Engineered Science
DOI: https://dx.doi.org/10.30919/es1629

A Self-Sovereign Identity Framework for Context-Aware De-Centralized Identifier Creation and Credential Verification

Shailaja N. Lohar,[1,*] Sachin D. Babar[2] and Parikshit N. Mahalle[3]

Abstract

Digital Identity is a key concept in the digital era. It is very important as it impacts how we interact, transact, and secure our information online. Several systems, like Federated and User-centric, are the basis for digital identity management. We must enhance this identity for data security and integrity. It is necessary for strengthening an identity system. A digital Identity concept known as Self-Sovereign Identity allows users to fully own their identification related data without depending on central authority. It is a strong contender for an efficient identity management system. SSI's strengths are its full ownership and selective disclosure of user credentials, without a third party verification. SSI uses Decentralized Identifiers as unique Identifiers. It uses encrypted identity proof via Verifiable Credentials. A peer-to-peer distributed file system called the InterPlanetary File System (IPFS) makes it possible to store and share data in a decentralized, content-addressable way. Verifiable credentials are stored on IPFS, which eliminates the need for centralized servers and provides decentralized, permanent, and tamper-resistant storage. This work also uses zk-SNARKs to selectively disclose identity-related information. This paper proposes a new Digital Identity Management framework. It is based on SSI methodology and principles. The work has the Blockchain as its core network. It gives strong security and integrity to the user identity data. Also, the proposed approach is validated against state-of-art Identity management systems.

Keywords: Digital identity management; Blockchain; De-centralized identity; Metamask; Smart contract; User-centric authentication.
Received: 06 March 2025; Revised: 19 June 2025; Accepted: 24 June 2025
Article type: Original research.

1. Introduction

Identifying and verifying individuals, organizations, or entities—whether in the physical or digital world—typically involves three key elements: claims, proofs, and verification as shown in Fig. 1, These fundamental components ensure the uniqueness, authenticity, and security of identities. In digital contexts, managing proofs associated with identity claims is particularly complex and is traditionally handled by various Identity Management (IdM) systems. With the exponential growth of internet users, concerns about the effectiveness, security, and privacy of Digital Identity Management Systems have intensified. Conventional identity systems, especially those based on centralized architectures, have been increasingly exposed to vulnerabilities such as data breaches, unauthorized access, lack of user control, and insufficient interoperability. These limitations undermine user trust and raise significant privacy risks.

In response to these challenges, Self-Sovereign Identity (SSI) has emerged as a transformative paradigm. Introduced by Christopher Allen,[1] SSI shifts control of identity from centralized authorities to individuals themselves. It empowers users to create, own, and manage their digital identities independently. Central to this shift is the use of decentralized technologies, especially blockchain,[2] which align naturally with the principles of SSI due to their properties such as immutability, tamper resistance, elimination of central points of failure, and enhanced transparency.

Blockchain-based identity management systems have already demonstrated potential in addressing many of the shortcomings of traditional models. Among these innovations, Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) play a pivotal role. DIDs are unique identifiers generated and managed independently of centralized registries,

[1]*Smt. Kashibai Navale College of Engineering (affiliated to Savitribai Phule Pune University (SPPU)), Vadgaon Budruk, Pune, Maharashtra, 411041, India*
[2]*STES's Sinhgad Institute of Lonavala, Pune, Maharashtra, 410401, India*
[3]*Department of Artificial Intelligence and Data science, Vishwakarma Institute of Technology, Pune, Maharashtra, 411037, India*
[*]*Email:* shailaja.lohar@gmail.com (S. N. Lohar)

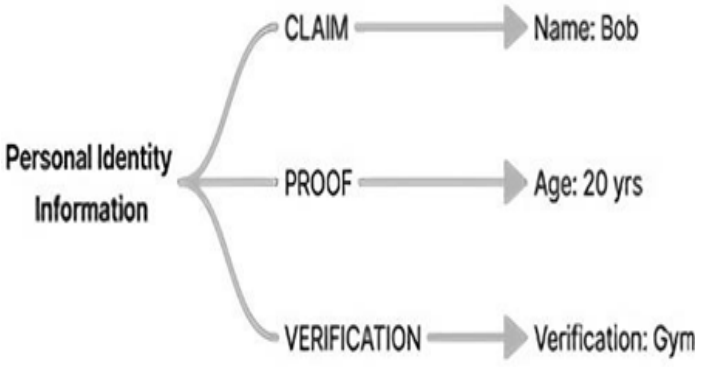

Fig. 1: Identity management in physical world.

while VCs serve as cryptographically verifiable proofs of identity-related claims as depicted in Fig. 2, These elements, when combined with cryptographic techniques such as zero-knowledge proofs (ZKPs), allow individuals to selectively disclose only necessary attributes without revealing full identity information—greatly enhancing privacy.

This paper proposes a blockchain-based decentralized identity solution built on the Ethereum platform. The system integrates smart contracts, IPFS (InterPlanetary File System),[3] and DIDs, in accordance with the standards established by the W3C.[4] The approach ensures that each identity is uniquely linked to a wallet address, allowing secure and private interactions in digital environments. Selective disclosure is enabled through zero-knowledge proofs, giving users full control over what identity attributes they wish to reveal.

The motivation for this work stems from the serious security and privacy limitations of existing centralized identity systems. Centralized models are prone to single points of failure, where data stored in centralized repositories becomes a lucrative target for cyberattacks. Breaches at such points can compromise millions of identities at once.[5] Additionally, these systems often share user data with third parties—sometimes without user consent—for marketing or analytics, further diminishing user privacy and control.

Unauthorized access and misuse of personal information—whether by external attackers or internal actors—remain pressing concerns. Moreover, federated systems such as OAuth-based logins allow cross-platform tracking and profiling, resulting in erosion of user autonomy. Once identity data is submitted in such systems, users typically lack the ability to control, revoke, or delete it. The inability to selectively disclose specific attributes also results in overexposure of personal information.

This paper addresses these critical issues by proposing a decentralized identity framework that uses smart contracts, zk-SNARKs, and blockchain-based verification. The solution eliminates single points of failure, enhances privacy via selective disclosure, reduces on-chain data exposure, and provides transparent, auditable identity interactions. While decentralized identity systems introduce their own challenges—such as cost, scalability, and complexity—they offer a more resilient, user-centric, and privacy-preserving alternative to traditional models.

