



Blockchain-Based Decentralized Identity Verification and Management System

Sneha. S¹, Swathi. N², Alice Steffi. S³, Kavya. R⁴, Anuradha.C. R⁵

Dept. of Computer Science of Engineering, East West College of Engineering¹⁻⁴

Assistant Professor, Dept. of Computer Science of Engineering, East West College of Engineering⁵

Abstract: Digital identity has become a fundamental component of modern digital services, including banking, healthcare, education, government services, e-commerce, and online authentication. Traditional identity management systems generally depend on centralized authorities or identity providers for storing, managing, and verifying users' personal information. Although these systems provide convenient authentication and centralized control, they introduce important limitations such as single points of failure, privacy concerns, data breaches, limited user control, and poor portability of identity information. Blockchain technology provides an alternative approach through decentralized identity management systems (DIMS) and self-sovereign identity (SSI). In these systems, users can control their digital identities and selectively share verified credentials without depending entirely on a centralized authority. Blockchain provides decentralization, immutability, cryptographic security, transparency, and smart-contract-based automation, making it suitable for secure identity verification and credential management. This paper presents a comprehensive review of blockchain-based decentralized identity verification and management systems. It examines centralized, federated, self-sovereign, attribute-based, and Know Your Customer (KYC) approaches and compares their control models, advantages, and limitations. Existing commercial solutions such as uPort, Sovrin, ShoCard, and Connect.me are also examined. The study further analyzes major security threats, including private-key compromise, Sybil attacks, eclipse attacks, blockchain reorganizations, off-chain data tampering, oracle manipulation, social engineering, metadata leakage, and regulatory compliance issues.

Keywords: Blockchain, Decentralized Identity, Self-Sovereign Identity, Digital Identity Management, Verifiable Credentials, Zero-Knowledge Proofs.

INTRODUCTION

Digital identity management has become critical because a large portion of modern communication, transactions, education, healthcare, banking, and government services are performed electronically. A digital identity represents information that can be used to identify and authenticate an individual or organization in a digital environment. Traditional identity management systems commonly use centralized databases controlled by governments, companies, banks, or third-party identity providers. Such architectures simplify management and provide consistent access control, but concentrating identity information in a central location creates significant security and privacy risks. A successful compromise of a centralized identity provider can expose large quantities of sensitive information. The uploaded study identifies single points of failure, privacy violations, limited user control, lack of portability, and regulatory difficulties as important limitations of traditional identity management systems. Blockchain introduces a decentralized architecture in which identity-related information and verification processes can be distributed across a network. Instead of depending completely on a single identity provider, decentralized identity systems can use cryptographic keys, decentralized identifiers, verifiable credentials, smart contracts, and distributed ledgers. Self-sovereign identity (SSI) is particularly important in this context because it aims to give individuals greater control over their digital identities and credentials. Users can store and present credentials while selectively disclosing information to service providers.

Blockchain contributes several properties that are useful for identity management:

1. **Decentralization** – reduces dependence on a single central authority.
2. **Immutability** – makes unauthorized modification of blockchain records difficult.
3. **Cryptographic security** – provides mechanisms for authentication and ownership verification.
4. **Smart contracts** – enable automated verification and rule enforcement.
5. **Transparency and auditability** – transactions and verification events can be recorded for later validation.

The source identifies authentication, integrity, privacy, trust, and simplicity as important characteristics of effective decentralized identity systems.



However, blockchain does not automatically solve all identity-management problems. Public blockchain transparency may create privacy risks, while decentralized systems can introduce key-management difficulties, interoperability problems, scalability limitations, usability barriers, and regulatory challenges.

Therefore, this paper examines the existing decentralized identity ecosystem, compares different approaches, analyzes security threats and mitigation techniques, identifies research gaps, and discusses applications and future research directions.

