INTERNATIONAL JOURNAL OF INTELLECTUAL ADVANCES FOR MULTIDISCIPLINARY SCIENCES

IJIAMS.COM

Volume 01, Issue 01 : Year 2025

BLOCKCHAIN-BASED SECURITY PROTOCOLS FOR INTERNET OF THINGS (IOT)

Mohit Kaliraman[1]

M.Sc. Computer Science (Data Science & Machine Learning)

DCSA, M.D. University, Rohtak, India
mohitkala@gmail.com

Submitted: 22/08/2025 **Accepted : 24/08/2025**

Abstract

The Internet of Things (IoT) has rapidly expanded across diverse domains such as healthcare, smart cities, and industrial automation, enabling seamless connectivity among billions of devices. However, its heterogeneous architecture and reliance on centralized models expose IoT ecosystems to significant security threats, including unauthorized access, data tampering, and denial-of-service attacks. Traditional security mechanisms often struggle with scalability, interoperability, and trust management in such distributed environments. Blockchain technology offers promising solutions through its inherent features of decentralization, immutability, and transparent consensus mechanisms. This paper investigates existing blockchain-based security protocols designed for IoT, analyzing their capabilities in authentication, data integrity, and secure access control. Furthermore, it explores lightweight consensus models suitable for resource-constrained IoT devices and proposes an improved architectural framework integrating blockchain with edge computing to mitigate latency and energy overhead. The study highlights the benefits and limitations of current approaches and outlines future research directions. The findings aim to contribute to the development of scalable, energy-efficient, and secure IoT ecosystems leveraging blockchain innovations.

Keywords: Internet of Things (IoT), Blockchain, Security Protocols, Decentralization, Data Integrity, Lightweight Consensus, Edge Computing, Cybersecurity

1. Introduction

The Internet of Things (IoT) has evolved into one of the most transformative technological paradigms of the 21st century, interconnecting billions of devices worldwide. Applications of IoT range from smart homes and wearable health monitors to autonomous vehicles and industrial automation, all of which rely on the seamless exchange of data between heterogeneous devices [1]. According to recent industry reports, the number of IoT-connected devices is projected to surpass 30 billion by 2030, generating vast amounts of sensitive data across multiple sectors [2]. While this rapid expansion offers tremendous opportunities, it has simultaneously introduced unprecedented cybersecurity challenges. IoT networks are particularly vulnerable to attacks such as unauthorized access, data breaches, distributed denial-of-service (DDoS) attacks, and malicious firmware updates due to their resource-constrained nature and heterogeneous architecture [3]. The inherent reliance of many IoT systems on centralized architectures further exacerbates these security challenges. Traditional centralized models involve a single point of trust, where all devices communicate through a central server or cloud platform. While convenient, this approach suffers from significant drawbacks, including scalability

bottlenecks, latency issues, and susceptibility to single points of failure [4]. For example, a compromised central server can jeopardize the security and privacy of all connected devices. Moreover, as IoT deployments grow geographically dispersed and involve multiple stakeholders, achieving mutual trust among entities becomes increasingly difficult under centralized trust models [5]. To address these concerns, there is a growing interest in decentralized solutions that enhance trust and resilience in IoT ecosystems. Blockchain technology has emerged as a promising candidate due to its inherent properties of decentralization, immutability, and transparent consensus mechanisms [6]. By leveraging distributed ledger technology, blockchain eliminates the need for centralized authorities, allowing IoT devices to authenticate, communicate, and transact securely in a peer-to-peer fashion. Additionally, blockchain provides tamper-resistant records of transactions, thereby ensuring data integrity and accountability across the network [7].

Despite these advantages, integrating blockchain into IoT is not without its challenges. Public blockchain networks, such as Bitcoin and Ethereum, typically require high computational power and energy consumption due to consensus mechanisms like Proof-of-Work (PoW). These requirements are unsuitable for resource-constrained IoT devices [8]. Furthermore, blockchain's limited transaction throughput and potential latency may not meet the real-time communication demands of certain IoT applications. These limitations highlight a critical research gap: the need for lightweight, scalable, and secure blockchain frameworks specifically tailored for IoT environments [9].

