JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

COMPREHENSIVE REVIEW OF BLOCKCHAIN-BASED DECENTRALIZED IDENTITY VERIFICATION AND MANAGEMENT SYSTEMS

Shafat-e-Rasool
Department of Information and Communication Engineering
BS Cyber Security and Digital Forensics, The Islamia University of Bahawalpur (IUB)
E-mail : rasoolshafat1@gmail.com
Aisha Nadeem
Department of Information and Communication Engineering
BS Cyber Security and Digital Forensics, The Islamia University of Bahawalpur (IUB)
F-mail : aishanadeem359@gmail.com
Muhammad Fahad Saeed
Department of Information and Communication Engineering
BS Cyber Security and Digital Forensics, The Islamia University of Bahawalpur (IUB)
E-mail : fahikhan5767@gmail.com
ENGR. Farhan Hassan
Assistant Professor, Department of Information and Communication Engineering
BS Cyber Security and Digital Forensics, The Islamia University of Bahawalpur (IUB)
farhan.hassan@iub.edu.pk

RECEIVED	*ACCEPTED*	*PUBLISHED*
12 Feb 2025	*24 Feb 2025*	*19 March 2025*

Abstract:
Digital identity management is undergoing a paradigm shift from centralized models to decentralized approaches leveraging blockchain technology. This comprehensive review analyzes blockchain based decentralized identity management systems (DIMS) and self sovereign identity (SSI) ecosystems.We examine academic works as well as commercial solutions, identifying five essential components of effective DIMS: authentication, integrity, privacy, trust, and simplicity. The paper provides a detailed taxonomy of existing approaches, comparing their architectures, security models, and implementation strategies.We perform a thorough security analysis of potential threats, including Sybil attacks, 51% attacks, and privacy breaches.The review highlights South Korea's DID Alliance as a successful case study of public sector adoption while identifying key challenges in scalability, interoperability, and regulatory compliance. Emerging solutions like zero-knowledge proofs and hybrid blockchain architectures are evaluated as promising directions. This work serves as both a reference for researchers and a guide for practitioners implementing decentralized identity solutions.

Keywords : Blockchain, decentralized identity, self-sovereign identity, digital identity management, privacy-preserving authentication.

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

Introduction

Digital identity management has become a critical infrastructure component in our increasingly online world. Traditional identity management systems (IMS) relying on centralized authorities like governments or corporations present numerous vulnerabilities including single points of failure, privacy violations, and lack of user control [1]. The emergence of blockchain technology has enabled a new paradigm of decentralized identity management systems (DIMS) that empower users through self-sovereign identity (SSI) principles. This review makes three key contributions:

• A comprehensive analysis an academic works and commercial solutions in blockchain-based identity management.

• A security framework evaluating DIMS against 12 identified threat vectors.

• Case studies of successful implementations including South Korea's DID Alliance and educational credential verification systems.

The paper is organized as follows: Section II reviews traditional IMS and their limitations. Section III introduces blockchain technology's relevance to identity management.Section IV analyzes commercial DIMS solutions. Section V examines academic research. Section VI presents our security analysis. Section VII discusses implementation case studies. Section VIII identifies future research directions.

1. Difference Between Centralized, Decentralized, Decentralized, Systems

The difference between this systems are given below.

3.0.1 Centralized System

Definition: A single central entity or node controls all operations.Examples: Traditional client-server architectures, centralized government databases, banking systems.

Pros: Simple management, consistent and unified data, easy to enforce policies.

Cons: Single point of failure (if the central server goes down, the whole system fails), scalability bottlenecks, potential security target.

3.0.2 Decentralized System

Definition: Control is spread across multiple nodes or entities, but some nodes may have more influence or control than others; not necessarily peer-to-peer.Examples:Blockchain networks (like Bitcoin and Ethereum), federated systems (like Mastodon, DNS), some organizational networks.