2. Related work

Identity management networks that leverage blockchain technology eliminate the need for intermediaries, offering users full control over their identities through cryptographic keys. This decentralization ensures that identity systems cannot be shut down or manipulated without consent, making blockchain a foundational component in Self-Sovereign Identity (SSI) systems.[6]

The Casper platform's SSI system integrates zero-knowledge proof mechanisms to validate identity information. This blockchain-powered identity system addresses the limitations of centralized identity management by enhancing privacy and user autonomy.[7]

According to the authors, the introduction of the General Data Protection Regulation (GDPR) in the EU emphasizes transparency, data portability, and privacy by design. SSI aligns well with these principles by allowing selective sharing of personal data and providing maximum control to individuals.[8]

Decentralized Identifiers (DIDs) support SSI by offering flexible and cost-effective identity solutions, especially for IoT devices. These identifiers enable users to manage, create, or discard identities as needed, enhancing privacy and sovereignty.[9]

Blockchain significantly enhances SSI by enabling decentralized governance, scalability, and permissionless identity sharing through mechanisms like DIDs and verifiable claims. These technologies also support private digital asset transfers without intermediaries.[10]

A decentralized social media system has been proposed using Ethereum and IPFS, where user information is managed on-chain and larger content is stored via IPFS. This system showcases the practical application of blockchain in digital identity and content storage.[11]

Decentralized identity models such as SSI have emerged to overcome the shortcomings of traditional IAM systems. Despite high expectations, blockchain-based IAM systems face slow adoption due to technical complexity and resistance from existing service providers.[12]

Fourteen core properties of SSI have been validated through foundational literature and integrated into a proposed architecture for decentralized digital identity management.[13]

Although DIDs and Verifiable Credentials (VCs) provide cryptographic assurance of identity, they lack native mechanisms to tie digital identities to real-world identities. Traditional systems rely on Certificate Authorities (CAs) for such linkage.[14]

A system utilizing Ethereum smart contracts and IPFS has been developed to manage SSI operations. The approach stores only encrypted identity data off-chain, reducing blockchain congestion and transaction costs.[15]

The Sovrin network gives users full control over which identity attributes they share. Verification of relying parties is supported through a web-of-trust model and the governance of the Sovrin Foundation.[16]

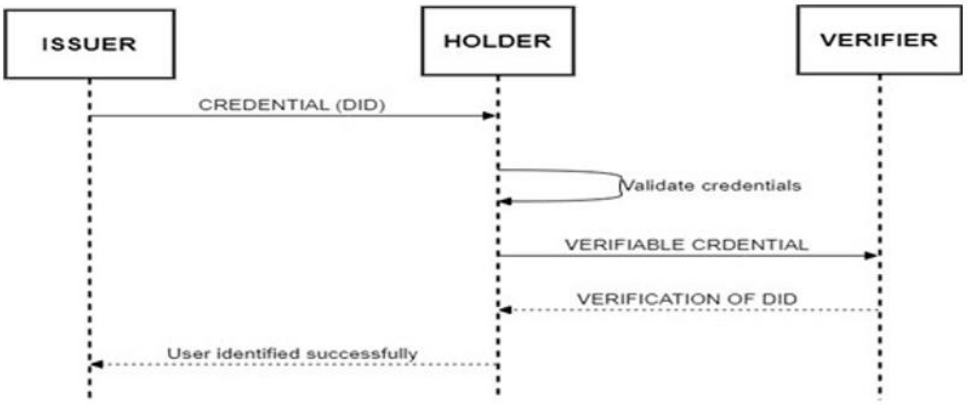

Fig. 2: Basic sequence diagram for SSI.

Blockchain-based identity systems have been proposed as alternatives to centralized systems like those from major corporations. These systems reduce the risk of data misuse and identity theft by allowing users to retain ownership over their personal data.[17]

A blockchain-driven healthcare identity framework has been proposed to support India's Ayushman Bharat Yojana. It uses proxy re-encryption and zero-knowledge proofs for secure, privacy-preserving sharing of electronic health records.[18]

3. Gap analysis

The previous section has elaborated the different Identity management systems based on de-centralized approach. It has also detailed the digital identity in terms of SSI framework and different aspects of these systems. However, need of control over Identity and secure verification are two main features that need to be addressed. In view of these observations, following table elaborates the Aspects of Identity management system, Problem to be addressed, and the Gap Analysis.

A decentralized approach better addresses the Issuer, verifier, and Holder. They are the three pillars of identity verification and authentication. The gap analysis highlights the need for an SSI-based Identity Management system. It must give users complete, secure control over their identity proof. Blockchain is a decentralized network. It will solve many problems caused by centralized identity management systems. Creating DID for every Identity context of a single user, makes the user, the sole owner of his Identity also securing the data.

4. Proposed work

The gap analysis explained in Table 1. It creates a need for an identity system that is: decentralized, secure, and privacy-protecting. It should have a single wallet for multiple user IDs. To achieve this, this paper proposes a system. It will use the Ethereum blockchain for wallet creation. This wallet will be linked to registered users via the DID specification. The DID will be contextual. To secure the identity, zk-snark[19] is used. It implements a zero-knowledge proof to verify user data. A smart contract links the wallet with a CID from IPFS. So, we are not storing any crucial data on the chain. We only have a cryptographically hashed DID on the IPFS.

The process of user registration, DID creation and Verification is depicted in Fig. 3. The registration will generate a unique DID with the help of IPFS content identifier and a contextual identifier which serves as a combination of Contextual ID and the wallet address generated and maintained on the Ethereum blockchain. The DID verification module is shown in the figure which shows the zero-knowledge proof for verifying the user age with the help of zk-SNARK algorithm. The first Algorithm explains the registration of users and generation of more credentials linked to same wallet.

4.1 Algorithm: create wallet input: Check for Registration
Output: DID (Decentralized Identifier)
Input: Request to create a Decentralized Identifier (DID)
Output: A newly generated DID associated with the user's wallet address.
Algorithm:
Connect to MetaMask Wallet:
The function Connect to Metamask is called to prompt the user to connect their MetaMask wallet. Once authorized, the connected wallet address is retrieved and stored in wallet Address.

1. Check for Registration:
The function If Address Linked(wallet Address) is executed to verify if the wallet address has already been registered with an existing DID.
   - If the function returns true, the system displays the message: "Address already registered," and the process is terminated.
   - If the function returns false, the algorithm proceeds to the next step.
2. Navigate to Issuer Interface:
The system invokes the function Navigate to Issuer to redirect the user to the credential issuance page.
3. Initiate Credential Issuance:
The user clicks on the "Issue More Credentials" button, handled by the function Click on Issue More Credentials, to begin the DID creation process.
4. Generate a New DID:

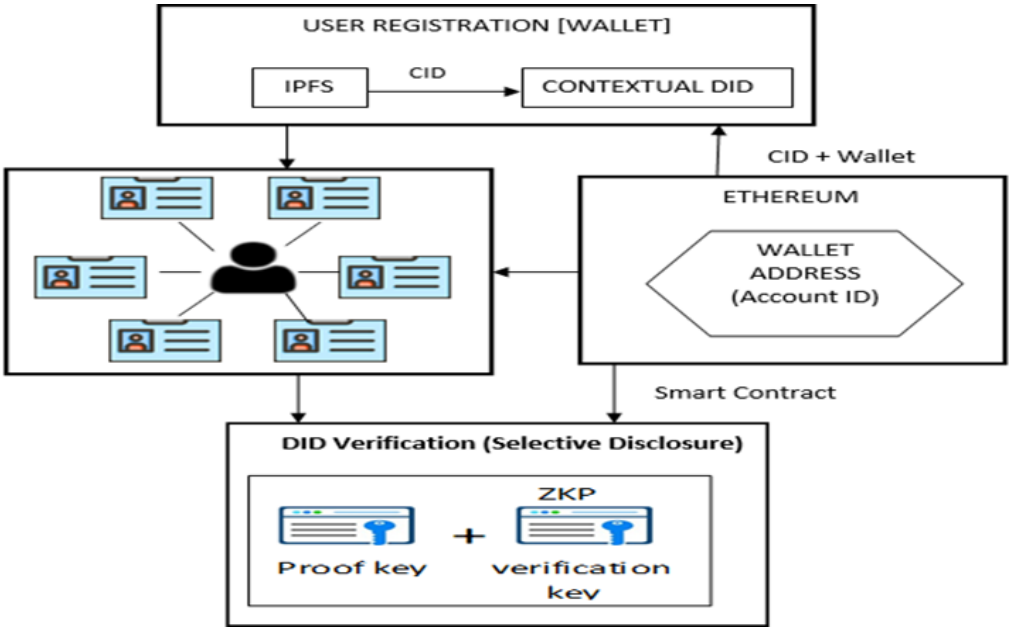

Fig. 3: Proposed system architecture.

5. The system calls Generate DID(wallet Address), which creates a new DID linked to the wallet address. The resulting DID is stored in the variable Did.

6. Return the DID: The newly generated DID is returned as the output of the algorithm for further identity operations. End

The Create Wallet algorithm is designed to generate a Decentralized Identifier (DID) for a user using their MetaMask wallet. It starts by connecting to MetaMask and retrieving the user's wallet address. The system then checks if this address is already registered. If it is, a message is displayed indicating that the address is already registered, and the process stops. If the address is not registered, the user is navigated to the issuer interface, where they proceed to issue more credentials. A DID is then generated based on the wallet address and returned to the user.

The main advantage of this algorithm is that it gives users control over their identity in a decentralized manner. It integrates well with blockchain tools like MetaMask, offering security and tamper resistance. The process is automated and user-friendly for those familiar with such tools. However, it lacks handling for possible errors like failed wallet connections or user rejection which can be considered in the future scope of this system.

The second Pseudo-code is for Issuing the DID to a user credential, the details of user are hashed and stored in the format did: name of user: hashed data.

Algorithm: Issuer
Input: Wallet Address
Output: DID (Decentralized Identifier)
1. Print: "Selecting Wallet Address" selected Address = Get Available Wallet Address() If selected Address is empty:
Selected Address = Display and Select
Print: "Entering holder details..." Prompt the user to:
a. Enter Credential Name
b. Enter Name of User
c. Enter Birth Year
Holder Details = {Credential Name, Name of User, Birth Year}
2. Generate DID:
Did = Blockchain. mint(selected Address, holder Details)
If Did == null:
Print: "DID minting failed"
Stop
3. Print: "DID generated successfully"
Return: Did
And encrypted with CID on IPFS along with the wallet address to link the credential to the particular user.

The next algorithm: Verifier, implements the zokrates library functions of proof key and verification key to disclose the age of user, without revealing other details, during verification.

Algorithm: Verifier Input: Wallet Address
Output: Verification Status
1. Select Wallet Address:
Selected Address = Select Wallet Address
2. Check DID Association: If Is Address Linked With DID(selected Address, generated DID)
Verification Status = ZKP Algorithm (generated DID)
Return verification Status Else
Print: "DID does not exist for the selected Wallet Address"
3. Stop

Finally, the ZKP algorithm is the strength of security for this system, which uses zokrates proof to reveal necessary information, hiding the other part from verifier.

Table 1: Security aspect in Identity Management and its Gap Analysis.

Aspect	Gap Analysis
Privacy and Control Over Personal Data	SSI gives users full control over their personal data. - Ethereum provides secure and transparent identity transactions. - Reduces reliance on third parties.
Interoperability Across Domains and Services	A single wallet managing multiple DIDs simplifies interactions across contexts. - Tailored DIDs for specific domains improve privacy and control. - Enhances user experience through seamless interoperability.
Decentralization and Trustless Environment	Ethereum smart contracts ensure a decentralized and trustless system. - Reduces dependence on intermediaries, improving security and transparency.
Immutable and Secure Data Storage Using IPFS	- IPFS enables decentralized and secure storage of identity- related data. - Documents and data can be stored off-chain and referenced on the blockchain.
Cost Efficiency and Scalability	Using a single wallet for multiple DIDs reduces redundancy and cost. - Smart contracts automate processes, lowering operational costs. - System architecture allows for scalability as adoption grows.
User Empowerment and Portability	Users gain ownership and control of their identity. - DIDs are portable and independent of specific platforms. - Seamless transfer of identity across services enhances accessibility and control.

Algorithm: ZKP Algorithm
Input: DID of User
Output: Verification of Age
1. Extract the CID from the given DID: cid = DID Parser. Extract CID (did)
2. Retrieve user data from the CID:
User Data = Extract User Data From CID(cid)
3. Extract the birth year from the user data: birth Year = Extract Birth Year (user Data)
4. Generate a proof using ZoKrates:
proof = Generate ZokratesProof (birth Year)
5. Verify the user's age:
- Calculate age = Current Year – birth Year
- If age < 18:
Print: "User under 18"
- Else
Print: "User 18+"
6. Return: Age verification result
7. Stop

The three algorithms mentioned above were used because they work together to provide a safe, user-controlled identification system that supports the ideas of self-sovereign identity. Users have control over their identity with the help of Create Wallet algorithm, which makes sure that a blockchain wallet is used to produce a unique, decentralized identify. By tying this identity to actual user information, the second algorithm personalizes it while preserving decentralization. Lastly, by offering a privacy-preserving way to verify private information, such as age, without disclosing all the information, the Verifier and ZKP Algorithm improve secrecy and confidence in identity verification. They work together to create a safe and comprehensive identity lifecycle, from creation to verification.

5. Mathematical framework

This model consists of comprehensive security evaluation based on the Components of the system and the mapping and relationship between them, with respect to security. The identity system is defined as:

$$\text{Identity System} = (U, W, DID, CID, D, \mathbb{Z}, SC) \quad (1)$$

where:
- U – Users
- W – Wallet
- DID – Decentralized Identifier
- CID – Content Identifier
- D – Identity Information
- $\mathbb{Z}$ – zk_SNARK proof
- SC – Smart Contract

User-to-Wallet Mapping
Each user ui is mapped to a unique wallet wi, as shown in Eq. (2):

$$\forall ui \in U, \exists wi \in W \text{ such that } fU(ui) = wi \quad (2)$$

Wallet-to-DID Mapping
Each wallet wi corresponds to a decentralized identifier DIDi, as defined in Eq. (3):

$$\forall wi \in W, \exists DIDi \in DID \text{ such that } fW(wi) = DIDi \quad (3)$$

Data-to-CID Mapping
User data Di is hashed to generate a unique content identifier CIDi, as shown in Eq. (4):

$$\forall Di \in D, \exists CIDi \in CID \text{ such that } fC(Di) = CIDi \quad (4)$$

