



Blockchain-Based Security Framework for Internet of Things (IoT) Networks: A Layered Architecture, Consensus Analysis, and Application Study in the ECE Domain

Anil Kumar, Megha Rai, Sunil Das, Sayan Bala

Abstract—The rapid proliferation of Internet of Things (IoT) devices across healthcare, industrial automation, smart agriculture, smart grid, and smart-city domains has magnified concerns surrounding data integrity, device authentication, and network resilience. Conventional client-server and cloud-centric IoT security models suffer from single points of failure, limited transparency, and poor scalability as the number of connected endpoints grows into the tens of billions. Blockchain technology, with its decentralized, immutable, and cryptographically verifiable ledger structure, has emerged as a promising complement to traditional IoT security mechanisms. This paper presents a comprehensive study of blockchain-based security for IoT networks from an Electronics and Communication Engineering (ECE) perspective. We review the layered architecture of IoT systems, identify dominant threat surfaces at the perception, network, edge, and application layers, and propose an integrated five-layer blockchain-IoT security architecture suited to resource-constrained embedded hardware. We present a comparative evaluation of consensus mechanisms — Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Delegated Proof of Stake (DPoS), Proof of Authentication (PoAh), and Proof of Authority (PoA) — with respect to energy consumption, latency, and scalability for constrained IoT nodes. A threat model mapping common blockchain-IoT attack vectors to mitigation strategies is developed, along with case-study discussion of healthcare (IoMT), supply-chain, and smart-grid deployments. The paper concludes with open research challenges — including scalability, interoperability, quantum-resistance, and regulatory alignment — and outlines future research directions relevant to hardware-software co-design in the ECE domain.

Keywords—Blockchain, Internet of Things (IoT), Network Security, Consensus Algorithms, Smart Contracts, Edge Computing, Embedded Systems, Distributed Ledger Technology (DLT), Cryptography, ECE

I. INTRODUCTION

The Internet of Things (IoT) represents one of the most transformative technological paradigms of the past decade, interconnecting billions of physical devices — sensors, actuators, embedded controllers, and gateways — through heterogeneous communication protocols. From an Electronics and Communication Engineering standpoint, IoT systems sit at the intersection of embedded hardware design, wireless communication, signal processing, and networked software, making them uniquely vulnerable to both traditional cyber threats and hardware-level exploitation. Industry projections indicate that the number of connected IoT endpoints will substantially

exceed 200 billion within this decade [16], each capable of generating, transmitting, and acting upon data that is frequently sensitive, safety-critical, or economically valuable. Historically, IoT security has relied on centralized architectures in which a cloud server or trusted third party is responsible for device authentication, data storage, and access control. While operationally simple, this model introduces a single point of failure: compromise of the central server can cascade into large-scale data breaches, denial-of-service events, or unauthorized actuation of physical devices. Furthermore, the resource-constrained nature of most IoT endpoints — limited processing power, memory, energy budget, and bandwidth — makes it difficult to deploy conventional, computation-heavy

security protocols directly on end devices. Blockchain technology, first popularized through Nakamoto's peer-to-peer electronic cash system [30], offers an alternative paradigm: a distributed, append-only ledger maintained collectively by a network of nodes without reliance on a central authority. Its core properties — immutability, transparency, decentralization, and cryptographic verifiability — map naturally onto several unresolved IoT security problems, including device identity management, tamper-evident data logging, and automated policy enforcement via smart contracts. However, direct application of conventional blockchain protocols, such as Bitcoin's energy-intensive Proof of Work, to IoT is impractical because of the significant computational and energy overhead of traditional consensus mechanisms [9]. This paper investigates the integration of blockchain technology into IoT security architectures with specific attention to the constraints imposed by embedded ECE hardware. The key contributions of this work are:

- A structured review of blockchain-IoT security literature spanning architecture, consensus, access control, and application domains.
- A proposed five-layer blockchain-integrated IoT security architecture suitable for constrained embedded devices.
- A comparative analysis of lightweight consensus algorithms (PoAh, DPoS, PoA, PBFT-variants) against traditional PoW/PoS in terms of energy, latency, and scalability.
- A threat model mapping blockchain-IoT attack vectors to corresponding mitigation techniques.
- Case-study discussion of blockchain-IoT deployments in healthcare (IoMT), supply chain, and smart-grid applications.
- Identification of open research challenges and future directions relevant to ECE hardware-software co-design.