Objectives of the Review

- To study blockchain-based decentralized identity management.
- To compare centralized and decentralized identity approaches.
- To analyze existing DIMS solutions.
- To identify major security threats.
- To examine privacy-preserving techniques.
- To study practical applications of decentralized identity.
- To identify research gaps and technical challenges.
- To discuss mitigation strategies and future research directions.

Digital identity has become an essential component of modern digital services. It is used to authenticate individuals, verify credentials, and provide access to online services. Traditional identity management systems generally depend on centralized authorities that store and manage users' personal information. Although centralized systems can provide convenient identity verification, they also introduce important security and privacy concerns. A centralized database can become a single point of failure, meaning that a successful attack on the central system may affect a large number of users. In addition, users often have limited control over how their personal information is collected, stored, and shared. Blockchain technology provides an alternative approach to identity management by distributing control and verification across a network rather than depending completely on a single authority. Blockchain provides important properties such as decentralization, immutability, cryptographic security, and programmable smart contracts. These properties can support secure identity verification, protect the integrity of identity records, and automate verification processes.

Blockchain-based Decentralized Identity Management Systems (DIMS) aim to give individuals greater control over their digital identities. A major approach within DIMS is **Self-Sovereign Identity (SSI)**, in which users can manage their identity information and decide what information should be shared with different parties. SSI supports concepts such as user ownership, selective disclosure, consent-based information sharing, and decentralized verification. However, widespread adoption is still affected by challenges such as interoperability, key management, governance, and the maturity of existing solutions.

Different identity management approaches have been developed to address the requirements of digital identity. These include **Federated Identity Management, Self-Sovereign Identity, Attribute-Based Credentials (ABC), and Know Your Customer (KYC)** systems. Federated identity systems provide convenience through third-party identity providers, whereas SSI focuses on user ownership and decentralized control. Attribute-Based Credentials allow users to disclose selected attributes rather than revealing complete identity information. KYC systems are widely used for regulatory identity verification, particularly in financial services, but traditionally depend on centralized identity storage.

One important advantage of blockchain-based identity systems is their ability to combine decentralized verification with cryptographic techniques. Sensitive identity information can be kept off-chain while cryptographic hashes, references, or verification-related information can be maintained on the blockchain. This approach can improve confidentiality while still providing integrity and tamper detection. Smart contracts can additionally automate identity verification and compliance-related processes.

The development of decentralized identity has also resulted in several commercial and practical solutions. The reviewed systems include **uPort, Sovrin, ShoCard, and Connect.me**, which demonstrate different approaches to decentralized identity, including blockchain-based wallets, decentralized identifiers, verifiable credentials, and identity verification. These solutions also demonstrate that different platforms provide different balances between usability, privacy, customization, and decentralization.

Security is another major consideration in decentralized identity systems. The reviewed literature identifies twelve major security threats covering cryptographic, network, data-integrity, user-centric, and regulatory concerns. These include



private-key compromise, Sybil attacks, eclipse attacks, off-chain data tampering, oracle manipulation, social engineering, metadata leakage, GDPR non-compliance, and jurisdictional conflicts. Therefore, a decentralized identity system must consider not only blockchain security but also the security of users, applications, off-chain storage, and regulatory processes.

Privacy is particularly important because digital identity systems process sensitive personal information. Privacy-enhancing technologies such as **Zero-Knowledge Proofs (ZKPs)**, **zk-SNARKs**, and **ring signatures** can help users prove required information without unnecessarily revealing additional personal data. These techniques represent an important direction for developing privacy-preserving decentralized identity systems.

Real-world implementations also demonstrate the potential of decentralized identity. The paper discusses the **South Korean DID ecosystem**, including the MyID Alliance and MYKEEPiN Alliance, where decentralized identity frameworks have been integrated across areas such as government, healthcare, finance, and other services. The paper also discusses educational credential verification, where a certificate can be hashed and the resulting hash recorded on a blockchain so that a verifier can later check whether the certificate is authentic and unchanged.