Zero-Knowledge Proof Generation and Verification The proof Proofi is generated using zk-SNARKs for a specific statement P, as described in Eq. (5):

$$\text{Proof}i = \mathbb{Z}(Di, P) \quad (5)$$

Verification of this proof is done using Eq. (6):

$$V(\text{Proof}i, P) \rightarrow \{\text{True}, \text{False}\} \quad (6)$$

Smart Contract Logic

Smart contracts ensure the mapping and validation of identity data. The validity of the wallet-to-CID mapping is evaluated using Eq. (7):

$$SC(wi, CIDi) \rightarrow \text{Valid} \quad (7)$$

Proof verification is handled using the logic in Eq. (8):

$$SC.\text{verify}(wi, \text{Proof}i) = V(\text{Proof}i, P) \quad (8)$$

Security and Privacy Definitions

Security Function

Security is modeled as a combination of confidentiality, integrity, and availability, expressed in Eq. (9):

$$S = \text{Confidentiality}(Di) + \text{Integrity}(DIDi) + \text{Availability}(wi) \quad (9)$$

Privacy Function

Privacy is defined using a cryptographic hash function H, as shown in Eq. (10):

$$\text{Privacy}(Di) = H(Di) \quad (10)$$

This ensures that only the hash of Di is stored, not the raw data.

Formalized Security Proof

• Confidentiality:

Data Di is protected by hashing it into CIDi, ensuring confidentiality via Eq. (11):

$$CIDi = H(Di) \quad (11)$$

Since H is cryptographically secure, it is computationally infeasible to derive Di from CIDi.

• Integrity:

Integrity of mappings is maintained through smart contracts, as shown in Eq. (12):

$$SC(wi, CIDi) \rightarrow \text{Valid} \quad (12)$$

Proof authenticity is confirmed using Eq. (13):

$$SC.\text{verify}(wi, \text{Proof}i) = \text{True} \Longrightarrow \text{Proof}i \text{ is valid} \quad (13)$$

Availability:

$$\text{Wallets } wi, \text{DIDs } DIDi, \text{ and data identifiers } CIDi \text{ are accessible at all times} \quad (14)$$

supported by decentralized storage systems, as noted in Eq. (14)

Comprehensive Security Evaluation

Overall system security is quantified using Eq. (15):

$$S = \text{Confidentiality}(H(Di)) + \text{Integrity}(SC(wi, CIDi)) + \text{Availability}(wi, DIDi, CIDi) \quad (15)$$

This model is subject to the constraints in Eq. (16) and (17):

$$CIDi = H(Di) \quad (16)$$

$$V(\text{Proof}i, P) = \text{True} \quad (17)$$

IPFS and blockchain ensure the availability of CIDi, DIDi, wi.

The given mathematical model provides a clearer structure of the relationships and processes involved in the decentralized identity system. By defining functions, mappings, and security measures explicitly, the model emphasizes the integrity, privacy, and functionality of the system while ensuring that all key features are addressed effectively.

The framework outlines a decentralized identity system where different elements such as users, wallets, decentralized identifiers (DIDs), identity information, content identifiers (CIDs), Zero-Knowledge Proofs (zk-SNARKs), and smart contracts collaborate to facilitate secure and private identity management. Each user is associated with a distinct wallet, and every wallet is connected to a matching DID, which serves as the user's digital identity. The identity information of the user is hashed to create a CID, thereby safeguarding privacy and security by blocking direct access to sensitive information.

This system employs zk-SNARKs to produce privacy-preserving proofs that enable the verification of specific details, such as age, without disclosing the underlying data. Smart contracts play a role in managing and confirming the relationships between wallets and CIDs, ensuring that only authorized relationships are recognized, as well as in verifying the authenticity of zk-SNARK proofs. These smart contracts are essential for upholding data integrity and validating claims without revealing sensitive information. The foundation of security in the system relies on three fundamental principles: confidentiality, integrity, and availability. Confidentiality is accomplished through hashing and storing only the hash of the user's information, thus ensuring that unprocessed data remains protected. Integrity is upheld via smart contracts that verify the relationships between wallets and CIDs. Availability is guaranteed by utilizing decentralized networks such as IPFS for data storage and blockchain technology to keep the identifiers accessible.

The comprehensive security of the system is assessed by integrating these principles into one function that guarantees user data stays private, the data mappings remain unchanged, and key identifiers are perpetually accessible. The framework emphasizes how the interplay of these components establishes a secure, privacy-oriented decentralized identity system.

6. GDPR compliance of the system

The proposed system relies on decentralized identity management. It aims for privacy and security. It uses zk-SNARKs, blockchain, and DIDs. The GDPR (General Data Protection Regulation)[25] has governed personal data in the

Table 2: SSI Principles achieved through the system.

SSI Principle	Compliance with the Proposed system	Score
Decentralization	The system is built on a decentralized blockchain (Ethereum), using smart contracts and IPFS for decentralized storage. Since blockchain-based systems are decentralized by design, this principle scores high, though it's not perfect due to potential reliance on certain blockchain nodes or infrastructure.	9
User Control	Users manage their own Decentralized Identifiers (DIDs) and credentials, giving them full control over what information they share. This principle is rated the highest as it fits perfectly with the core of Self-Sovereign Identity systems.	10
Consent	User consent is a major component of the system, and credentials are only issued and verified based on the user's approval. While near-perfect, there might be edge cases where implicit or platform-specific consent mechanisms could reduce control slightly.	9
Minimal Disclosure	The use of zero-knowledge proofs (zk-SNARKs) ensures users can share only the necessary data (*e.g.*, just confirming age rather than revealing a birthdate). This is one of the strongest features, thus it scores perfectly.	10
Security	Security is strong due to zk-SNARKs and blockchain integrity, but no system is immune to potential attacks on either the blockchain or user endpoints, which explains the score being close to but not fully perfect.	9
Transparency	While blockchain ensures transparency through an immutable ledger, the complexity of understanding blockchain interactions might hinder full transparency for all users. Hence, it scores slightly lower.	8
Interoperability	The system works with Ethereum and zk-SNARKs, making it interoperable with other decentralized platforms, but this interoperability may be limited outside the blockchain space, preventing a perfect score.	8
Verifiability	Credentials can be verified on the blockchain through smart contracts, ensuring trust in their authenticity. The system is robust, though certain real-world verification processes might complicate full implementation.	9
Privacy	Privacy is ensured through selective disclosure and zero- knowledge proofs, fully protecting sensitive user data. Hence, this principle receives a perfect score.	10

EU since 2018. The authorities made the regulations of GDPR for the protection of personal data. Article 4 of GDPR categorizes personal data into several broad categories. This article defines 'Personal data' as information used to identify a person. 'Processing' is the operation of personal data. 'Controller' is an entity that determines the purpose of processing the data. Applying the GDPR to SSI will consider the three types of data in SSI, DID's, credentials, and hashes. Data subjects create DID. Though DID is related to 'Personal Data', means information relating to individual users. The data subject controls the disclosure of this data. It pertains to Article 5.1.e, which restricts identifying personal data and its context. The proposed work achieves this with the help of zero-knowledge proof. We can classify the blockchain and smart contracts as 'Controllers'.[20] The system uses zk-SNARK and smart contracts to generate identities. This secures personal data, as required by Article 32.[21]

7. Experimental setup

The proposed system aims to use a decentralized approach to identity management. Its key operations are the Issuer, Verifier, and Holder roles. These are fundamental to any identity management framework. The setup tests a decentralized identity system. It uses Ethereum, IPFS, and smart contracts. They manage multiple DIDs per user across different contexts. The system generates Decentralized Identifiers (DIDs) as

Fig. 4: Chart representing the score (0-10) of self-sovereign identity (SSI) achieved principle's.

unique, structured IDs. They allow verification of details, like a user's age, based on their credentials. The system creates a DID for each credential linked to a user's wallet address. The interface for entering holder details is shown in the Supporting Information (Fig. S1).

