# Blockchain-Driven Security and Privacy Mechanisms in IoT: A Systematic Review

Zakari Idris Matinja[1], Zainab Aliyu Musa[1], Rumana Kabir Aminu[2], Ogochukwu John Okonko[1], Maryam Alka[3], and Umar Kabir Umar[4]

[1]Department of Computer Science, Federal Polytechnic Bauchi, Nigeria
[2]Department of Computer Science, FCT College of Education Zuba, Abuja , Nigeria
[3]Department of Computer Science, University of Birmingham, UK
[4]Department of Computing Technologies, SRM Institute of Science and Technology, Tamil Nadu, India

(corresponding author: uk2265@srmist.edu.in)

Abstract

The rapid advancement in the field of Internet of Things (IoT) has brought to light notable threats to data security and user privacy due to the growing network of internet-enabled devices and the exchange of confidential user data. Conventional security approaches often underperform in addressing these issues effectively, emphasizing the need of advanced solutions to maintain data integrity, authentication, and confidentiality. Blockchain technology is gearing attention for its ability to provide a robust solution due to its decentralized architecture, cryptographic security, and immutability. This review examines how blockchain can be integrated with IoT security by analyzing existing frameworks, methodologies, and implementations. By assessing the advantages and limitations of blockchain-based security models, the study provides a comprehensive understanding of how this technology enhances privacy, mitigates cyber threats, and fosters trust among IoT devices. The review categorizes various blockchain-driven security solutions for IoT, with a focus on consensus mechanisms, smart contracts, and access control models. Key findings suggest that while blockchain significantly strengthens IoT security, constraints encompassing scalability, increased computational burden, and energy consumption remain key obstacles. Additionally, the study highlights emerging trends, including lightweight blockchain protocols and hybrid security models, designed to address these issues. Moreover, the review identifies research gaps and suggests future directions for optimizing blockchain's role in IoT security. By offering critical viewpoint on the rapidly changing IoT landscape protection; this article serves as a useful reference for researchers and industry experts aiming to develop privacy-aware and secure IoT infrastructure

Keywords: Internet of Things (IoT), Blockchain Technology, Cyber Threats, Security and Privacy, Data Authentication, Data Confidentiality.

## 1. Introduction

The Internet of Things (IoT) infrastructure is a rapidly growing ecosystem of sensor-equipped physical devices with integrated software, and network functions that enable them to gather, transmit, and share data through the internet. By linking the physical world with digital systems, IoT creates opportunities for on-the-fly monitoring, intelligent strategic decision-making, and seamless automation. This technological framework is transforming a wide range of sectors such as healthcare, logistics, agriculture, and intelligent city planning by enabling more efficient, responsive, and data-driven operations. For example, in healthcare environments, IoT supports telemedicine-based patient monitoring and timely diagnostics, while in agriculture, it facilitates precision farming through environmental sensing. Across these fields, IoT technology is pivotal in enhancing productivity, enabling predictive maintenance, and optimizing resource usage, thereby contributing to improved operational performance and strategic planning [1]. At the heart of the Internet of Things (IoT) are several essential components that works together to create a seamless and intelligent system capable of real-time decision-making. These components include sensors and actuators, which serve as the primary tools for detecting physical shifts in environmental parameters, including temperature and humidity motion, or pressure and initiating corresponding actions. Once data is captured, it is processed by microcontrollers or embedded processors that analyze and interpret the input locally or prepare it for transmission. Communication

modules, such as ZigBee, Bluetooth, Wi-Fi, or cellular networks, facilitate the wireless exchange of data between devices and central systems. The accumulated data is often propagated to cloud-based infrastructure, where it can be stored, further analyzed, and integrated with large-scale data processing tools. Finally, user-facing dashboards and graphical interfaces provide visualization and control mechanisms, enabling user to system interaction, monitor performance, and make informed decisions. Together, these interconnected elements form the backbone of IoT infrastructure, enabling smart, autonomous systems across various applications [2].

Internet of Things (IoT) systems function through a multi-layered architecture designed to manage data flow from the physical environment to user applications. This framework is usually composed of three fundamental layers: the perception layer, the network layer, and the application layer. The perception layer acts as the cornerstone, where hard objects are fitted with sensing and actuation equipments to detect and acquire real-world environment data such as temperature, motion, or light levels. This raw data is then passed to the network layer, which is accountable for transmitting it securely and efficiently using various communication technologies and protocols, including Wi-Fi, Bluetooth, ZigBee, and cellular networks. The final stage is the application layer, where the gathered information is processed, analyzed, and transformed into actionable insights or services tailored to user needs. This layer supports a broad spectrum of practical uses, from intelligent homes and healthcare monitoring to automation of industrial functions and intelligent transportation systems. Together, these layers form an integrated framework that enables IoT systems to observe environmental changes, interpret data in real time, and drive intelligent responses across diverse domains [3]. The Internet of Things (IoT) relies on a wide range of wireless communication technologies, each tailored to specific use cases based on criteria such as coverage range, energy efficiency, data transmission rate, and deployment environment. Among the most commonly used technologies are Wi-Fi, Low Power Wide Area Networks (LPWAN), 5G, ZigBee, LoRa (Long Range), and Narrowband IoT (NB-IoT). Wi-Fi, known for its high data throughput, is typically utilized in short-range, high-bandwidth indoor environments like smart homes and offices. On the other hand, LPWAN technologies including LoRa and NB-IoT are engineered for long-distance transmission with reduced power requirements, making them ideal for large-scale, rural, or remote deployments including smart farming and monitoring of the environments, and utility metering. ZigBee is often employed in mesh network configurations for low-power, short-range use cases like industry control and home automation. Meanwhile, the advent of 5G introduces ultra-minimum delay and high-throughput connection, supporting on-the-fly applications such as self driven vehicles and tele-surgery. Each technology plays a vital role in shaping IoT ecosystems by addressing specific operational requirements and ensuring efficient data exchange across diverse environments [4].

### 1.1. Issues in IoT Systems

Internet of Things (IoT) network often faces some challenges, which includes security challenges, privacy concern, scalability issues, interoperability and standardization, energy constraints, and data management and processing.

A. Security Challenges in IoT

Security stands as one of the fundamental concern facing the Internet of Things (IoT) ecosystem. The massive scale and heterogeneity of interconnected devices significantly broaden the attack surface, making IoT networks increasingly susceptible to cyber vulnerabilities including unauthorized access, malware infiltration, DoS threats and information breaches. These risks are further intensified by the frequently restricted processing and memory capacity and power availanility in the IoT infrastructures, which restrict the implementation of robust security protocols. A critical objective in securing IoT systems is maintaining the principles of the CIA triad: confidentiality, integrity, and availability. However, enforcing these principles consistently across all layers of the IoT architecture poses significant difficulties. Many devices operate in unprotected environments, lack secure update mechanisms, and communicate over vulnerable networks. As a result, developing lightweight, scalable, and adaptive security solutions customized for the distinct constraints of IoT remains a top priority for researchers and practitioners alike[5].

B. Privacy Concern in IoT

Internet of Things (IoT) devices frequently gathers and propagates delicate personal information, including medical data, real-time location, behavioral patterns, and daily routines. This continuous and often passive data collection raises significant privacy concerns, especially when data is inadequately protected or mismanaged. Without strong

encryption mechanisms or proper access controls, personal information becomes vulnerable to unauthorized access, interception, or misuse, potentially leading to serious privacy breaches and identity theft. Additionally, many IoT systems depend on third-party cloud platforms for data processing and storage. While these services offer scalability and convenience, they also introduce concerns around data ownership, user consent, and control. Users may have limited visibility into how their data is managed, shared, or retained by cloud providers, which creates trust issues and complicates regulatory compliance—especially under privacy laws such as the General Data Protection Regulation (GDPR). Ensuring user privacy in the IoT landscape thus requires not only technical safeguards, like end-to-end encryption and anonymization, but also clear governance frameworks and transparent data practices that empower users to control how their information is collected and used [6].

C. Scalability Issues in IoT

Scalability presents a significant challenge in the development and operation of IoT networks. As the scale of connected devices increases into billions, ensuring seamless data collection, processing, and communication across the network becomes increasingly complex. Traditional centralized computing models, where all data is sent to a cloud infrastructure for execution, often struggle to manage the scale, speed, and diversity of data generated by large-scale IoT deployments. These centralized systems can experience bottlenecks, increased delay, and exorbitant bandwidth usage, which hinder real-time responsiveness and overall efficiency. To address these limitations, researchers and engineers are turning to distributed system models, with edge computing emerging as a promising solution. In edge-enabled computation, data processing takes place in proximity to the source at the network edge on devices such as gateways, routers, or even the sensors themselves. This approach reduces the necessity of transmitting extensive data to central data centers, thereby lowering latency, conserving bandwidth, and enabling faster decision-making. Edge computing also supports greater scalability by distributing workloads across a broader infrastructure, making it more adaptable to growing and geographically dispersed IoT ecosystems. As IoT adoption continues to expand, designing systems that can scale efficiently while maintaining performance and reliability will be essential for long-term success [7]