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 discusses IoT layered architecture and associated security challenges. Section 4 introduces blockchain fundamentals relevant to IoT. Section 5 presents the proposed integrated architecture. Section 6 compares consensus mechanisms. Section 7 develops a threat model. Section 8 discusses application case studies. Section 9 discusses open challenges. Section 10 outlines future research directions, and Section 11 concludes the paper.

II. RELATED WORK

Research on blockchain-IoT integration has grown rapidly since 2016, spanning survey papers, architectural proposals, and applied case studies. Zubaydi, Varga, and Molnár conducted a systematic literature review on the use of blockchain for ensuring security and privacy in IoT, cataloguing major techniques applied across identity management, data integrity, and access control [1]. Raval et al. presented a state-of-the-art review of blockchain-driven IoT security covering literature from 2016 to 2023, and additionally proposed a secure healthcare data-sharing system incorporating AI, smart contracts, and the InterPlanetary File System (IPFS) for off-chain storage [2]. Several IEEE-indexed surveys have specifically classified blockchain's role in IoT security. An early classification scheme organized blockchain-IoT applications into resource management, decentralized information sharing, and security enhancement [3]. Subsequent surveys focused on privacy protection, identity authentication, and access control as the three principal pillars of blockchain-based IoT security, comparing the technical advantages and limitations of different design choices [4], while a broader survey highlighted the early-stage nature of blockchain deployment at the low end of the computing spectrum, noting an unclear roadmap for constrained devices [5]. On the industrial side, Latif et al. surveyed blockchain applications for the Industrial Internet of Things (IIoT), covering security challenges, architectural patterns, and open research directions specific to manufacturing and process-control environments [6]. A related review examined blockchain-based AI methods for managing IIoT, discussing integration challenges between machine-learning pipelines and distributed ledgers [7]. Reviews of the Social Internet of Things (SIoT) have similarly emphasized that blockchain and AI/ML approaches are increasingly combined, with more than fifty of the surveyed papers referencing blockchain-based trust-management mechanisms in socially-connected device networks [8]. A significant body of work addresses the central bottleneck of applying blockchain to constrained IoT hardware: consensus algorithm overhead. Traditional Proof of Work is widely regarded as unsuitable for IoT due to its energy and computational demands [9]. Lightweight alternatives have therefore been proposed, including a Proof-of-Authority-and-Association scheme that improves reliability for real-time IoT data validation [10], and the Proof-of-Authentication (PoAh) algorithm, validated on constrained hardware such as Raspberry Pi single-board computers, demonstrating latency on the order of a few seconds while bypassing centralized dependencies entirely [11]. Delegated Proof of Stake (DPoS) has been combined with IPFS-based distributed storage and network sharding to improve throughput and reduce latency in large-scale IoT data-sharing frameworks, achieving low-latency performance under moderate-to-high transaction loads [12], [13]. A dedicated systematic review of 85 articles published between 2016 and 2023 further consolidated the case for lightweight consensus mechanisms tailored to resource-constrained IoT devices [14]. Access control and authentication