Despite these developments, decentralized identity systems still face challenges related to scalability, interoperability, privacy, usability, key management, and regulatory compliance. Different blockchain platforms and identity systems may not easily communicate with one another, while users may find private-key and credential management difficult. Regulatory requirements can also conflict with the immutable nature of blockchain-based records. These challenges create important research opportunities for developing more interoperable, scalable, privacy-preserving, and user-friendly identity systems.

Therefore, this paper reviews blockchain-based decentralized identity verification and management systems, examines existing identity-management approaches and blockchain architectures, analyzes major security threats, and discusses practical applications and mitigation strategies. It also identifies current research gaps and future directions, particularly in interoperability, privacy preservation, usability, regulatory compliance, and system performance.

LITERATURE REVIEW

1. Traditional Identity Management

Traditional identity systems generally depend on a centralized organization or identity provider. Examples include government identity databases, banking databases, enterprise authentication systems, and centralized KYC systems. The main advantage is simple administration. However, centralized identity storage creates a valuable target for attackers. The uploaded paper identifies data breaches, privacy violations, lack of portability, and excessive dependence on centralized providers as important limitations.

Centralized Identity:

In a centralized system, one primary entity control identity information and authentication.

Advantages:

- Simple administration.
- Centralized policy enforcement.
- Easy data management.
- Established regulatory processes.

Limitations:

- Single point of failure.
- Large-scale data breach risk.
- Limited user control.
- Privacy concerns.
- Vendor dependency

2. Federated Identity Management

Federated identity allows users to authenticate through a trusted third-party identity provider and use the same credentials across multiple services.

Examples include OpenID Connect and SAML-based systems.

The major advantage is convenience through Single Sign-On (SSO). However, users remain dependent on the identity provider and may have limited control over how their information is collected and shared.



3. Self-Sovereign Identity

Self-Sovereign Identity gives individuals greater control over their digital identities. Instead of relying completely on a centralized identity provider, users manage their credentials using cryptographic mechanisms and decentralized infrastructure.

Important characteristics include:

1. User ownership.
2. Decentralized identity.
3. Selective disclosure.
4. Consent-based data sharing.
5. Cryptographic verification.
6. Credential portability.

The study notes that SSI can improve privacy and interoperability but still faces adoption, interoperability, governance, and private-key-management challenges.

4. Attribute-Based Credentials

Attribute-Based Credentials (ABC) allow users to disclose only the required identity attributes instead of revealing their complete identity.

For example, a user may prove that they are above a required age without revealing their exact date of birth.

This approach reduces unnecessary data exposure and can use cryptographic techniques such as zero-knowledge proofs.

5. Know Your Customer Systems

KYC systems are widely used by financial institutions and regulated organizations. They verify customer identities to meet regulatory requirements and reduce financial crime.

However, conventional KYC systems frequently depend on centralized collection and storage of sensitive information. This creates privacy and security risks and can make repeated identity verification necessary.

6. Blockchain for Identity Management

Blockchain provides several characteristics that make it useful for decentralized identity.

Decentralization

Identity verification does not have to depend on one central database.

Immutability

Blockchain records are resistant to unauthorized modification after confirmation.

Cryptographic Security

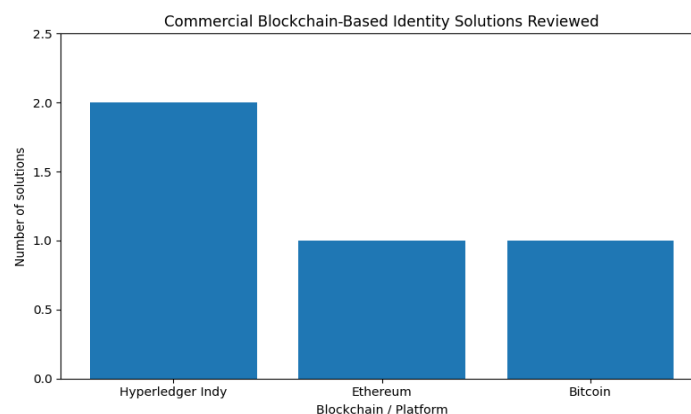
Public/private key cryptography enables users to prove ownership of credentials.

