic	Ethereum	Not specified	Centralized	Dynamic	Policy based

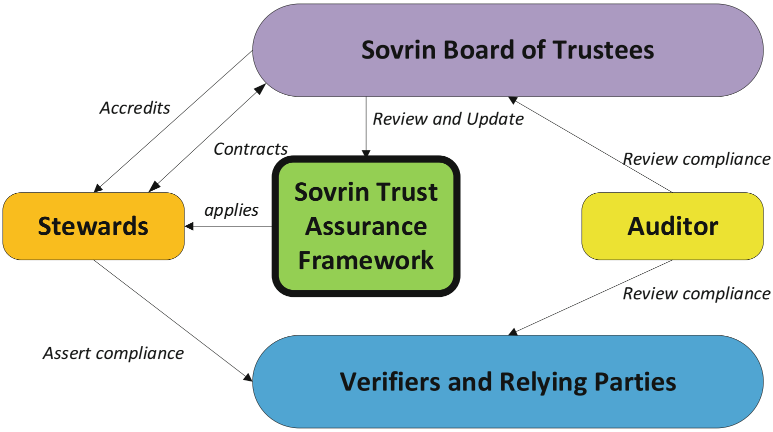


Fig. 14 Sovrin trust assurance framework

A. Sovrin

Sovrin [8] is a private, global, nonprofit foundation to govern self-sovereign identity network. It is the first of its kind trust framework for advocating self-sovereign identity. The foundation believes in portable identity which allows general users to perform verification and authentication of identity, while preserving personal information. The foundation proposed the idea of having identity claim, credentials to replace the use of physical documents. Identity data includes social security number, name, address, education, employment data, etc.

The Sovrin protocol is built on public permissioned blockchain using open standards and the open-source Hyperledger Indy project. All Sovrin identifiers and public keys are pseudonymous by default. Sovrin uses pairwise-pseudonymous identifiers, a separate decentralized identity (DID) for every relationship.

Sovrin network comprises an identity network and a trust network. The trust network executes a proprietary trust framework (Fig. 14). Identity owners can use their Sovrin identities to establish a basic level of trust [49]. Trustees and trust anchors play a role in building the Sovrin web of trust. The web of trust mechanism is not the most efficient because every new node in the network will add to the existing long chain. This makes it very costly to maintain the trust chain, and a mesh of cross-certifying nodes does not scale well [50].

Sovrin's board of trustees are also required to accredit stewards which later apply the trust assurance framework. Stewards also assert compliance to other verifiers and relying parties. All transactions will be reviewed for compliance by the auditor.

Another problem with the Sovrin web of trust is the use of delegated trust similar to PGP 5.0. This concept involves the delegation of trust from a pre-defined trust anchor. Delegated trust is hierarchical and centralized, hence inheriting all problems of a centralized trust model.

B. uPort

uPort [51] aims to be an open self-sovereign identity system that operates on the Ethereum blockchain. uPort enables users to handle their identity and credential in a secure manner like every other SSI project. It provides portability of identity and credential data to other blockchain network such as Bitcoin. uPort utilizes two protocols, namely, the identity and claim protocols. The Identity Protocol is an address on a decentralized network, controlled by a private signing key, and makes use of a decentralized public key infrastructure (PKI) that enables signature validation. On the other hand, the claim protocol refers to a standard message format that enables source attribution and facilitates interoperability between various blockchain and identity networks. The claim protocol supports the JSON Web Token (JWT) and Ethereum transactions. Among products and tools offered by uPort is the self-sovereign wallet. Being unmanaged and fully self-sovereign, there is no entity identity proofing of user accounts in uPort [52].

uPort also offers uPort Serto, a product suite for organizations to set up identity ecosystems. The Serto product suite includes a mobile wallet, a credential management platform, a privacy preserving graph data, and a credential discovery platform. uPort Serto took the approach of mapping verifiable credentials and decentralized identifiers (DIDs) into existing ecosystems based on local law, international agreements, and even internal business rules which gives them the advantage of fulfilling data compliance such as General Data Protection Regulation (GDPR).

uPort itself is a trust management platform; therefore, the trust control is static and archaic. Enterprises can assign trust rating for digital identities using the tools that come with the product suite.

