Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Decentralized Identity Using Blockchain: Enhancing Security and Privacy in Digital Identity Management

Bhaskardeep Khaund
Microsoft, USA
Corresponding Author: Bhaskardeep Khaund, **E-mail**: bhaskardeepkhaund@gmail.com

| ABSTRACT
Decentralized identity represents a paradigm shift in digital authentication, enabling individuals to maintain sovereignty over personal credentials without reliance on centralized authorities. This transformative approach leverages blockchain architecture to create persistent, portable identity frameworks that fundamentally alter the relationship between identity holders, verifiers, and digital systems. Distributed ledger technology provides the technological foundation for these frameworks, offering cryptographic security mechanisms that protect against unauthorized access while ensuring data integrity. The implementation of decentralized identifiers creates globally unique, highly available identifiers controlled exclusively by their owners, while verifiable credentials enable trusted attestations that remain cryptographically protected yet independently verifiable. Privacy enhancements through blockchain include granular disclosure controls, allowing individuals to reveal only necessary information during authentication processes. The cryptographic underpinnings of blockchain-based identity solutions mitigate numerous vulnerabilities inherent in traditional identity systems, eliminating single points of failure that historically enabled large-scale data breaches. These technological advantages translate into meaningful benefits across various domains, including financial services, healthcare, and cross-border identity verification. The emergence of interoperable identity protocols signals a transition toward user-centric identity ecosystems where individuals exercise genuine authority over their digital presence. At the same time, organizations benefit from enhanced security postures and streamlined verification processes.

| KEYWORDS

Decentralized identity, Blockchain technology, Digital authentication, Privacy enhancement, Self-sovereign identity

| ARTICLE INFORMATION

ACCEPTED: 01 June 2025 **PUBLISHED:** 19 June 2025 **DOI:** 10.32996/jcsts.2025.7.101

1. Introduction

Digital identity management represents a cornerstone of modern information systems, enabling authentication and authorization across numerous digital platforms and services. Traditional identity frameworks rely predominantly on centralized architectures where credential issuers maintain complete control over identity verification processes and data storage [1]. The expanding digital ecosystem, however, reveals significant limitations in these conventional approaches, particularly regarding security vulnerabilities, privacy concerns, and user autonomy. Blockchain technology presents a transformative alternative by distributing identity verification across decentralized networks, eliminating single points of failure while enhancing credential portability and user control [2]. This fundamental architectural shift addresses numerous shortcomings in existing identity systems while creating new possibilities for secure, privacy-preserving identity verification across digital environments without reliance on centralized authorities or intermediaries.

1.1 Evolution of Digital Identity in the Era of Digitalization

Digital identity systems have undergone substantial transformation since their inception, evolving from simple username-password combinations to sophisticated multi-factor authentication frameworks. The proliferation of digital services across

financial, healthcare, governmental, and commercial domains has exponentially increased the number of digital identities managed by individuals, creating fragmentation and inconsistent security practices. Contemporary identity management extends beyond basic authentication to encompass comprehensive profile management, consent mechanisms, and cross-platform verification capabilities [2]. Modern frameworks increasingly incorporate biometric verification, behavior-based authentication, and contextual risk assessment to enhance security while improving user experience. This evolution reflects broader technological shifts toward mobile-first interfaces, cloud-based services, and interconnected digital ecosystems requiring seamless yet secure identity verification across diverse platforms and applications.

1.2 Vulnerabilities and Limitations of Traditional Identity Systems

Traditional identity systems exhibit fundamental structural vulnerabilities stemming from their centralized architectures and custodial data management approaches [1]. The concentration of personally identifiable information within central repositories creates attractive targets for malicious actors, evidenced by numerous high-profile data breaches affecting millions of users. Beyond security concerns, these systems frequently compromise user privacy through excessive data collection and limited disclosure control mechanisms. Users typically lack genuine ownership of their identity credentials, instead relying on third-party providers who maintain ultimate control over verification processes, attribute management, and credential revocation [2]. This dependency relationship creates significant limitations regarding credential portability, cross-domain verification, and user autonomy in managing digital identity presentations across diverse service contexts.