Smart Contracts

Smart contracts can automate verification rules, credential expiration checks, and trust conditions.

Privacy-Preserving Architecture

The reviewed architecture separates encrypted personal data from blockchain records. Sensitive files can be stored off-chain while cryptographic keys, hashes, or references are maintained through blockchain mechanisms.





COMPARATIVE ANALYSIS

The literature identifies four major identity-management approaches: Federated Identity Management, Self-Sovereign Identity, Attribute-Based Credentials, and KYC.

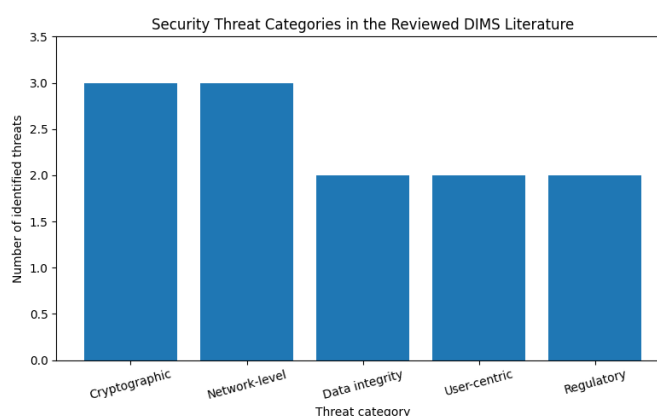
Feature	Federated Identity	SSI	Attribute-Based Credentials	KYC
Control	Centralized	Decentralized	Decentralized	Centralized
User control	Low–Moderate	High	High	Low
Privacy	Moderate	High potential	High	Lower
Selective disclosure	Limited	Supported	Strong	Limited
Third-party dependency	High	Reduced	Reduced	High
Main strength	Convenience	User ownership	Privacy	Regulatory compliance
Main limitation	Dependency on IdP	Key management	Complexity	Centralized data
Typical application	SSO	SSI ecosystem	Selective verification	Banking/KYC

This comparison indicates that decentralized approaches provide greater opportunities for user control and selective disclosure, while centralized approaches generally provide more mature administrative and regulatory structures.

Comparison of Commercial DIMS Solutions

The reviewed study discusses four commercial solutions: uPort, Sovrin, ShoCard, and Connect.me.

Solution	Blockchain Platform	Main Feature	Primary Application	Limitation
uPort	Ethereum	Mobile wallet and social recovery	KYC, authentication	Limited attribute validation
Sovrin	Hyperledger Indy	DIDs and verifiable credentials	Enterprise SSI	Complex user experience
ShoCard	Bitcoin	Document verification	Travel identity	Uses centralized components
Connect.me	Sovrin	User-friendly SSI wallet	Consumer identity	Limited customization





CHALLENGES AND RESEARCH GAPS

The paper identifies **12 major security threats**, grouped into five categories: cryptographic, network-level, data integrity, user-centric, and regulatory threats.

The count is:

Threat category	No. of threats
Cryptographic	3
Network-level	3
Data integrity	2
User-centric	2
Regulatory	2

The major research gaps/challenges discussed are scalability, interoperability, privacy preservation, key management, usability, regulatory compliance, and future quantum resistance. The paper particularly identifies interoperability, privacy, usability, regulatory frameworks, and performance as important future research directions.

i. Scalability

Blockchain networks can experience transaction delays and increased transaction costs as usage grows. This becomes particularly important when identity systems must support large numbers of users and frequent verification operations.

The source identifies high transaction fees and network latency as barriers to real-time applications.

Research gap: More research is required into high-throughput identity architectures that maintain security and decentralization.

ii. Interoperability

Different decentralized identity systems can operate on different blockchain platforms and protocols. Lack of interoperability can prevent credentials from being used across different ecosystems.

