

BLOCKCHAIN-ENABLED INTERNET OF THINGS AND COMPUTER NETWORKING: A COMPREHENSIVE REVIEW OF SECURE, DECENTRALIZED AND INTELLIGENT CONNECTIVITY

Ms.S.Karthika

Student,

Department of Artificial Intelligence & Data Science,

Dr.NGP Institute of Technology,

Coimbatore.

Email: Karthisomu27@gmail.com

Review Article

Abstract

The Internet of Things (IoT) connects large populations of sensors, actuators, gateways, machines, vehicles, and cloud services through heterogeneous computer networks. Although this connectivity enables real-time monitoring and intelligent automation, it also introduces significant security, privacy, trust, scalability, and data-management challenges. Blockchain has emerged as a complementary technology for IoT because its distributed ledger, cryptographic verification, consensus mechanisms, and smart contracts can reduce dependence on centralized trust models. This review examines the combined role of blockchain, computer networking, and IoT, emphasizing network architecture, device authentication, secure communication, decentralized data management, access control, smart contracts, edge/fog computing, and intelligent IoT applications. The review compares conventional centralized IoT architectures with blockchain-assisted designs and discusses the trade-offs involving latency, energy consumption, storage, throughput, consensus overhead, and resource constraints. Recent research indicates that blockchain can strengthen trust and accountability, but direct deployment of conventional blockchain protocols on resource-constrained IoT devices is often impractical. Lightweight consensus, permissioned ledgers, edge-assisted blockchain, off-chain storage, and adaptive security mechanisms are therefore important research directions. The paper concludes that the most effective future IoT networking



architecture will combine distributed trust with edge intelligence, efficient communication protocols, privacy-preserving analytics, and context-aware security.

Keywords—Blockchain, Internet of Things, computer networks, IoT security, edge computing, fog computing, smart contracts, decentralized systems.

I. INTRODUCTION

The Internet of Things has transformed computer networking from a system primarily designed to connect conventional computers into a large-scale environment in which physical objects continuously generate, exchange, and consume data. Sensors and embedded devices communicate through wireless and wired technologies and interact with gateways, edge nodes, cloud platforms, and application services. IoT therefore represents both a networking paradigm and an application ecosystem in which sensing, communication, computation, and actuation operate as an integrated loop [1], [2].

The scale and heterogeneity of IoT create security and management problems that are more difficult than those found in conventional enterprise networks. Many devices have limited memory, processing capability, and battery capacity. They may operate unattended, use heterogeneous communication protocols, and remain exposed for long periods. Weak credentials, insecure firmware, compromised gateways, and unauthorized data access can consequently affect the complete IoT system. Traditional centralized security models can provide useful administration but also create single points of failure and require continuous trust in central authorities [3].

Blockchain provides a distributed approach to establishing trust among participating entities. Instead of maintaining a single authoritative database, participating nodes maintain synchronized records that are protected by cryptographic mechanisms. Smart contracts can automate authorization, transactions, device registration, and policy enforcement. Researchers have therefore investigated blockchain as a security and management layer for IoT networks [4]–[6]. However, blockchain itself introduces communication, storage, computation, and consensus overhead. A practical architecture must consequently adapt blockchain principles to the characteristics of IoT networking rather than simply placing conventional blockchain infrastructure beside sensors.

This review analyzes the convergence of the three technologies—blockchain, computer networking, and IoT. The discussion focuses on how distributed trust can be integrated with communication infrastructure and how edge and fog computing can reduce the burden imposed on constrained devices. The objective is



to identify the major opportunities, limitations, and research directions for secure and scalable blockchain-enabled IoT networks.

II. IOT AND COMPUTER NETWORKING FOUNDATIONS

An IoT network typically contains four functional layers: sensing devices, communication/gateway infrastructure, edge or fog computing nodes, and cloud/application services. At the sensing layer, devices acquire temperature, motion, location, environmental, industrial, healthcare, or machine-state information. The networking layer transports these observations using technologies such as Wi-Fi, Bluetooth Low Energy, Zigbee, LoRaWAN, cellular networks, Ethernet, and emerging 5G/6G systems. Gateways translate protocols, aggregate traffic, and provide local processing before data reach centralized or distributed services [1], [2].

IoT communication differs from conventional Internet traffic because many devices produce small packets, may sleep periodically, and often require energy-efficient communication. In industrial environments, deterministic latency and reliability can be more important than raw bandwidth. In smart-city environments, massive device density and mobility may dominate. Consequently, network design must consider latency, packet loss, reliability, energy consumption, device mobility, spectrum availability, and security simultaneously.

Network virtualization, software-defined networking (SDN), network function virtualization, edge computing, and 5G provide mechanisms for dynamically managing IoT traffic. SDN can separate control and forwarding functions, allowing programmable policies for routing and security. Edge computing moves processing closer to data sources and can reduce latency and backhaul traffic. These technologies create useful execution points for blockchain services because edge nodes are generally more capable than end devices [7], [8].

III. BLOCKCHAIN FUNDAMENTALS FOR IOT

Blockchain is a distributed ledger in which transactions or records are grouped into blocks and linked through cryptographic hashes. A consensus mechanism determines how participating nodes agree on the valid state of the ledger. Public blockchains permit broad participation, whereas permissioned blockchains restrict participation to authorized entities. For IoT deployments, permissioned architectures are often attractive because device identities and organizational relationships are usually known in advance and high transaction throughput is desirable [4], [5].



The principal blockchain functions relevant to IoT include decentralized trust, immutable event records, identity management, access control, provenance, and automated policy enforcement. For example, a device can be registered through a ledger transaction, a gateway can verify its authorization before forwarding data, and a smart contract can determine whether a service is permitted to access a particular data stream. These functions can reduce dependence on a single authentication server and improve auditability [6].

Nevertheless, blockchain is not automatically secure or efficient. Consensus mechanisms can introduce latency and communication overhead, ledger growth creates storage requirements, and smart contracts may contain implementation vulnerabilities. Furthermore, immutability can conflict with privacy requirements because sensitive information should not necessarily be stored permanently. A practical IoT blockchain should therefore store minimal on-chain metadata and use protected off-chain repositories for large or sensitive data objects.

IV. BLOCKCHAIN-ENABLED IOT NETWORK ARCHITECTURE

A suitable integrated architecture can be organized into five logical components: IoT devices, network gateways, edge/fog nodes, a blockchain network, and cloud/application services. Devices primarily sense and actuate. Gateways perform protocol conversion, device authentication, traffic filtering, and aggregation. Edge nodes execute low-latency analytics and interact with blockchain peers. Blockchain nodes maintain trust-related records and execute smart contracts, while cloud services provide large-scale analytics, visualization, and long-term storage.

The interaction begins when a device generates an observation. The gateway validates the device identity and applies network policies. Instead of placing the complete observation on-chain, the gateway can calculate a cryptographic digest and record metadata such as device identity, timestamp, data type, access policy, and storage reference. The original data remain in an encrypted edge or cloud repository. Authorized users can later verify that the retrieved data correspond to the recorded digest. This arrangement combines blockchain integrity with practical storage efficiency.

Edge-assisted blockchain is particularly important because IoT devices cannot generally participate in computationally expensive consensus processes. Edge nodes can act as blockchain peers, validators, policy engines, or transaction aggregators. Batch processing can further reduce the number of ledger



transactions. Such an architecture distributes trust while retaining a manageable communication path between constrained devices and the ledger [8], [9].

V. SECURITY APPLICATIONS

A. Device Identity and Authentication

Large IoT deployments require scalable identity management. Conventional password-based authentication is inadequate for many unattended devices. Blockchain can maintain decentralized device-registration records and support cryptographic identities. A gateway can verify whether a device is registered, whether its credentials remain valid, and whether its requested service is authorized. This can improve traceability when devices join, leave, or change operational roles [6].

B. Access Control and Smart Contracts

Smart contracts can encode access policies such as who may read a sensor stream, which gateway can control an actuator, or under what conditions a machine can exchange data with another organization. Automated enforcement reduces manual intervention and creates auditable policy execution. Attribute-based policies can be represented using device type, location, organizational role, service type, or security level. The challenge is to keep contract logic simple enough for reliable execution and flexible enough for dynamic IoT environments.

C. Data Integrity and Provenance

IoT data can pass through several gateways, edge servers, and cloud services before reaching an application. Data provenance is therefore important in healthcare, industrial monitoring, supply chains, and critical infrastructure. Hashes recorded on a blockchain can provide evidence that a stored dataset has not been modified after registration. This does not prove that the original sensor reading was truthful, but it provides strong integrity evidence for subsequent processing [5], [10].

D. Network Attack Mitigation

Blockchain can support distributed blacklists, device reputation, and collaborative security records. When a device is identified as malicious, authorized network nodes can update a shared security record that influences future access decisions. Combined with SDN, such information could dynamically modify routing or isolation policies. However, blockchain should complement rather than replace intrusion detection, encryption, secure firmware, and conventional network defense mechanisms.



VI. INTEGRATION WITH EDGE AND FOG COMPUTING

The combination of blockchain, IoT, and edge/fog computing addresses a fundamental mismatch between blockchain requirements and IoT constraints. Edge nodes have greater computing and storage capacity than sensors while remaining closer to devices than centralized cloud infrastructure. They can perform data filtering, aggregation, anomaly detection, and transaction batching before interacting with blockchain networks [7], [8].

Fog architectures can distribute blockchain functions across multiple intermediate nodes. For example, local fog clusters can maintain regional ledgers while periodically synchronizing selected state with a higher-level consortium blockchain. This reduces long-distance communication and can improve responsiveness. It also enables local operation during temporary cloud connectivity problems. The design must nevertheless prevent malicious edge nodes from becoming trusted intermediaries without adequate verification.

A further opportunity is blockchain-assisted edge resource management. Smart contracts can represent service agreements between IoT devices, edge providers, and applications. Resource requests can be authenticated and recorded, while policies determine computing allocation or data-sharing rights. Such mechanisms are particularly relevant to smart manufacturing, connected vehicles, and distributed sensing systems.

VII. PERFORMANCE AND NETWORKING CHALLENGES

Issue	IoT requirement	Blockchain impact	Possible solution	Research priority
Latency	Fast response	Consensus delay	Edge validation, batching	High
Energy	Long battery life	Computation/communication overhead	Lightweight protocols	High
Storage	Small device memory	Growing ledger	Off-chain storage	High
Scalability	Massive device count	Transaction congestion	Sharding, sidechains	High

Privacy	Protected sensor data	Immutable records	On-chain hashes + encryption	High
Trust	Reliable device behavior	Malicious peers/contracts	Permissioned consensus	High
Interoperability	Heterogeneous protocols	Ledger integration complexity	Standard APIs/gateways	Medium

Table I. Major challenges in blockchain-enabled IoT networking and representative mitigation strategies.

VIII. APPLICATION DOMAINS

Smart manufacturing can use blockchain-enabled IoT to record machine states, production events, maintenance actions, and supply-chain transactions. A sensor gateway can submit tamper-evident event metadata while edge analytics identify abnormal machine behavior. Blockchain can then provide a shared history across manufacturers, suppliers, and service providers. This is particularly useful when multiple organizations need to verify process information without placing all operational data under one company's database [10].

Smart cities provide another important application. Distributed sensors monitor traffic, parking, air quality, energy usage, waste management, and public infrastructure. Blockchain can support device identity, data provenance, and controlled data sharing between municipal departments and service providers. Connected vehicles can also use distributed trust mechanisms for message verification and service transactions, although mobility and stringent latency requirements require specialized designs [11].

Healthcare IoT can benefit from verifiable data provenance and fine-grained access control. Wearable and medical devices generate sensitive information that may be shared among patients, clinicians, laboratories, and service providers. Blockchain can maintain permissions and integrity records while encrypted medical data remain off-chain. Privacy, regulatory compliance, emergency access, and key recovery must be carefully addressed [12].

Agricultural IoT, logistics, and energy systems also benefit from combining sensing and distributed trust. Environmental sensors can provide verifiable information about crop conditions, while supply-chain participants can use ledger records to track product events. In smart grids, distributed devices can report



energy measurements and participate in automated transactions. Across these domains, the blockchain should be selected according to actual trust and coordination requirements rather than treated as a mandatory component.

IX. RESEARCH GAPS AND FUTURE DIRECTIONS

Several research gaps remain. First, interoperability is still a major problem because IoT systems use diverse protocols, data models, and administrative domains. Standardized gateway interfaces and semantic models are required for blockchain services to operate across heterogeneous networks. Second, scalable consensus remains difficult when millions of devices generate frequent events. Permissioned consensus, delegated validation, sharding, sidechains, and directed acyclic graph techniques deserve further investigation [13].

Third, privacy-preserving blockchain-IoT systems require stronger mechanisms for selective disclosure, secure multiparty processing, zero-knowledge techniques, and decentralized identity. Immutability should not imply permanent exposure of sensitive information. Fourth, AI can be integrated with blockchain-enabled networks to detect anomalies, predict device failures, optimize routing, and adapt security policies. A promising architecture combines AI at the edge with blockchain for trust and auditability rather than attempting to place machine learning computation directly on the ledger [14].

Finally, future 5G/6G and edge-native IoT networks will require joint optimization of communication, computation, security, and trust. Blockchain services should be adaptive to network conditions, device energy levels, traffic intensity, and application criticality. Benchmark datasets and common evaluation frameworks are also needed so that proposed systems can be compared using latency, throughput, energy, storage, security, and scalability rather than isolated accuracy or transaction metrics.

X. CONCLUSION

The convergence of blockchain, computer networking, and IoT offers a promising foundation for secure and trustworthy distributed sensing systems. IoT supplies large-scale sensing and actuation, computer networks provide the communication infrastructure, and blockchain introduces decentralized trust, verifiable records, and programmable policies. The combination can strengthen device identity, access control, data provenance, and collaborative security. However, conventional blockchain mechanisms are often too resource-intensive for direct deployment on constrained IoT devices. Edge and fog computing, permissioned ledgers, lightweight consensus, transaction batching, and off-chain storage therefore form



essential components of practical designs. Future research should focus on interoperability, privacy, scalable consensus, AI-assisted security, adaptive networking, and energy-aware blockchain services. Rather than replacing existing IoT security and networking technologies, blockchain is best viewed as a complementary trust layer whose functions are carefully selected according to application requirements.

REFERENCES

- [1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.
- [2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.
- [3] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed Internet of Things,” *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013, doi: 10.1016/j.comnet.2012.12.018.
- [4] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
- [5] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” in *Proc. IEEE/ACS 13th Int. Conf. Computer Systems and Applications*, 2016, pp. 1–6.
- [6] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and solutions,” *arXiv preprint arXiv:1608.05187*, 2016.
- [7] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge computing: Vision and challenges,” *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016, doi: 10.1109/JIOT.2016.2579198.
- [8] 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, doi: 10.1016/j.future.2018.05.046.
- [9] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of blockchains in the Internet of Things: A comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019, doi: 10.1109/COMST.2018.2886932.



- [10] A. Bahga and V. K. Madiseti, “Blockchain platform for industrial Internet of Things,” *Journal of Software Engineering and Applications*, vol. 9, no. 10, pp. 533–546, 2016.
- [11] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. Ghias, and L. H. Koh, “Blockchain for future smart grid: A comprehensive survey,” *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2021, doi: 10.1109/JIOT.2020.2993601.
- [12] A. Stagnaro, “The case for blockchain in healthcare,” *Gartner Research*, 2017.
- [13] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.
- [14] A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for IoT,” in *Proc. 2nd IEEE Int. Conf. Internet-of-Things Design and Implementation*, 2017, pp. 173–178, doi: 10.1109/IoTDI.2017.36.
- [15] M. Belotti, N. Božić, G. Pujolle, and S. Secci, “A vademecum on blockchain technologies: When, which, and how,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3796–3838, 2019, doi: 10.1109/COMST.2019.2934780.