Traditional Identity System Characteristics	Key Vulnerabilities and Limitations
Centralized data storage	Single points of failure creating high-value targets for attackers, catastrophic breach potential affecting millions of users simultaneously
Third-party dependency	Reliance on intermediaries for verification, limited user control over personal data, identity provider service disruptions affecting multiple services
Static credential verification	Susceptibility to credential theft, replay attacks, and unauthorized access through compromised authentication factors
Limited portability	Fragmented identities across services, repetitive registration requirements, inconsistent security practices across platforms
Extensive data collection	Privacy vulnerabilities through unnecessary attribute disclosure, data mining risks, and correlation of user activities across services
Jurisdictional constraints	Compliance challenges across regulatory boundaries, interoperability issues between identity frameworks, and limited global recognition

Table 1: Vulnerabilities and Limitations of Traditional Identity Systems [1,2]

2. Foundations of Blockchain for Decentralized Identity

Blockchain technologies provide essential infrastructure for implementing secure, user-controlled digital identity systems through distributed verification mechanisms [3].

2.1 Distributed Ledger Architecture

The distributed ledger architecture underlying blockchain emerged in 2008 as a framework for decentralized transaction validation [3]. Initially conceptualized for cryptocurrency applications, this approach has evolved to address broader implementations, including identity management. The fundamental innovation eliminates dependency on centralized authorities, instead distributing validation across participating nodes, maintaining consensus through cryptographic protocols. This arrangement creates resistance to manipulation, as alterations require simultaneous modification across multiple independent ledger copies. The chronological chaining of transaction blocks through cryptographic linkage further strengthens data integrity by establishing immutable historical records [4].

2.2 Blockchain Typologies and Identity Applications

Blockchain implementations for identity management follow two principal architectural patterns [3]. Public blockchain architectures operate as permissionless systems, allowing unrestricted participation in transaction validation. These systems maximize transparency and censorship resistance, making them suitable for identity applications requiring independence from centralized authorities. Security derives from cryptographic verification rather than participant vetting. Permissioned blockchain architectures restrict participation to authorized validators, creating controlled environments with enhanced privacy characteristics and transaction throughput capabilities. These systems typically employ governance frameworks limiting network participation while maintaining distributed validation principles [4].

2.3 Fundamental Principles for Identity Systems

Blockchain-based identity systems derive their capabilities from three fundamental principles [4]. Decentralization eliminates single points of failure by distributing identity verification across independent participants, preventing service disruption through individual node failures. Transparency enables credential verification without reliance on centralized authorities, allowing authorized participants to independently confirm identity assertions through cryptographic verification. Immutability establishes permanent records of credential issuance and verification activities, creating auditable histories that prevent unauthorized alterations [3].

3. Self-Sovereign Identity Architecture

Self-sovereign identity (SSI) represents a fundamental shift in digital identity management, transferring control from institutional authorities to individuals. This architectural approach leverages blockchain's distributed verification capabilities to establish credential frameworks where users maintain exclusive control over identity information [4]. Unlike conventional systems where credentials remain under issuer control, SSI architectures enable individuals to store credentials locally while using blockchain for verification without revealing underlying data. This separation creates privacy-preserving verification pathways while eliminating dependencies on credential issuers after initial certification [5]. The technical implementation typically involves decentralized identifiers anchored to blockchain networks, verifiable credentials issued by trusted entities, and digital wallets for secure credential storage and presentation, collectively creating infrastructures for portable, user-controlled digital identity.

3.1 Principles of User-Controlled Identity

User-controlled identity systems operate on essential principles that distinguish them from traditional identity frameworks [4]. The principle of existence establishes that digital identities exist independently of specific platforms or authorities, ensuring persistence across different service contexts. Persistence guarantees that identities remain consistent and accessible regardless of issuer availability or status changes. Control principles ensure exclusive user authority over identity presentations, preventing unauthorized disclosure through intermediaries. Transparency requirements mandate a clear understanding of how identity data functions and who maintains verification capabilities. Minimalism and contextual presentation principles limit disclosure to necessary attributes for specific verification contexts, enhancing privacy through selective revelation rather than complete credential exposure [5].

