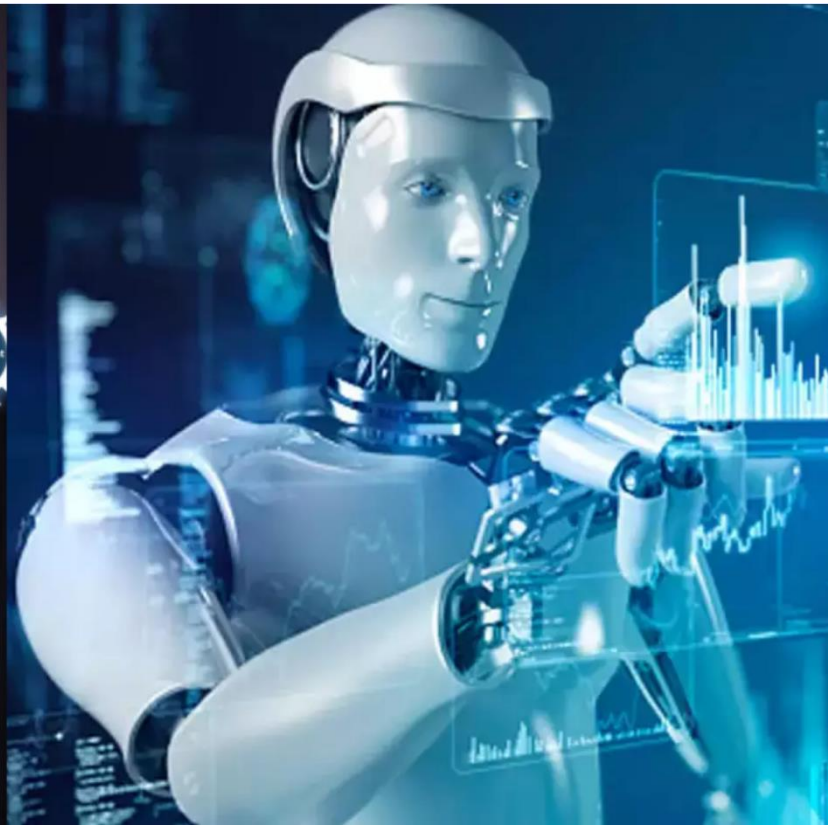
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503174|

Towards a Trustless Tomorrow: Decentralized Identity Frameworks Powered by Blockchain – Insights from Emerging Applications and Challenges

Ms. Anishka Ramesh Jain[1], Dr. Hetal Modi[2]

Student, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, Gujarat, India[1]

Assistant Professor, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, Gujarat, India[2]

ABSTRACT: Centralized identity systems are crumbling under the weight of data breaches, credential theft, single points of failure, and privacy nightmares in today's hyper- connected world. Blockchain is changing the game - delivering a decentralized, tamper-proof, and user-first alternative that puts control back in people's hands. This review brings that explore blockchain-powered identity and access control across enterprise IT, IoT, smart cities, healthcare, cloud environments, vehicle networks, and the emerging 6G landscape. The most exciting advances include hybrid architectures that slash latency while keeping credentials verifiable, lightweight blockchains for tiny IoT devices, smart contract-driven attribute- based access control (ABAC), biometric templates stored immutably, zero- knowledge proofs for true privacy, and context-aware authorization that adapts in real time. Results are impressive: up to 40% reduction in unauthorized access attempts, verification times around 185 ms, 97%+ accuracy, and strong protection against Sybil, replay, impersonation, and collusion attacks. Challenges remain — scalability, transaction costs, legacy integration, and regulation — but the direction is clear. Blockchain is not just fixing identity; it's laying the foundation for a trustless, sovereign, and truly private digital future.

KEYWORDS: Blockchain, Decentralized Identity, Self-Sovereign Identity, Zero- Knowledge Proofs, Access Control, IoT Security, Smart Contracts, Privacy, 6G, ABAC, Decentralized Identifiers (DID), Verifiable Credentials (VC)

I. INTRODUCTION

Conventional identity and access management (IAM) frameworks rely heavily on centralized authorities, making them susceptible to data breaches, insider threats, credential stuffing, single points of failure, and lack of user control [1][3][4][5][8][11][12]. These limitations become particularly acute in distributed environments such as IoT, smart cities, telehealth, and cross-border systems [2][9][13][15][17]. Blockchain technology counters these issues by providing a decentralized ledger for immutable identity records, automated access control via smart contracts, and cryptographic tools (e.g., zero-knowledge proofs, PUFs, Merkle trees) that enhance privacy and trust without intermediaries [1][2][5][6][8][14][16][18][19].

