iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VII **Month of publication:** July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73275

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Blockchain-Based Secure Identity for IoT Networks

M Rupasri, T Meenakshi, Y Gayatri
Dr. Lankapally Bullayya College, India

Abstract: ***This review article examines the state of blockchain-enabled identity management in Internet of Things (IoT) networks, focusing on decentralized and secure mechanisms for device identification, authentication, and access control. Traditional centralized identity systems face limitations such as single points of failure, scalability bottlenecks, and vulnerability to breaches. We systematically survey recent literature on blockchain-based frameworks applied to IoT, categorizing approaches by blockchain platform, identity credential models, consensus mechanisms, and smart contract implementations. The analysis highlights key performance metrics such as system latency, throughput, resource overhead, and energy consumption, and compares existing prototypes deployed across diverse IoT scenarios. We assess the security and privacy implications, including resistance to spoofing, Sybil attacks, unauthorized access, data tampering, and insider threats. Additionally, the review identifies open research challenges such as managing identity lifecycle in constrained devices, achieving interoperability across heterogeneous networks, balancing decentralization with scalability, and integrating with emerging technologies like edge computing and zero-knowledge proofs. Finally, we offer recommendations for future research directions and practical deployment strategies to advance blockchain-based identity solutions in IoT ecosystems. Our comprehensive synthesis aims to guide researchers and practitioners in developing robust, scalable, and trustworthy identity frameworks using blockchain for the evolving IoT landscape.***

Keywords: IoT identity management, blockchain, device authentication, smart contracts, security, privacy, decentralized systems.

I. INTRODUCTION

The Internet of Things (IoT) is rapidly transforming how physical systems interact with digital infrastructure, enabling a wide range of applications in smart homes, healthcare, manufacturing, transportation, and critical infrastructure. It is estimated that over 30 billion IoT devices will be connected by 2030, generating massive volumes of data and requiring robust communication, interoperability, and security protocols. As the scale and heterogeneity of IoT ecosystems grow, secure and reliable identity management becomes a fundamental requirement for maintaining trust, confidentiality, and operational integrity.

Traditional identity management solutions in IoT are predominantly centralized, relying on cloud-based authentication servers or trusted third-party identity providers to manage device enrollment, authentication, and revocation. However, these models present critical vulnerabilities, such as single points of failure, limited scalability, susceptibility to spoofing and impersonation attacks, and lack of transparency and auditability. In scenarios such as autonomous vehicle networks or smart grid systems, these limitations could lead to catastrophic failures or systemic breaches.

Blockchain technology has emerged as a potential enabler of decentralized and tamper-resistant identity management for IoT. As a distributed ledger maintained by consensus across multiple nodes, blockchain eliminates the need for centralized trust, ensuring that records of device identities and access transactions are immutable and verifiable. Smart contracts—self-executing code on the blockchain—can enforce identity policies such as device registration, authentication, delegation, and revocation, enabling automated and secure interactions among devices without centralized oversight.

Numerous blockchain-based identity models have been proposed to secure IoT networks, each with different design choices regarding ledger architecture (public, private, or consortium), consensus mechanisms (e.g., Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance), and identity frameworks (self-sovereign identity, decentralized identifiers, or public key infrastructures). For example, Sovrin and uPort offer self-sovereign identity systems built on blockchain, which could be adapted to IoT environments to grant devices control over their identity attributes without relying on centralized identity providers . Moreover, solutions such as IOTA and Hyperledger Fabric have been explored for their lightweight consensus protocols and suitability for resource-constrained IoT nodes.

Despite their promise, blockchain-based identity systems face several unresolved challenges, including energy consumption, latency, data privacy, and interoperability. Additionally, implementing identity lifecycle management (enrollment, authentication, update, revocation) across billions of devices with limited computational and storage capacity remains nontrivial. There is also an ongoing debate around balancing transparency with privacy, especially when storing identity data on immutable public ledgers.

This review paper systematically analyzes the current landscape of blockchain-based identity solutions for IoT. It classifies and compares existing frameworks based on architecture, performance, scalability, and security. Furthermore, it identifies key open research questions and offers future directions for designing secure, decentralized, and scalable identity management systems in IoT ecosystems.

II. LITERATURE REVIEW

The convergence of blockchain technology and Internet of Things (IoT) identity management has become a focal point of research in response to the shortcomings of traditional centralized solutions. This section reviews key contributions in the field, categorizing them by architectural model, identity management strategy, and security capabilities.

