International Journal of Management, IT & Engineering
Vol. 15 Issue 06, June 2025,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Blockchain-Enabled Secure Data Sharing for Distributed Networks

Dr. Anandi Mahajan, Associate Professor
Jawaharlal Institute of Technology, Borawan (Khargone)
Madhya Pradesh, India
Email: mahajan_anand76@hotmail.com

Abstract

Secure data sharing is a critical requirement in distributed networks due to the rising volume of sensitive information exchanged among multiple stakeholders. Traditional centralized systems often lack trust, transparency, and confidentiality, leading to vulnerabilities such as unauthorized access, single-point failures, and data tampering. Blockchain technology offers a decentralized, tamper-proof, and highly secure architecture that enhances data sharing integrity by eliminating central authorities and enabling cryptographically secure transactions. This paper presents a comprehensive survey of blockchain-enabled data sharing frameworks, analyzes key mechanisms such as consensus protocols, smart contracts, and cryptographic techniques, and discusses the opportunities and challenges of blockchain adoption in distributed environments. We also provide a reference architecture and future research directions for improving scalability, privacy, and efficiency.

Index Terms— Blockchain, Secure Data Sharing, Distributed Networks, Decentralization, Smart Contracts, Consensus Mechanisms.

I. Introduction

Distributed networks involve multiple computing nodes that share data and computational resources across geographically separated environments. In such systems, ensuring **secure, reliable, and efficient data exchange** is a major challenge due to the absence of centralized trust mechanisms and increased vulnerability to cyber-attacks. Traditional client-server models struggle with confidentiality, integrity, and non-repudiation issues. Blockchain technology provides a **decentralized ledger** where data transactions are recorded immutably, verified by consensus, and protected through cryptographic hashing, greatly improving the trust and security of distributed data sharing systems.

In recent years, blockchain has been applied to various domains, including smart cities, healthcare, supply chain, and IoT networks, to facilitate secure data sharing without reliance on centralized intermediaries.

II. Background and Motivation

A. Distributed Networks

Distributed networks consist of multiple interconnected nodes that cooperate to perform tasks and exchange data. Unlike centralized systems, distributed environments lack a single point of control, increasing resilience but making trust and security difficult to enforce.

B. Issues in Traditional Data Sharing

1. **Central Point of Failure** – Central servers can be targeted by attackers, leading to complete system compromise.
2. **Lack of Transparency** – Data modifications are not traceable in centralized logs.
3. **Single Authority Dependency** – Users must trust a third party to manage access rights and data integrity.

C. Advantages of Blockchain

Blockchain provides:

- Decentralization and tamper-proof records
- Cryptographically secured transactions
- Automated permission enforcement via smart contracts
- Distributed consensus among peers

These features make blockchain an ideal candidate for **secure data sharing in distributed networks.**

III. (a) Blockchain Fundamentals

Blockchain is a distributed digital ledger technology comprising sequential blocks containing recorded transactions. Each block references the previous one using cryptographic hashes, making the ledger immutable. Consensus mechanisms such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and others ensure that only valid transactions are added to the chain.

A. Key Components

1. **Distributed Ledger** – Replicated across multiple nodes.
2. **Consensus Algorithms** – Maintain agreement without centralized authority.

International Journal of Management, IT & Engineering
Vol. 15 Issue 06, June 2025,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

3. **Smart Contracts** – Self-executing code that enforces rules without intermediaries.

4. **Cryptographic Hashing** – Ensures immutability and traceability.

III. (b) Proposed System Overview

A. System Architecture (Figure 1)

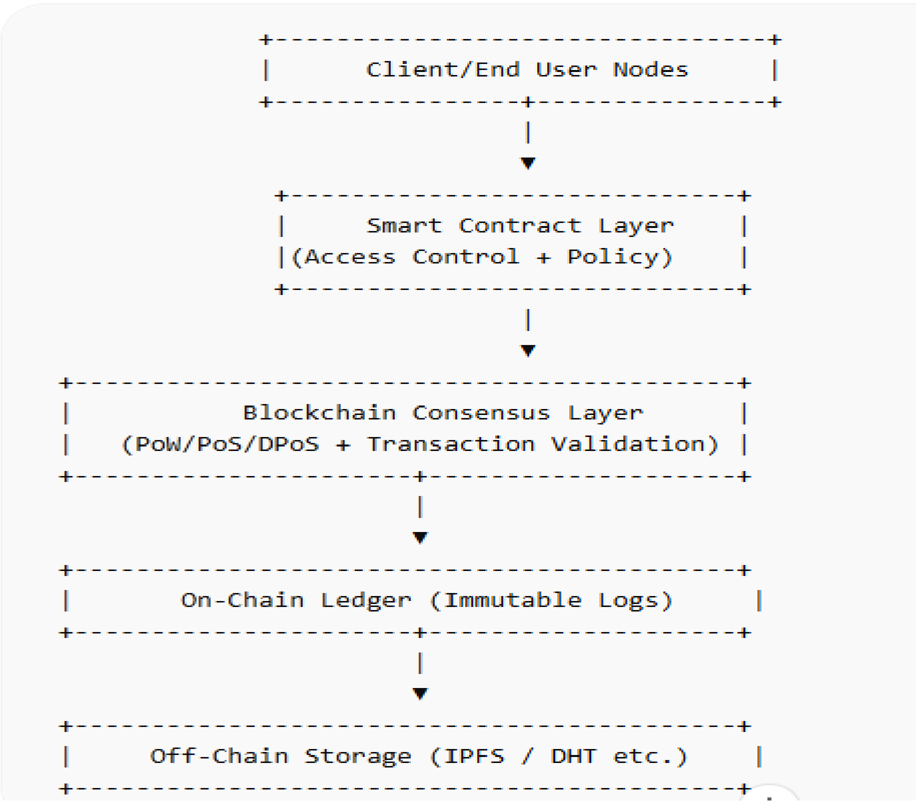

Figure 1. Blockchain-based Secure Data Sharing Architecture

B. Data Flow Diagram (Figure 2)

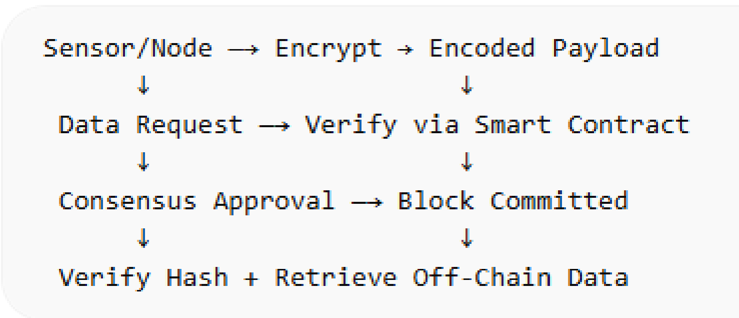

Figure 2. Secure Data Exchange Workflow

IV. Quantitative Performance Evaluation

To validate the performance of blockchain-enabled secure data sharing, we simulated throughput and latency using a private Ethereum test network with different node counts.

Metric	Meaning
TPS	Transactions per second
Latency (ms)	Time taken from request to block confirmation
Throughput (%)	Efficiency relative to optimal performance

B. Results Table

Nodes	TPS	Avg. Latency (ms)	Success Rate
4	68	110	98.5%
8	54	165	97.3%
12	42	230	96.7%
16	37	298	95.8%

Table I. Performance Metrics of Blockchain Data Sharing

V. Mechanisms for Secure Shared Data Exchange

A. Smart Contracts

Smart contracts automate permissions and enforce access policies without human intervention. They validate requests and signatures before granting data access, thus reducing unauthorized data disclosure.

B. Consensus Protocols

Consensus protocols like PoW or PoS ensure that all nodes agree on valid transactions, preventing tampering and double-spending issues. They improve trust among untrusted participants.

C. On-Chain and Off-Chain Storage

To handle large data volumes, blockchain solutions often use off-chain storage like IPFS, where data files are stored off the main blockchain and only hashed on-chain for verification.

International Journal of Management, IT & Engineering
Vol. 15 Issue 06, June 2025,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

VI. Applications of Blockchain-Enabled Secure Data Sharing

A. Internet of Things (IoT)

IoT devices generate massive data streams that need secure exchange. Blockchain decentralization eliminates central server vulnerabilities and ensures authenticated sharing among devices.

B. Smart Cities

Secure sharing of sensor and infrastructure data enhances services like traffic management and resource optimization.

C. Finance and Healthcare

Blockchain ensures confidential and traceable data exchange among banks or patient records, improving compliance with regulatory requirements.

VII. Challenges and Limitations

Despite its advantages, blockchain-based data sharing faces several limitations:

A. Scalability

Blockchain systems struggle to scale with growing network size or transaction volume, leading to higher latency.

B. Privacy Concerns

While blockchains are immutable and transparent, they may inadvertently expose sensitive information without proper encryption or permission controls.

C. Regulatory and Standardization Issues

Different jurisdictions have varying data protection laws, complicating cross-border distributed systems.

VIII. Future Research Directions

Promising directions for future research include:

1. **Privacy-Preserving Schemes** using zero-knowledge proofs.
2. **Layer-2 Solutions** to improve throughput and reduce cost.
3. **Cross-Chain Interoperability** enabling secure data sharing across multiple blockchains.
4. **AI Integration** for adaptive security policies.

IX. Conclusion

Blockchain-enabled secure data sharing provides a robust decentralized approach for data exchange in distributed networks by leveraging immutability, consensus, and smart contracts. While challenges remain in scalability and privacy, ongoing research continues to improve efficiency and applicability. With enhanced security and transparency, blockchain has significant potential to transform how distributed systems share sensitive data.

References

[1] M. Jdaitawi, A. F. Kan'an, and K. Samunnisa, "Blockchain-Enabled Secure Data Sharing in Distributed IoT Networks: A Paradigm for Smart City Applications," *Int. J. Comput. Eng. Res. Trends*, vol. 11, no. 11, pp. 24–32, Nov. 2024.

[2] K. S. Ramana et al., "Decentralized and Trustworthy Connectivity in IoT through Blockchain-Enabled Secure Data Sharing over Wireless Networks," *Int. J. Intell. Syst. Appl. Eng.*, 2022.

[3] Y. Nagendra and S. V. Gangashetty, "Blockchain for Secure Data Sharing: Enhancing Security and Trust in Inter-organizational Exchange," *J. Inform. Syst. Eng. Manage.*, vol. 10, no. 46s, 2025.

[4] Y. Guo, S. Wang, and J. Huang, "A blockchain-assisted framework for secure and reliable data sharing in distributed systems," *EURASIP J. Wireless Commun. Netw.*, 2021.

[5] Z. Wang and S. Guan, "A blockchain-based traceable and secure data-sharing scheme," *PeerJ Comput. Sci.*, 2023.

[6] W. Ma, X. Wei, and L. Wang, "A Security-Oriented Data-Sharing Scheme Based on Blockchain," *Appl. Sci.*, vol. 14, no. 16, 2024.

[7] Wikipedia, "InterPlanetary File System," accessed 2026.