C. Evernym

Evernym [53] is another blockchain-based SSIDM built on Hyperledger Indy [38]. This project introduces a concept called "Trust over IP" (ToIP). This is an architecture that can establish trust between peers over the network. This solution ensures interoperability with Hyperledger Aries [40] and open standards such as W3C DIDs [26] and W3C verifiable credentials [24]. Like uPort, Evernym operates as a trust management platform with a verifiable credential trust triangle between issuer, holder, and verifier. The trust control is also static, using policy- and reputation-based approaches.

D. Jolocom

Jolocom [54] is an open-source project to provide sets of protocols for building a dynamic self-sovereign identity ecosystem. The entire stacks are based on open standards such as W3C DIDs and verifiable credentials. Jolocom also provides a smart wallet for users to create and manage identities in a visual and user-friendly manner. These sets of protocols are compatible with any public permissioned, public permissionless, or private blockchain network. The project aims to realize a truly decentralized and modern digital identity management. Jolocom is playing the role of trust management platform; therefore, trust control is static. There is no mechanism to compute trust in a decentralized manner based on the exchange of verifiable claims for associated identities in the ecosystem.

E. Quantifiable Trust Model

Grüner et al. [55] analyzed decentralized IDM trust requirements based on blockchain. Their paper presented a comparison study of trust requirements for traditional IDM and decentralized IDM through defining topology patterns. The topology pattern reflects the relevant entities and their interaction paths. Trust requirements for isolated, centralized, federated, and decentralized IDM were formally defined, compared, and presented. The authors concluded that the benefit of decentralized trust model is reduced reliance of trust toward the identity and attribute providers.

The authors also proposed the concept that replaces trust with a central identity provider by aggregated trust into attestation issuers [56]. The calculated numerical trust metric serves as an independent basis for the definition of assurance level to simplify and automate reasoning about trust by service providers without requiring a dedicated evaluation of a trusted third party. However, the security assumption of the trust model is based on preconfigured trust of identities.

F. WiP

Bendiab et al. presented a blockchain-based decentralized model [57] to provide authentication and trust computation. This trust model does not require entities' preconfigured trust relationships, but trustworthiness is computed based on their behavior over time. The behavior data can be captured from the transactions stored in the blockchain. The authors proposed a much-desired dynamic trust control. Nevertheless, the proposed credibility value is a preset range which lacks test and experiments to ensure its accuracy and usability in the environment.

G. SCPKI

Al-Bassam et al. proposed a smart contract-based PKI (SCPKI) [58], an alternative PKI approach that uses smart contracts to build a decentralized web of trust adopted from the Pretty Good Privacy (PGP) [47] system. It addresses the issue of rogue certificates issued by certificate authorities in traditional public key infrastructures. The smart contract allows users to add, sign, and revoke attributes. This gradually builds a web of trust where users vouch for each other's identity attributes, but it does not provide the trustworthiness of verifiable claims. Due to the implementation of smart contracts on the Ethereum platform, charges are incurred for identity transactions as a result of the cost of paying the blockchain miners to process a transaction. Lastly, actions may be delayed by transaction processing time.

H. Centralized Trust Registry

Baars et al. [59] claim that reliability of an identity is only as good as the authority issuing that identity so a system should not be dependent on a trusted third party. Although there are many cases where community-based reputation systems (distributed reputation-based approach) can be useful, most business transactions are required to trace back a chain of responsibility in case things go wrong. The system should also allow acquirers to determine the validity of a claim. The project proposed a decentralized exchange of data but a centralized issuance of trustworthiness by having a trust registry. This way the SSIDM is independent from the systems of the issuer and allows availability of claims even when the issuer itself stops its services.

5 Research Directions

Existing trust models in SSIDM still very much rely on the web of trust, as well as governance and trust frameworks in a centralized manner. There is a need for research in this area to improve trust models of a decentralized nature. More use cases and prototypes are also needed to evaluate their accuracy and usability.