A. Centralized vs. Decentralized Identity in IoT

Traditional Public Key Infrastructure (PKI)-based solutions have long been used to manage IoT identities, but they rely on certificate authorities (CAs) that represent single points of failure . To overcome this, blockchain-based systems offer distributed trust mechanisms, eliminating centralized authorities and enhancing availability. For instance, analyzed existing centralized approaches and identified scalability and trust concerns as primary inhibitors for wide-scale IoT adoption.

B. Blockchain Architectures for IoT Identity

Several works have explored using public and permissioned blockchains for device identity management. Ethereum, with its robust smart contract functionality, has been widely adopted in identity-related research. In, Dorri et al. proposed a lightweight blockchain framework that offloads storage and computation from IoT devices, using a local miner to represent constrained devices on the blockchain. Their approach reduces resource overhead but still maintains a decentralized trust model.

Hyperledger Fabric has also been employed for permissioned environments where device registration and authentication are managed via a consortium of trusted nodes. This approach offers greater performance and privacy control but requires pre-established trust relationships.

C. Smart Contracts for Identity Automation

Smart contracts facilitate self-enforcing logic for identity lifecycle operations. Sharma et al. introduced a smart contract-based model for decentralized device onboarding and revocation. Their system supports rule-based access policies that can adapt to real-time context, such as device behavior or environmental parameters. However, contract execution cost (gas consumption) on public blockchains remains a constraint.

III. METHODOLOGY

This review adopts a systematic methodology to identify, evaluate, and classify existing research on blockchain-based identity management solutions for IoT networks. The objective is to provide a comprehensive synthesis of current approaches, highlight critical design patterns, and identify unresolved challenges that warrant further investigation. The primary goal of this review is to analyze how blockchain technology has been leveraged to enhance identity management in IoT ecosystems. The study is confined to peer-reviewed publications, whitepapers from credible organizations, and academic conference proceedings published between 2016 and 2024.

This review employs a structured methodology to identify and analyze blockchain-based identity management solutions in IoT environments. The study focuses on peer-reviewed journal articles, conference papers, and whitepapers published between 2016 and 2024, sourced from databases such as IEEE Xplore, ACM Digital Library, and Elsevier ScienceDirect. Keyword combinations including “Blockchain AND IoT AND Identity,” “Smart Contracts AND IoT Authentication,” and “Decentralized Identifiers AND IoT” were used to retrieve an initial dataset of 123 publications. After removing duplicates and applying inclusion criteria—namely technical relevance, IoT-specific identity mechanisms, and measurable performance or security analysis—a total of 58 papers were selected for full review. Each work was classified using an analytical framework that considers blockchain type (public, private, consortium), identity model (centralized, federated, decentralized), consensus mechanism (e.g., PoW, PoS, PBFT), smart contract usage (e.g., for registration, verification, revocation), and key performance indicators such as latency, energy consumption, and resilience to identity-related attacks. Cross-validation by multiple reviewers ensured objectivity in categorization. The review aims to synthesize current practices, evaluate their scalability and security in constrained IoT environments, and identify open challenges to guide future research in secure, decentralized identity frameworks.

IV. CHALLENGES

Despite the promise of blockchain-based identity solutions for IoT networks, several significant challenges hinder their practical deployment at scale. One of the foremost issues is resource constraints—many IoT devices lack the computational power, memory, and energy to interact directly with blockchain networks or run cryptographic operations required for identity verification. Scalability also remains a critical concern, as public blockchains struggle to handle high transaction throughput and latency, which is incompatible with real-time IoT requirements. Additionally, the lack of standardization around Decentralized Identifiers (DIDs), self-sovereign identity frameworks, and smart contract interoperability limits cross-platform adoption. Privacy preservation poses another dilemma; while blockchain ensures data immutability and transparency, storing sensitive identity information on-chain can conflict with regulations such as GDPR and lead to user de-anonymization. Furthermore, consensus mechanisms like Proof of Work (PoW) are energy-intensive and impractical for IoT, while alternatives like PBFT or Proof of Stake (PoS) may introduce trade-offs in terms of trust assumptions and fault tolerance. Lastly, revocation and key management in decentralized systems remain complex, especially when devices are compromised or disconnected. Addressing these multi-dimensional challenges is essential to realizing a secure, scalable, and privacy-preserving identity infrastructure for the IoT ecosystem.