Pros: Reduced risk of a single point of failure, increased resilience, better fault tolerance.

Cons: Coordination complexity (e.g., consensus mechanisms), potential inefficiencies or slower performance compared to centralized systems.

3.0.3 Distributed System

Definition: Tasks and data are split across multiple nodes; nodes often operate independently and collaboratively in a peer-to-peer or clustered manner.Examples: Distributed databases (e.g., Apache Cassandra, MongoDB sharding), content delivery networks (CDNs), large-scale scientific computing systems.

Pros: Excellent scalability, high fault tolerance, local data processing reduces latency.

Cons: Complexity in maintaining data consistency, challenges in synchronization, potential network partition issues.[2][3][4][5]

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

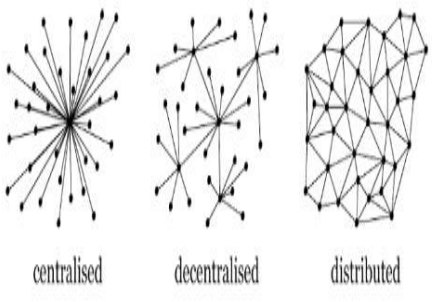

Figure 1: Difference Between Centralized,Decentralized,Decentralized Systems.

2. Classification of Identity Management Systems

Classification of IMS Approaches:
Existing identity systems can be categorized into four main types:

- **Federated Identity Management.**
- **Self-Sovereign Identity (SSI).**
- **Attribute-Based Credentials (ABC).**
- **Know Your Customer (KYC).**

4.0.1 Federated Identity Management

Definition: In federated identity systems, users authenticate through a trusted third-party identity provider (IdP). This allows them to access multiple services or applications using a single set of login credentials.[3][4]
Examples: OpenID Connect, Security Assertion Markup Language (SAML), Identity providers like Google, Facebook, or Microsoft.
Key Characteristics:

- Centralized identity storage and control by a third party.
- Simplifies access across platforms (Single Sign-On-SSO).
- Widely adopted in enterprise environments.

Advantages:

- Improved user convenience.
- Reduced password fatigue.
- Simplifies user access management for organizations.

Limitations:

- Dependency on central IdPs introduces a single point of control.
- Users may have little control over how their data is stored and shared.
- Raises privacy concerns, as providers can track user activity across platforms.

4.0.2 Self-Sovereign Identity (SSI)

Definition: SSI gives individuals full control over their digital identities. Users manage their own credentials and personal data, often stored on decentralized networks like blockchains.
Examples: Sovrin, uPort.
Key Characteristics:

- User-owned identity – no reliance on centralized authorities.
- Supports selective disclosure and consent-based data sharing.
- Built on decentralized and cryptographic foundations.

Advantages:

- Empowers users to own and manage their identity.
- Reduces the risk of mass data breaches.
- Enhances privacy, interoperability, and portability.

Limitations:

- Still an emerging technology – limited adoption and interoperability.
- Requires users to securely manage their private keys, which can be a barrier for non-technical users.
- Governance models are still evolving.

4.0.3 Attribute-Based Credentials (ABC)

Definition: ABC systems focus on sharing only the necessary identity attributes rather than full identity disclosure. For example, proving that someone is over 18 without sharing their full birthdate.
Examples: IRMA (I Reveal My Attributes), IBM Idemix, Microsoft U-

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

Prove.

Key Characteristics:

- Selective attribute disclosure.
- Strong focus on privacy and minimal data exposure.
- Often use zero-knowledge proofs or cryptographic techniques.

Advantages:

- Enhanced privacy – share only what is needed.
- Useful in scenarios requiring partial identity verification (e.g., voting, age verification).
- Limits data collection and reduces attack surface.

Limitations:

- Implementation can be technically complex.
- Less common than other identity models – limited awareness and adoption.
- May require integration with other identity systems for full functionality[6].