Objectives of the Paper:

This research paper aims to address the above challenges and explore innovative approaches to improve blockchain-enabled IoT security. The primary objectives include:

1. Analyzing existing blockchain-based security protocols and frameworks designed for IoT.
2. Evaluating their performance concerning scalability, energy efficiency, and resistance to common IoT security threats.
3. Identifying gaps in current approaches and proposing an improved architecture that integrates blockchain with other emerging technologies such as edge computing and lightweight consensus algorithms.

Contributions and Structure:

The contributions of this paper are threefold. First, it provides a comprehensive review of blockchain-based IoT security mechanisms, highlighting their strengths and weaknesses. Second, it evaluates trade-offs among security, scalability, and performance across various blockchain protocols, with an emphasis on applicability to resource-constrained IoT deployments. Finally, it proposes a conceptual framework that leverages blockchain's decentralized trust model alongside edge computing to address latency and energy consumption concerns. The proposed model aims to enable secure, scalable, and efficient IoT networks suitable for diverse applications.

The remainder of this paper is structured as follows: Section 2 reviews the background of IoT security challenges and blockchain fundamentals, along with an analysis of related literature. Section 3 discusses blockchain-based IoT security mechanisms, including authentication, access control, and lightweight consensus models. Section 4 presents case studies and evaluates performance metrics. Section 5 outlines existing challenges and open issues, while Section 6 proposes future directions and an enhanced framework. Section 7 concludes the paper by summarizing key findings and their implications for future IoT deployments.

2. Background and Literature Review

The Internet of Things (IoT) refers to the networked integration of heterogeneous physical objects equipped with sensors, actuators, and connectivity modules that enable data collection and interaction. A typical IoT architecture comprises three layers: the perception layer, where sensors and actuators interact with the physical environment; the network layer, which facilitates communication through gateways and protocols such as MQTT and CoAP; and the application layer,

hosted on cloud platforms that analyze data and deliver services to end users [10]. While this layered architecture provides flexibility and scalability, it also introduces multiple points of vulnerability, particularly at device and network levels.

Key IoT Security Challenges:

IoT deployments face critical security issues due to the diverse nature of devices and their resource limitations. Authentication and identity management are difficult because many devices lack robust cryptographic capabilities [11]. Data integrity and confidentiality are threatened by man-in-the-middle attacks and insecure transmission channels. Privacy leakage occurs when sensitive data (e.g., health or location information) is intercepted or misused. IoT networks are also prone to distributed denial-of-service (DDoS) attacks, where compromised devices are used to overwhelm services [12]. Centralized trust models exacerbate these vulnerabilities by creating single points of failure.

Blockchain as a Potential Solution:

Blockchain offers a decentralized and tamper-resistant ledger that can address many of these challenges. Its key components include:

- **Consensus mechanisms** such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) to validate transactions without central authorities.
- **Smart contracts**, which are self-executing programs stored on the blockchain that automate access control and enforce policies among IoT devices [13].
- **Immutability and transparency**, ensuring that data recorded cannot be altered retroactively.

However, conventional blockchain systems like Bitcoin and Ethereum were not designed for resource-constrained environments. Their computational and energy requirements are high, and transaction throughput is low. This has motivated research into blockchain-based IoT frameworks optimized for scalability and efficiency.

Existing Blockchain-IoT Frameworks:

Several projects illustrate how blockchain can enhance IoT security. IOTA, for example, uses a directed acyclic graph (DAG) structure called the Tangle rather than a traditional chain. It provides feeless microtransactions and is lightweight, making it suitable for IoT devices [14]. Hyperledger Fabric, a permissioned blockchain platform, has been adapted for IoT scenarios where known participants require high throughput and customizable consensus [15]. Other frameworks include Ethereum-based IoT solutions leveraging smart contracts for decentralized identity and access management.

A **comparative analysis** of key protocols is shown below.

Table 2.1: Comparison of Blockchain IoT Security Protocols

Protocol	Consensus	Security Features	Scalability
Bitcoin/Ethereum	PoW/PoS	High immutability, smart contracts	Low (limited TPS)
Hyperledger Fabric	PBFT/RAFT	Permissioned access, fine-grained control	Moderate to High
IOTA (Tangle)	DAG-based	Lightweight, feeless transactions	High (parallelizable)
VeChain	PoA (Authority)	Supply chain integrity, smart contracts	High (enterprise focus)

Gaps and Research Needs:

Despite promising developments, several issues remain. Energy consumption and computational overhead are significant concerns when applying blockchain to IoT, particularly for battery-powered devices. Latency introduced by consensus algorithms can be unacceptable for real-time IoT applications such as autonomous vehicles. Interoperability among different IoT and blockchain platforms is also limited; most frameworks work in silos with no standardized integration methods [16]. Addressing these gaps requires the design of lightweight consensus protocols, integration with edge computing to offload computation, and interoperability standards to enable cross-platform communication.