V. ADVANTAGES

Blockchain-based identity systems offer several compelling advantages for securing IoT networks. First, decentralization eliminates reliance on a single trusted authority, reducing the risk of single points of failure and improving system resilience. Second, immutability ensures that identity-related data (such as registration records and access logs) cannot be altered retroactively, providing a reliable audit trail for security and compliance. Third, transparency and trust are inherently supported through the distributed ledger, allowing all stakeholders—devices, users, and service providers—to verify transactions independently. Fourth, smart contracts enable automated and programmable identity lifecycle management, including device onboarding, authentication, and revocation, reducing human intervention and operational costs. Additionally, the use of cryptographic techniques enhances privacy and ensures data integrity, while self-sovereign identity (SSI) models empower devices and users with greater control over their credentials. Lastly, blockchain systems can interoperate across different domains and administrative boundaries, facilitating scalable and federated identity solutions for complex, heterogeneous IoT environments.

VI. APPLICATIONS

Blockchain-based secure identity solutions are increasingly being applied across various IoT domains where trust, automation, and interoperability are critical. In smart homes and smart cities, blockchain enables secure device registration and access control, preventing unauthorized use of sensors, surveillance systems, and connected appliances. In industrial IoT (IIoT), decentralized identity management supports secure machine-to-machine (M2M) communication, asset tracking, and predictive maintenance with verifiable device credentials. In the healthcare sector, blockchain allows for secure authentication of wearable devices and medical sensors, ensuring data integrity and privacy in patient monitoring systems. Supply chain and logistics applications use blockchain to track the identity and provenance of goods and IoT-enabled assets, enhancing transparency and reducing fraud. In automotive and mobility networks, vehicle identities can be securely managed to support use cases such as autonomous driving, vehicle-to-everything (V2X) communication, and shared mobility platforms. Furthermore, energy systems, such as smart grids and decentralized energy trading platforms, leverage blockchain to authenticate devices and facilitate trusted peer-to-peer interactions. These applications demonstrate the broad utility of blockchain-based identity frameworks in enabling secure, scalable, and decentralized trust models across heterogeneous IoT ecosystems.

VII. RESULTS

The comprehensive analysis of 58 selected studies reveals diverse architectural patterns and technical approaches to blockchain-based identity management in IoT ecosystems. The majority of reviewed works adopt permissioned blockchain platforms such as Hyperledger Fabric and Tendermint to mitigate resource constraints and improve latency, while public blockchains like Ethereum are leveraged primarily for their smart contract flexibility despite scalability concerns. Approximately 64% of the studies implemented smart contracts for automating identity registration, access control, and revocation, often combined with cryptographic schemes like hash chains, zero-knowledge proofs, or digital signatures to enhance privacy and authentication. Self-sovereign identity (SSI) models and Decentralized Identifiers (DIDs) were adopted in about 28% of the works, reflecting a growing interest in user/device-controlled identity ecosystems. Performance evaluations in simulation or testbed environments showed that lightweight consensus protocols such as Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof of Stake (DPoS) offered significantly