The Supporting information document includes Fig. S1–S3 that illustrate various aspects of the system: Fig. S3 shows the Holder interface where a specific credential is issued, while Fig. S2 displays a list of credentials issued to the wallet address holder, along with the corresponding DIDs. Fig. S3 demonstrates verification through selective disclosure, where only the user's age is revealed as being above or below 18, without disclosing other personal details. For verification, a smart contract is implemented using the ZoKrates library, which enables zk-SNARK[17] based zero- knowledge proof. The blockchain is connected via Metamask, using the same wallet address, and the verification process is carried out on a test network. This setup demonstrates a secure, privacy-preserving identity management solution, where credentials can be selectively disclosed and verified using zero-knowledge proofs, ensuring the user's privacy.

The integration of zk-SNARKs with smart contracts on the blockchain, facilitated by Metamask, provides a robust and decentralized mechanism for credential issuance and verification, ensuring trust and transparency in the system. Extending the result discussion to compliance with SSI principles, following analysis provides a hypothetical attainment of the principle through the proposed system. Further, the Analysis is depicted with a graph to show the achieved principle.

Table 3: Evaluation aspects for comparison.

Aspect	System	Type of IDM system
Privacy	Oauth [22]	De-centralized Identity Management
Scalability	uPort[23]	
User Control	Sovrin[24]	
Interoperability	Microsoft ION[25]	
Trustless Verification Across System		
Third-party Login	Gmail, Facebook	Federated Identity Management

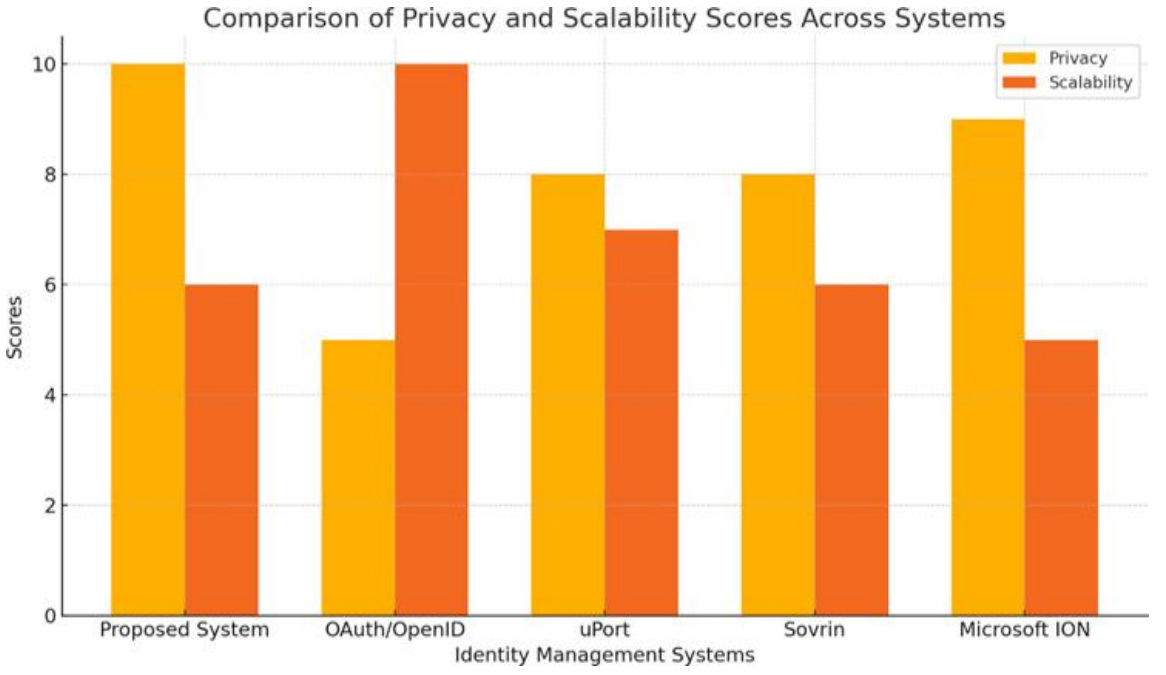

Fig. 5: Comparison of privacy and scalability.

The achievement of core Self-Sovereign Identity (SSI) principles was evaluated and scored on a scale from 0 to 10, as illustrated in Fig. 4. These principles include privacy, verifiability, interoperability, transparency, security, minimal disclosure, consent, user control, and decentralization. The chart reflects a strong adherence to most principles, with privacy, minimal disclosure, and decentralization scoring the highest, indicating the robustness of the system in aligning with SSI standards. The scores are subjective and are based on how well each principle is theoretically implemented in the system. Each score reflects a balance between how the system is expected to function and potential real-world limitations. The scores aim to provide a relative comparison of how strongly each principle is achieved.

8. Implementation details

The system integrates various components, including blockchain technology, decentralized networks, cryptographic libraries, and smart contracts, to enable secure, privacy-preserving identity management. Below are the key elements and their roles in the implementation. The Ethereum blockchain facilitates the implementation of smart contracts that oversee Decentralized Identifiers (DIDs). These contracts enable the creation, cancellation, and administration of DIDs, providing transparency and security through unalterable transactions. Additionally, they employ gas optimization techniques to reduce transaction fees. A DID registry is constructed using smart contracts, allowing one wallet to handle multiple DIDs across different contexts. Each DID is

Table 4: Comparison of existing identity management systems with proposed framework.