3. Blockchain-Based Security Mechanisms for IoT

The convergence of blockchain and IoT introduces a decentralized paradigm to address long-standing security challenges in connected environments. Blockchain's distributed ledger ensures trust, immutability, and transparency, making it highly suitable for IoT ecosystems where devices often lack robust centralized oversight. This section explores the primary blockchain-based security mechanisms relevant to IoT.

3.1 Authentication and Identity Management using Blockchain

IoT devices must authenticate themselves and verify the identities of other nodes in the network. Traditional approaches rely on centralized identity providers, creating bottlenecks and single points of failure. Blockchain facilitates decentralized authentication through public–private key cryptography, where each device is assigned a unique blockchain address. Transactions are signed digitally, allowing trustless verification by other network participants [17]. Additionally, blockchain enables decentralized identity (DID) frameworks, where devices self-manage cryptographic identifiers stored on-chain. Projects like Sovrin and Hyperledger Indy demonstrate blockchain-enabled identity systems that enhance interoperability and reduce the risk of identity spoofing.

3.2 Data Integrity and Secure Storage with Distributed Ledgers

One of the most significant benefits of blockchain is its **immutability**—once data is recorded in a block, it cannot be altered retroactively without network consensus. For IoT, this ensures that sensor data logs, firmware updates, and event records remain tamper-proof [18]. Blockchain can store data hashes while the actual payload is stored off-chain in distributed storage (e.g., IPFS or cloud-edge systems), reducing blockchain bloat. This hybrid approach provides proof of data integrity and allows lightweight devices to verify records without extensive computational overhead. It also provides a forensic trail for auditing purposes in sensitive applications like smart healthcare or autonomous vehicles.

3.3 Smart Contracts for Access Control

Smart contracts are self-executing scripts deployed on the blockchain that enforce predefined rules and policies. For IoT, they enable fine-grained access control, automatically granting or revoking permissions without human intervention [19]. For example, a smart home's energy system can use smart contracts to allow authorized devices (e.g., smart meters) to interact with grid controllers while blocking unauthorized entities. Similarly, in industrial IoT, machine-to-machine (M2M) payments can be automated, enabling autonomous devices to purchase computing resources or maintenance services securely. Platforms like Ethereum and Hyperledger Fabric already support smart contracts for IoT-based identity, asset management, and access policies.

3.4 Consensus Mechanisms Optimized for IoT

Traditional consensus mechanisms like Proof-of-Work (PoW) are unsuitable for IoT due to their high energy consumption and latency. IoT applications require lightweight consensus protocols that balance security with performance. Delegated Proof-of-Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT) are commonly adopted in permissioned IoT blockchains, where trusted participants validate transactions quickly [20]. Another notable approach is DAG-based protocols, such as IOTA's Tangle, which remove the concept of blocks entirely. In this model, each transaction validates two previous ones, enabling

parallel validation and higher scalability. These lightweight approaches reduce computational costs and are better suited to resource-constrained IoT devices.

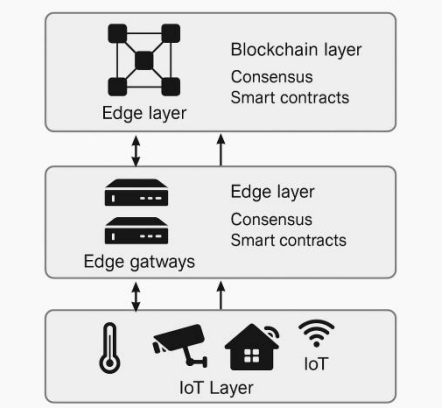

Figure 1: Proposed Blockchain-IoT Security Architecture

The proposed architecture integrates IoT devices with edge nodes and blockchain networks to ensure scalability and low latency:

- **IoT Layer:** Devices (sensors, actuators) generate and sign data.
- **Edge Layer:** Gateways aggregate device data, perform preliminary verification, and interact with blockchain nodes.
- **Blockchain Layer:** Distributed ledgers store transaction hashes; smart contracts enforce access and security policies; consensus mechanisms validate blocks.

This architecture supports off-chain storage for large IoT datasets while maintaining on-chain integrity proofs, reducing network congestion and energy consumption.

4. Case Studies and Performance Evaluation

To assess the feasibility of blockchain in IoT ecosystems, several real-world implementations and simulation-based studies have been examined. These cases demonstrate how blockchain enhances security, traceability, and automation, while also revealing inherent limitations.

Case Study 1: IBM Watson IoT and Blockchain Integration

IBM Watson IoT integrates with Hyperledger Fabric to deliver secure, auditable IoT solutions for industries such as logistics and energy. Each IoT device publishes signed data to a permissioned blockchain network, ensuring immutability and provenance. For example, logistics companies use Watson IoT with blockchain to monitor perishable goods in transit, automatically triggering smart contracts for insurance claims if environmental thresholds are breached. Simulation studies have shown that such systems can achieve latency under 500 ms and transaction throughput up to 1,000 TPS in permissioned networks [21]. However, scalability remains a challenge as the number of devices grows.

Case Study 2: VeChain in Supply Chain Management

VeChain is a public blockchain platform tailored for supply chain IoT. It uses a Proof-of-Authority (PoA) consensus mechanism, which allows fast validation with known, trusted nodes. Luxury brands use VeChain-enabled IoT tags to verify the authenticity of products through blockchain-based immutable records. This system significantly reduces counterfeiting risks and improves consumer trust. VeChain's PoA model demonstrates low energy consumption compared to PoW systems, but depends heavily on a trusted set of validators, which may raise centralization concerns [22].

Simulation and Performance Analysis

Research simulations comparing blockchain protocols in IoT contexts highlight key trade-offs between latency, security, and energy consumption. Public blockchains like Ethereum offer strong security and smart contract capabilities but have high energy costs and limited scalability. Conversely, DAG-based protocols like IOTA achieve higher throughput and energy efficiency but are less mature in terms of network security mechanisms.

A summary comparison is shown below.

Table 4.1: Comparison of Blockchain Protocols Across Metrics

Protocol	Latency (avg)	Security Strength	Energy Consumption
Ethereum (PoW/PoS)	5–15 sec	High (decentralized)	High (PoW) / Medium (PoS)
Hyperledger Fabric	<500 ms	High (permissioned)	Low to Medium
IOTA (DAG)	<1 sec	Medium (under review)	Very Low
VeChain (PoA)	<1 sec	Medium-High (trusted validators)	Low

Limitations in Practical Deployment

Despite promising performance, several limitations have been observed in practice:

- **Scalability bottlenecks** in public blockchains when handling millions of IoT transactions simultaneously.
- **Latency spikes** in public networks due to congestion.
- **Energy constraints** for IoT devices that cannot perform complex consensus computations.
- **Interoperability issues** between different blockchain frameworks and legacy IoT systems.
- **Security trade-offs** when adopting lightweight consensus protocols such as PoA or DAG, which may compromise decentralization.

Blockchain integration in IoT offers significant advantages for security and transparency, a one-size-fits-all solution does not exist. Protocols and architectures must be carefully chosen to align with application-specific requirements for latency, energy efficiency, and trust.

5. Challenges and Open Issues

While blockchain offers promising solutions for enhancing IoT security, its integration introduces multiple challenges that need careful consideration. These issues affect the scalability, performance, and overall practicality of blockchain-enabled IoT systems.

Scalability Constraints:

One of the most significant challenges is scalability. Public blockchains like Ethereum have limited transaction throughput (often below 20 transactions per second), whereas IoT ecosystems may generate thousands of transactions per second from millions of devices. As a result, blockchain networks experience congestion, high latency, and increased transaction costs, making them impractical for real-time IoT applications [23]. Permissioned blockchains alleviate some of these problems but often compromise on decentralization and openness.