3.2 Reduced Dependence on Third-Party Authorities

The architectural design of self-sovereign identity systems deliberately minimizes dependencies on centralized authorities after initial credential issuance [5]. Traditional identity frameworks require continuous availability of identity providers for verification processes, creating fragility through reliance on these intermediaries. Blockchain-based SSI systems, conversely, enable offline verification through cryptographic proofs that validate credential authenticity without contacting issuers. This capability addresses critical limitations in conventional systems, particularly in contexts where connectivity constraints or issuer unavailability would otherwise prevent successful authentication. The elimination of centralized honeypots containing aggregated identity data reduces breach vulnerability while preventing correlation capabilities that compromise privacy through cross-context tracking [4]. Operational continuity improves significantly as verification processes continue functioning despite issuer service interruptions or organizational changes.

4. Decentralized Identifiers (DIDs) Implementation

Decentralized Identifiers (DIDs) provide the foundational infrastructure for blockchain-based identity systems by establishing persistent digital identifiers that remain under the exclusive control of their creators [5]. Unlike conventional identifiers that depend on centralized registries, DIDs leverage distributed ledger technology to enable self-sovereign identity management without intermediary dependencies [6]. These globally unique identifiers maintain persistence across platforms while preserving privacy through cryptographic mechanisms that prevent correlation across different services and contexts. The implementation architecture separates identifier registration from ongoing authentication processes, creating robust identity frameworks resistant to censorship and institutional control.

4.1 Technical Structure and Components

The technical structure of Decentralized Identifiers follows a standardized format comprising three essential components: the scheme identifier, method specification, and method-specific identifier [5]. This standardized structure ensures cross-platform interoperability while accommodating diverse blockchain implementations. DID documents, stored on distributed ledgers, contain cryptographic material including verification methods, authentication protocols, and service endpoints required for identity verification. The separation between identifiers and verification methods enables cryptographic rotation without identifier changes, addressing key management challenges inherent in distributed systems [6]. Resolution mechanisms transform DIDs into DID documents through standardized processes that locate and retrieve associated data from appropriate ledgers, establishing the cryptographic connection between identifiers and their controllers while maintaining the privacy-preserving characteristics essential for secure digital identity.

4.2 Authentication Mechanisms Across Digital Platforms

Authentication mechanisms for Decentralized Identifiers enable consistent identity verification across heterogeneous digital platforms without revealing underlying credential details [6]. Challenge-response protocols verify identifier control through cryptographic operations that demonstrate possession of corresponding private keys without exposing sensitive cryptographic material. These mechanisms support both synchronous and asynchronous verification workflows, accommodating diverse interaction patterns across digital services. The cryptographic foundation enables zero-knowledge proofs that verify credential attributes without disclosing actual values, enhancing privacy through minimal information disclosure [5]. Authentication flexibility extends to delegation capabilities, allowing controlled authentication by designated third parties while maintaining cryptographic verification paths to original identifier controllers. This architecture supports sophisticated access management scenarios while preserving the fundamental self-sovereign characteristics that distinguish DID-based authentication from conventional centralized approaches.

5. Verifiable Credentials Framework

Verifiable Credentials (VCs) establish a standardized format for expressing and cryptographically validating digital attestations within blockchain-based identity systems [7]. These credentials enable trusted entities to issue tamper-evident claims that individuals can store independently and present selectively across diverse service contexts. The framework separates the roles of issuers, holders, and verifiers, creating a privacy-preserving triangle of trust that eliminates continuous issuer dependency while maintaining credential authenticity through cryptographic validation mechanisms [7].