The reviewed paper recommends cross-chain protocols, interoperable identity frameworks, and standards such as W3C DIDs and Verifiable Credentials.

Research gap: Universal credential and identity interoperability remains an important research area.

iii. Privacy

Although blockchain provides transparency and integrity, public transaction information can potentially expose metadata and identity relationships.

The source identifies zero-knowledge proofs, zk-SNARKs, ring signatures, and selective disclosure as possible privacy-enhancing approaches.

Research gap: Privacy-preserving verification must be improved without creating excessive computational overhead.

iv. Key Management

Private keys are fundamental to decentralized identity. Losing or compromising a private key can result in loss of control over an identity.

The reviewed paper identifies private-key compromise as a critical threat and discusses hardware-secure storage and improved recovery mechanism.

Research gap: User-friendly key recovery and identity recovery mechanisms are required for non-technical users.

v. Usability

Decentralized identity can involve seed phrases, private keys, multi-signature mechanisms, and complex recovery procedures. Such mechanisms may be difficult for ordinary users.

The source proposes social recovery, biometric authentication, simplified wallets, and improved interfaces.

Research gap: Future systems should reduce technical complexity while preserving security.

vi. Regulatory Compliance

Blockchain immutability can conflict with regulations requiring modification or deletion of personal information. GDPR compliance is therefore a major challenge.



The source recommends hybrid architectures where proofs are maintained on-chain while personal information is kept off-chain.

Research gap: Identity systems require governance models capable of addressing data deletion, consent, revocation, and jurisdictional differences.

vii. Quantum Security

Current cryptographic mechanisms may face future risks from sufficiently powerful quantum computers.

The reviewed paper identifies post-quantum cryptography and lattice-based zero-knowledge approaches as possible research directions.

APPLICATIONS

Blockchain-based Decentralized Identity Management Systems (DIMS) can be applied in several domains where secure identity verification, privacy, data integrity, and user control are important. The reviewed paper discusses practical examples in education, government, healthcare, finance, and travel, demonstrating how decentralized identity can reduce dependence on centralized identity providers.

1. Education and Academic Credential Verification

Blockchain-based identity systems can be used to verify educational certificates and academic credentials.

- An educational institution can issue a digital certificate to a student.
- A cryptographic hash of the certificate is generated.
- The hash is stored on the blockchain rather than storing the complete certificate publicly.
- When an employer or another institution needs to verify the certificate, it can generate a new hash from the submitted document.
- The new hash is compared with the blockchain record.
- If both hashes match, the certificate can be verified as authentic and unchanged.
- This reduces the possibility of certificate tampering and provides a decentralized method of verification.
- It also reduces the need for a verifier to contact the issuing institution for every verification request.
- Blockchain provides transparency and tamper resistance while decentralized verification reduces dependence on a single authority.

Example: Blockchain-based educational credential verification is presented in the paper as a practical application of decentralized identity.

2. Healthcare

Decentralized identity can be applied to healthcare environments where identity, credentials, and access to services need to be securely managed.

- Patients can be associated with digitally verifiable identities.
- Healthcare-related credentials can be verified using decentralized mechanisms.
- Decentralized identity can reduce dependence on a single identity provider.
- Privacy-preserving techniques can help prevent unnecessary disclosure of personal information.
- Verifiable credentials can support trusted communication between different organizations.
- Interoperability is particularly important when identity information needs to be used across multiple healthcare organizations.
- The South Korean DID ecosystem discussed in the paper demonstrates integration of decentralized identity frameworks in the healthcare sector.

Research importance: Healthcare applications require a balance between identity verification, privacy, interoperability, and regulatory compliance.

3. Banking and KYC

Know Your Customer (KYC) is an important application area for digital identity systems, particularly in financial services.