represent another major research thread. Blockchain-based access-control frameworks employing Ethereum smart contracts have been proposed for both generic IoT/Web3 environments [15] and for domain-specific systems such as healthcare, where attribute-based and role-based access policies are enforced through on-chain logic [17], [21]. A decentralized authentication scheme named ChainGuard demonstrated the use of blockchain-based identities and dynamic role assignment to eliminate central points of failure across healthcare, cloud, and financial-service domains [18]. Multi-layered blockchain architectures have also been proposed for electronic health record (EHR) sharing combined with drug supply-chain management, integrating consortium-blockchain design with fuzzy-logic-based adaptive security [19]. Healthcare-specific integration has attracted particular research attention given the sensitivity of medical data. Machine-learning-augmented blockchain architectures for the Internet of Health Things (IoHT) have been proposed to combine malware detection, data classification, and lightweight cryptographic security for real-time healthcare monitoring [20]. Broader reviews of blockchain-enhanced IoT ecosystems for healthcare emphasize data encryption, authentication, authorization, and access control as core mechanisms for resolving interoperability and trust issues in heterogeneous medical-device networks [22]. Systematic literature reviews of blockchain-enabled access-control frameworks for preventing cyber-attacks in IoT further consolidate this body of work, cataloguing trust-based authorization schemes and permissioned-blockchain access protocols validated across smart-home, vehicular ad-hoc network (VANET), and healthcare use cases [24]. Despite this substantial body of research, most existing surveys either focus narrowly on a single application domain (e.g., healthcare or supply chain) or a single design axis (e.g., consensus or access control), without integrating hardware-level ECE constraints into the discussion. Table 1 summarizes representative prior work along these dimensions. The present paper distinguishes itself by explicitly grounding the architecture and consensus analysis in the resource limitations of embedded ECE hardware — microcontrollers, RF transceivers, and low-power sensor nodes — while consolidating consensus, access-control, and application-domain findings into a single coherent framework.

TABLE V

Research Focus	Representative Studies	Key Gap Addressed in This Paper
General blockchain-IoT security surveys	[1], [2], [4], [5], [16]	Hardware-level ECE constraints not explicitly modeled
Industrial IoT (IIoT) integration	[6], [7]	Limited cross-domain consensus comparison

Lightweight consensus design	[9]-[14]	No unified quantitative comparison across six algorithms
Access control & authentication	[15], [17], [18], [24]	Access-control schemes not linked to layered architecture
Healthcare / IoMT applications	[19]-[22]	Domain-specific; lacks generalized threat model

III. IOT LAYERED ARCHITECTURE AND SECURITY CHALLENGES

A typical IoT deployment can be decomposed into four canonical layers: the perception (sensing) layer, the network (communication) layer, the middleware/edge layer, and the application layer. Each layer introduces distinct security requirements and attack surfaces that must be addressed by any integrated security framework.

3.1 Perception Layer The perception layer comprises sensors, actuators, RFID tags, and embedded microcontroller-based nodes (e.g., ESP32, ARM Cortex-M series) responsible for physical-world data acquisition. This layer is particularly vulnerable to physical tampering, side-channel attacks, node capture, and firmware-level exploitation, since many low-cost sensor nodes lack hardware security modules (HSMs) or trusted execution environments (TEEs).

3.2 Network Layer The network layer is responsible for transporting data between devices, gateways, and back-end infrastructure using protocols such as 6LoWPAN, Zigbee, LoRaWAN, NB-IoT, Bluetooth Low Energy (BLE) mesh, and 5G/6G cellular links. Threats at this layer include eavesdropping, man-in-the-middle attacks, routing manipulation (e.g., sinkhole and wormhole attacks), and jamming of the radio-frequency spectrum.

3.3 Edge / Middleware Layer The edge (or fog) layer aggregates and pre-processes data close to the point of generation, reducing latency and bandwidth demands on the core network. It typically hosts lightweight blockchain validation nodes and protocol-translation gateways (e.g., MQTT/CoAP to HTTP). This layer is exposed to distributed denial-of-service (DDoS) attacks, malicious code injection, and compromised gateway impersonation.

3.4 Application Layer The application layer delivers IoT services to end users — dashboards, mobile applications, and automated control logic for domains such as smart healthcare, smart agriculture, and industrial automation. Risks at this layer include insecure APIs, insufficient access control, data-privacy leakage, and business-logic exploitation of smart contracts. Table 2 summarizes the primary security requirements and representative threats at each layer, forming the basis for the architecture proposed in Section 5.

TABLE VI

Layer	Primary Security Requirements	Representative Threats
Perception	Device authentication, tamper resistance, secure boot	Node capture, side-channel attacks, firmware exploitation
Network	Confidentiality, integrity, secure routing	Eavesdropping, MITM, sinkhole/wormhole routing attacks, jamming
Edge / Middleware	Availability, gateway integrity, distributed validation	DDoS, gateway spoofing, malicious code injection
Application	Access control, privacy, smart-contract correctness	Insecure APIs, privilege escalation, contract vulnerabilities

IV. BLOCKCHAIN FUNDAMENTALS RELEVANT TO IOT SECURITY

A blockchain is a distributed ledger comprising cryptographically linked blocks, each containing a set of validated transactions, a timestamp, and a hash pointer to the preceding block. Modification of any historical block invalidates all subsequent hash pointers, providing strong tamper-evidence. Three architectural variants are commonly considered for IoT deployment:

- Public (permissionless) blockchains — open to any participant, offering maximum decentralization at the cost of higher latency and energy consumption (e.g., Ethereum mainnet).
- Private (permissioned) blockchains — restricted to pre-approved participants, offering lower latency and finer access control, suited to enterprise or industrial IoT deployments (e.g., Hyperledger Fabric).
- Consortium blockchains — governed jointly by a group of trusted organizations, balancing decentralization with performance; commonly proposed for cross-organizational supply-chain and healthcare data sharing [19].

Smart contracts — self-executing programs deployed on the blockchain — enable automated, tamper-proof enforcement of access-control policies, device-to-device micropayments, and data-provenance verification without manual intervention. When combined with off-chain storage systems such as IPFS, smart contracts allow bulky sensor data to be stored off-chain while only cryptographic hashes and access metadata are recorded on-chain, substantially reducing on-chain storage overhead — an important

consideration given the storage constraints of embedded gateway hardware [2], [12].

V. PROPOSED BLOCKCHAIN-INTEGRATED IOT SECURITY ARCHITECTURE

Building on the layered analysis in Section 3, we propose a five-layer blockchain-integrated security architecture (Figure 1) that explicitly separates resource-constrained sensing hardware from computation-heavy blockchain operations. The architecture follows a hierarchical trust-delegation model: perception-layer devices authenticate to nearby edge gateways using lightweight cryptographic primitives (e.g., elliptic-curve digital signatures), while the computationally expensive consensus process is delegated to edge and fog nodes with greater processing capacity.

5.1 Design Rationale The rationale for this layered separation is threefold. First, embedded ECE hardware such as low-power microcontrollers typically cannot execute full consensus protocols within their energy and memory budgets; delegating consensus to edge nodes avoids this bottleneck. Second, placing the blockchain security layer between the edge and application layers allows a single distributed ledger to serve multiple application domains (healthcare, agriculture, industrial automation) simultaneously, improving infrastructure reuse. Third, off-chain storage via IPFS at the blockchain layer keeps on-chain data volume manageable, addressing the scalability concerns raised in [12] and [13].

5.2 Identity and Access Management Each perception-layer device is provisioned with a unique cryptographic identity (public/private key pair) during manufacturing or commissioning. Device identities are registered on-chain through a smart contract, which subsequently governs access permissions using attribute-based access control (ABAC) policies, consistent with approaches demonstrated in [15] and [17]. Revocation of a compromised device's access can be executed atomically through the same smart-contract interface, avoiding the propagation delay associated with centralized certificate-revocation lists.

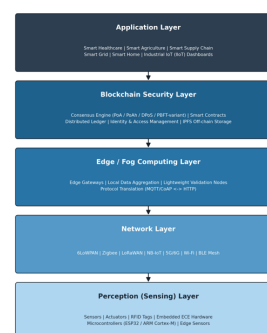


Fig. 1.

VI. COMPARATIVE ANALYSIS OF CONSENSUS MECHANISMS

The choice of consensus mechanism critically determines the feasibility of blockchain integration into IoT networks, since it directly governs energy consumption, transaction latency, and achievable throughput. Table 3 summarizes six consensus mechanisms considered in this study, and Figure 2 presents a relative comparison across three normalized metrics: energy consumption, consensus latency, and IoT suitability/scalability, synthesized from the performance characteristics reported in [9]–[14].