5.1 Cryptographic Validation Processes

The cryptographic foundations of Verifiable Credentials ensure data integrity and source authenticity through digital signatures that bind credential content to issuing authorities [7]. These signatures utilize public-key cryptography, where issuers sign credentials with private keys while corresponding public keys enable verification without requiring issuer availability. The validation process confirms signature integrity, credential structure compliance, and issuer legitimacy through cryptographic material anchored to blockchain networks. Additionally, revocation mechanisms enable credential invalidation without accessing or modifying the credential itself, typically through cryptographic accumulators or status registries that maintain privacy while providing authoritative status information [7].

5.2 Credential Issuance and Verification Workflows

Verifiable Credential workflows encompass structured processes for issuance, storage, presentation, and verification across distributed identity ecosystems [7]. The issuance process begins with subject authentication, followed by attribute verification and credential generation with appropriate cryptographic signatures and metadata. Holders store these credentials in digital wallets with cryptographic protection, maintaining exclusive control over subsequent presentations. When authentication requirements arise, holders generate presentations containing only necessary credential attributes, preserving privacy through selective disclosure. Verification workflows validate cryptographic integrity, confirm issuer authorization, check revocation status, and evaluate credential properties, including expiration dates and usage restrictions, without contacting issuers, creating efficient verification pathways that function across organizational boundaries [7].

6. Enhanced Security Through Immutability

Blockchain immutability provides fundamental security enhancements for digital identity systems through cryptographically secured, tamper-evident record keeping [8]. Unlike conventional databases vulnerable to unauthorized modifications, blockchain-based identity systems create append-only structures where previous records remain permanently visible and verifiable. This architectural characteristic prevents retroactive alterations to identity assertions, credential issuance events, and authentication activities, establishing authoritative historical records that resist manipulation attempts while creating transparent audit trails accessible to authorized participants [8].

6.1 Tamper-Resistant Identity Records

The tamper-resistance of blockchain-based identity records derives from distributed consensus mechanisms that validate and permanently record identity transactions [8]. Each identity assertion or credential issuance undergoes validation through cryptographic consensus protocols before permanent recording in blocks linked through cryptographic hashing. This structure creates computational impracticality for retroactive modifications, as alterations would require consensus manipulation across multiple distributed nodes maintaining independent ledger copies. The resulting immutable records establish definitive chronologies for credential issuance, revocation events, and authorization changes, creating persistent historical documentation that remains independently verifiable regardless of subsequent system or organizational changes [8].

6.2 Mitigation of Fraud and Identity Theft

Immutable blockchain records substantially mitigate identity fraud through cryptographic verification pathways that eliminate common attack vectors present in traditional systems [8]. The prevention of retroactive record manipulation removes opportunities for credential falsification, unauthorized privilege escalation, and historical revision attacks frequently targeting centralized identity databases. Cryptographic binding between identifiers and controllers prevents successful impersonation, as attackers cannot modify controller designations without detection. Additionally, transparent historical records enable anomaly detection through pattern analysis, identifying suspicious modification attempts or credential presentations inconsistent with established behavioral patterns. These capabilities collectively reduce attack surface while enhancing forensic capabilities for investigating compromise attempts [8].

7. Privacy Preservation Capabilities

Blockchain-based identity systems offer advanced privacy preservation capabilities that fundamentally transform how personal information functions within digital environments [8]. Unlike conventional identity frameworks, where complete credential disclosure occurs during verification, decentralized architectures enable granular information control through cryptographic mechanisms that support minimal disclosure principles. These capabilities address growing privacy concerns related to data aggregation, surveillance capabilities, and cross-context tracking by establishing technical frameworks where individuals determine precisely what information becomes accessible during authentication processes [9]. The resulting privacy architecture aligns technological capabilities with emerging regulatory requirements while responding to increasing user demand for enhanced personal data protection.