- Banks and financial institutions need to verify the identity of customers.
- Traditional KYC processes often depend on centralized storage and repeated verification.
- Decentralized identity can allow users to maintain reusable digital credentials.
- Users can provide only the required identity attributes instead of unnecessarily sharing complete identity information.
- Verifiable credentials can help organizations validate information provided by customers.



- Blockchain can provide a tamper-resistant record for verification-related information.
- Smart contracts can support automated verification and compliance processes.
- The paper identifies privacy and interoperability as important limitations in conventional KYC systems.

Benefit: A decentralized approach can support secure identity verification while giving users greater control over their identity information.

4. Government Services

Government services are another important application area for decentralized identity.

- Governments provide many services that require reliable identity verification.
- Decentralized identifiers can provide a digital representation of an individual that can be verified across services.
- Verifiable credentials can be used to prove specific attributes without necessarily revealing unrelated information.
- Decentralized identity can reduce dependence on a single centralized identity database.
- Blockchain can provide tamper-resistant verification records.
- Interoperability can allow identity credentials to be used across different government departments.
- The paper discusses the South Korean DID ecosystem, where decentralized identity frameworks have been integrated into government-related services.

Research importance: Government deployment requires strong interoperability, privacy protection, governance, and regulatory compliance.

5. Travel and Identity Document Verification

Blockchain-based identity can also be used for travel-related identity verification.

- Travelers need to provide identity and document information to different organizations.
- Repeated verification can create inconvenience and increase dependence on centralized databases.
- Blockchain-based systems can provide verifiable digital representations of identity documents.
- A verifier can check whether the presented credential is authentic.
- Decentralized verification can potentially reduce repeated manual verification.
- Privacy-preserving techniques can help minimize unnecessary disclosure of traveler information.
- The paper specifically reviews **ShoCard**, which uses Bitcoin-based infrastructure for travel document verification.

Example: ShoCard demonstrates the use of blockchain technology for travel-related document verification.

6. Employment and Professional Credentials

Decentralized identity can also support the verification of educational and professional qualifications.

- Job applicants can hold digital credentials issued by universities or professional organizations.
- Employers can verify the authenticity of credentials.
- The verification process can use cryptographic proofs instead of relying entirely on manual document checking.
- Users can selectively disclose relevant qualifications.
- Verifiable credentials can make credentials portable between organizations.
- Blockchain-based verification can help detect modification or falsification of credentials.

Research importance: The educational credential-verification model discussed in the paper provides a foundation that can also be applied to professional credential verification.

7. Cross-Organization Identity Verification

Decentralized identity is particularly useful when an individual needs to interact with multiple independent organizations.

- Different organizations can issue and verify digital credentials.
- Users can maintain their credentials instead of depending completely on one identity provider.
- Decentralized identifiers and verifiable credentials can support interoperability.
- Selective disclosure allows users to provide only the information required by a particular organization.
- Blockchain can provide a trusted infrastructure for verification.
- This approach is especially important for ecosystems involving government, healthcare, finance, education, and other service providers.



MITIGATION STRATEGY

Challenge / Threat	Mitigation strategy
Private-key compromise	Hardware-secure modules
Weak key derivation	Strong salted key derivation and secure derivation paths
Quantum attacks	Post-quantum cryptography and lattice-based ZK techniques
Sybil attacks	Stake-weighted validation such as Proof of Stake
Eclipse attacks	Randomized peer selection and IP rotation
Blockchain reorganization	Additional confirmations for critical identity claims
Off-chain data tampering	Periodic cryptographic hash audits
Oracle manipulation	Multiple oracles and consensus mechanisms
Social engineering	Time-locked multisignature recovery
Metadata leakage	Ring signatures and zk-SNARKs
GDPR issues	Store personal information off-chain with revocable blockchain pointers
Jurisdictional conflicts	Geofenced claim issuance and jurisdiction-aware smart contracts

These mitigation approaches are directly aligned with the 12-threat framework presented in the paper.

i.Private-Key Compromise

Problem: Theft of a private key can provide control over a user's identity.