TABLE VII

Mechanism	Core Principle	Suitability for IoT
PoW	Computational puzzle solving by miners	Poor — high energy & latency, unsuitable for constrained nodes
PoS	Validator selection weighted by staked tokens	Moderate — lower energy than PoW, still resource-intensive
PBFT	Multi-round voting among known validator set	Good for permissioned IoT networks with small validator sets
DPoS	Elected delegates validate on behalf of stakeholders	Good — high throughput, low latency, scalable
PoAh	Authentication-based validation without mining	Very good — validated on Raspberry Pi-class hardware
PoA	Pre-approved authority nodes validate blocks	Very good — low overhead, suited to industrial/consumer IoT

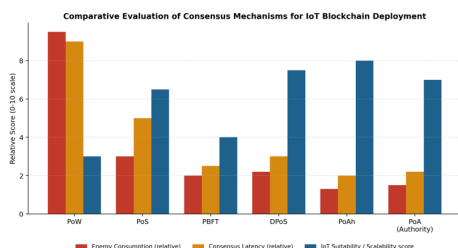


Fig. 2.

VII. THREAT MODEL AND MITIGATION STRATEGIES

Integrating blockchain into an IoT network does not eliminate all security risks; it shifts and, in some cases, introduces new attack surfaces specific to distributed-

ledger operation. Figure 3 illustrates six representative threat categories relevant to blockchain-secured IoT systems, and Table 4 maps each threat to corresponding mitigation strategies drawn from the reviewed literature.

TABLE VIII

Threat	Description	Mitigation Strategy
51% / majority attack	Adversary gains control of majority validating power to rewrite ledger history	Permissioned validator sets; reputation-weighted voting (PoAh, PoA) [10], [11]
Sybil attack	Adversary creates multiple fake identities to gain disproportionate network influence	On-chain device identity registration; hardware-rooted keys [15], [17]
Eclipse attack	Victim node is isolated and fed a manipulated view of the network	Diverse peer selection; edge-gateway redundancy [3]
Smart-contract vulnerabilities	Logic errors (re-entrancy, integer overflow) exploited to bypass access control	Formal verification; audited contract templates [18], [19]
Private-key compromise	Theft of a device's cryptographic key enables impersonation	Hardware security modules; key-rotation smart contracts [17]
DoS / DDoS on validator nodes	Flooding attacks degrade or halt consensus availability	Rate-limiting at edge gateways; delegated validator redundancy (DPoS) [12], [13]

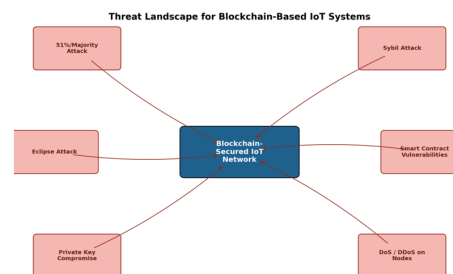


Fig. 3.

VIII. APPLICATION CASE STUDIES

8.1 Healthcare (Internet of Medical Things — IoMT) In IoMT deployments, wearable sensors and bedside monitors continuously generate vital-sign data that must remain both tamper-evident and privacy-

preserving. Blockchain-based access-control frameworks for IoT-healthcare systems use local gateways interfaced with Ethereum-based smart contracts to implement distributed, auditable authentication [23]. Related work integrating machine learning with blockchain for IoHT systems has demonstrated real-time malware detection alongside lightweight cryptographic protection of patient data streams [20]. Multi-layered consortium blockchain designs have further been proposed to jointly manage electronic health record (EHR) sharing and pharmaceutical supply-chain provenance, addressing both clinical data integrity and counterfeit-drug prevention within a single ledger infrastructure [19].

8.2 Supply Chain Management Blockchain-based supply-chain frameworks leverage IoT sensors (RFID tags, GPS trackers, environmental sensors) to record provenance data at each stage of a product's journey. Intelligent contract-based access-control frameworks combining permissioned blockchain (e.g., Hyperledger Fabric) with federated learning have been proposed to detect anomalous participant behavior across multi-party supply chains without requiring raw data sharing between competing organizations, preserving confidentiality while enabling collaborative anomaly detection [25].