4.0.4 Know Your Customer (KYC)

Definition: KYC systems are used primarily in the financial and regulatory sectors to verify a customer's identity. These processes are mandated by law to prevent fraud, money laundering, and terrorist financing.

Examples: Bank or telecom account verification, National ID-based systems in regulated environments.

Key Characteristics:

- Centralized identity verification and storage.
- Strict compliance with legal and regulatory frameworks (e.g., AML, CFT).
- Involves document submission, biometric verification, and database cross-checks.

Advantages:

- Mandatory for legal compliance in many sectors.
- Helps detect and prevent financial crimes.
- Standardized and well-established process.

Limitations:

- Highly centralized, leading to privacy and security concerns.
- Limited user control over how personal data is stored and shared.
- Prone to data breaches and misuse due to sensitive information being collected centrally.
- Often lacks interoperability with modern decentralized identity models.[7]

2.1 Limitations of Current Centralized Identity Systems

Most traditional IMS approaches, especially federated and KYC systems, rely on centralized architectures, which come with inherent risks and limitations:

- **Single Point of Failure:** If a centralized identity provider is compromised, the attacker gains access to a vast amount of user data, affecting millions of users. High-profile breaches (e.g., Equifax, Facebook) highlight this vulnerability.
- **Privacy Violations:** Central authorities often collect more data than necessary and track user behavior across platforms. Users have limited visibility or control over how their information is used.
- **Lack of Portability:** Identity data is often locked within specific platforms, making it difficult to transfer identity across services. This leads to vendor lock-in and repeated verification processes.
- **Regulatory Challenges:** Compliance with privacy regulations like the General Data Protection Regulation (GDPR) is difficult for centralized systems, which struggle with data minimization, consent management, and the right to be forgotten.[8]

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

Table 1: Comparison of Identity Management System (IMS) Approaches

IMS Type	Control Model	Key Strength	Main Limitation
Federated Identity	Centralized	Convenience (SSO)	Dependency on third party IdP
Self-Sovereign Identity	Decentralized	User ownership, privacy	Key management complexity, early-stage
Attribute-Based Credentials	Decentralized	Selective disclosure, privacy	Complexity, limited adoption
Know Your Customer	Centralized	Regulatory compliance	Privacy risks, limited user control

3. BLOCKCHAIN TECHNOLOGY FOR IDENTITY MANAGEMENT

Blockchain provides several properties essential for robust identity management.

- **Decentralization.**
- **Immutability.**
- **Cryptographic Security.**
- **Smart Contracts.**
- **Privacy Challenges and Solutions.**

5.0.1 Decentralization

Eliminates reliance on a single central authority, reducing vulnerabilities like data breaches or censorship. Control is distributed across a network of nodes, ensuring no single entity can manipulate or compromise identities.

5.0.2 Immutability

Once recorded on the blockchain, identity data cannot be altered or deleted without network consensus. Prevents fraudulent modifications (e.g., fake credentials, backdated records) by making all changes transparent and permanent.

5.0.3 Cryptographic Security

Uses Public Key Infrastructure (PKI) for secure authentication, where users control private keys to prove ownership of their identities. Ensures tamper-proof verification and protects against impersonation or unauthorized access.

5.0.4 Smart Contracts

Enable automated, rule-based verification (e.g., checking credential expiration, validating issuer trustworthiness).Reduce human intervention, streamline processes (e.g.,KYC checks), and enforce compliance programmatically.