D. Interoperability and Standardization in IoT

One of the major obstacles to the pervasive integration and interoperability of IoT technologies is the lack of universally accepted standards across device manufacturers, software developers, and service providers. With countless vendors producing IoT components using proprietary protocols and interfaces, achieving seamless communication between devices from different sources can be highly problematic. This fragmentation results in compatibility issues, data silos, and integration challenges, which ultimately hinder the design and implementation of cohesive and scalable IoT ecosystems. In the absence of standardized frameworks, organizations often resort to custom-built or vendor-specific solutions, which not only increase implementation costs but also limit flexibility and long-term sustainability. The resulting lack of interoperability can impair real-time data sharing, reduce system efficiency, and obstruct innovation particularly in complex, multi-vendor environments such as smart cities, industrial automation, and healthcare. Recognizing these challenges, various international standardization bodies and industry alliances are committed to advancing and disseminating common standards for communication protocols, data formats, and security frameworks. These efforts aim to create a more unified and interoperable IoT landscape, where devices and services from diverse sources can seamlessly integrate and cooperate [8]

E. Energy Constraints

A considerable segment of Internet of Things (IoT) devices, particularly those deployed in remote, mobile, or hard-to-reach environments, rely on battery power for operation. These devices often function in locations where frequent human intervention for maintenance or battery replacement is either logistically difficult or economically unfeasible. As a result, energy efficiency becomes a critical design consideration in IoT systems. Prolonging battery life without compromising performance is essential to ensuring the long-term functionality and reliability of these devices. To address this challenge, developers and engineers focus on creating low-power hardware components and optimizing software algorithms to reduce energy consumption. One common strategy involves incorporating power-saving mechanisms such as sleep or idle modes, where devices enter a low-energy state when not actively sensing or transmitting data. Additionally, duty cycling techniques are used to minimize the active periods of sensors and communication modules. Beyond traditional power-saving methods, innovative solutions like energy-harvesting

technologies are gaining traction. These technologies allow IoT devices to produce energy from naturally available sources like solar radiation, thermal gradients, radio frequency signals, or mechanical vibrations. By harvesting energy from their environment, devices can extend operational lifespans and, in some cases, operate indefinitely without the need for battery replacements. The push for energy-efficient IoT systems is not only a matter of practicality but also a step toward sustainability, reducing electronic waste and lowering the ecological consequences of large-scale IoT deployments [9]

F. Data Management and Processing

In light of the expanding IoT ecosystem, the volume of data generated by billions of interconnected devices is increasing at an unprecedented rate. This explosive growth has made streamlined data processing and advanced analytics essential for extracting meaningful insights and enabling timely decision-making. In many IoT applications such as autonomous vehicles, industrial automation, smart healthcare, and emergency response systems real-time data processing is critical. Delays in analyzing and responding to data can compromise performance, safety, and user experience. To meet these demands, conventional cloud service models, which centralize data execution in remote cloud infrastructure, are being supplemented by distributed computing paradigms such as edge and fog computing. Edge computing facilitates processing near the data origin or near the devices themselves allowing for swift data processing with negligible delay. Fog computing operates through a decentralized architecture, much like edge computing but typically processes data at intermediary nodes between the edge devices and centralized cloud infrastructure, offering a hierarchical architecture that balances performance and scalability. By limiting the need for transmitting massive volumes of raw data to remote cloud infrastructures, both edge infrastructure and the fog infrastructure significantly lower network latency, decrease bandwidth usage, and enable faster system responses. These benefits make them particularly valuable for time-sensitive applications and contribute to more resilient, efficient, and scalable IoT infrastructures. As IoT ecosystems grow more complex, the incorporation of cloud technology, edge, and fog computing will serve a crucial function in guaranteeing seamless data handling and responsive operations across a wide range of industries [10].