Mitigation:

Hardware-secure key storage.

Multi-factor authentication.

Multi-signature recovery.

Social recovery mechanisms.

Secure backup procedures.

The reviewed study specifically identifies hardware-secure modules as one mitigation approach.

ii.Sybil Attacks

Problem: Attackers create multiple fake identities or nodes.

Mitigation:

Stake-based validation.

Strong identity verification.

Reputation mechanisms.

Permissioned governance where appropriate.

iii.Eclipse Attacks

Problem: A malicious actor attempts to isolate a node from the legitimate network.

Mitigation:

Randomized peer selection.



Frequent peer/address changes.

Multiple independent network connections.

The source recommends randomized peer selection and frequent IP rotation.

iv. Off-Chain Data Tampering

Problem: Identity information stored outside the blockchain can potentially be modified.

Mitigation:

Cryptographic hashes.

Periodic integrity verification.

Smart-contract-based audits.

Secure off-chain storage.

v. Oracle Manipulation

Problem: A compromised external identity provider can provide fraudulent information to the blockchain.

Mitigation:

Multiple independent oracles.

Consensus among data providers.

Reputation mechanisms.

Cryptographic verification.

vi. Social Engineering

Problem: Attackers may manipulate users or trusted recovery contacts.

Mitigation:

Multi-signature recovery.

Time delays for recovery.

Strong authentication.

User education.

Multiple independent recovery parties.

The source discusses time-locked multi-signature recovery as a mitigation strategy.

vii. Metadata Leakage

Problem: Public blockchain activity may reveal relationships or activity patterns.

Mitigation:

Zero-knowledge proofs.

Ring signatures.

Selective disclosure.

Privacy-preserving transaction mechanisms.

FUTURE WORK

Future research in blockchain-based decentralized identity management should focus on improving **interoperability, privacy, usability, regulatory compliance, and system performance**. Interoperability can be improved through cross-chain mechanisms and wider adoption of **W3C Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs)** so that identity information can be verified across different platforms and organizations. Privacy can be strengthened through **Zero-Knowledge Proofs (ZKPs), zk-SNARKs, and ring signatures**, allowing users to prove required information without unnecessarily revealing personal data. Usability should be improved through user-friendly digital identity wallets, biometric authentication, and social recovery mechanisms for lost credentials or keys. Future systems should also support regulatory requirements through **hybrid blockchain architectures, revocable credentials, consent management, and jurisdiction-aware smart contracts**. In addition, scalability and performance can be improved using **Layer-2 solutions, rollups, state channels, sharding, sidechains, and hybrid public-private blockchain architectures**. Research should also investigate stronger protection against emerging threats, including quantum-computing attacks, to develop secure, scalable, interoperable, privacy-preserving, and user-friendly decentralized identity systems.

CONCLUSION

Blockchain-based decentralized identity management represents an important development in digital identity architecture. Traditional identity systems provide centralized control and convenience but can create single points of



failure, privacy concerns, limited portability, and large-scale data-breach risks.

Decentralized identity systems based on blockchain and self-sovereign identity principles provide an alternative model in which users can obtain greater control over their credentials and selectively disclose information. Blockchain contributes decentralization, immutability, cryptographic security, transparency, and smart-contract automation.

The literature reviewed in this study demonstrates that decentralized identity has applications in education, healthcare, finance, government, travel, and authentication. Existing solutions such as uPort, Sovrin, ShoCard, and Connect.me demonstrate different approaches to implementing decentralized identity. However, these systems continue to face challenges involving scalability, interoperability, privacy, usability, key management, security, and regulatory compliance.

The security analysis demonstrates that decentralized identity introduces its own threat landscape, including private-key compromise, Sybil attacks, eclipse attacks, off-chain data tampering, oracle manipulation, social engineering, metadata leakage, and regulatory conflicts.