5.0.5 Privacy Challenges and Solutions

Public blockchains present privacy challenges that require mitigation strategies. Figure 2 illustrates how encryption techniques can preserve privacy in blockchain identity systems while maintaining verifiability. The diagram illustrates a secure cloud storage system that integrates encryption and blockchain technology. First, a user file is encrypted, transforming it into file ciphertext, which is then uploaded to a cloud disk system. Simultaneously, the encryption

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

key used for this file is also encrypted to generate a key ciphertext. This encrypted key is stored separately in a blockchain system to ensure security and immutability. By separating the storage of the encrypted file and the encrypted key—placing the file in the cloud and the key on the blockchain the system enhances data confidentiality and integrity, making unauthorized access or tampering Significantly more difficult.[9][10][11][12]

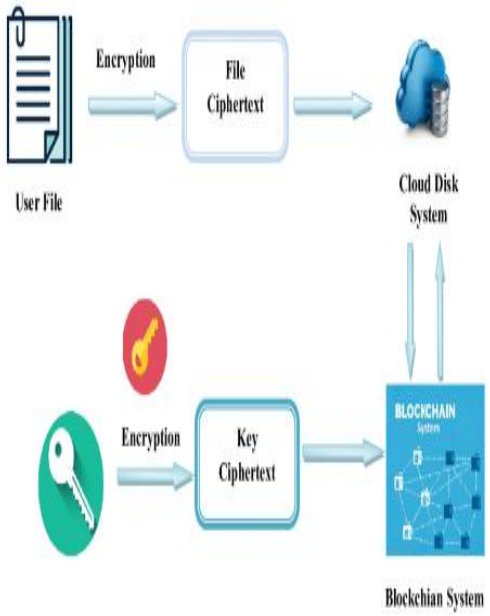

Figure 2: Privacy-preserving blockchain
architecture showing encryption layers and data flow between user systems, cloud storage, and blockchain components.

IMPORTANCE Together, these features create a trust less, tamper-resistant identity framework where: Users own and control their data (self Sovereign identity). Fraud is **mathematically improbable due to cryptography and consensus. Systems are **efficient and transparent, ideal for high-stakes use cases (e.g., passports, academic credentials). Blockchain's combination of decentralization + immutability + cryptography + automation addresses
core flaws in traditional identity systems (e.g., central databases prone to hacks or misuse.)

4. Commercial Decentralized Identity Management Solutions

This section analyzes four notable commercial blockchain-based decentralized identity management solutions:

- **uPort.**
- **Sovrin.**
- **ShoCard.**
- **Connect.me.**

1. uPort is built on the Ethereum blockchain and offers a mobile wallet with social recovery features. It is primarily used for Know Your Customer (KYC) and general authentication purposes. However, it does not support attribute validation, which restricts its applicability in scenarios requiring detailed credential checks.

2. Sovrin Operating on Hyperledger Indy, focuses on decentralized identifiers (DIDs) and verifiable credentials. It is suitable for enterprise self sovereign identity (SSI) use cases. Despite its powerful architecture, Sovrin suffers from a complex user experience (UX), which may hinder mass adoption.

3. ShoCard Leveraging the Bitcoin blockchain, is designed for document verification, especially in travel-related identity verification. However, it incorporates centralized components, which contradict the decentralized philosophy of blockchain technology.

4. Connect.me Is built on the Sovrin network and offers a user-friendly SSI wallet tailored for general consumer use. Nevertheless, it provides limited customization options, which may be

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

inadequate for advanced enterprise use cases.[13][14]

Table 2: Comparison of Commercial Blockchain-Based DIMS Solutions

Solution	Blockchain Platform	Key Features	Primary Use Cases	Limitations
uPort	Ethereum	Mobile wallet with social Recovery	KYC, authentication	No support for attribute validation
Sovrin	Hyperledger Indy	DIDs, verifiable credentials	Enterprise SSI	Complex user experience
ShoCard	Bitcoin	Document verification tools	Travel identity verification	Uses centralized components
Connect.me	Sovrin	User-friendly SSI wallet	Consumer identity management	Limited customization options

5. Academic Research in Decentralized Identity Management Systems

A systematic review revealed five prominent research themes in the field of Decentralized Identity Management Systems (DIMS). These themes reflect the evolving priorities and challenges in building secure, privacy-preserving, and user-centric identity solutions:

- **Authentication mechanisms.**
- **Data integrity preservation.**
- **Privacy-enhancing techniques.**
- **Trust establishment models.**
- **Usability improvements.**

1. Authentication Mechanisms: Methods that ensure only authorized users can access digital services and data. This is vital for defending against identity spoofing and unauthorized access in decentralized environments.