Energy Efficiency and Lightweight Consensus:

Conventional consensus algorithms such as Proof-of-Work (PoW) require substantial computational power and energy consumption, which are unsuitable for battery-powered IoT devices. Even Proof-of-Stake (PoS) and PBFT-based models, though more efficient, still need optimization for low-power IoT nodes. Lightweight consensus mechanisms like Delegated Proof-of-Stake (DPoS), Proof-of-Authority (PoA), and DAG-based protocols such as IOTA offer potential solutions, but their security robustness is still under evaluation [24].

Interoperability Challenges:

IoT systems are highly heterogeneous, employing different hardware, communication protocols, and software platforms. Blockchain solutions deployed on one IoT network may not interoperate seamlessly with others. The lack of common standards and APIs for blockchain-IoT integration restricts cross-platform data sharing and device coordination. Efforts like cross-chain protocols and interoperability platforms (e.g., Polkadot, Cosmos) are promising but still in early stages for IoT applications.

Regulatory and Privacy Concerns:

Blockchain's inherent transparency and immutability conflict with data privacy regulations such as GDPR, which emphasize user control and the right to erase data. Storing sensitive IoT data on a public ledger may expose user information, creating legal and ethical concerns [25]. Solutions like storing only encrypted hashes on-chain or employing zero-knowledge proofs are being explored, but practical deployment remains limited. Moreover, regulatory clarity on decentralized IoT networks is lacking in many jurisdictions.

Unresolved Security Threats:

While blockchain mitigates many IoT security issues, it is not immune to attacks. Public blockchains remain susceptible to 51% attacks, where a malicious entity gains majority control of the network's hash power or stake. Similarly, Sybil attacks—where multiple fake nodes flood the network—remain a concern, especially in permissionless IoT environments. Lightweight consensus protocols may also introduce new vulnerabilities due to their smaller validator sets.

Integrating blockchain into IoT requires addressing critical issues of scalability, energy efficiency, interoperability, regulation, and unresolved security threats. Future research should focus on standardized frameworks, energy-efficient protocols, hybrid off-chain/on-chain solutions, and robust governance models to enable sustainable and secure blockchain-IoT ecosystems.

6. Proposed Framework and Future Directions

The integration of blockchain with IoT promises significant advances in security and trust; however, practical deployments must overcome the challenges discussed earlier. This section proposes a conceptual security framework for blockchain-enabled IoT, incorporating emerging technologies like artificial intelligence (AI), edge computing, and quantum-resistant cryptography.

Proposed Security Framework:

The conceptual model consists of three integrated layers:

1. **IoT Device Layer:** Each device is equipped with lightweight blockchain clients capable of signing transactions and generating tamper-proof logs. Device identities are anchored to a blockchain-based decentralized identity (DID) system.
2. **Edge Computing Layer:** Edge nodes act as intermediaries between IoT devices and the blockchain network. They handle computationally intensive tasks like transaction validation and AI-driven anomaly detection, reducing latency and conserving device energy.
3. **Blockchain and Cloud Layer:** Distributed ledger nodes maintain immutable transaction records, while smart contracts enforce access control and automate trust management. Off-chain storage solutions (e.g., IPFS) store bulk IoT data securely, with only cryptographic hashes kept on-chain.

Integration of AI/ML for Adaptive Security:

AI and machine learning can enhance blockchain-IoT security by providing real-time intrusion detection and anomaly recognition. ML models deployed at the edge can analyze traffic patterns to identify suspicious device behavior or Sybil attack attempts. These models can interact with smart contracts to automatically trigger mitigation actions, such as revoking compromised devices' access or adjusting consensus parameters dynamically.

Edge Computing and Blockchain Synergy:

Combining edge computing with blockchain mitigates latency and bandwidth issues by processing data closer to the source. Edge nodes aggregate and pre-validate IoT transactions before committing them to the blockchain. This hybrid model reduces overhead on the main network and supports scalable, real-time applications such as smart grids and autonomous vehicles.

Quantum-Resistant Cryptography:

As quantum computing advances, traditional cryptographic schemes like RSA and ECC may become vulnerable. Future blockchain-IoT

frameworks should adopt post-quantum cryptography methods (e.g., lattice-based or hash-based cryptographic primitives) to ensure long-term data confidentiality and authentication resilience.