Consequently, blockchain should not be considered a complete solution to identity management by itself. Effective decentralized identity requires a combination of blockchain infrastructure, cryptography, privacy-preserving techniques, secure key management, standardized credentials, usable wallets, governance frameworks, and regulatory compliance.

The future of decentralized identity is therefore likely to depend on the successful integration of interoperability standards, privacy-preserving cryptography, hybrid architectures, scalable blockchain technologies, and user-friendly identity-management mechanisms. The reviewed study concludes that standards such as W3C DIDs and Verifiable Credentials, together with privacy-preserving authentication, are important for the continued development of decentralized identity systems.

REFERENCES

- 1) Atzori, M. (2015). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? SSRN.
- 2) Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management*, 34(5), 1481-1505.
- 3) Ahmed, M. R., Islam, A. K. M. M., Shatabda, S., & Islam, S. (2022). Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey. *IEEE Access*, 10, 113436-113481.
- 4) Baars, D. S. (2016). Towards selfsovereign identity using blockchain technology. University of Twente.
- 5) Lim, S. Y., et al. (2018). Blockchain technology the identity management and authentication service disruptor: a survey. *International Journal on Advanced Science, Engineering and Information Technology*, 8(4-2), 1735-1745.
- 6) IRMA (I Reveal My Attributes) project. [url:https://www.irmacard.org/irma](https://www.irmacard.org/irma)
- 7) Z. Guan, A. Li, and Z. Chen, Analysis of man-in-the-middle of attack on bitcoin address, in *Proc. 15th Int. Joint Conf. e-Business Telecommun.*, 2018, pp. 388395.
- 8) O. Dib, C. Huyart, and K. Toumi, A novel credential protocol for protecting personal attributes in blockchain, *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106586.
- 9) PoC KYConblockchain with Tradle. Tech. rep. Utrecht: Rabobank Nederland, 2016.
- 10) Ferdous, M. S., Poet, R. (2012). A comparative analysis of Identity Management Systems. 2012 International Conference on High Performance Computing & Simulation (HPCS).
- 11) Zaeem, R. N., Chang, K. C., Huang, T. C., Liao, D., Song, W., Tyagi, A., ... Barber, K. S. (2021). Blockchain Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study. In *IEEE/WIC/ACM International Conference on Web Intelligence* (pp. 128 135).
- 12) Wft. (n.d.). Wet op het financieel. 13) Blockchain Lab. (2016). uPort: A Platform for Self-Sovereign Identity.
- 14) Takemiya, M., Vanieiev, B. (2018). Sora identity: Secure, digital identity on the blockchain. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC).
- 15) A. Muhle, T. Gayvoronskaya, and C. Meinel, A quanti able trust model for blockchain-based identity management, in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Com mun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 14751482.
- 16) B Cm ECC: A light weight blockchain-based authentication and key agreement protocol for Internet of Things, *Mathematics*, vol. 9, pp. 5259, Dec. 2016.
- 17) F.Xue, S.Zhang, X.Cai, Y.Cao, W.Zha ng, and J.Chen, Ahybrid blockchainbased identity authentication scheme for multi WSN, *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241251, Apr. 2020.
- 18) Wiki. [url:https://en.bitcoin.it/wiki/Off-Chain](https://en.bitcoin.it/wiki/Off-Chain)
- 19) Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51Attack.



- 20) E. A New Era for Data Protection in the EU; European Commission: Brussels, Belgium, 2018.
- 21) “South Korea leading new standards for decentralized ID”, available at: [https:// identity review.com/south-korea-leadingnew standards-for-decentralizedid/](https://identityreview.com/south-korea-leadingnew-standards-for-decentralizedid/).
- 22) C. Anushka, P. Deepti, and A. Purnima, Anonymity: A secure identity management using smart contracts, in Proc. Int. Conf. Sustain. Comput. Sci., Technol. Manag. (SUSCOM). Rajasthan, India: Amity Univ., 2019.