7.1 User Control Over Personal Data Disclosure

The architectural design of blockchain-based identity systems places comprehensive control over personal data disclosure with individual users rather than institutional custodians [8]. Self-custodial credential storage eliminates dependency on third-party data repositories, preventing unauthorized access through institutional compromise. Cryptographic mechanisms enable users to create multiple derived identifiers from a single master key, preventing correlation across different service contexts. This identifier compartmentalization establishes domain-specific personas that resist tracking while maintaining cryptographic verifiability. Additionally, consent mechanisms embedded within verification protocols create auditable records of disclosure permissions, establishing technical enforcement of data sharing boundaries that prevent function creep and unauthorized repurposing of identity information [9].

7.2 Minimized Data Exposure Through Selective Disclosure

Selective disclosure capabilities enable credential verification without revealing complete credential contents, substantially reducing unnecessary data exposure during authentication processes [9]. Zero-knowledge proof mechanisms verify specific attributes or conditions without transferring actual credential values, allowing binary confirmation of qualifications or characteristics without revealing underlying data. Predicate proofs enable verification of relational conditions such as age thresholds or geographic parameters without disclosing precise values, supporting regulatory compliance while preserving informational privacy. These cryptographic capabilities eliminate the traditional correlation between authentication strength and privacy sacrifice, enabling high-assurance verification without comprehensive data exposure [8]. Implementation frameworks support progressive disclosure patterns where initial interactions reveal minimal information, with additional attributes disclosed only when specifically required for subsequent interaction stages.

8. Implementation Domains: Blockchain-Based Identity Applications

The practical implementation of blockchain-based identity solutions extends across multiple sectors, demonstrating the versatility and transformative potential of decentralized identity architectures. These implementations address domain-specific challenges while leveraging the fundamental security and privacy advantages inherent in distributed ledger technologies [9].

8.1 Financial Services Identity Verification

Financial institutions have emerged as early adopters of blockchain-based identity solutions, recognizing significant operational efficiencies and security enhancements compared to traditional verification methods. The implementation of decentralized

identity frameworks in banking environments reduces dependency on centralized credential repositories, thereby minimizing exposure to large-scale data breaches that historically characterize the sector. Financial service providers utilizing these technologies report substantial reductions in customer onboarding timeframes while simultaneously strengthening compliance with regulatory requirements [9].

The integration of blockchain-based identity verification with Know Your Customer (KYC) protocols demonstrates particular promise, enabling credential reusability across institutional boundaries while maintaining regulatory compliance. This cross-institutional verification capability significantly reduces redundant identity verification processes, creating measurable cost efficiencies while enhancing customer experiences. Leading financial entities have established industry consortia dedicated to developing standardized implementations that enable verifiable credential exchange while preserving privacy and security requirements essential to financial transactions [10].

8.2 Healthcare Data Access and Consent Management

Healthcare environments present unique identity verification challenges due to heightened privacy requirements, complex authorization hierarchies, and the sensitive nature of medical information. Blockchain-based identity frameworks offer sophisticated consent management capabilities, enabling patients to maintain granular control over health data access while creating immutable audit trails for all information exchanges [10]. The implementation of decentralized identifiers in healthcare settings facilitates secure authentication across organizational boundaries, addressing interoperability challenges that frequently impede information exchange between providers. This cross-institutional capability proves particularly valuable for patient mobility scenarios, emergency access situations, and coordinated care delivery involving multiple specialists. Early implementations demonstrate enhanced privacy protection through selective disclosure mechanisms that reveal only necessary attributes while maintaining comprehensive provenance records of all credential presentations and verifications [9].

9. Centralized vs. Blockchain Identity Architectures

Understanding the fundamental architectural differences between traditional and blockchain-based identity systems provides essential context for evaluating their respective capabilities and limitations [10]. Traditional identity architectures centralize control and data storage within institutional boundaries, creating streamlined management at the cost of consolidated vulnerability. In contrast, blockchain-based architectures distribute verification processes across decentralized networks, eliminating single points of failure while enhancing user autonomy [10]. These structural distinctions manifest across multiple dimensions, including authentication mechanisms, administrative models, security profiles, and privacy characteristics. The following comparative analysis examines these architectural variances to establish a framework for evaluating implementation considerations across different operational contexts.