A trust engine automates the computation of trustworthiness of digital identities and verifiable credentials. In recent years, machine learning and deep learning have proven to be remarkably good at solving complex problems such as computer vision, big data, and natural language processing. Machine learning also plays an important role in establishing and measuring trustworthiness [60]. By investigating useful features that are capable of distinguishing successful transactions from unsuccessful ones, sophisticated machine learning algorithms can be applied to analyze past transactions. If these algorithms manage to model efficiently what a successful or unsuccessful transaction is, they can be used to predict the trustworthiness of a potential transaction [61].

Trustworthiness of SSIDM stakeholders can be facilitated by computational trust models, and the accuracy of trust rating can be effectively improved. There are a variety of attributes and multitudes of characteristics to support the computation of trustworthiness in SSIDM, for instance, the transaction history in account provisioning, revocation, and recovery; the number of verifiable claim exchange, claims, or counterclaims issued; and the number of correct or incorrect attested claims.

These are data that are globally readable on the ledger. The immutable data on the blockchain can be trusted by all stakeholders. Therefore, instead of having a centralized certificate authority, the data on ledger can provide a richer set of parameters that could be explored to determine trust rating in a dynamic manner.

Additionally, trust and reputation from other layers such as DIDs and digital wallet in the ecosystem can be considered. Trust rating from blockchain and DLT consensus and peer-to-peer communication layer can also be incorporated to achieve a comprehensive trust framework (Fig. 15).

The SSIDM architecture presented in Sect. 2 is still constantly evolving; therefore, it is difficult to ensure the interoperability of trust model with different

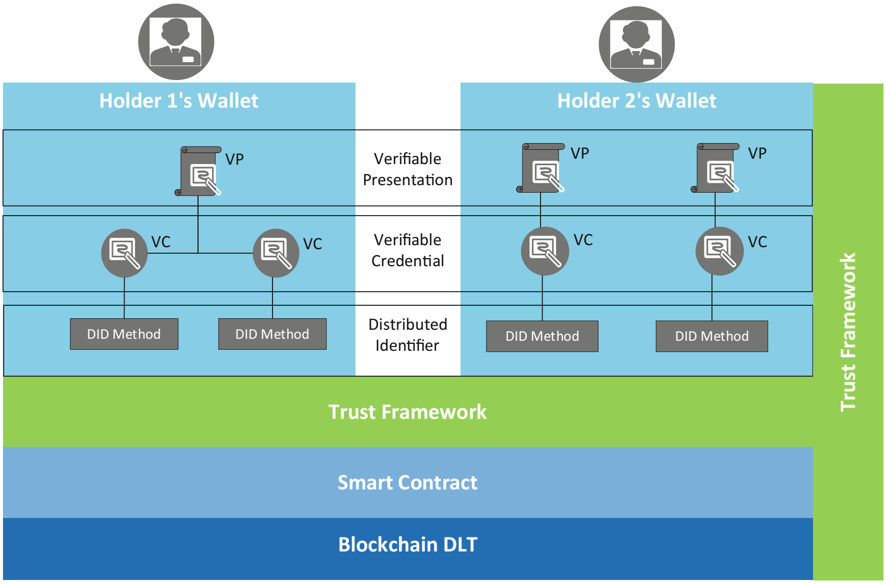


Fig. 15 Trust framework for blockchain-based SSIDM

ledgers. There is a challenge to ensure that the trust framework comprising of trust model and trust engine is working as desired in a variety of SSIDM platforms.

6 Conclusion

In this paper, we presented a comprehensive review of the architecture, components, trust management, and approaches for blockchain-based SSIDM. Despite blockchain being an effective technology for self-sovereign identity management, it does not comprise an effective trust framework. As with any other IDM solutions, blockchain-based SSIDM requires a unique model to ensure trustworthiness of entities in the ecosystem.

Every trust management approach in the literature has its own strengths and weaknesses. Existing solutions are lacking in certain ways especially the trust computation in digital identities and verifiable claims. We believe, with the introduction of a dynamic computation of trustworthiness, this open issue can be addressed and subsequently can break the adoption barrier of blockchain-based SSIDM.

Acknowledgments This work was supported in part by the Fundamental Research Grant Scheme, Ministry of Higher Education Malaysia (FRGS/1/2018/ICT04/UNITAR/03/1).

References

1. Y. Liu et al., Blockchain-based identity management systems: A review. J. Netw. Comput. Appl. **166**, 102731 (2020)
2. S.Y. Lim, M.L.M.K, T.F. Ang, Security issues and future challenges of cloud service authentication. Acta Polytechnica Hungarica **14**(2), 69–89 (2017)
3. M. Swan, *Blockchain: Blueprint for a New Economy* (O'Reilly Media, Inc, 2015)
4. D.R. Andrew Tobin, The Inevitable Rise of Self-Sovereign Identity. 2017
5. S.Y. Lim et al., Blockchain technology the identity management and authentication service disruptor: A survey. Int. J. Adv. Sci. Eng. Inf. Technol **8**(4–2), 1735–1745 (2018)
6. P.D.F. Aaron Wright, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (2015)
7. M. Schäffner, Analysis and evaluation of blockchain-based self-sovereign identity systems. Master's thesis (2019)
8. D. Reed, J. Law, D. Hardman, The technical foundations of Sovrin. The Technical Foundations of Sovrin (2016)
9. L. Lesavre, *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems* (2020)
10. A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision. Decis. Support. Syst. **43**(2), 618–644 (2007)
11. J.-H. Cho, K. Chan, S. Adali, A survey on trust modeling. ACM Computing Surveys (CSUR) **48**(2), 1–40 (2015)
12. W. Dou, *The research on trust-aware P2P topologies and constructing technologies [Ph. D. Thesis]* (National University of Defense Technology, Changsha, 2003)
13. E. Gilman, D. Barth, *Zero Trust Networks* (O'Reilly Media, Incorporated, 2017)
14. J.M. De Valmaseda, G. Ionescu, M. Deriaz, TrustPos model: Trusting in mobile users' location, in *International Conference on Mobile Web and Information Systems*, (Springer, 2013)
15. Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of Things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
16. H. Yu et al., A survey of trust and reputation management systems in wireless communications. Proc. IEEE **98**(10), 1755–1772 (2010)
17. W. Sherchan, S. Nepal, C. Paris, A survey of trust in social networks. ACM Comput. Surveys (CSUR) **45**(4), 1–33 (2013)
18. J.-H. Cho, A. Swami, R. Chen, A survey on trust management for mobile ad hoc networks. IEEE Commun. Surveys Tutorials **13**(4), 562–583 (2010)
19. T. Grandison, M. Sloman, A survey of trust in internet applications. IEEE Commun Surveys Tutorials **3**(4), 2–16 (2000)
20. A.B. Filho et al., A study on trust models in cloud computing, in *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, (2019)
21. A. Albuali, T. Mengistu, D. Che, ZTIMM: A zero-trust-based identity management model for volunteer cloud computing, in *International Conference on Cloud Computing*, (Springer, 2020)
22. K. Bendiab et al., A novel Blockchain-based trust model for cloud identity management. arXiv preprint arXiv:1903.04767 (2019)
23. A. Mühle et al., A survey on essential components of a self-sovereign identity. Comput. Sci. Rev **30**, 80–86 (2018)
24. D.L. Manu Sporny, D. Chadwick, *Verifiable Credentials Data Model 1.0*. 2019.; Available from: https://www.w3.org/TR/vc-data-model/
25. L. Lesavre et al., A taxonomic approach to understanding emerging blockchain identity management systems. arXiv preprint arXiv:1908.00929 (2020)
26. M.S. Drummond Reed, D. Longley, C. Allen, R. Grant, M. Sabadello, *Decentralized Identifiers (DIDs) v1.0 Core Architecture, Data Model, and Representations* (W3C: W3.org, 2021)

27. N. Naik, P. Jenkins, Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology, in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, (IEEE, 2020)
28. X. Li et al., A survey on the security of blockchain systems. Futur. Gener. Comput. Syst. **107**, 841–853 (2020)
29. T.W. Brent Zundel, M. Varley, M. Csernai, *Peer DID Method Specifcation Report* (Rebooting the Web of Trust VIII, 2019)
30. K.K. Daniel Buchner, *DID Credential Manifest* (GitHub, 2019)
31. T.F.C. Jeff Bohrer, S. Gance, M. Gylling, V. Haag, A. Hripak, N. Otto, J. Pitcher, A. Reis, J. Schmidt, Open Badges 2.0 Implementation Guide IMS Final Release (2018)
32. H. Fabric, *Smart Contracts and Chaincode* (2020); Available from: https://hyperledger-fabric.readthedocs.io/en/release-2.2/smartcontract/smartcontract.html.
33. V. Acharya, A.E. Yerrapati, N. Prakash, *Oracle Blockchain Quick Start Guide: A Practical Approach to Implementing Blockchain in your Enterprise* (Packt Publishing Ltd, 2019)
34. H. Howard, *ARC: Analysis of Raft Consensus* (University of Cambridge, Computer Laboratory, 2014)
35. HyperledgerIndy. *Indy's Plenum Documentation*. 2018; Available from:https://hyperledger-indy.readthedocs.io/projects/plenum/en/latest/main.html.
36. T. Neudecker, H. Hartenstein, Network layer aspects of permissionless blockchains. IEEE Commun. Surveys Tutorials **21**(1), 838–857 (2018)
37. S.S. Gupta, *Blockchain.* IBM Onlone (http://www.ibm.com), 2017
38. LinuxFoundation. *Hyperledger Indy* 2020; Available from: https://github.com/hyperledger/indy-node#about-indy-node
39. D.K. Michael Lodder, *Anonymous credentials 2.0*. 2019.; Available from: https://wiki.hyperledger.org/download/attachments/6426712/Anoncreds2.1.pdf?version=1&modificationDate=1551851745000&api=v2
40. LinuxFoundation. *Hyperledger Aries* 2020; Available from: https://github.com/hyperledger/aries
41. LinuxFoundation. *Hyperledger Ursa* 2020; Available from: https://github.com/hyperledger/ursa
42. Androulaki, E., et al., *Hyperledger fabric: a distributed operating system for permissioned blockchains*, in *Proceedings of the Thirteenth EuroSys Conference*. 2018, Association for Computing Machinery: Porto, Portugal. p. Article 30
43. LinuxFoundation, *Hyperledger Fabric* 2020; Available from: https://github.com/hyperledger/fabric#releases
44. R.C. Mayer, J.H. Davis, F.D. Schoorman, An integrative model of organizational trust. Acad. Manag. Rev. **20**(3), 709–734 (1995)
45. P.S. Challagidad, V. Reshmi, M.N. Birje, *Reputation Based Trust Model in Cloud Computing* (2017)
46. J. Kindervag, *No More Chewy Centers: The Zero-Trust Model of Information Security* (Forrester Research, Inc., dated Mar, 2016) 23
47. S. Garfinkel, *PGP: Pretty Good Privacy* (O'Reilly Media, Inc, 1995)
48. A. Selvaraj, S. Sundararajan, Evidence-based trust evaluation system for cloud services using fuzzy logic. Int. J. Fuzzy Syst **19**(2), 329–337 (2017)
49. Sovrin, Sovrin Provisional Trust Framework (2017)
50. D. Weller, R. Dijksman, *Blockchain's Relationship with Sovrin for Digital Self-Sovereign Identities* (2019)
51. R.H. Christian Lundkvist, J. Torstensson, Z. Mitton, M. Sena, *UPORT: A Platform for Self-Sovereign Identity* (2016)
52. P. Mell, J. Dray, J. Shook, Smart contract federated identity management without third party authentication services. arXiv preprint arXiv:1906.11057 (2019)
53. C. Grinyer, Designing blockchain based services, in *Tensions, Paradoxes+ Plurality: Proceedings of the ServDes. 2020 Conference*, (Linköping University Electronic Press, 2020)