System/ Framework	Privacy Score (0-10)	Scalability Score (0-10)	User Control (0-10)	Interoperability (10)	Trustles6 Verification (0-10)	Decentralization (10)	Security (0-10)
Proposed System	10	6	10	8	10	10	10
OAuth/OpenID	5	10	4	7	3	3	6
uPort	8	7	9	9	8	8	8
Sovrin	8	6	9	7	9	9	9
Microsoft ION	9	5	9	8	8	10	9

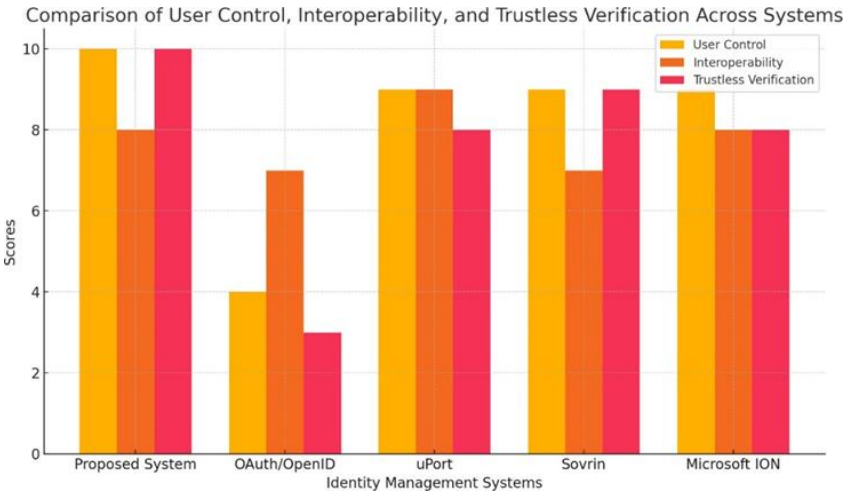

Fig. 6: Comparison of user control, interoperability, trustless verification.

associated with a public key, giving users authority over their identity management. DIDs are shared selectively according to the specific requirements of services, thereby maintaining privacy and control over the data. Confidential user information, such as credentials, is stored off-chain on the Inter Planetary File System (IPFS). The cryptographic hashes of this information are recorded on-chain to guarantee immutability, while the original data is encrypted prior to being uploaded to IPFS, ensuring user privacy. Users are also able to modify or revoke access to their information through the metadata stored on IPFS. The system employs Zero-Knowledge Proofs (zk-SNARKs)[17] to facilitate privacy-preserving identity verification. This enables the validation of specific attributes, like age or nationality, without disclosing any sensitive information. Tools such as ZoKrates or Snark js are utilized for secure and efficient computations necessary for implementing these proofs.

Ethereum wallets, such as Metamask, allow users to manage multiple DIDs from one wallet. Each DID is linked to a unique key pair, which simplifies identity management across various applications. The wallet offers a user-friendly interface for the creation, sharing, and administration of credentials. trusted organizations, including universities or government agencies, issue credentials through smart contracts. When verifying credentials, verifiers ask for particular information, and the blockchain confirms the authenticity of these credentials using zk-SNARKs. Updates and cancellations of credentials are handled via the DID registry and IPFS**.** This implementation ensures secure, decentralized, and privacy-centric identity management using cutting-edge blockchain and cryptographic technologies.

9. Results and discussions

The proposed system effectively demonstrates a practical and secure implementation of Self-Sovereign Identity (SSI) using blockchain and cryptographic technologies. It leverages the Ethereum blockchain to facilitate the management of Decentralized Identifiers (DIDs) through smart contracts, enabling users to register, update, and revoke their identities in a decentralized manner. This approach aligns with W3C standards and builds upon earlier solutions such as uPort and Sovrin by providing enhanced decentralization and compatibility with widely-used tools like MetaMask.

Additionally, the system permits trusted authorities to issue digital credentials, as illustrated in the interface screenshots featuring memberships such as IETE. These credentials are securely stored via IPFS, with only a hash recorded on the blockchain, thereby reducing data exposure and storage expenses. A significant aspect of the system is its incorporation of Zero-Knowledge Proofs, allowing users to validate information, like age, without disclosing personal details. The user interface of the system is user-friendly, enabling users to manage multiple DIDs pertaining to different roles, such as a student or organization member. Screenshots indicate that the interface is intuitive and supports the sharing and verification of credentials. The system implements secure encryption, facilitates credential revocation, and grants users full control over their data, contrasting with traditional identity systems like Aadhaar. This method is distinctive as it accommodates context-specific identities, minimizes gas usage on the blockchain, and allows for dynamic management of data stored in IPFS. These characteristics render it more adaptable and effective compared to numerous existing solutions. In summary, the project presents a functional prototype that strikes a balance between user privacy, data security, and real-world applicability while aligning with global identity standards.

The experimental setup section describes the detailed implementation of the system. The system's efficiency is highlighted with its achievements of SSI principles. This makes the system decentralized, overcoming the limitations of

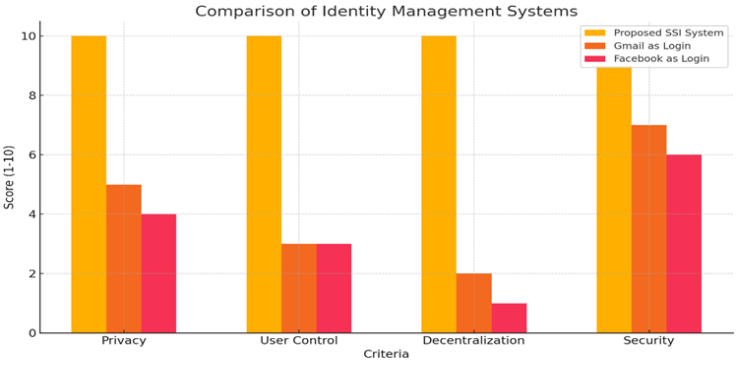

Fig. 7: Comparison with federated identity management system.

centralized Identity management systems. The significance of the results for the experimental setup of the decentralized identity management system, designed to achieve Self-Sovereign Identity (SSI) principles, can be discussed from several key perspectives:

Enhanced Privacy and Security: The results demonstrate that the system adheres to the core SSI principle of giving individuals control over their own identities. By decentralizing identity management, the system mitigates the vulnerabilities inherent in centralized systems, such as data breaches and identity theft, highlighting a significant improvement in data privacy and security.

Reduction of Single Points of Failure: The experimental outcomes show that decentralization minimizes the risk of a single point of failure, which is common in centralized identity systems. This ensures that no central authority can monopolize or misuse identity data, improving system resilience and availability.

Improved User Autonomy: The results underscore the system's success in granting users full ownership and control of their personal information, allowing them to share only what is necessary with third parties. This enhances user autonomy, a key SSI objective, aligning the system with modern privacy laws like GDPR.

Scalability and Interoperability: Through decentralization, the system avoids bottlenecks typical of centralized architectures, improving scalability. The results also suggest that the system's decentralized nature facilitates interoperability across different platforms, providing a more seamless user experience in varied environments.

Trustless Architecture: The use of blockchain or other decentralized technologies likely underpins the trust less nature of the system, reducing reliance on intermediaries. This contributes to a system where trust is distributed and maintained through cryptographic methods, providing transparency and reliability in identity verification.

Cost Efficiency: Decentralization can reduce operational costs associated with maintaining a centralized infrastructure, especially in large-scale systems. The results may indicate reduced overhead for identity management, making the system more cost-effective and sustainable.

By achieving SSI principles, the system offers a significant leap towards a more secure, user-controlled, and resilient identity management framework, which addresses the limitations of centralized systems.