2. Data Integrity Preservation: Techniques designed to maintain the accuracy and consistency of identity data during storage and transmission.

This includes the use of blockchain and cryptographic methods to detect tampering and ensure trust.

3.Privacy-Enhancing Techniques: Mechanisms such as encryption, anonymization, zero knowledge proofs, and differential privacy that protect user information from exposure or misuse.

4. Trust Establishment Models: Frameworks that define, measure, and build trust among users, issuers, and verifiers in decentralized or federated networks. These models often leverage smart contracts, attestations, and reputation systems.

5. Usability Improvements: Enhancements focused on making

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

decentralized identity tools more user friendly and accessible. This includes reducing cognitive load, simplifying key management, and improving interface design to encourage adoption.These research directions form the basis for ongoing academic and practical efforts to improve decentralized identity systems[15].

6. Security Analysis of Decentralized Identity Management Systems

Through a review of technical literature and threat modeling practices, we identified 12 major security threats that impact Decentralized Identity Management Systems (DIMS). These threats span cryptographic vulnerabilities, network-based attacks, data integrity issues, user-centric exploits,and regulatory compliance challenges. Each threat vector is accompanied by mitigation strategies drawn from both academic proposals and industry implementations.

8.0.1 Cryptographic Threats

1. Private Key Compromise

Risk: Theft of private keys (e.g., through mobile malware) can lead to full control over a user's digital identity. Mitigation: Use of hardware-secure modules(e.g., Apple's T2 enclave) for secure key storage.

2. Weak Key Derivation

Risk: Predictable derivation paths in hierarchical deterministic(HD) wallets may leak relationships between identities.

Mitigation: Implementation of BIP-32 with salted derivation paths.

3. Quantum Vulnerabilities

Risk: Advances in quantum computing (e.g., Shor's algorithm)may break elliptic curve cryptography (ECC).

Mitigation: Transition to post-quantum cryptographic schemes such as lattice-based zero-knowledge proofs.

8.0.2 Network-Level Threats

4. Sybil Attacks: Malicious nodes create fake identities to disrupt consensus protocols (notably in permissioned ledgers like Sovrin). **Mitigation:** Use of Proof-of-Stake (PoS) mechanisms with stake-weighted validation.

5. Eclipse Attacks: Attackers isolate a node to manipulate its view of the network and transactions.

Mitigation: Implement randomized peer selection and frequent IP address rotation.

6. Blockchain Reorganizations (Reorgs): Short-lived forks (e.g., in Ethereum with 15s block time) may reverse or invalidate transactions. **Mitigation:** Require 12 or more confirmations before accepting critical identity claims.

8.0.3 Data Integrity Threats

7. Off-Chain Data Tampering: Identity attributes stored on systems like IPFS may be altered without triggering blockchain-based alerts. **Mitigation:** Periodic cryptographic hash audits enforced through smart contracts.

8. Oracle Manipulation Risk: Malicious or compromised identity providers (e.g., SAML issuers) may inject fraudulent claims.

Mitigation: Utilize multiple oracles with Schelling point consensus for verification.

8.0.4 User-Centric Threats

9. Social Engineering Attacks: In uPort's social recovery protocol, trusted contacts can be coerced into resetting a user's identity keys.

Mitigation: Use time-locked multisignature recovery schemes (e.g., 3-of-5 recovery with a 48-hour delay).

10.Metadata Leakage: Public analysis of blockchain transactions can reveal user identity patterns or links between derived keys.

Mitigation: Incorporate privacy-preserving techniques such as ring

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

signatures or zk-SNARKs (e.g., as used in Zcash).