Architectural Component	Traditional Centralized Architecture	Blockchain-Based Decentralized Architecture
Authentication Protocol	Unified authentication through consolidated portals	Distributed verification across independent services
Operational Environment	Unified management within the singular domain	Distributed operations across multiple environments
Administrative Authority	Consolidated governance and policy enforcement	Distributed control with user sovereignty
System Resilience	Vulnerability to singular failure points	Enhanced fault tolerance through distribution
Interface Complexity	Streamlined user experience with reduced complexity	Enhanced user agency with increased interaction requirements
Information Architecture	Centralized data repositories with aggregated storage	Distributed credential management with local storage
Privacy Characteristics	Limited disclosure control with institutional management	Enhanced selective disclosure with user-determined sharing
Security Profile	Concentrated attack surface with breach magnification	Distributed risk profile with impact containment

Table 2: Comparative Analysis of Identity Management Architectures [4], [5]

10. Challenges in Adoption

Contemporary digital identity verification methodologies predominantly rely on centralized management frameworks administered by governmental entities, financial institutions, and major technology corporations. These centralized architectures necessitate the aggregation and storage of substantial volumes of personally identifiable information, creating significant security vulnerabilities and attack vectors for malicious actors. The Equifax security breach of 2017, which compromised the confidential data of approximately 147 million American citizens, exemplifies the inherent vulnerabilities associated with centralized identity repositories [11].

While blockchain technology demonstrates considerable transformative potential for digital identity management, implementation challenges persist. Current blockchain-based identity solutions remain in nascent developmental stages, requiring broader adoption across digital environments. Interoperability concerns present additional complexity, specifically, establishing coherent communication protocols between disparate blockchain platforms to ensure frictionless identity verification across heterogeneous service domains [11]. Additionally, the establishment of globally recognized standards and regulatory frameworks remains essential to ensure universal acceptance of blockchain-based identity credentials.

Feature	Traditional Centralized Identity	Blockchain-Based Identity	Benefits
Data Storage	Stored in centralized databases	Distributed across network nodes	Enhanced security through the elimination of single points of failure
User Control	Limited; managed by third parties	High; user-controlled credentials	Greater privacy and personal data sovereignty
Verification Process	Requires intermediary validation	Direct cryptographic verification	Reduced dependency on institutional verification
Accessibility	Requires formal documentation	Accessible without prerequisites	Inclusion of underserved populations
Vulnerability to Breaches	High risk of mass data exposure	Distributed risk profile	Improved resistance to large-scale data compromises
Trust Framework	Institution-dependent	Cryptographically assured	Mathematically verifiable trust mechanisms
Global Portability	Limited by jurisdictional boundaries	Borderless verification potential	Universal accessibility across geographic regions
Implementation Status	Widely established	Early adoption phase	Opportunity for standards development
Applications	Primarily formal identification	Extends to credential verification	Broader utility across digital services
Privacy Controls	Limited selective disclosure	Granular attribute disclosure	Enhanced protection of sensitive information

Table 3: Comparison of Traditional and Blockchain-Based Identity Management [11,12]

10.1. Challenges in Blockchain-Based Identity Adoption

Through decentralized identity management protocols, individuals can establish and verify their identities utilizing cryptographically secured credentials maintained in digital wallet infrastructures. These digital identifiers achieve verification through distributed public blockchain networks, ensuring global accessibility [12]. This technological paradigm presents

significant implications for economic inclusion, enabling individuals lacking traditional documentation to establish financial accounts, register for essential services, and participate meaningfully in digital economic activities.

Several national jurisdictions, including India, have initiated the implementation of blockchain-based identity frameworks to complement existing systems such as Aadhaar. Similarly, international organizations, including the United Nations and World Bank, actively explore blockchain solutions addressing global identity challenges, particularly for refugee and displaced populations [12].