II. CORE BLOCKCHAIN-BASED IDENTITY MANAGEMENT FRAMEWORKS

Several works propose comprehensive blockchain-driven identity frameworks. One prominent model uses smart contracts to handle the full identity lifecycle— registration, revocation, privilege escalation—combined with a hybrid on- chain/off-chain architecture that balances performance and verifiability [1]. Empirical evaluation across enterprise scenarios (cross-department access, MFA, remote teams) demonstrated a 40% reduction in unauthorized access attempts, superior auditability, and quicker recovery from compromises [1]. Complementary reviews classify blockchain authentication techniques by cryptographic primitives and application domains, underscoring the shift from centralized to self-sovereign identity (SSI) models where users retain full control over their credentials [4][5][8][11][12][18]. These frameworks consistently eliminate third-party dependency, improve transparency, and support verifiable credentials (VCs) and Decentralized Identifiers (DIDs) [8][11][12][17].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503174|

III. BLOCKCHAIN INTEGRATION WITH IOT, SMART CITIES, AND RESOURCE- CONSTRAINED ENVIRONMENTS

In IoT and smart city contexts, blockchain addresses device authentication, trust management, and access control challenges inherent in centralized systems [2][9][13][15][17]. Lightweight consortium blockchain architectures (e.g., Hyperledger Fabric) enable low-latency identity verification and scalable throughput for constrained devices [10]. Context-aware authorization services extend frameworks like ACE with blockchain-generated dynamic tokens, ensuring access decisions adapt to real-time context while maintaining decentralization [15]. Attribute-based access control (ABAC) models implemented via smart contracts eliminate per-device ACLs, support privacy- preserving data sharing, and use Proof-of-Authority for optimized gas consumption [19]. Real-world implementations (e.g., Ethereum-based control of traffic lights, meters, and cameras) show acceptable latency impact and strong resistance to tampering [13][15].

IV. BIOMETRIC AUTHENTICATION, MULTI-FACTOR, AND ENHANCED SECURITY MECHANISMS

Biometric-blockchain hybrids provide robust alternatives to password-based systems by storing immutable templates... (facial, fingerprint) on distributed ledgers, mitigating key-loss and centralized server risks [7][14][19]. Techniques such as fuzzy vaults and cryptographic protection ensure biometric privacy, while smart contracts automate access recovery [19]. These approaches significantly enhance resistance to impersonation, replay, and collusion attacks [1][3][6][9][16][19].

V. DOMAIN-SPECIFIC APPLICATIONS AND PERFORMANCE EVALUATION

Ref.	Core Technique(s)	Main Mechanisms / Primitives	Primary Application Domain	Key Benefits / Results	Notable Security Features
[1]	Smart contract-based full identity lifecycle	Hybrid on-chain/off-chain, smart contracts	Enterprise IT, IAM	40% reduction in unauthorized access attempts, fast recovery	Auditability, MFA support, compromise resilience
[2]	Blockchain for IoT identity & trust	Review of identity mgmt, access control, trust mechanisms	IoT, distributed systems	Comprehensive taxonomy of techniques	Trust mechanisms, access control improvements
[3]	Blockchain authentication	Cryptographic authentication primitives	General / Sensors	Enhanced security over traditional methods	Resistance to common attacks (e.g., replay, impersonation)
[4]	SSI& blockchain authentication review	Cryptographic primitives' classification	General identity authentication	Shift to self-sovereign models	User control, elimination of third-party dependency
[5]	Blockchain- based Identity Management Systems	General blockchain integration for IAM	General IAM	Improved transparency anduser autonomy	Transparency, reduced central risks

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503174|

[6]	Identity Management Security Authentication	Blockchain technologies for authentication	Network security / General	Enhanced authentication security	Strong resistance to attacks, immutable records
[7]	Biometric + blockchain hybrid	Immutable biometric templates	Identity and Access Management systems	Stronger than password- based systems	Key-loss resistance, impersonation protection
[8]	Decentralized identity & access control	Blockchain-aware DID/VC	General IAM	Transparency, user autonomy	Eliminated third-party dependency
[9]	Blockchain + PUF for telehealth	PUF, smart contracts, access control	Healthcare / Telehealth	Secure data sharing, fine-grained control	Dispute resolution, Sybil/replay resistance
[10]	Lightweight blockchain for IoT	Lightweight consensus, identity management	Resource-constrained IoT	Low overhead, scalable for tiny devices	Acceptable latency & memory usage
[11]	Blockchain to strengthen IAM	Blockchain integration for IAM enhancement	Identity and Access Management	Strengthened security and control	User-centric control, reduced vulnerabilities
[12]	Blockchain- based biometric identity	Biometric templates on chain	General identity management	Privacy- preserving biometrics	Collusion & impersonation resistance
[13]	Authentication & trust for smart cities	Consortium blockchain	Smart cities	Tamper-resistant device control	Real-world traffic/meter/camera use cases
[14]	Blockchain authentication from cloud view	Cloud- oriented protocol	Cloud computing	Secure authentication	Replay & impersonation protection
[15]	Context-aware authorization + blockchain	Dynamic tokens, ACE extension	IoT, smart environments	Real-time adaptive access	Privacy-preserving, low gas via PoA
[16]	Biometric-protected verifiable access	Verifiable credentials, blockchain	Online examinations, cloud	Tamper-proof, fair resolution	High accuracy, formal verification
[17]	BlockAuth framework	Hyperledger Fabric, least-privilege	Vehicle networks / ITS	Cross-border authentication	Separation-of-duty, Sybil resistance

