International Journal of Advance Innovations, Thoughts and Ideas

Commentary Open Access

Blockchain: Data Security, Privacy, Challenges.

Dr. Victor Hwang*

Department of Information Security, Seoul Institute of Technology, Seoul, South Korea

***Corresponding Author:** Dr. Victor Hwang, Department of Information Security, Seoul Institute of Technology, Seoul, South Korea, E-mail: victor.hwang@sit.ac.kr

Received: 04-Sep-2025, Manuscript No. ijaiti-25-173460; **Editor assigned:** 08-Sep-2025, PreQC No. ijaiti-25-173460(PQ); **Reviewed:** 22-Sep-2025, QC No. ijaiti-25-173460; **Revised:** 25-Sep-2025, Manuscript No. ijaiti-25-173460(R); **Published:** 02-Oct-2025, **DOI**: 10.4172/2277-1891.1000359

Citation: Hwang DV (2025) Blockchain: Data Security, Privacy, Challenges.. Int J Adv Innovat Thoughts Ideas 14: 359.

Abstract

This collection explores how blockchain technology strengthens data privacy and security across smart cities, healthcare, and the Internet of Things. It highlights blockchain's role in enabling privacy-preserving data sharing through cryptographic techniques like zero-knowledge proofs and homomorphic encryption. The papers cover securing sensitive records, managing consent, and ensuring data integrity and authenticity. While offering immutability and decentralization, research also addresses key challenges such as scalability, latency, and regulatory compliance. This body of work underscores blockchain's potential as a robust solution for evolving digital privacy needs.

Keywords

Blockchain; Data Privacy; Data Security; Smart Cities; Healthcare; Internet of Things; Zero-Knowledge Proofs; Homomorphic Encryption; Data Sharing; Decentralization

Introduction

This survey explores how blockchain technology can enable privacy-preserving data sharing within smart city environments. It examines various architectural models and cryptographic techniques, like zero-knowledge proofs and homomorphic encryption, which integrate with blockchain to ensure data confidentiality and integrity while facilitating necessary data exchange for smart city services. The article highlights challenges in scalability and regulatory compliance[1].

This systematic review analyzes various blockchain-based solutions aimed at enhancing data privacy and security in healthcare systems. It categorizes existing approaches, focusing on how blockchain can secure Electronic Health Records, manage patient consent, and facilitate secure data exchange, addressing common vulnerabilities and regulatory requirements like HIPAA and GDPR. The paper identifies key benefits such as immutability and decentralization, along with challenges related to performance and integration[2].

This comprehensive survey examines the role of blockchain technology in ensuring data privacy and security within the expansive landscape of the Internet of Things (IoT). It reviews various blockchain architectures and consensus mechanisms adapted for IoT, discussing their strengths in maintaining data integrity, authenticity, and access control. The paper also highlights current limitations, including scalability, latency, and energy consumption, and proposes future research directions[3].

This survey provides an overview of decentralized data protection mechanisms for IoT ecosystems that leverage blockchain technology. It discusses how blockchain can enhance data privacy, security, and trust in IoT by enabling tamper-proof data storage, secure access control, and transparent data provenance. The paper explores various blockchain models suitable for IoT applications and

identifies key challenges such as resource constraints of IoT devices and interoperability issues[4].

This systematic review investigates the application of blockchain technology in ensuring privacy and security across various health applications. It analyzes current research trends, methodologies, and proposed solutions for securing sensitive health data, managing patient consent, and facilitating trusted data sharing. The review identifies the potential of blockchain to address critical issues like data breaches and unauthorized access, while also outlining challenges such as regulatory hurdles and technological integration complexities[5].

This systematic literature review comprehensively covers blockchain-based solutions designed for privacy-preserving data sharing. It categorizes existing schemes by their underlying privacy mechanisms, such as zero-knowledge proofs, homomorphic encryption, and secure multiparty computation, and their application contexts. The paper assesses how blockchain enhances trust, transparency, and auditability in data sharing while addressing privacy concerns, and discusses challenges like scalability, latency, and regulatory compliance[6].

This paper proposes a secure and privacy-preserving blockchain-based framework for data sharing in smart healthcare systems. It addresses the critical need for robust security and privacy mechanisms when handling sensitive medical data. The authors detail how blockchain's distributed ledger technology can ensure data integrity, facilitate secure access control, and manage consent effectively, thereby enhancing trust among various healthcare stakeholders while mitigating risks of data breaches[7].

This article introduces a blockchain-based scheme specifically designed for protecting data privacy in medical data sharing scenarios. It leverages the immutability and transparency of blockchain to create a secure environment for sharing sensitive patient information while maintaining privacy. The proposed scheme integrates cryptographic techniques to ensure authorized access and data integrity, offering a practical solution to current challenges in medical data management and exchange[8].

This survey provides an extensive review of how blockchain technology can be utilized to address data privacy and security concerns across various domains. It discusses the fundamental principles of blockchain that contribute to its security features, such as decentralization, immutability, and cryptographic hashing. The paper explores different blockchain-based solutions for secure data storage, access control, and identity management, while also identifying open research problems and future directions in this evolving field[9].

This comprehensive survey focuses on blockchain-based solutions for secure data sharing within Internet of Things (IoT) environments. It examines various architectural models and cryptographic methods that leverage blockchain's inherent security properties to ensure data integrity, authenticity, and privacy for IoT devices and applications. The paper highlights the potential of blockchain to address common IoT security vulnerabilities, discussing challenges related to scalability, interoperability, and resource constraints of IoT devices[10].