Challenges and Solutions	Key Points
Performance Issues	Limited transaction speed, high energy usage, and slow verification times
Technical Solutions	Layer-two scaling methods, proof-of-stake systems, faster verification paths
Implementation Status	Ongoing optimization work, adoption of efficient models, and improvement of response times
Governance Problems	No unified standards, regulatory compliance issues, and fragmented management
Governance Solutions	Standard protocols development, working with regulators, and industry partnerships
Progress Made	Core standards emerging, testing in regulatory sandboxes, and better industry coordination

Table 4: Challenges in Blockchain-Based Identity Adoption [11]

11. *Conclusions*

The integration of blockchain technology with digital identity management demonstrates transformative potential across technical, social, and economic dimensions. Blockchain-based identity solutions fundamentally restructure identity verification by eliminating intermediary dependencies while enhancing security through cryptographic protection and distributed consensus mechanisms. The resulting architectures resist tampering, unauthorized modification, and credential forgery through immutable record-keeping and cryptographic binding between identifiers and their controllers. User-centric identity ecosystems enabled by blockchain technology deliver meaningful benefits, including enhanced privacy through selective disclosure capabilities, reduced credential replication across multiple systems, and simplified identity verification across organizational boundaries. These advantages translate into practical improvements for both individuals and organizations, reducing administrative overhead while strengthening security postures against increasingly sophisticated threats. The sovereignty provided to identity holders represents a significant advancement in digital rights, allowing individuals to control their data and manage consent in previously impossible ways. Future implementation pathways will likely focus on scalability enhancements, including layer-two solutions and optimized consensus mechanisms specifically designed for identity management requirements. Standardization efforts around credential formats, verification protocols, and trust frameworks will prove essential for widespread adoption, requiring coordination across technical communities, regulatory bodies, and industry stakeholders. As these technological foundations mature, blockchain-based identity solutions stand poised to address longstanding challenges in digital identity management while enabling new models for secure, private authentication across digital environments.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.
The opinions stated are personal and do not represent the stance or policies of any affiliated entity.

References

[1] Aarti Amod Agarkar et al., "Blockchain aware decentralized identity management and access control system," ScienceDirect, vol. 31, Feb. 2024. https://www.sciencedirect.com/science/article/pii/S2665917424000084

[2] Atharva Thorve et al., "Decentralized Identity Management Using Blockchain," in 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Dec. 2022, doi: 10.1109/ICAC3N56670.2022.10074477. https://www.researchgate.net/publication/369616566_Decentralized_Identity_Management_Using_Blockchain

[3] Blockchain Identity Management Institute, "Identity Decentralization and Blockchain." https://identitymanagementinstitute.org/identity-decentralization-and-blockchain/

[4] Christopher Dabhi, "How Does Blockchain Enhance Privacy in Digital Identity Systems?" Aliancetek.com, Jan. 2025. https://www.alliancetek.com/blog/post/2025/01/01/blockchain-privacy-digital-identity-systems.aspx

[5] Consensys, "Blockchain in Digital Identity," https://consensys.io/blockchain-use-cases/digital-identity

[6] Dock Labs, "Blockchain Identity Management: Beginner's Guide 2025," Apr. 2025. https://www.dock.io/post/blockchain-identity-management

[7] Hao Yu et al., "Blockchain-enabled privacy protection scheme for IoT digital identity management," ScienceDirect, Mar. 2025. https://www.sciencedirect.com/science/article/pii/S2667295225000248

[8] IBM, "Blockchain for digital identity and credentials." https://www.ibm.com/blockchain-identity

[9] Kosmos, "Blockchain Identity Management: A Complete Guide," Jul. 2024. https://www.1kosmos.com/blockchain/blockchain-identity-management-a-complete-guide-2/

[10] Okta, "Decentralized Identity: The future of digital Identity management," Sep. 2024. https://www.okta.com/blog/2021/01/what-is-decentralized-identity/

[11] Sangeeta Shah Bharadwaj et al., "Decentralized Identity Management Using Blockchain: Cube Framework for Secure Usage of IS Resources," Journal of Global Information Management, Dec. 2022.https://dl.acm.org/doi/abs/10.4018/JGIM.315283