8.0.5 Regulatory and Compliance Threats

11. GDPR Non-Compliance: Immutable on-chain identity claims may violate data protection rights, such as the "right to be forgotten."

Mitigation: Store personal data off-chain and use revocable, on-chain references or pointers.

12. Jurisdictional Conflicts: Stewards of global identity networks (e.g., Sovrin) may be subject to conflicting legal jurisdictions.

Mitigation: Implement geofenced claim issuance based on IP detection and smart contract enforcement.
[16][17][18][19][20]

Threat	Category	Impact	Likelihood	Priority Level
Private Key Compromise	Cryptographic Threat	High	High	Critical
Weak Key Derivation	Cryptographic Threat	Medium	Medium	Moderate
Quantum Vulnerabilities	Cryptographic Threat	High	Low	Low (Future Risk)
Sybil Attacks	Network-Level Threat	High	Medium	High
Eclipse Attacks	Network-Level Threat	Medium	Medium	Moderate
Blockchain Reorganizations	Network-Level Threat	High	Low	Moderate
Off-Chain Data Tampering	Data Integrity Threat	Medium	High	High
Oracle Manipulation	Data Integrity Threat	High	Medium	High
Social Engineering	User-Centric Threat	High	High	Critical
Metadata Leakage	User-Centric Threat	Medium	High	High
GDPR Non-Compliance	Regulatory Threat	High	Medium	High

This layered threat model highlights the need for multi-dimensional security frameworks in DIMS, balancing cryptographic strength, network resilience, user-centric design, and regulatory compliance.

9 Case Studies

9.1 South Korea's DID Alliances

South Korea has emerged as a global leader in the adoption of decentralized identity management systems (DIMS), particularly within the public sector. Key initiatives include:

- **MyID Alliance:** A consortium of over 83 companies collaborating on mobile authentication solutions, led by ICONLOOP.

- **MYKEEPiN Alliance:** Comprises 92 members focusing on commercial DID services, supported by RaonSecure.

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

• **Government Integration:** Decentralized identity is being applied across military, healthcare, and financial sectors for secure authentication and credentialing [21].

These alliances aim to create interoperable and privacy-preserving identity frameworks compliant with global standards like W3C DID.

9.2 Educational Credential Verification with Blockchain

Blockchain-based identity systems offer an effective solution to academic certificate fraud by ensuring the integrity and authenticity of educational credentials through a secure and decentralized process Figure 3 illustrates the blockchain-based verification process, and the steps are outlined below:

1. Certificate Information Submission: An educational institution issues a certificate (e.g.,diploma or degree), and the data is forwarded to a verifier.

2. Hash Generation: The verifier computes a hash from the certificate data, creating a unique digital fingerprint of the document.

3. Blockchain Storage and Comparison: The hash is stored on a blockchain. When verification is required, the certificate data is rehashed and compared to the on-chain value.

4. Verification Outcome: If the hashes match, the certificate is verified as authentic and unaltered.

Key Benefits:

• Tamper-Proof: Once recorded on the blockchain, the certificate's integrity cannot be modified without detection.

• Transparency: Employers and institutions can easily verify credentials through a public ledger.

• Decentralized Trust: Eliminates reliance on centralized certificate-issuing authorities.[22]

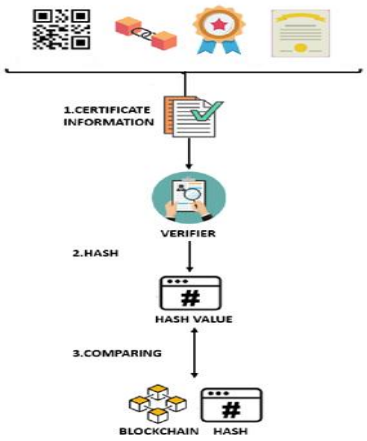

Figure 3: Blockchain-Based Educational Credential Verification Process.