Description

Blockchain technology provides a foundational approach for enhancing data privacy and security across various domains. This is achieved through its core principles, including decentralization, immutability, and the use of cryptographic hashing [9]. These features are crucial for creating environments where data integrity and authenticity are maintained, and access control can be securely managed. The fundamental idea here is leveraging a distributed ledger to ensure that once data is recorded, it cannot be tampered with, offering a transparent and auditable record of transactions and data interactions. This inherent trustworthiness makes it a compelling solution for sensitive data applications.

In smart city environments, blockchain enables privacy-preserving data sharing by employing advanced cryptographic techniques. Think about zero-knowledge proofs and homomorphic encryption; these are integrated with blockchain to guarantee data confidentiality and integrity, even as essential data exchange happens for urban services [1]. What this really means is that critical information can flow between different city departments or services without revealing the underlying sensitive details, balancing utility with privacy. Beyond smart cities, a broader look at blockchain-based solutions shows how they are designed specifically for privacy-preserving data sharing across various contexts, categorizing these schemes by their underlying privacy mechanisms, such as secure multiparty computation, alongside the previously mentioned methods [6]. The goal is to boost trust, transparency, and auditability in data sharing practices.

The healthcare sector significantly benefits from blockchain's capabilities in securing sensitive information. Systematic reviews highlight numerous blockchain-based solutions aimed at boosting data privacy and security within healthcare systems [2, 5]. These solutions focus on securing Electronic Health Records, streamlining patient consent management, and facilitating safe data ex-

changes. The aim is to tackle common vulnerabilities and comply with strict regulations like HIPAA and GDPR [2]. Here's the thing: blockchain's distributed ledger technology can ensure data integrity and facilitate secure access, which helps manage consent effectively. This approach ultimately reduces the risk of data breaches and builds trust among healthcare stakeholders [7, 8]. A blockchain-based scheme for medical data sharing, for example, uses immutability and transparency to create a secure environment, integrating cryptographic techniques for authorized access and data integrity [8].

The Internet of Things (IoT) presents unique challenges for data privacy and security due to its expansive nature and resource constraints. Blockchain technology is emerging as a critical tool for decentralized data protection in IoT ecosystems [3, 4, 10]. Surveys explore how different blockchain architectures and consensus mechanisms are adapted for IoT environments, emphasizing their strengths in maintaining data integrity, authenticity, and access control for interconnected devices [3]. What this really means is blockchain can provide tamper-proof data storage and transparent data provenance, which are vital for trust in IoT applications. Despite the significant potential, these deployments face hurdles, including scalability, latency, energy consumption, and interoperability, especially given the limited resources of many IoT devices [3, 4, 10].

Conclusion

Blockchain technology shows significant promise in bolstering data privacy and security across diverse domains. Research highlights its application in smart cities, where it facilitates privacy-preserving data sharing using techniques like zero-knowledge proofs and homomorphic encryption to ensure confidentiality and integrity of exchanged data [1]. In healthcare, blockchain offers solutions for securing Electronic Health Records, managing patient consent, and facilitating secure data exchange, addressing regulatory requirements such as HIPAA and GDPR [2, 5]. It helps mitigate data breaches and unauthorized access by leveraging features like immutability and decentralization, which enhance trust among stakeholders [7, 8]. The Internet of Things (IoT) is another key area benefiting from blockchain's decentralized data protection mechanisms. Comprehensive surveys reveal how blockchain architectures and consensus mechanisms are adapted to maintain data integrity, authenticity, and access control for IoT devices [3, 4, 10]. Blockchain provides tamper-proof data storage and transparent data provenance, which are essential for secure IoT ecosystems. Across these applications, the technology enhances trust, transparency, and auditability in data sharing [6]. Despite its potential, challenges remain. Scalability, latency, energy consumption, and interoperability issues are frequently cited limitations, particularly in resource-constrained IoT environments [3, 4, 10]. Regulatory compliance and technological integration complexities also pose hurdles [1, 2, 5]. Overall, blockchain's fundamental principles—decentralization, immutability, and cryptographic hashing—form the bedrock for developing robust solutions for secure data storage, access control, and identity management in evolving digital landscapes [9].

References

1. M A, R A, R S, S A, M A et al. (2023) Blockchain-based privacy-preserving data sharing in smart cities: A survey. Future Gener Comput Syst 142:22-41

2. S E, F A, Y H, T A, E A et al. (2023) Blockchain-Based Solutions for Data Privacy and Security in Healthcare: A Systematic Review. Appl Sci 13:1007

3. D N, Q P, D N, H N, Y K et al. (2021) Blockchain for data privacy and security in the Internet of Things: A comprehensive survey. J Netw Comput Appl 185:103031

4. N S, P S, B K, K K et al. (2021) Decentralized Data Protection for IoT in the Blockchain Context: A Survey. IEEE Access 9:41415-41432

5. M S, M A, M A, S S, S S et al. (2022) A systematic review of blockchain in privacy and security of health applications. Future Gener Comput Syst 128:36-54

6. M A, M V, M P, S T, M T et al. (2021) Blockchain-based solutions for privacy-preserving data sharing: A systematic literature review. J Netw Comput Appl 185:103009

7. Y L, C S, S L, J N, B C et al. (2021) Towards a secure and privacy-preserving blockchain-based data sharing in smart healthcare. Future Gener Comput Syst 118:35-46

8. K F, Y R, Y W, H L, Y Y et al. (2020) A blockchain-based data privacy protection scheme for medical data sharing. J Parallel Distrib Comput 143:146-152

9. W Y, J L, H L, T L, X W et al. (2020) Blockchain for data privacy and security: A survey. J Syst Archit 107:101736

10. A D, M K, K S, R J et al. (2019) Blockchain-based secure data sharing in IoT: A comprehensive survey. Comput Electr Eng 77:31-46