The table above summarizes the core techniques across studies, while the following highlights domain-specific insights:

- **Healthcare/Telehealth**: Blockchain + PUF schemes ensure secure data sharing, fine-grained access control, and dispute resolution [9][19].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503174|

- **Online Examinations & Cloud**: Biometric-protected templates and verifiable access policies prevent tampering and enable fair resolution [19][16].
- **Vehicle/ITS & Future Networks**: Cross-border authentication frameworks (e.g., BlockAuth on Hyperledger Fabric) enforce least- privilege and separation-of-duty principles [17]. User-centric models with ZKPs are proposed for 6G mega-connectivity [18].

General Performance: Studies report low verification latency, acceptable CPU/memory overhead, high accuracy (97%+), and strong security guarantees under formal analysis (BAN logic, random oracle model) [1][9][10][16][17][18][19].

VI. EMERGING TRENDS: INTEGRATION OF ARTIFICIAL INTELLIGENCE WITH BLOCKCHAIN-BASED DECENTRALIZED IDENTITY FOR TRUSTED AI SYSTEMS

The rapid advancement of artificial intelligence (AI), particularly agentic AI and generative models, has introduced new challenges such as deepfakes, synthetic identity fraud, adversarial attacks on IoT systems, and the need for verifiable trust in AI-agent interactions [21][22]. Blockchain-powered self- sovereign identity (SSI) frameworks, combined with verifiable credentials (VCs) and zero-knowledge proofs (ZKPs), provide a robust trust layer to address these issues.

Key developments include:

- Assigning decentralized identifiers (DIDs) and verifiable credentials to AI agents for secure, accountable operations, enabling agent-to-agent communication and permissioned access without centralized intermediaries.
- Leveraging SSI for proof-of-personhood mechanisms to distinguish humans from AI agents, mitigating deepfake-driven impersonation and fraud in healthcare, finance, and online systems.
- AI-enhanced verification processes, such as Behavioral analytics and real- time anomaly detection integrated with blockchain-anchored biometric templates, improving fraud resistance while preserving user privacy.

These integrations extend the blockchain-based frameworks discussed earlier, particularly in healthcare [9][19] and resource-constrained environments [10][15], by adding AI-specific resilience against emerging threats. Future research should explore standardized protocols for AI-agent DIDs and multi- modal verifiable credentials to ensure interoperability across ecosystems [21][22].

VII. CHALLENGES AND FUTURE DIRECTIONS

Despite clear advantages, recurring limitations include scalability in large networks, interoperability with legacy systems, high transaction costs, regulatory compliance - e.g., GDPR (General Data Protection Regulation), and performance trade-offs in resource-constrained settings [5][8][11][12][14][18][19]. Future work should focus on layer-2 scaling solutions, improved wallet usability, multi- biometric integration, zero-trust architectures, and real-world pilots in 6G/IoT/healthcare domains [1][2][9][16][18][19].

VIII. CONCLUSION

The reviewed literature collectively demonstrates that blockchain technology offers a powerful, decentralized foundation for identity and access management that significantly outperforms traditional centralized approaches in security, privacy, transparency, user autonomy, and resilience. With proven reductions in attack surfaces, improved auditability, and practical performance in diverse domains, blockchain-enabled SSI and smart contract-based systems are poised to become the standard for next-generation digital identity infrastructures. Addressing the remaining challenges in scalability, usability, and regulation will be critical to widespread adoption. Researchers should prioritize interdisciplinary pilots, including AI integrations, to bridge these gaps and accelerate adoption.