10 Future Research Directions

Based on our analysis of current decentralized identity management systems (DIMS), we identify five major directions for future research and development:

10.1 Interoperability

Most blockchain identity systems currently operate in isolation, which limits seamless integration across different platforms and ecosystems. Future research should focus on:

• Cross-chain protocols
• Interoperable identity frameworks
• Adoption of standards such as W3C Verifiable Credentials and Decentralized Identifiers (DIDs).

These efforts will allow digital identities to function universally, regardless of the underlying blockchain infrastructure.

10.2 Privacy Enhancements

While blockchain promotes transparency, protecting user privacy especially for sensitive identity data remains a challenge. Future research should explore advanced cryptographic techniques such as:

• Zero-Knowledge Proofs (ZKPs)
• zkSNARKs
• Ring signatures

These enable selective disclosure of identity attributes, allowing verification

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

without exposing unnecessary personal information.

10.3 Usability Improvements

Key management remains a major usability hurdle. Complex recovery processes (e.g., seed phrases, multi-signature wallets) deter mainstream users. Promising areas of research include:

- **Social recovery mechanisms (e.g., uPort's trustee model)**
- **Biometric authentication**
- **User-friendly wallets and simplified interfaces**

Improving usability will be crucial for adoption among non-technical users.

10.4 Regulatory Frameworks

Compliance with global regulations, such as the General Data Protection Regulation (GDPR) and eIDAS, is difficult due to blockchain's immutability. Research must address:

- **Hybrid architectures (on-chain proofs with off-chain data).**
- **Governance mechanisms that allow data revocation and consent management.**
- **Geofencing and jurisdiction-aware smart contracts.**

Legal compliance is essential for institutional adoption of DIMS.

10.5 Performance Optimization

Scalability remains a bottleneck. High transaction fees and network latency impede real-time applications. Future solutions should consider:

- **Layer-2 protocols (e.g., rollups, state channels).**
- **Sharding and sidechains.**
- **Hybrid public-private blockchain architectures.**

These improvements aim to enhance throughput without sacrificing security or decentralization.

Why These Directions Matter

Addressing these five areas interoperability, privacy, usability, regulation, and performance is vital to ensure that decentralized identity systems can mature into scalable, secure, and user-friendly alternatives to traditional identity management.

11 CONCLUSION

This comprehensive review demonstrates that blockchain technology enables significant advances in decentralized identity management through self-sovereign identity principles. While challenges remain in scalability, usability, and regulatory compliance, emerging solutions show promise for overcoming these barriers. The successful implementa tion of DIMS in South Korea's public sector and educational credentialing systems provides valuable models for future deployments. As the field matures, we anticipate increasing convergence around standards like W3C Verifiable Credentials and continued innovation in privacy preserving authentication techniques.

12 ACKNOWLEDGMENT

The authors would like to express their sincere and heartfelt gratitude to Engr. Farhan Hassan for his invaluable supervision. His insightful guidance, critical feedback, and unwavering support were instrumental throughout the duration of this research project. During the preparation of this manuscript, the authors used AI-assisted tools for the sole purpose of improving grammar, spelling,and language clarity. Specifically, [Choose one or more of the following, or insert the specific tool you used: e.g., Grammarly, ProWritingAid, language models developed by OpenAI (ChatGPT), Google (Gemini)] were utilized for automated proofreading and editing. The intellectual content, analysis, and conclusions of this paper are entirely the work of the human authors.

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

13 Reference

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 self-sovereign 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
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., Liau, 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.Zhang,andJ.Chen, Ahybrid blockchain-based 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
19) Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51Attack. Appl. Sci. 2019, 9, 1788.

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 1 (2025)

20) E. A New Era for Data Protection in the EU; European Commis sion: Brussels, Belgium, 2018.
21) "South Korea leading new standards for decentralized ID", avail able at: https:// identity review.com/south-korea-leading-new standards-for-decentralized-id/.
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.