This study examines the potential of blockchain technology integration with IoT security by reviewing current frameworks, methodologies, and practical applications. It evaluates the benefits and limitations of blockchain-based security models, offering a detailed insight into how this technology can enhance privacy, reduce cyber threats, and build trust among IoT devices. The review categorizes various blockchain-enabled security solutions for IoT, emphasizing consensus mechanisms, smart contracts, and access control strategies. Key conclusions indicate that while blockchain significantly improves IoT security, challenges like scalability, high computational demands, and energy usage continue to pose significant barriers. The study also discusses emerging trends, such as lightweight blockchain protocols and hybrid security approaches, aimed at overcoming these challenges. Additionally, it identifies areas for further research and suggests potential paths to optimize blockchain's effectiveness in IoT security. The study is organized as follows. Chapter one introduces the IoT, its key components, communication protocols and challenges faced by the IoT network. Chapter two discusses the use of blockchain technology in IoT security and privacy and derived taxonomy of the security and privacy solutions developed using the blockchain technology. Chapter three presents the summary of various research presented by researchers in IoT security and privacy. Chapter four draw and inference from the summary of various researches presented by researchers in IoT security and privacy and suggests some possible solutions and improvements. Lastly, chapter five concludes the study.

**Blockchain Technology in IoT Security and Privacy**

The swift advancement of the IoT technology has resulted to considerable threats to security and privacy of the IoT ecosystem that necessitate the introduction of several protection techniques that can minimize these security challenges. Currently, cryptographic methods, blockchain based methods, AI and Machine Learning based methods, and privacy preserving techniques are widely employed in securing the IoT ecosystem. These techniques ensure the protection of connected devices within the IoT ecosystem from various attacks that result in compromise of IoT device functionalities and breach of user data and privacy. The IoT ecosystem consist of numerous resource constrained components with limited computation and storage infrastructures. These limitations expose the IoT devices to several vulnerabilities like weak authentication, obsolete firmware and absence of encryption against user data. The attackers

takes advantages of the limitations of the IoT devices to exploit the system, taking control of individual devices or group of devices, disrupt system services and gain an unauthorized access to users data. The IoT devices usually collect sensitive information about the users, process and share the collected information over the network. Storing these data without sufficient protection rise some serious privacy concern like identity theft, surveillance and profiling. Several security and privacy preservation techniques like user-controlled data access, secure boot mechanisms, frequent update of software, de-identification, encrypted communication protocols, establishment of policies for devices access at various levels and strict adherence to privacy policies can be adopted to ensure data privacy. Figure 1 presents the taxonomy of the security and privacy in IoT using blockchain technology.

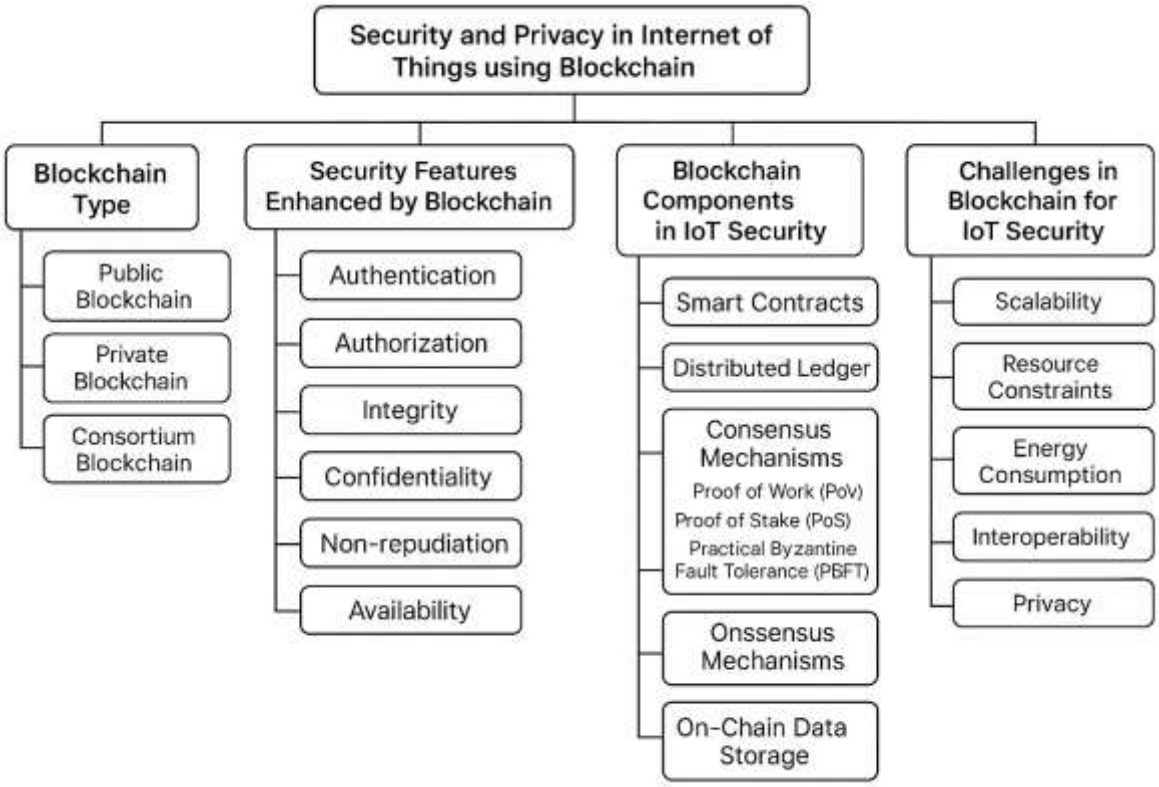


Figure 1 Taxonomy of Security and Privacy in IoT Using Blockchain Technology

I. Blockchain Type

In this category, the type of blockchain technology used in addressing the security and privacy in IoT ecosystem is considered. The types of blockchain considered include the private blockchain, public blockchain and consortium blockchain. In private blockchain technology, access to known entities in the decentralized networks is restricted, ensuring maximum control over the user data and transactions. The public blockchain require no prior authorization for anyone to participate in the transactions in the decentralized network. The transparency and immutability offered by the public blockchain technology makes it to be the most suitable for applications demanding open access and verifiable transactions. The consortium blockchain technology is a decentralized network technology controlled by group of organizations, with an efficient balanced decentralization. In Internet of Things ecosystem, the consortium blockchain technology can improve data privacy and streamline the operations of some specific sectors.

II. Security Features Enhancement

In this category, the techniques are classified based on the security features considered in addressing the security and privacy concern in IoT ecosystem. The security and privacy features enhanced include authentication, authorization, data integrity and confidentiality. Authentication and authorization enhancement using blockchain technology provide a decentralized identity management restricting access to the IoT network to only authorized devices. Access controls are automated using smart contracts, thus mitigating single point of failure and minimizing dependence on central authorities. In data integrity and confidentiality, the immutable nature of the blockchain technology is employed to ensure integrity of the IoT system as the recorded transactions in blockchain cannot be altered retroactively. When blockchain technology is integrated with data encryption, it can uphold confidentiality in the data collected by the IoT devices, safeguarding the system from unauthorized access.

## III. Blockchain Components

Blockchain components include the smart contracts and consensus mechanisms. In Internet of Things network, the smart contracts automate the process of device authentication and data communication through self-execution of defined agreements in the execution codes, improving the system efficiency and eliminating the need for intermediaries. This approach requires a rigorous security audit as the code may have some vulnerabilities that can be exploited. The consensus mechanism ensure that all the participants involved in the blockchain transactions agrees on the ledger state. Proof of work (PoW) in consensus mechanism offers a robust security in IoT but can swiftly exhaust the system batteries due to its high energy consumption, thus making it unsuitable for IoT network. Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) can be employed in place of the PoW mechanism due to their low energy consumption and faster transaction times, satisfying the requirements of the IoT network.

## IV. Challenges in Blockchain for IoT Security

The blockchain technology plays a vital role in addressing security and privacy challenges in the IoT networks. Despite the advantages of the technology, solutions adopting the technology are accompanied with some challenges like high energy consumption, scalability issues, resource constraints and interoperability. The vast number of devices in the IoT ecosystem uses battery cells as source of power and has limited computational resources, thus making it challenging to implement protocols with high energy consumption and resource intensive. In addition, the devices faces scalability issues as the continuously generate data streams from the environments they are installed. Several researches explore the potentials of employing the blockchain method to improve the level of security and trust of the IoT network, identifying the challenges faced by the system including privacy, security and interoperability.

**State-of-the-art Techniques**

To ensure the security and privacy of the IoT network, several solutions employing blockchain technology have been developed by researchers in the academia and industry. For example, the research by [11, 13, 20, 25, and 30] focus on developing a blockchain based authentication and access control system that authenticates the IoT devices in the network and manage access control. The aim of these methods is to ensure secure access to the IoT network through user authentication. The solutions developed by the authors include a private blochchain based lightweight framework for the authentication of IoT devices, a permission blockchain solution for access management in clustered IoT network, and a public blockchain identity-based mechanism for device identification and an Authenticated Devices Configuration Protocol (ADCP) for management of authenticated overlay Internet of Things (IoT) networks. To ensure the security and privacy of user sensitive data stored on the devices and during transmission, the authors of [15, 18, 22, 26, and 27] targeted the securing data stored in the cloud and when they are being transferred from one node to the other. The solutions aimed at protecting the integrity, privacy and the availability of user sensitive data in transit and on cloud storage. These solutions proposed by the authors include an integrated blockchain-based homomorphic encryption model for confidential transmission, blockchain based sensor data validation system for sensor data validation, blockchain indices for secure access, and a lightweight solution for the resource-constrained IoT devices.

In addition to the solutions developed authentication and access control and secure data storage and transmission, trust management and reputation methods have been developed to establish trust among the various IoT devices in the network and validate transaction integrity using the blockchain technology. In this aspect of security and privacy for

IoT network, decentralized trust models are developed for the IoT ecosystem. The solutions developed include smart contracts, fog-enabled framework, blockchain-based firmware update and smart device reputation system for autonomous IoT trust interactions, trust control and service trusts [12, 14, 21, 23, and 29]. On the other hand, consensus and lightweight blockhain optimizations have been developed by researchers [16, 17, 19, 24, and 28] to ensure energy efficiency and scalability in IoT system. The techniques developed by the researchers include decentralized key management system, hybrid edge-blockchain architecture, lightweight BFT consensus protocol and scalable access control and integrated blockchain secure multi-party computation for use in consortium network and added confidentiality. Table 1presents the summary of the state of the art methods and their limitations.

Table 1 Summary of the state-of-the-art

| Reference | Proposed Method | Blockchain Type | Security Feature Enhanced | Blockchain Components | Limitations |
|---|---|---|---|---|---|
| Dorri et al. (2017) | Lightweight BIoT framework | Private | Authentication, Access control | Consensus, Smart Contracts | Scalability issues |
| Christidis & Devetsikiotis (2016) | Smart contracts for autonomous IoT | Public | Trust, Data integrity | Smart Contracts, Ledger | High energy consumption |
| Novo (2018) | Permissioned blockchain for IoT clusters | Consortium | Authorization | Smart Contracts, Consensus | Not scalable to massive devices |
| Sharma et al. (2019) | BIoT for fog-enabled systems | Private | Trust Management | Consensus, Distributed Ledger | Fog node dependency |
| Yue et al. (2017) | Healthcare IoT with blockchain | Private | Privacy, Data integrity | Smart Contracts, Cryptography | Delays in emergency cases |
| Liang et al. (2020) | Decentralized key management | Consortium | Confidentiality | Public/Private Keys | Key revocation issues |
| Ali et al. (2021) | Hybrid edge–blockchain framework | Consortium | Data privacy | Edge Nodes, Ledger | Resource-intensive |
| Singh et al. (2020) | Blockchain with homomorphic encryption | Public | Data confidentiality | Encryption, Ledger | Computational overhead |
| Ren et al. (2020) | Lightweight consensus with BFT | Private | Device authentication | Consensus Mechanism | Limited fault tolerance |
| Zhou et al. (2020) | Identity-based blockchain scheme | Public | Identity authentication | Identity Mgmt, Smart Contracts | High latency |
| Salman et al. (2018) | Blockchain for secure update | Public | Firmware integrity | Smart Contracts, Hashing | Storage complexity |
| Wang et al. (2019) | Blockchain for sensor trust | Public | Data authenticity | Hash, Ledger | Costly for small sensors |
| Moinet et al. (2017) | Reputation-based IoT blockchain | Private | Trust | Reputation Layer, Consensus | Collusion vulnerability |
| Yang et al. (2021) | Consortium BIoT framework | Consortium | Access control | Distributed Ledger, Smart Contracts | Needs trusted initial setup |
| Chen & Wang (2021) | Authenticated overlay networks (ADCP) | Consortium | Authentication | Access Control, Consensus (ACC) | Key exchange risks |
| Alam & Chowdhury (2022) | Secure data storage indices | Public | Data Access Control | Ledger Indexing, Smart Contracts | Data not fully on-chain |
| Zhang & Wu (2022) | Lightweight blockchain security | Private | Secure data transmission | Optimized Consensus | Limited to lightweight use-cases |
| Zhou & Li (2021) | Blockchain + Multi-party computation | Consortium | Confidentiality | MPC Layer, Consensus | High implementation complexity |

| | | | | | |
|---|---|---|---|---|---|
| Liu & Zhang (2022) | Service agreement via smart contracts | Private | Transparency, Trust | Smart Contracts, Ledger | Service complexity scalability |
| Chen & Wang (2021) | ADCP for secure comms | Consortium | Authentication, Secure routing | Smart Contracts, Ledger | Requires full node support |

**Inference from the State-of-the-art**

With the continuous integration of more smart devices to the Internet of Things (IoT) networks, the volume of data generated by these devices has experienced a significant increase. These devices are resource constrained and uses battery cells as source of power to keep them alive. Resource intensive tasks can exhaust their power source and the limited processing and storage capabilities possessed by these devices. In addition to high computational and energy overhead, interoperability between the different IoT platforms and the blockchain networks is another major hurdle in the IoT ecosystem. Most blockchain solutions developed to address the security and privacy in IoT networks are platform specific, which limits integration and scalability. Considering the latency due to transaction delay in blockchain, the solutions developed can improve security and privacy of the IoT networks but can hinder real-time IoT applications, which are sensitive to any form of delay. The deployment and management of the blockchain technology in the IoT network is complex, which remains a barrier for non-technical users.

To address the aforementioned limitations in the blockchain based security and privacy systems, there is need for an integrated technological innovation, IoT architecture restructuring, development of lightweight consensus mechanisms, standardization of blockchain protocols, and adoption of middleware solutions, hybrid blockchain architecture, blockchain-as-a-service platforms and system optimization.

**Conclusion**

With the continuous adoption of Internet of Things (IoT) technology in various areas like smart homes, health care, transportation, agriculture, manufacturing, retail, energy, environmental monitoring, smart cities, supply chain and logistics and more, the number of smart devices integrated into the larger network (internet) have increased drastically. The drastic growth in the number of devices in the IoT network is proportional to the volume of data generated by the IoT network. These devices tend to be resource constrained and uses battery cells as their source of power, which became the major challenges in the IoT network. The large volume of sensitive data generated by the IoT devices necessitate the need for a robust security and privacy mechanism in the IoT network to ensure the safety of these sensitive data. Several security solutions have been developed by researchers to ensure the safety of the data in the IoT network with blockchain technology being one of the technologies employed in the development of security and privacy solutions for IoT. This study explores the integration of blockchain technology with IoT security by reviewing current frameworks, methodologies, and practical applications. The study evaluates the benefits and limitations of blockchain-based security models, offering a detailed insight into how this technology can enhance privacy, reduce cyber threats, and build trust among IoT devices. The review categorizes various blockchain-enabled security solutions for IoT, emphasizing consensus mechanisms, smart contracts, and access control strategies. Key conclusions indicate that while blockchain significantly improves IoT security, challenges like scalability, high computational demands, and energy usage continue to pose significant barriers. The study also discusses emerging trends, such as lightweight blockchain protocols and hybrid security approaches, aimed at overcoming these challenges. Additionally, it identifies areas for further research and suggests potential paths to optimize blockchain's effectiveness in IoT security.

**References**

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

2. Ray, P. P. (2016). A survey on Internet of Things architectures. *Journal of King Saud University - Computer and Information Sciences*, 30(3), 291–319. https://doi.org/10.1016/j.jksuci.2016.10.003
3. Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4), 2233–2243. https://doi.org/10.1109/TII.2014.2300753
4. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010
5. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018
6. Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 4(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.411
7. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2014). Fog computing: A platform for Internet of Things and analytics. In *Big data and Internet of Things: A roadmap for smart environments* (pp. 169–186). Springer. https://doi.org/10.1007/978-3-319-05029-4_7
8. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010
9. Rault, T., Bouabdallah, A., & Challal, Y. (2014). Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks*, 67, 104–122. https://doi.org/10.1016/j.comnet.2014.03.027
10. Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal*, 3(6), 854–864. https://doi.org/10.1109/JIOT.2016.2584538
11. Li, D., Wu, S., Chen, H., & Li, H. (2018). A blockchain-based authentication and security mechanism for IoT. *Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 1–6. https://doi.org/10.1109/ICCCN.2018.8487341
12. Zheng, Z., Xie, S., & Dai, H. (2020). Blockchain-based IoT security and privacy enhancement using smart contracts. *IEEE Transactions on Industrial Informatics*, 16(5), 3502–3510. https://doi.org/10.1109/TII.2019.2941069
13. Zhao, Y., & Liu, J. (2021). Securing IoT devices with blockchain-based trust management. *Computers, Materials & Continua*, 67(3), 2717–2732. https://doi.org/10.32604/cmc.2021.016982
14. Akkaya, M., Khan, M. A., & Salah, K. (2024). Blockchain-enhanced smart contracts for formal verification of IoT security. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2024.01.007
15. Kumar, R., & Tripathi, R. (2021). IoT privacy preservation using blockchain. *Journal of Cyber Security Technology*, 5(2), 74–96. https://doi.org/10.1080/19393555.2021.1919795
16. Kumar, S., & Sahoo, S. (2020). Blockchain-based access control for secure IoT data sharing. *Future Generation Computer Systems*, 109, 468–477. https://doi.org/10.1016/j.future.2020.02.031
17. Chowdhury, P., & Alam, M. (2022). Securing IoT communication using blockchain with lightweight encryption. *Wireless Communications and Mobile Computing*, 2022, 1–12. https://doi.org/10.1155/2022/8903146
18. Singh, A., & Gupta, R. (2021). A blockchain-based privacy-preserving solution for IoT. *IEEE Transactions on Cloud Computing*, 9(6), 2035–2045. https://doi.org/10.1109/TCC.2020.2986235
19. Jiang, H., & Xie, L. (2022). Blockchain-assisted secure data aggregation for IoT. *Journal of Network and Computer Applications*, 186, 103129. https://doi.org/10.1016/j.jnca.2021.103129
20. Hassan, M., & Noura, H. (2021). A secure and scalable IoT framework using blockchain for healthcare applications. *Future Generation Computer Systems*, 116, 456–469. https://doi.org/10.1016/j.future.2020.11.027
21. Zhang, H., & Wu, Y. (2022). Lightweight blockchain-based security solutions for IoT applications. *Sensors*, 22(3), 1092. https://doi.org/10.3390/s22031092
22. Zhang, C., & Xu, Y. (2020). Blockchain-enabled access control for secure IoT systems. *IEEE Transactions on Industrial Informatics*, 16(5), 3425–3434. https://doi.org/10.1109/TII.2020.2952853
23. Zhou, Z., & Li, X. (2021). Secure IoT communication with blockchain and multi-party computation. *IEEE Transactions on Information Forensics and Security*, 16, 2064–2075. https://doi.org/10.1109/TIFS.2021.3060900
24. Liu, Q., & Zhang, S. (2022). Blockchain-based secure and transparent IoT service management. *Journal of Cloud Computing: Advances, Systems and Applications*, 11(1), 27–40. https://doi.org/10.1186/s13677-022-00278-6

25. Chen, Y., & Wang, J. (2021). Blockchain-based authentication and secure communication in IoT. *Security and Privacy*, 4(3), e319. https://doi.org/10.1002/spy2.319
26. Alam, M., & Chowdhury, P. (2022). Securing data access using blockchain technology through IoT cloud integration. *Security and Privacy*, 5(2), e356. https://doi.org/10.1002/spy2.356
27. Zhang, H., & Wu, Y. (2022). Lightweight blockchain-based security solutions for IoT applications. *Sensors*, 22(3), 1092. https://doi.org/10.3390/s22031092
28. Zhou, Z., & Li, X. (2021). Secure IoT communication with blockchain and multi-party computation. *IEEE Transactions on Information Forensics and Security*, 16, 2064–2075. https://doi.org/10.1109/TIFS.2021.3060900
29. Liu, Q., & Zhang, S. (2022). Blockchain-based secure and transparent IoT service management. *Journal of Cloud Computing: Advances, Systems and Applications*, 11(1), 27–40. https://doi.org/10.1186/s13677-022-00278-6
30. Chen, Y., & Wang, J. (2021). Blockchain-based authentication and secure communication in IoT. *Security and Privacy*, 4(3), e319. https://doi.org/10.1002/spy2.319