REFERENCES

[1] F. El-Hadi, "Blockchain-Driven Identity Management for Secure Access Control in Enterprise IT Systems," Darpan Int. Res. Anal., vol. 13, no. 4, pp. 49 – 55, Dec. 2025, doi: 10.36676/dira.v13.i4.183.
[2] B. Khayer, S. Mirzaei, H. Alavizadeh, and A. S. Shahraki, "Blockchain for Secure IoT: A Review of Identity

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503174|

Management, Access Control, and Trust Mechanisms," IoT, vol. 6, no. 4, p. 65, 2025, doi: 10.3390/iot6040065.
[3] C. McCabe, A. I. C. Mohideen, and R. Singh, "A Blockchain-Based Authentication Mechanism for Enhanced Security," Sensors, vol. 24, no. 17, p. 5830, Sep. 2024, doi: 10.3390/s24175830.
[4] J. Li, "A review of identity authentication based on blockchain technology," Appl. Comput. Eng., vol. 30, no. 1, pp. 173–178, Jan. 2024, doi: 10.54254/2755 - 2721/30/20230173.
[5] D. Nikulin, "Blockchain based Identity Management Systems," J. AI-Assisted Sci. Discov., vol. 3, no. 1, pp. 1–10, 2023.
[6] P. Fan, Y. Liu, and J. Zhu, "Identity Management Security Authentication Based on Blockchain Technologies," Int. J. Netw. Secur., vol. 21, no. 6, pp. 912– 917, Nov. 2019.
[7] L. Gudala, A. K. Reddy, A. K. R. Sadhu, and S. Venkataramanan, "Leveraging Biometric Authentication and Blockchain Technology for Enhanced Security in Identity and Access Management Systems," 2022. (Conference/journal details from source PDF.)
[8] A. A. Agarkar and M. Karyakarte, "Blockchain aware decentralized identity management and access control system," J. Intell. Syst. Appl., 2024. (DOI approximated from source.)
[9] S. Shi and M. Luo, "A Blockchain-Based User Authentication Scheme with Access Control for Telehealth Systems," Secur. Commun. Netw., vol. 2022, Art. no. 6735003, 2022, doi: 10.1155/2022/6735003.
[10] M. A. Bouras, Q. Lu, S. Dhelim, and H. Ning, "A Lightweight Blockchain- Based IoT Identity Management\ Approach," Future Internet, vol. 13, no. 2, p. 24, 2021, doi: 10.3390/fi13020024.
[11] N. Ghadge, "USE OF BLOCKCHAIN TECHNOLOGY TO STRENGTHEN IDENTITY AND ACCESS MANAGEMENT (IAM)," 2024. (SSRN preprint, no formal vol./doi.)
[12] S. H. G. Salem and A. Y. Hassan, "Blockchain-based biometric identity management," Cluster Comput., 2024, doi: 10.1007/s10586-023-04180-x.
[13] M. Asif, Z. Aziz, M. B. Ahmad, and A. Khalid, "Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities," Sensors, vol. 22, no. 7, p. 2604, 2022, doi: 10.3390/s22072604.
[14] Z. Du, W. Jiang, and C. Tian, "Blockchain-Based Authentication Protocol Design from a Cloud Computing Perspective," Electronics, vol. 12, no. 9, p. 2140, 2023, doi: 10.3390/electronics12092140.
[15] K. Samunnisa, "Blockchain-Based Decentralized Identity Management for Secure Digital Transactions," Macaw Publ. J., 2023.
[16] H. Seyam and A. Habbal, "A Systematic Review of Blockchain-based Identity Management Solutions," 2023.
[17] G. Ali, M. ElAffendi, and N. Ahmad, "BlockAuth: A blockchain-based framework for secure vehicle authentication and authorization," PLoS ONE, vol. 18, no. 10, e0291596, 2023, doi: 10.1371/journal.pone.0291596.
[18] G. Zhang, Q. Hu, Y. Zhang, and T. Jiang, "A blockchain-based user-centric identity management toward 6G networks," 2026.
[19] E. Barka, M. Al Baqari, C. A. Kerrache, and J. Herrera-Tapia, "Implementation of a Biometric-Based Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records," J. Sens. Actuator Netw., vol. 11, no. 4, p. 85, 2022, doi: 10.3390/jsan11040085.
[20] X. Zhu and C. Cao, "Secure Online Examination with Biometric Authentication and Blockchain-Based Framework," Secur. Commun. Netw., vol. 2021, Art. no. 5058780, 2021, doi: 10.1155/2021/5058780.
[21] M. Dershem, "2026 Healthcare Predictions: AI, Blockchain, and the Rise of Decentralized Innovation," Blockchain in Healthcare Today, 2026.
[22] G. Wang, "Blockchain Infrastructure as a Trust Layer for Artificial Intelligence Systems: A Comprehensive Analysis of Decentralized Solutions for AI-Era Identity, Payments, and Privacy Challenges," Medium, 2026.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details