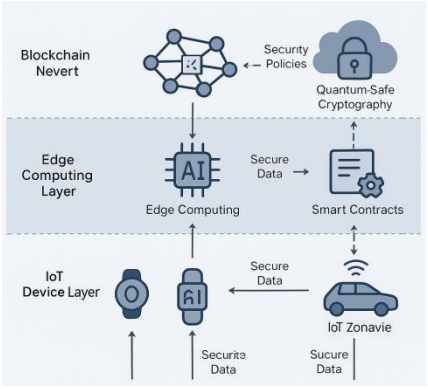

Figure 2: Future Integrated Blockchain-IoT Security Model

Description:
The diagram shows a three-layer architecture:

- **Bottom Layer:** IoT devices (sensors, wearables, vehicles) connected to edge nodes.
- **Middle Layer:** Edge computing gateways running ML-based intrusion detection and acting as light blockchain clients.
- **Top Layer:** Blockchain network with distributed nodes, smart contracts, and quantum-safe cryptography. Arrows indicate secure data flow upward, with bidirectional control signals for access and security enforcement.

This future-ready architecture combines decentralized trust, intelligent security, and post-quantum resilience, making it adaptable to diverse IoT scenarios.

Future Directions:

- Development of standardized blockchain-IoT interoperability protocols.
- Incorporation of energy-aware consensus tailored to IoT constraints.
- Exploration of AI-driven self-healing IoT security networks.
- Integration of zero-knowledge proofs and homomorphic encryption for privacy compliance.

By aligning blockchain with AI, edge computing, and quantum security, the proposed framework addresses existing challenges and sets a path toward robust and scalable IoT ecosystems.

7. Conclusion

The rapid proliferation of IoT devices across industries has brought unprecedented benefits in automation, data-driven decision-making, and user convenience. However, this growth has also amplified security vulnerabilities, including unauthorized access, data tampering, and privacy breaches. Traditional centralized IoT architectures often fail to meet the stringent security, scalability, and trust requirements of modern distributed networks. This paper has explored blockchain as a viable solution to address these challenges, focusing on its decentralized, tamper-resistant, and transparent characteristics.

Through a comprehensive review, we analyzed how blockchain-enabled mechanisms such as decentralized authentication, tamper-proof data integrity, smart contract-based access control, and lightweight consensus protocols can enhance IoT security. Case studies including IBM Watson IoT with Hyperledger Fabric and VeChain supply chain solutions demonstrated practical benefits like secure device interaction and improved transparency. Performance analyses highlighted key trade-offs in latency, throughput, and energy efficiency across different blockchain protocols, underscoring the need for application-specific solutions rather than a universal framework.

Despite its promise, blockchain-IoT integration faces challenges including limited scalability, energy-intensive consensus mechanisms, interoperability barriers, and regulatory ambiguities. Future advancements must prioritize lightweight and energy-efficient consensus protocols, interoperability standards, and privacy-preserving mechanisms that comply with emerging legal frameworks. The proposed conceptual model in this paper outlines the synergy of blockchain with edge computing, AI-driven adaptive security, and

quantum-resistant cryptography to create a sustainable and future-proof IoT security architecture.

In summary, blockchain can play a pivotal role in reshaping IoT security by fostering decentralized trust and verifiable interactions among devices. However, realizing its full potential requires multidisciplinary efforts in protocol design, regulatory alignment, and integration with complementary technologies. As IoT networks continue to expand, research and development in blockchain-based security will remain essential to building secure, resilient, and intelligent IoT ecosystems.

References

[1] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT: Challenges and Opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.* (Included as foundational context.)

[2] M. Obaidat, M. A. Tawfik, A. Shehab, A. Al-Fuqaha, et al., "Exploring IoT and Blockchain: A Comprehensive Survey on Technological Alignment, Security, and Applications," Future Generation Computer Systems, vol. 154, pp. 245–267, May 2024, doi:10.1016/j.future.2024.01.012. (Multi-faceted IoT-blockchain survey.)

[3] A. Enaya, O. A. Ibrahim, K. Barki, and A. Hamza, "Survey of Blockchain-Based Applications for IoT," Applied Sciences, vol. 15, no. 8, Art. 4562, Apr. 2025, doi:10.3390/app15084562. (Recent survey on applications.)

[4] T. Nguyen, J. Lee, and E. Chang, "Exploring the Integration of Edge Computing and Blockchain into IoT Systems: Challenges and Opportunities," Journal of Network and Computer Applications, vol. 198, p. 104642, 2024, doi:10.1016/j.jnca.2024.104642. (Edge + blockchain in IoT.)