9.1 Evaluation of proposed system against state-of-art existing identity management system

To evaluate the proposed system and for the purpose of analysis, we assume the scores relevant to the system's characteristics, strengths, and weaknesses. The relative comparison score with other systems is used for evaluation parameters. These scores serve as a tool to illustrate differences between systems on a common scale (in this case, 1 to 10). For example, scoring Gmail's privacy at 5 compared to 10 for the SSI system conveys that Gmail provides relatively moderate privacy compared to the near-complete privacy offered by the SSI system. the SSI system scores higher on privacy because it uses zero- knowledge proofs, while Gmail and Facebook score lower due to their centralized nature and potential for data sharing with third-party services, this approach is Rationale- based. The proposed system is compared with other state-of art Identity Management Systems, with respect to major key aspects. The following Table represents the systems used for comparison and the aspect of analysis. The next section shows the analysis of comparison of the proposed and existing system, with respect to the aspects mentioned in Table 3. It also extends to the types of Identity management system.

The diagram in Fig. 5, illustrates the Privacy and Scalability ratings of five distinct Identity Management Systems. The horizontal axis lists the systems: Proposed System, OAuth/OpenID, uPort, Sovrin, and Microsoft ION. The vertical axis indicates the scores, which range from 0 to 10. Orange bars signify Privacy scores, whereas yellow bars denote Scalability scores. The Proposed System achieves an exceptional Privacy score of 10, while its Scalability score is lower at 6. In contrast, OAuth/OpenID displays an inverse trend, with a Privacy score of 5 and a high Scalability score of 10. uPort demonstrates a more balanced performance, earning scores of 8 in Privacy and 7 in Scalability. Sovrin similarly maintains a good equilibrium, scoring 8 in Privacy and 6 in

Scalability. Microsoft ION has a strong Privacy score of 9, yet its Scalability score is comparatively lower at 5. This analysis indicates that most systems exhibit a trade-off between privacy and scalability, as those that are strong in one aspect tend to perform less effectively in the other.

The Fig. 6, is a bar graph that compares User Control, Interoperability, and Trustless Verification among various Identity Management Systems. The horizontal axis lists five systems: Proposed System, OAuth/OpenID, uPort, Sovrin, and Microsoft ION, while the vertical axis displays scores ranging from 0 to 10. In the graph, yellow bars denote User Control, orange bars represent Interoperability, and red bars reflect Trustless Verification.

The Proposed System achieves the highest scores in both User Control (10) and Trustless Verification (10), along with a strong Interoperability score of 8. OAuth/OpenID receives lower scores in all three categories: User Control (4), Interoperability (7), and Trustless Verification (3). uPort excels with high ratings across the board: User Control and Interoperability (9) and Trustless Verification (8). Sovrin demonstrates similar strengths, attaining scores of 9 for User Control, 7 for Interoperability, and 9 for Trustless Verification. Microsoft ION also maintains high scores in all three categories: User Control (9), Interoperability (9), and Trustless Verification (8).

The bar chart in Fig. 7, depicts comparison of various Identity Management Systems across four key criteria: Privacy, User Control, Decentralization, and Security. The chart evaluates three systems: the Proposed SSI System (represented by yellow bars), Gmail as Login (depicted with orange bars), and Facebook as Login (shown with red bars). The y-axis indicates scores that range from 1 to 10.

The Proposed SSI System achieves the highest scores in all four categories, attaining a perfect score of 10 in Privacy, User Control, Decentralization, and Security. Conversely, Gmail as Login and Facebook as Login receive significantly lower scores. Gmail is rated 5 for Privacy, 3 for User Control, 2 for Decentralization, and 7 for Security. Facebook, on the other hand, scores even lower in several areas, receiving 4 for Privacy, 3 for User Control, 1 for Decentralization, and 6 for Security. This analysis from Fig. 6, clearly indicates that the Proposed SSI System provides significantly improved privacy, control, decentralization, and security compared to conventional federated login systems like Gmail and Facebook.

Overall, the proposed system stands out for its focus on privacy, user sovereignty, and decentralized verification, making it a superior choice for secure and privacy-preserving identity management compared to both traditional and existing decentralized solutions.

10. Conclusion

The proposed identity management system is secure and privacy-preserving. It aligns with key Self-Sovereign Identity (SSI) principles. The system lets users prove their credentials without revealing personal information. It does this by integrating zk-SNARKs with Ethereum smart contracts. It ensures users control their identity data. This safeguards their privacy and enables trust less, decentralized credential verification. Using Metamask as a wallet helps users. It offers an easy way to manage Decentralized Identifiers (DIDs) and credentials. This implementation shows the system's alignment with SSI's core principles. It creates a strong foundation for decentralized, privacy-enhanced identity management. A comparison with state-of-the-art systems shows the proposed system is better. It is better for privacy-preserving, self-sovereign identity management.

This study proposes a novel Identity Management System, that integrates the selective disclosure strength from zk-SNARK's thus inculcating Self-Sovereign Identity, by addressing the ownership and privacy-preserving of digital Identity. This work also makes the Identity Management de-centralized differentiating it from traditional federated identity management systems or user centric systems, because it provides trustless verification in practical way, allowing selective disclosure while maintaining data integrity and non-repudiation that are fundamental to Blockchain Technology, thus adhering to a de-centralized Identity Management. Use of Metamask for managing DID's and credentials enhances usability and accessibility. The system bridges the gap between user acceptance and cryptographic expertise by improving accessibility and usability with tools like Metamask for managing DID's and credentials. With its scalable, user-centered, and technically sound identity verification methodology, this study significantly advances the field and has practical applications in e-governance, online services, and safe digital interactions.

Acknowledgments

The authors gratefully acknowledge the support of the Department of Computer Engineering Smt. Kashibai Navale College of Engineering Pune, for providing the required support and infrastructure to carry out this research work. The authors also thank colleagues and reviewers for their valuable suggestions and feedback during the preparation of this manuscript.

Conflict of Interest

There is no conflict of interest.

Supporting Information

Applicable.

CRediT Statement

Shailaja N. Lohar: Conceptualization, Methodology, Formal analysis, Writing – original draft, Project administration. **Sachin D. Babar**: Validation. **Parikshit N. Mahalle**: Supervision, Resources, review & editing.

Biographies

Dr. Parikshit Narendra Mahalle, received his Ph.D. in Wireless Communication from Aalborg University, Aalborg, Denmark on research problem statement Identity management framework for Internet of Things (IoT) - Ph. D. in 2013 and is Post Doc Researcher at CMI, Aalborg University, Copenhagen, Denmark. He is an accomplished academic and researcher with over 24 years of experience in teaching, research, and development. He is currently the Dean of Research and Development. as well as the Professor at Department of Artificial Intelligence and Data Science and also Dean Research, at Vishwakarma Institute of Information Technology, Pune.

Dr. Sachin Dilip Babar, received his Ph.D. in Wireless Communication from Aalborg University, Aalborg, Denmark on research problem statement "Embedded Security for Internet of Things" in 2013. He is currently working as Principal, STES's Sinhgad Institute of Technology, Lonavala, India. Has served as Professor & Head of Department of Computer Engineering Department at STES's SIT, Lonavala. With an academic experience of more than 23 years, He has published more than 30 research papers in reputed Journals and Conferences.