54. J.L. Charleen Fei, E. Rusu, K. Szawan, K. Wagner, N. Wittenberg, *Jolocom: Decentralization By Design* (2018)
55. A. Grüner et al., *A Comparative Analysis of Trust Requirements in Decentralized Identity Management* (Springer International Publishing, Cham, 2020)
56. A. Grüner et al., 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)*, (IEEE, 2018)
57. K. Bendiab et al., WiP: A novel blockchain-based trust model for cloud identity management, in *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing*, (IEEE, 2018)
58. M. Al-Bassam, *SCPKI: A Smart Contract-Based PKI and Identity System* (2017), pp. 35–40
59. D. Baars, Towards self-sovereign identity using blockchain technology (2016)
60. X. Liu, A. Datta, E.-P. Lim, *Computational Trust Models and Machine Learning* (CRC Press, 2014)
61. H. Jiang et al., To trust or not to trust a classifier, in *NeurIPS*, (2018)

Shu Yun Lim is currently a senior lecturer and Ph.D. candidate at the Faculty of Business and Technology, UNITAR International University, Malaysia. She obtained a bachelor's degree in information technology majoring in information system engineering from Multimedia University, Malaysia, in 2005 and a master of engineering in ubiquitous network engineering from Dongseo University, South Korea, in 2007. From 2007 to 2010, she was a researcher in British Telecom Malaysian Research Centre, Malaysia. She has published extensively in the area of information security and network security. Currently, her research interests include forensics analysis of cloud services, authentication, and identity management solutions, in particular self-sovereign identity management on blockchain DLT.

Omar Bin Musa is currently an associate professor at the Faculty of Business and Technology, UNITAR International University. He graduated with a bachelor's degree in electronics engineering from SUNY College at Buffalo, NY. He completed an MBA in operations management at Ohio University, Athens, Ohio, in 1988. He started his academic career in 1990 at the Faculty of Economics and Management Sciences, International Islamic University Malaysia (IIUM). He then worked in the IT industry from 1997 to 2004 and returned to academia in 2005. His current research interests are in strategic IT management, business intelligence and analytics, and Blockchain Technologies and Applications. AP Omar is a recipient of several ongoing research and industry grants including the Fundamental Research Grant Scheme from the Ministry of Higher Education, Malaysia.

Bander Ali Saleh Al-Rimy is a senior lecturer at Universiti Teknologi Malaysia (UTM), Johor, Malaysia. He received the B.Sc. degree in computer engineering from the Faculty of Engineering, Sana’a University, Yemen, in 2003; the M.Sc. degree in information technology from OUM, Malaysia, in 2013; and the Ph.D. degree in computer science (information security) from the Faculty of Engineering, Universiti Teknologi Malaysia (UTM), in 2019. His research interests include but are not limited to malware, IDS, network security, and routing technologies. Dr. Al-Rimy has been a recipient of several academic awards and recognitions including but not limited to the UTM Alumni Award, the UTM Best Postgraduate Student Award, the UTM Merit Award, the UTM Excellence Award, the OUM Distinction Award, and the Best Research Paper Award.

Abdullah Almasri is currently an assistant professor at the School of Mathematical and Computer Sciences, Heriot-Watt University Malaysia Campus. He graduated from Universiti Kebangsaan Malaysia (UKM), in 2015. He got his master of computer applications (MCA) from Jamia Hamdard University, New Delhi, India, in 2006 and his diploma of postgraduate in informatics and B.Sc. (mathematics, informatics section) from Al-Baath University, Syria, in 2003 and 2002, respectively. He worked at the Faculty of Business and Technology (UNITAR International University) from 2015 to 2020. His research is focused on artificial intelligence, machine learning, and deep learning and, most recently, blockchain technology.