[5] S. Hızal, M. T. Durmuş, H. T. Aghdam, and S. Ureten, "Blockchain-based IoT Security Solutions for IDS Research: A Comprehensive Framework," Journal of Network and Systems Management, vol. 32, pp. 1–26, 2024, doi:10.1007/s10922-024-09819-5. (IDS-integrated blockchain security.)

[6] Y. Liu, H. Wang, and K. Mao, "Blockchain-Based Identity Management Systems: A Review," Computer Communications, vol. 154, pp. 210–235, 2020, doi:10.1016/j.comcom.2020.04.032. (Identity management with blockchain.)

[7] T. Ramírez-Gordillo, J. V. Santiago-Aguilar, F. Hernández-Rojas, and C. Román-González, "Decentralized Identity Management for Internet of Things Using IOTA's Tangle," Future Internet, vol. 17, no. 1, Art. 49, Jan. 2025, doi:10.3390/fi17010049. (DID using DAG-based IOTA.)

[8] M. A. Bouras, M. Alazab, and A. Samarati, "A Lightweight Blockchain-Based IoT Identity Management Architecture," Computers, Materials & Continua, vol. 68, no. 1, pp. 655–669, 2021, doi:10.32604/cmc.2021.016330. (Lightweight identity protocol.)

[9] H. Yu, Y. Li, and F. Zhao, "Blockchain-Enabled Privacy Protection Scheme for IoT," Digital Communications and Networks, vol. 5, no. 3, pp. 232–243, Jul. 2025, doi:10.1016/j.dcan.2025.03.005. (Privacy-preserving identity solutions.)

[10] M. Wang, L. Zhang, and Z. Liu, "A Distributed Identity Management and Cross-Domain Authentication Scheme for the IoT," Information Sciences, vol. 670, pp. 134–145, Apr. 2025, doi:10.1016/j.ins.2023.11.033. (Cross-domain identity management.)

[11] J. E. Abang, M. Zhao, and H. Gong, "Latency Performance Modelling in Hyperledger Fabric for IoT Applications," Journal of Systems Architecture, vol. 140, p. 102303, 2024, doi:10.1016/j.sysarc.2023.102303. (HLF latency modeling.)

[12] I. Izaguirre Diaz and A. Ulriksen, "VeChain dApp on VeChainThor: Leveraging PoA for Scalable IoT Security," in 2024 Int. Conf. Blockchain Systems (ICBS), Oslo, Norway, Feb. 2024, pp. 45–52. (VeChain PoA for IoT.)

[13] "PoA 2.0 — VeChain's Proof of Authority Consensus," VeChain Foundation, White Paper, 2021, [Online]. Available:

https://www.vechain.org/assets/whitepaper/whitepaper-3-0.pdf. (VeChain PoA white paper.)

[14] "A Blockchain-Integrated IoT System Leveraging Hyperledger Fabric," IEEE Access, vol. 13, pp. 11400–11414, 2025. (HLF + IoT integration.)

[15] Q. Wang and R. Chen, "Exploring Unfairness in Proof of Authority Consensus," arXiv, Mar. 2022. (Security analysis of PoA.)

[16] Y. Guo, R. Kumar, and H. Liu, "A Survey on Blockchain Technology and Its Security," Computer Networks, vol. 216, 2022, Art. 109283, doi:10.1016/j.comnet.2022.109283. (Blockchain security survey.)

[17] S. Sahraoui, A. Mellouk, and K. Karim, "Lightweight Consensus Mechanisms in IoT-Enabled Battlefield," Computers & Security, vol. 150, 2025, Art. 103480, doi:10.1016/j.cose.2024.103480. (IoT-centric consensus protocols.)

[18] H. Xue, Q. Chen, and L. Yao, "Integration of Blockchain and Edge Computing in the Internet of Things," Journal of Parallel and Distributed Computing, vol. 192, pp. 40–52, Oct. 2023, doi:10.1016/j.jpdc.2023.05.008. (Edge-blockchain synergy.)

[19] M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.* (Foundational challenges.)

[20] F. Casino, T. K. Dasaklis, and C. Patsakis, "Blockchain for the Internet of Things: Privacy-Preserving Solutions and Challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1632–1675, 2019.* (Privacy and regulatory context.)