Mrs. Shailaja Nitin Lohar, has completed her Master's in Engineering degree in Information Technology in 2015 from MAEERS's Maharashtra Institute of Technology, Pune, India. She is a Research Scholar at Smt. Kashibai Navale College of Engineering, with research interest in Blockchain and Internet of Things. She is currently working as an Assistant Professor at Pimpri Chinchwad College of Engineering and Research, Ravet, Pune. She has 12 years of academic experience.

References

[1] Allen, C. (2016). *The Path to Self-Sovereign Identity*. Available online: http://www.lifewithalacrity.com/2016/04/thepath-to-self-soverereign-identity. html (accessed on 01 October 2024).

[2] S. Lohar, S. D. Babar, P. Mahalle, A proposed approach for Digital Identity management using Self Sovereign Identity, *International Journal of Next-Generation Computing*, 2022

[3] T. V. Doan, Y. Psaras, J. Ott, V. Bajpai, Toward decentralized cloud storage with IPFS: opportunities, challenges, and future considerations, *IEEE Internet Computing*, 2022, **26**, 7-15, doi: 10.1109/MIC.2022.3209804.

[4] F. Yang, S. Manoharan, A security analysis of the OAuth protocol, *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*. August 27-29, 2013, Victoria, BC, Canada. IEEE, 2013, 271-276, doi: 10.1109/PACRIM.2013.6625487.

[5] W.-M. Lee, Using the MetaMask crypto-wallet. *Beginning Ethereum Smart Contracts Programming*. Berkeley, CA: Apress, 2023, 111-144, doi: 10.1007/978-1-4842-9271-6_5.

[6] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, M. Avital, Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation, *Blockchain: Research and Applications*, 2021, **2**, 100014, doi: 10.1016/j.bcra.2021.100014.

[7] E. Bandara, X. Liang, P. Foytik, S. Shetty, K. De Zoysa, A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform, *International Conference on Computer Communications and Networks (ICCCN)*. July 19-22, 2021. Athens, Greece. IEEE, 2021, doi: 10.1109/icccn52240.2021.9522184.

[8] Der, U., Jähnichen, S., &Sürmeli, J. (2017). Self-sovereign identity: Opportunities and challenges for the digital revolution. ArXiv. https://arxiv.org/abs/1712.01767

[9] Y. Kortesniemi, D. Lagutin, T. Elo, N. Fotiou, Improving the privacy of IoT with decentralised identifiers (DIDs), *Journal of Computer Networks and Communications*, **2019**, 8706760, doi: 10.1155/2019/8706760.

[10] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, A. Skarmeta, Privacy-preserving solutions for blockchain: review and challenges, *IEEE Access*, 2019, **7**, 164908-164940.

[11] Q. Xu, Z. Song, R. S. Mong Goh, Y. Li, building an ethereum and IPFS-based decentralized social network system, *IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*. December 11-13, 2018, Singapore. IEEE, 2018, 1-6, doi: 10.1109/PADSW.2018.8645058.

[12] M. Kuperberg, Blockchain-based identity management: a survey from the enterprise and ecosystem perspective, *IEEE Transactions on Engineering Management*, 2019, **67**, 1008-1027, doi: 10.1109/TEM.2019.2926471.

[13] K. C. Toth, A. Anderson-Priddy, Self-sovereign digital identity: a paradigm shifts for identity, *IEEE Security & Privacy*, 2019, **17**, 17-27, doi: 10.1109/MSEC.2018.2888782.

[14] C. Brunner, U. Gallersdörfer, F. Knirsch, D. Engel, F. Matthes, DID and VC: Untangling Decentralized Identifiers and

Verifiable Credentials for the Web of Trust *the 3rd International Conference on Blockchain Technology and Applications*. Xi'an China. ACM, 2020, doi: 10.1145/3446983.3446992.
[15] T. Zhou, X. Li, H. Zhao, EverSSDI: blockchain-based framework for verification, authorisation and recovery of self-sovereign identity using smart contracts, *International Journal of Computer Applications in Technology*, 2019, **60**, 281, doi: 10.1504/ijcat.2019.100300.
[16] S. El Haddouti, M. D. Ech-Cherif El Kettani, Analysis of identity management systems using blockchain technology, *International Conference on Advanced Communication Technologies and Networking (CommNet)*. April 12-14, 2019 Rabat, Morocco. IEEE, 2019, 1-7, doi: 10.1109/COMMNET.2019.8742375.
[17] A.-E. Panait, R. F. Olimid, A. Stefanescu, Identity management on blockchain - privacy and security aspects, *Proceedings of the Romanian Academy - Series A: Mathematics, Physics, Technical Sciences, Information Science*, 2020, **21**, 45-52.
[18] B. Sharma, R. Halder, J. Singh, Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption, *International Conference on Communication Systems & Networks (COMSNETS)*. January 7-11, 2020, Bengaluru, India. IEEE, 2020, 1-6, doi: 10.1109/COMSNETS48256.2020.9027413.
[19] F. Yang, S. Manoharan, A security analysis of the OAuth protocol, *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*. August 27-29, 2013, Victoria, BC, Canada. IEEE, 2013, 271-276, doi: 10.1109/PACRIM.2013.6625487.
[20] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, S. Islam, Blockchain-based identity management system and self-sovereign identity ecosystem: a comprehensive survey, *IEEE Access*, 2022, **10**, 113436-113481.
[21] S. Lohar, S. Babar, P. Mahalle, Threat analysis and attack modeling for identity management solutions. *ICT for Intelligent Systems*. Singapore: Springer Nature Singapore, 2024, 73-88, doi: 10.1007/978-981-97-6678-9_7.
[22] N. Naik, P. Jenkins, uPort open-source identity management system: an assessment of self-sovereign identity and user-centric data platform built on blockchain, *IEEE International Symposium on Systems Engineering (ISSE)*. October 12 - November 12, 2020, Vienna, Austria. IEEE, 2020, 1-7, doi: 10.1109/ISSE49799.2020.9272223.
[23] N. Naik, P. Jenkins, Sovrin Network for Decentralized Digital Identity: Analysing a Self-Sovereign Identity System Based on Distributed Ledger Technology *IEEE International Symposium on Systems Engineering (ISSE)*. September 13-October 13, 2021. Vienna, Austria. IEEE, 2021, doi: 10.1109/isse51541.2021.9582551.
[24] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, S. Islam, Blockchain-based identity management system and self-sovereign identity ecosystem: a comprehensive survey, *IEEE Access*, 2022, **10**, 113436-113481.
[25] G. Kondova, J. Erbguth, Self-sovereign identity on public blockchains and the GDPR *Proceedings of the 35th Annual ACM Symposium on Applied Computing*. Brno Czech Republic. ACM, 2020, doi: 10.1145/3341105.3374066.
[26] T. V. Doan, Y. Psaras, J. Ott, V. Bajpai, Toward decentralized cloud storage with IPFS: opportunities, challenges, and future considerations, *IEEE Internet Computing*, 2022, **26**, 7-15, doi: 10.1109/MIC.2022.3209804.