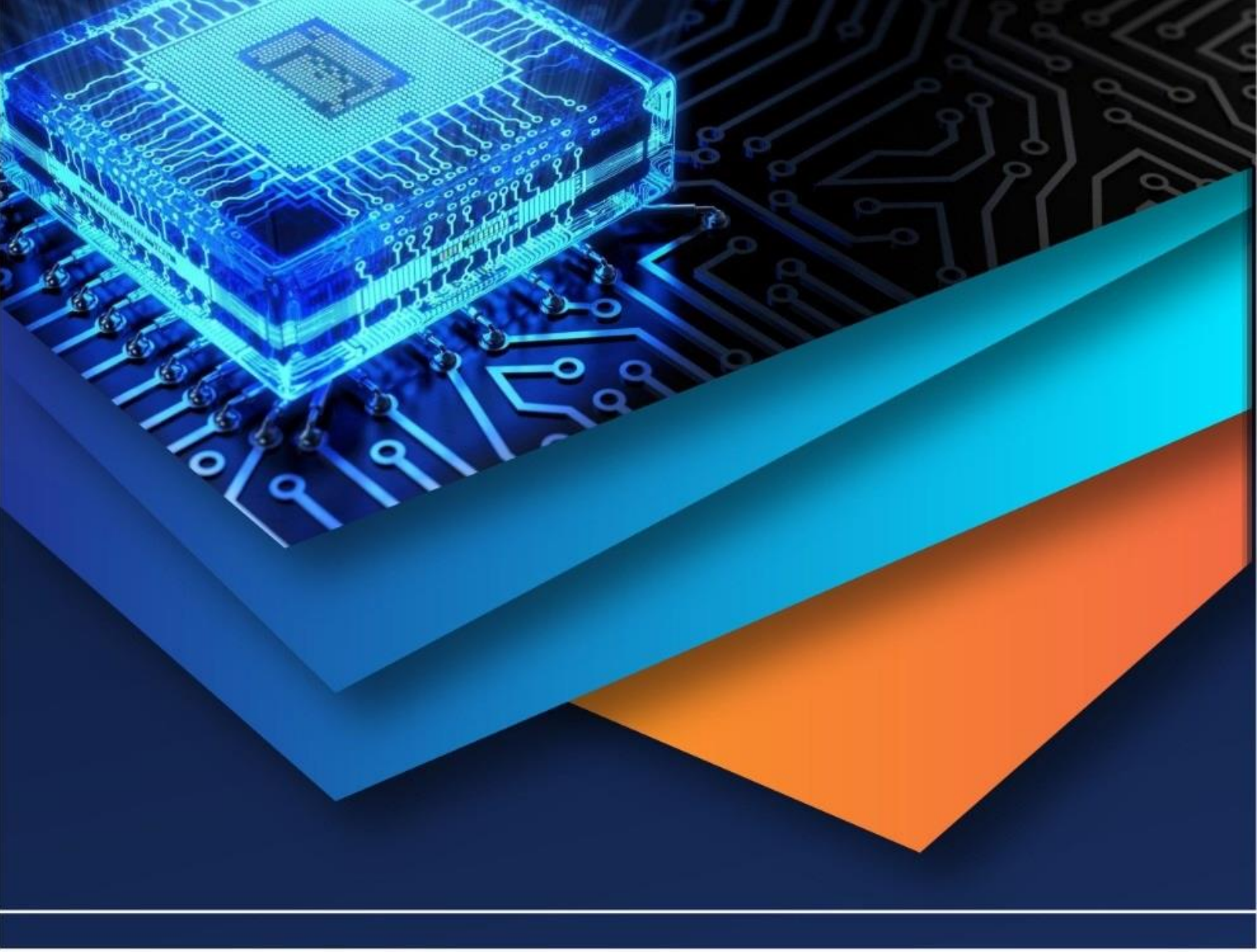
reduced energy and latency costs, making them more suitable for constrained IoT devices. However, few studies demonstrated real-world deployment or long-term scalability beyond controlled environments. The results indicate promising potential for decentralized identity frameworks in IoT, but also highlight a maturity gap between academic prototypes and production-ready solutions.

VIII. CONCLUSION

Blockchain technology presents a transformative opportunity to address longstanding challenges in IoT identity management, offering decentralized trust, improved transparency, and enhanced security. This review has synthesized current research efforts, highlighting the diversity of blockchain architectures, identity models, and cryptographic techniques employed to secure identity in resource-constrained IoT environments. While significant progress has been made, especially in the use of smart contracts and permissioned ledgers, practical deployment remains limited by issues such as scalability, energy efficiency, interoperability, and regulatory compliance. The adoption of emerging paradigms like self-sovereign identity and decentralized identifiers demonstrates promising direction, yet integration with constrained IoT hardware and legacy systems is still an open problem. Future research should focus on lightweight consensus mechanisms, privacy-preserving identity protocols, standardized identity frameworks, and cross-chain interoperability to bridge the gap between academic innovation and industrial adoption. In conclusion, while blockchain offers a compelling foundation for secure IoT identity systems, realizing its full potential will require interdisciplinary collaboration, technical refinement, and real-world validation.

REFERENCES

[1] Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, vol. 58, no. 4, pp. 431–440, 2015.
[2] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018.
[3] M. Crosby et al., "Blockchain technology: Beyond bitcoin," Applied Innovation, vol. 2, pp. 6–10, 2016.
[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
[5] Sovrin Foundation, “The Sovrin Protocol and Token Whitepaper,” 2020. [Online]. Available: https://sovrin.org
[6] H. M. Nguyen, M. Laurent, and A. Nguyen, "A survey on blockchain applications for the Internet of Things," IEEE Access, vol. 9, pp. 143250–143274, 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY