STM JOURNALS

International Journal of
Mobile Computing Technology

ISSN: 3049-0871
Volume 4, Issue 1, 2026
January—April
DOI (Journal): 10.37591/IJMCT

https://journals.stmjournals.com/ijmct

Review IJMCT

# Blockchain-Enabled Secure Data Sharing in Mobile IoT Networks

Bhavisha Vishalbhai Parvadiya*

***Abstract***

*The rapid proliferation of mobile Internet of Things (IoT) devices has resulted in an exponential increase in data generation, storage, and sharing, which poses significant challenges related to security, privacy, integrity, and trustworthiness. Traditional centralized architectures for IoT data exchange are inherently vulnerable to single points of failure, unauthorized access, data tampering, and limitations in scalability. Blockchain technology, with its decentralized ledger structure, cryptographic integrity, and consensus mechanisms, provides a promising approach for enabling secure and reliable data sharing in mobile IoT networks. This paper presents a comprehensive analysis of blockchain-enabled secure data sharing frameworks, detailing critical architectural components such as smart contracts, lightweight consensus protocols, and cryptographic primitives. Furthermore, it evaluates performance and security benefits, including enhanced data integrity, accountability, and resilience against attacks. Finally, the paper identifies key challenges, including resource constraints, scalability issues, and privacy concerns, and outlines potential future research directions for integrating blockchain technology into dynamic mobile IoT environments.*

**Keywords:** Blockchain, decentralized ledger, mobile IoT networks, privacy preservation, secure data sharing, smart contracts

## INTRODUCTION

Mobile Internet of Things (IoT) networks comprise interconnected devices, sensors, and actuators that collect, process, and exchange data across dynamic network topologies. These networks underpin critical applications such as smart healthcare, intelligent transportation, industrial automation, and smart cities. However, the inherent mobility and heterogeneity of IoT devices introduce severe security, privacy, and trust challenges [1, 2]. Centralized data management systems, which are typically used in traditional IoT deployments, often suffer from single points of failure, making them vulnerable to attacks, data tampering, and unauthorized access [3].

Blockchain technology, originally created to support decentralized cryptocurrencies, offers a robust solution for secure, transparent, and tamper-resistant data sharing in mobile IoT networks [4]. Its decentralized ledger architecture eliminates reliance on a single trusted entity, whereas cryptographic techniques and consensus mechanisms ensure data integrity and trustworthiness [5, 6]. Moreover, the integration of smart contracts enables automated access control and policy enforcement, thereby reducing the dependency on human oversight [7].

This study provides a comprehensive analysis of blockchain-enabled secure data sharing in mobile IoT networks. It examines key architectural components, explores performance and security advantages, and highlights challenges such as scalability, resource constraints, and privacy preservation. Furthermore, it outlines future research directions for deploying blockchain-enabled IoT systems in real-world mobile scenarios [8–10].

***Author for Correspondence**
Bhavisha Vishalbhai Parvadiya
E-mail: bhavishaparvadia@gmail.com

Assistant Professor, Department of Computer Science and Engineering, Sardar Patel College of Administration and Management, Gujarat, India

Received Date: January 30, 2026
Accepted Date: February 07, 2026
Published Date: March 20, 2026

**Citation:** Bhavisha Vishalbhai Parvadiya. Blockchain-Enabled Secure Data Sharing in Mobile IoT Networks. International Journal of Mobile Computing Technology. 2026; 4(1): 38–44p.

 

## BLOCKCHAIN FUNDAMENTALS FOR MOBILE IoT

Blockchain is a distributed ledger technology in which data is organized into blocks linked by cryptographic hashes. Each node in the network maintains a copy of the ledger, and transactions are verified through consensus protocols, such as proof of work (PoW), proof of stake (PoS), proof of authority (PoA), or practical Byzantine fault tolerance (PBFT) [1, 5]. These mechanisms prevent unauthorized modifications and ensure consistency across all network nodes.

In mobile IoT networks, blockchain provides several key benefits:

1. *Decentralization*: Eliminates reliance on centralized servers, thereby increasing network resilience and availability [2].
2. *Data integrity*: Cryptographic hashing ensures that data cannot be altered once recorded, thereby protecting against tampering [3].
3. *Auditability*: Immutable ledgers enable verifiable audit trails for all data transactions, enhancing transparency [4].
4. *Automated access control*: Smart contracts enforce predefined rules for data sharing without requiring intermediaries [7].

By leveraging these properties, blockchain can address critical security and trust issues in mobile IoT networks, supporting secure and reliable data exchange even in dynamic and heterogeneous environments [6, 8].

### Security Challenges in Mobile IoT Networks

Mobile IoT networks face multiple security threats owing to their distributed and resource-constrained nature. Key challenges include:

- *Unauthorized access*: Devices often transmit sensitive data over insecure wireless channels, making them vulnerable to eavesdropping and spoofing attacks [2].
- *Data integrity threats*: Centralized servers may be compromised, allowing attackers to modify or delete IoT data [3].
- *Scalability issues*: Traditional security frameworks struggle to accommodate a growing number of devices and high-volume data streams [4].
- *Privacy concerns*: IoT data often contains sensitive personal or organizational information, requiring robust privacy-preserving mechanisms [6].

Blockchain addresses these challenges by decentralizing data storage, validating transactions through consensus, and enforcing strict access control through smart contracts, thereby enhancing trust and security [1, 5, 7].

### Blockchain-Enabled Secure Data Sharing Frameworks

Blockchain-enabled secure data sharing frameworks for mobile IoT networks typically integrate multiple components to ensure data confidentiality, integrity, and trustworthiness, as shown in Figure 1. The primary elements included:

- *Decentralized ledger*: Each IoT device or network node maintains a copy of the distributed ledger that stores transaction records or data hashes. This decentralized approach prevents single points of failure and ensures tamper-proof data storage. Any modification to the data is immediately detectable because of the cryptographic linkage between blocks [1, 3].
- *Smart contracts*: Smart contracts are self-executing scripts stored on the blockchain that define access policies and automate transactions between devices. In mobile IoT networks, smart contracts control who can access, modify, or share the data. They also enforce policies consistently without relying on centralized servers, thereby reducing administrative overhead and human error [2, 7].
- *Consensus mechanisms*: Lightweight consensus protocols, such as PoA and PBFT, are preferred for IoT networks owing to the resource constraints of devices. These mechanisms ensure

 

agreement on ledger states while minimizing energy consumption and computational overheads [1, 2].

- *Cryptographic primitives*: Blockchain frameworks employ cryptographic techniques, including public-key encryption, digital signatures, and hash functions, to secure data and authenticate devices. These primitives prevent unauthorized access, verify the data origin, and maintain confidentiality across mobile IoT networks [5, 6].

By combining these components, blockchain-enabled frameworks provide a secure, transparent, and autonomous environment for data sharing. Such systems are particularly suitable for mobile IoT applications in smart cities, healthcare, intelligent transportation, and industrial monitoring, where security and trust are paramount [4, 8, 9].

Algorithm 1: Blockchain-Based Secure Data Sharing Process in Mobile IoT Networks

- *Input*: Sensor data, access control policies
- *Output*: Secure, verified data access

1. An IoT device generates sensor data and encrypts it using public-key cryptography.
2. A cryptographic hash of the data is created.
3. The hash is submitted to the blockchain as a transaction.
4. Smart contracts validate access permissions and device identity.
5. The consensus mechanism verifies and confirms the transaction.
6. Validated transaction is recorded on the distributed ledger.
7. Authorized users retrieve data through smart-contract-controlled access.

**Performance and Security Evaluation**

The adoption of blockchain in mobile IoT networks significantly enhances both security and performance, although it introduces tradeoffs that must be carefully managed. Empirical studies and simulations have shown that blockchain-enabled frameworks improve data integrity, prevent unauthorized access, and enhance accountability among IoT devices [1, 2].

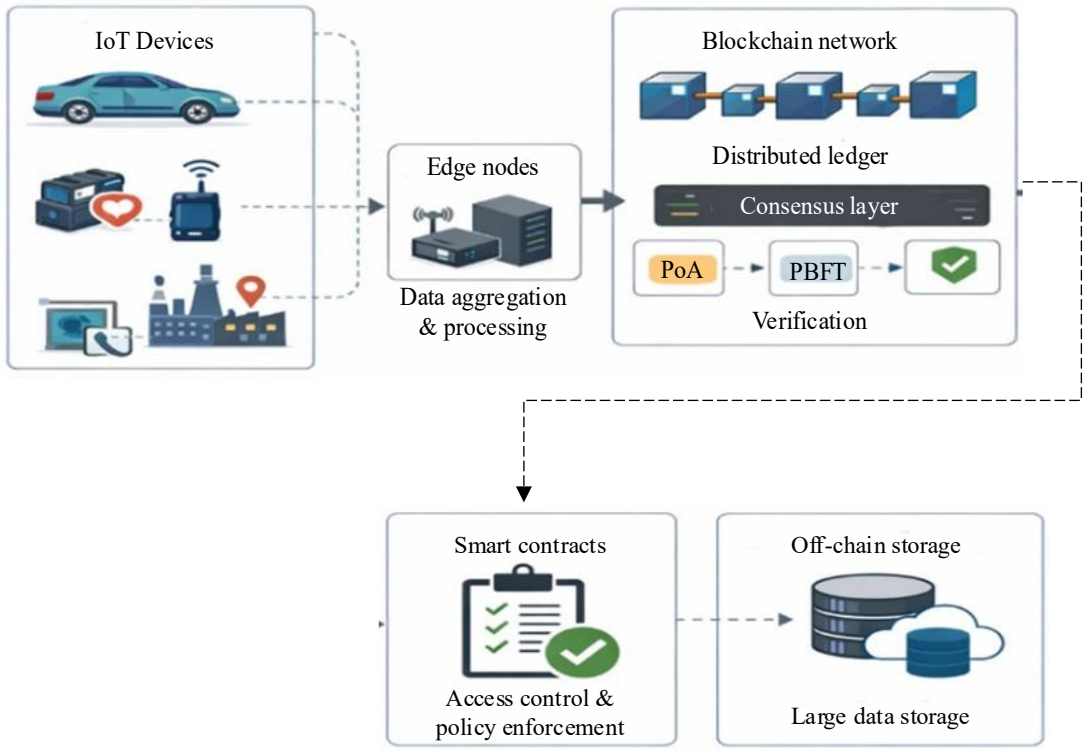


**Figure 1.** Blockchain-enabled secure data sharing architecture for mobile IoT networks.

 

***Data Integrity and Tamper Resistance***

The cryptographic chaining of blocks ensures that any unauthorized modification is easily detectable. Consequently, IoT data stored or referenced on the blockchain remains immutable, which is particularly crucial for applications such as healthcare monitoring, autonomous vehicles, and industrial automation [3, 4].

***Access Control and Trust***

Smart contracts enforce fine-grained access policies, automate authorization, and reduce reliance on centralized intermediaries. This reduces the risk of insider threats and human errors while maintaining trust among distributed IoT devices [2, 7].

***Network Performance***

Blockchain introduces latency owing to transaction validation and consensus processes. Lightweight consensus mechanisms, such as PoA or PBFT, help mitigate these delays, enabling near real-time data sharing in mobile IoT networks [1, 5]. Performance evaluations have demonstrated that these protocols balance security and computational efficiency, making them suitable for resource-constrained IoT devices [6, 8].

***Scalability Considerations****:* While blockchain enhances security, its scalability is limited by transaction throughput and storage requirements. Techniques such as off-chain data storage, sharding, and edge-assisted blockchain processing have been proposed to improve scalability without compromising security [9, 10].

Overall, blockchain-enabled frameworks provide significant security and trust advantages for mobile IoT networks. However, careful design of consensus mechanisms, data storage strategies, and smart contract policies is essential to achieve optimal performance in real-world deployments (Table 1).

**Challenges and Limitations**

Despite its potential, the integration of blockchain technology into mobile IoT networks presents several critical challenges and limitations.

***Resource Constraints***

Many IoT devices have limited computational power, memory, and energy resources. Traditional blockchain protocols, particularly those based on PoW, are resource-intensive and unsuitable for lightweight IoT devices. Even lightweight consensus mechanisms require careful tuning to balance security and resource consumption [1, 2].

***Scalability Issues***

As the number of devices and transactions in IoT networks increases, the blockchain ledger can become large and complex, leading to increased storage requirements and slower transaction processing times. Techniques such as off-chain storage, hierarchical ledgers, or sharding can partially address these issues, but they introduce additional architectural complexity [3, 4].

**Table 1.** Comparison of security characteristics in traditional IoT and blockchain-enabled IoT.

| Security aspect | Traditional IoT | Blockchain-enabled IoT |
|---|---|---|
| Data integrity | Vulnerable to tampering | Cryptographically immutable |
| Trust model | Centralized authority | Decentralized trust |
| Access control | Manual/server-based | Smart contracts |
| Auditability | Limited | Fully traceable |

 

### *Latency and Real-Time Constraints*

Many mobile IoT applications, such as autonomous driving and remote healthcare monitoring, require low-latency communication. Blockchain-based transaction validation and consensus processes can introduce delays that may affect real-time decision-making [5, 6].

### *Privacy Concerns*

While blockchain ensures data integrity and transparency, the immutability and visibility of the ledger can conflict with privacy requirements. Sensitive IoT data may require encryption, anonymization, or privacy-preserving techniques, such as zero-knowledge proofs, to prevent unauthorized disclosure [2, 7].

### *Interoperability and Standardization*

IoT networks often involve heterogeneous devices, protocols, and platforms. Integrating blockchain seamlessly across such diverse systems remains challenging because of the lack of standardized frameworks for interoperability and consensus [8, 9].

### *Regulatory and Legal Challenges*

The decentralized nature of blockchain may conflict with existing regulatory frameworks governing data privacy and security, particularly in the healthcare, finance, and transportation sectors. Compliance with standards, such as the general data protection regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA), may require additional safeguards [10].

Addressing these challenges is essential for the practical deployment of blockchain-enabled secure data sharing in mobile IoT networks. Future research should focus on developing lightweight, scalable, and privacy-preserving blockchain architectures tailored to dynamic IoT environments.

## Future Research Directions and Scope for Extension

While blockchain has demonstrated substantial potential for secure data sharing in mobile IoT networks, several research avenues remain open to enhance its effectiveness, scalability, and usability.

### *Lightweight Consensus Mechanisms*

Future research should focus on developing energy-efficient and computation-friendly consensus algorithms suitable for resource-constrained IoT devices. Mechanisms such as PoA, PBFT, and hybrid approaches can be optimized to reduce latency and energy consumption while maintaining security [1, 2].

### *Hybrid Blockchain–Edge Architectures*

Integrating blockchain with edge computing can offload computationally intensive tasks from IoT devices to nearby edge nodes. This hybrid approach can enhance transaction throughput, reduce latency, and improve overall network performance while maintaining decentralization [3, 4].

### *Privacy-Preserving Techniques*

As mobile IoT networks handle sensitive data, privacy-enhancing methods, such as zero-knowledge proofs, homomorphic encryption, and secure multiparty computation, should be incorporated into blockchain frameworks. These techniques allow the verification of data integrity and compliance without exposing raw data [2, 7].

### *Interoperability and Standardization*

Research should explore frameworks and protocols that enable seamless interoperability across heterogeneous IoT devices, networks, and blockchain platforms. Standardized APIs, data formats, and consensus protocols will facilitate large-scale deployment and integration [8, 9].

 

### *AI-assisted Blockchain Optimization*

Artificial intelligence and machine learning can optimize blockchain operations in IoT networks. For example, predictive models can assist in dynamic block size adjustments, transaction scheduling, and anomaly detection, thereby improving both efficiency and security [5, 10].

### *Real-World Prototyping and Evaluation*

Large-scale deployment of blockchain-enabled IoT systems in practical scenarios, such as smart cities, autonomous vehicles, and healthcare monitoring, is essential to validate theoretical models. Performance metrics, such as latency, throughput, energy consumption, and security compliance, must be empirically assessed [6, 9].

By pursuing these research directions, blockchain-enabled mobile IoT networks can achieve secure, scalable, and privacy-preserving data sharing, unlocking their full potential for critical, real-world applications.

## CONCLUSION

Blockchain technology offers a robust and decentralized framework for secure data sharing in mobile IoT networks. By combining distributed ledgers, cryptographic primitives, and smart contracts, blockchain addresses key challenges such as data integrity, unauthorized access, and trustworthiness in dynamic and heterogeneous IoT environments.

Although blockchain enhances security, transparency, and accountability, its practical deployment faces several challenges, including resource constraints, scalability limitations, latency concerns, privacy preservation, and interoperability issues. Emerging solutions, such as lightweight consensus protocols, hybrid blockchain–edge computing architectures, and privacy-preserving cryptographic techniques, provide promising avenues for overcoming these challenges.

Future research should focus on optimizing blockchain operations for IoT resource constraints, enabling seamless integration across heterogeneous networks, and conducting large-scale, real-world evaluations. By addressing these challenges, blockchain-enabled mobile IoT networks can achieve secure, efficient, and privacy-preserving data sharing, unlocking their potential for application in healthcare, smart cities, intelligent transportation, and industrial automation.

## REFERENCES

1. Jdaitawi M, Kan'an AF, Samunnisa K. Blockchain-enabled secure data sharing in distributed IoT networks: A paradigm for smart city applications. Int J Comput Eng Res Trends. 2024;11(11):24–32.
2. UshaRani R. Blockchain-based secure data sharing for IoT applications. J Inf Syst Eng Manag. 2025;10:83–89. doi:10.52783/jisem.v10i37s.6381.
3. Rani S, Gupta D, Herencsar N, Srivastava G. Blockchain-enabled cooperative computing strategy for resource sharing in fog networks. Internet Things. 2023;21:100672. doi:10.1016/j.iot.2022.100672.
4. Roberts J, Nair V. Blockchain-based solutions for secure data sharing in IoT environments. Int J Adv Electr Comput Eng. 2023;12(2):7–12. doi:10.65521/ijaece.v12i2.146.
5. Sodhro AH, Pirbhulal S, Muzammal M, Li Z. Towards blockchain-enabled security technique for industrial internet of things based decentralized applications. J Grid Comput. 2020;18(4):615–628. doi:10.1007/s10723-020-09527-x.
6. Katya E, Chaudhary S. Secure data sharing in IoT networks using blockchain and machine learning. Res J Comput Syst Eng. 2022;3(2):8–15. doi:10.52710/rjcse.50.
7. Shafagh H, Burkhalter L, Hithnawi A, Duquennoy S. Towards blockchain-based auditable storage and sharing of IoT data. Proceedings of the 2017 Cloud Computing Security Workshop (CCSW '17), Dallas, TX, USA, 2017. p. 45–50. doi:10.1145/3140649.3140656.

 

8. Attkan A, Ranga V. Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex Intell Syst. 2022;8(4):3559–3591. doi:10.1007/s40747-022-00667-z.
9. Bhavsingh M, Samunnisa K, Pannalal B. A blockchain-based approach for securing network communications in IoT environments. Int J Comput Eng Res Trends. 2023;10(10):37–43. doi:10.22362/ijcert/2023/v10/i10/v10i106.
10. Ma L, Duan B, Zhang B, Li Y, Fu Y, Ma D. A trusted IoT data sharing method based on secure multi-party computation. J Cloud Comput. 2024;13(1):138. doi:10.1186/s13677-024-00704-x.

 