8.3 Smart Grid and Industrial IoT In smart-grid and industrial automation contexts, blockchain enables secure peer-to-peer energy trading and tamper-evident logging of sensor telemetry from process-control equipment. Layered lightweight blockchain frameworks (LLBF) have been proposed specifically for Industrial IoT edge computing, redesigning block structure and size to match the resource profile of IIoT edge devices while improving throughput and balancing transaction load across the network [26].

IX. OPEN CHALLENGES

- **Scalability:** On-chain storage and consensus overhead remain difficult to reconcile with the transaction volume generated by dense sensor deployments, even with lightweight consensus and off-chain storage [12], [13].
- **Interoperability:** Heterogeneous IoT communication protocols (6LoWPAN, LoRaWAN, NB-IoT) and diverse blockchain platforms (Ethereum, Hyperledger Fabric) lack standardized interfaces, complicating cross-domain deployment [6].
- **Energy constraints:** Battery-powered perception-layer devices cannot sustain even lightweight cryptographic signing operations indefinitely, necessitating careful energy-aware protocol design [11].
- **Regulatory and data-privacy compliance:** Immutable

ledgers conflict with data-protection regulations that mandate a right to erasure, requiring hybrid on-chain/off-chain data-management strategies [22].

- **Smart-contract security assurance:** Formal verification tooling for resource-constrained smart-contract execution environments remains immature relative to mainstream blockchain platforms [18].
- **Quantum-resistance:** Widely used elliptic-curve cryptographic primitives are theoretically vulnerable to future quantum attacks, motivating early exploration of post-quantum signature schemes for long-lived IoT deployments.

X. FUTURE RESEARCH DIRECTIONS

Building on the challenges identified above, several promising directions merit further investigation by the ECE research community:

- **Hardware-software co-design** of ultra-low-power cryptographic accelerators (ASIC/FPGA-based) to enable on-device blockchain participation without prohibitive energy cost.
- **Integration of federated learning** with blockchain-based access control to enable collaborative anomaly detection while preserving data locality, as demonstrated in early supply-chain prototypes [25].
- **Development of standardized, protocol-agnostic middleware** to bridge heterogeneous IoT communication stacks with diverse blockchain platforms.
- **Exploration of hybrid on-chain/off-chain architectures** that satisfy both immutability requirements and regulatory right-to-erasure obligations.
- **Empirical, hardware-in-the-loop benchmarking** of post-quantum signature schemes on representative embedded ECE platforms (e.g., ARM Cortex-M, RISC-V microcontrollers).
- **Extension of the proposed five-layer architecture** to 5G/6G-enabled massive machine-type communication (mMTC) scenarios involving extremely dense sensor deployments.

XI. CONCLUSION

This paper has presented a comprehensive study of blockchain-based security for IoT networks from an Electronics and Communication Engineering

perspective. Through a structured review of the literature, we identified that while blockchain offers meaningful advantages for IoT security — decentralized trust, tamper-evident logging, and automated policy enforcement via smart contracts — its practical deployment on resource-constrained embedded hardware requires careful selection of lightweight consensus mechanisms such as PoAh, PoA, and DPoS in place of traditional PoW or PoS. We proposed a five-layer blockchain-integrated IoT security architecture that explicitly separates constrained sensing hardware from computation-heavy consensus operations, developed a threat model mapping key attack vectors to mitigation strategies, and discussed representative case studies across healthcare, supply-chain, and smart-grid domains. Open challenges — including scalability, interoperability, energy constraints, regulatory compliance, and quantum-resistance — indicate that blockchain-IoT security remains a fertile area for continued research, particularly at the intersection of embedded hardware design and distributed-systems engineering that defines the ECE discipline.

XII. REFERENCES

- [1] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: A systematic literature review," *Sensors*, 2023.
- [2] K. J. Raval, N. K. Jadav, T. Rathod, S. Tanwar, V. Vimal, and N. Yamsani, "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions," *Peer-to-Peer Networking and Applications*, Springer Nature, 2024.
- [3] "A Survey of Blockchain Applications in IoT Systems," in *Proc. IEEE Conference*, 2019, IEEE Xplore, doc. 9068170.
- [4] "Survey on Blockchain-Based Internet of Things Security Technologies," in *Proc. IEEE Conference*, IEEE Xplore, doc. 10925121.
- [5] "A Survey of IoT and Blockchain Integration: Security Perspective," *IEEE Access / IEEE Journals & Magazine*, doc. 09622256.
- [6] S. Latif, Z. Idrees, Z. e Huma, and J. Ahmad, "Blockchain technology for the industrial internet of things: A comprehensive survey on security challenges, architectures, applications, and future research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 32, e4337, 2021.
- [7] "Blockchain-based AI Methods for Managing Industrial IoT: Recent Developments, Integration Challenges and Opportunities," *arXiv:2405.12550*, 2024.
- [8] "A comprehensive survey on securing the Social Internet of Things: protocols, threat mitigation, technological integrations, tools, and performance metrics," *PMC*, 2025.
- [9] "A Survey on Security Threats in Blockchain-based Internet of Things Systems," in *Proc. IEEE Conference*, 2022, IEEE Xplore, doc. 9952581.
- [10] "Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices," *ScienceDirect / Future Generation Computer Systems*, 2021.
- [11] S. Kumar, A. Bhushan, and B. K. Bhargava, "PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks," *arXiv:2001.07297*, 2020.
- [12] "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," *Scientific Reports, Nature*, vol. 14, 2024.
- [13] "Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm," *Scientific Reports, Nature*, 2024.
- [14] V. Upadhyay, A. Vaish, and J. Kokila, "The need for Lightweight Consensus algorithms in IoT environment: A review," in *Proc. 16th Int. Conf. on Contemporary Computing (IC3-2024)*, Noida, India, ACM, 2024.
- [15] "Securing RC Based P2P Networks: A Blockchain-based Access Control Framework utilizing Ethereum Smart Contracts for IoT and Web 3.0," *arXiv:2412.03709*, 2024.
- [16] "Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions," *Big Data and Cognitive Computing, MDPI*, vol. 8, no. 12, art. 174, 2024.
- [17] "Frontiers | Blockchain-enabled access control to prevent cyber attacks in IoT: Systematic literature review," R. Singh, D. Kukreja, and D. K. Sharma, *Frontiers in Big Data*, vol. 5, art. 1081770, 2023.
- [18] "ChainGuard: A Blockchain-based Authentication and Access Control Scheme for Distributed

- Networks," arXiv:2412.00677, 2024.
- [19] "A Scalable Multi-Layered Blockchain Architecture for Enhanced EHR Sharing and Drug Supply Chain Management," arXiv:2402.17342, 2024.
 - [20] "A Machine-Learning-Blockchain-Based Authentication Using Smart Contracts for an IoHT System," PMC, 2022.
 - [21] "An Efficient Blockchain-Based Access Control Framework for IoT-Healthcare System," Wireless Personal Communications, Springer Nature, 2024.
 - [22] "Blockchain-enhanced IoT ecosystem for healthcare: Transformative potentials, applications, challenges, solutions, and future perspectives," ScienceDirect, 2024.
 - [23] "Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey," Cluster Computing, Springer Nature, 2025.
 - [24] "A Survey on Security Threats in Blockchain-based Internet of Things Systems" (access-control focused discussion), IEEE Xplore, doc. 9952581, 2022.
 - [25] "ICBAC: an Intelligent Contract-Based Access Control framework for supply chain management by integrating blockchain and federated learning," arXiv preprint, 2026.
 - [26] "A Novel Blockchain Framework for Industrial IoT Edge Computing," PMC, 2020.
 - [27] "Security and Privacy Enhancing in Blockchain-based IoT Environments via Anonymous Auditing," arXiv:2403.01356, 2024.
 - [28] "Blockchain in IoT Security: A Survey," in Proc. IEEE Conference, 2018, IEEE Xplore, doc. 8615409.
 - [29] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, 2018.
 - [30] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
 - [31] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," IEEE Transactions on Services Computing, vol. 13, no. 4, pp. 625-638, 2020.
 - [32] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and M. S. Khan, "A kangaroo-based intrusion detection system on software-defined networks," Computer Networks, vol. 184, art. 107688, 2021.