AG Publishing House

Research Trends in Multidisciplinary Research (Volume-1)

Volume 1
Year: 2025

AG PH Books

A Comprehensive Review of Blockchain Security: Challenges and Future Prospects

Dr. Chandini A Gopalakrishna[1*]

[1]*Associate Professor*

Abstract

The blockchain is a useful method and service that has shown excellent development and application potential. But there have also been significant security concerns, and a number of attack issues and security flaws in blockchain-based systems have surfaced. Extensive attention has been recently directed towards blockchain security concerns. Review the many studies on the difficulties and potential for blockchain security in this article. This review provides a comprehensive examination of blockchain security, identifying key vulnerabilities such as 51% attacks, smart contract flaws, Sybil attacks, phishing, and insider threats. Real-world case studies and formal verification experiments highlight existing weaknesses and the need for robust defense mechanisms. While blockchain offers inherent advantages for data security, particularly in sectors like healthcare, its limitations hinder widespread adoption. Future advancements will rely on improved technologies, regulatory frameworks, and interdisciplinary applications. Emerging innovations like AI, quantum-resistant cryptography, and interoperability frameworks are poised to play a crucial role in enhancing blockchain resilience and ensuring secure, scalable deployments.

Keywords: Blockchain Security, Challenges, Future Prospects, 51% Attacks, Smart Contract Flaws, Sybil Attacks, Artificial Intelligence (AI), Quantum-Resistant Cryptography.

1 Introduction

Due to its reputation as an information-recording system, the blockchain technology has grown in popularity in recent years. A distributed database called a blockchain facilitates the recording of

* ISBN No. - 978-93-49490-34-5

transactions in a corporate network. The benefits of blockchain, which include security, data integrity, and anonymity without allowing third parties to influence transactions, are among the primary drivers of interest in the technology [1]. Modern technologies including supply chain management, virtual reality, the Internet of Things, artificial intelligence, and cyber security all employ blockchain technology. Security, privacy, compliance, and governance are among the numerous obstacles that blockchain technology encounters, which continue to elicit apprehensions [2]. Blockchain technology facilitates secure peer-to-peer communication and makes transactions publicly readable, but once they are recorded, no one can change them. The security implications or hazards that these technologies pose can be difficult to understand, despite the fact that the majority of them are constantly being developed [3], [4]. Blockchain technology is seen by many as a breakthrough in cryptography or cybersecurity. Additionally, it serves as the foundation for smart contracts and digital currencies like Bitcoin [5]. By maintaining its essential qualities of decentralisation, immutability, anonymity, and appropriateness for the electronic money transaction process, the blockchain has grown in significance in the digital world. On the other hand, a number of organisations are doing research on the potential of Blockchain technology to develop various decentralised applications due to its successful experience [6], [7].

A. Blockchain security

The term "blockchain security" refers to the extensive procedures and safeguards put in place to shield blockchain applications and networks against different types of online attacks. It includes decentralised systems, consensus processes, and cryptographic algorithms that guarantee the availability, secrecy, and integrity of data on the blockchain. Ensuring the security of blockchain technology is becoming more and more important as it develops and gets more widely used in order to stop criminal activity and preserve system confidence [8].

B. Key Concepts in Blockchain Security

To understand how blockchain technology secures data and transactions, one must have a solid understanding of the fundamental ideas of blockchain security. Among these concepts are decentralisation, consensus mechanisms, and cryptographic techniques [9].

- **Cryptographic Techniques:** Blockchain security is predicated on cryptography. This process entails the utilisation of digital signatures, hash functions, and private and public keys to safeguard data and transactions. Funds are received using public keys, and transactions are signed using private keys, which guarantee that only the legitimate owner may approve a transaction [10]. It is almost hard to change input data without being detected since hash functions transform it into a fixed-size string of characters that is unique to each input.
- **Consensus Mechanisms:** Protocols known as consensus methods make sure that everyone on the network agrees that transactions are legitimate. The consensus mechanism that is most widely recognised is Proof of Work (PoW), which is employed by Bitcoin. In this mechanism, miners solve intricate mathematical problems to verify transactions and record them in the blockchain [11]. Another approach is Proof of Stake (PoS), in which validators are selected according to how many coins they own and are prepared to "stake" as security. Additional

systems, each with a unique strategy for reaching agreement, including Practical Byzantine Fault Tolerance (PBFT), Delegated Proof of Stake (DPoS), and others.

- **Decentralization:** Blockchain technology is fundamentally based on the principle of decentralisation. In order to improve security and avoid a single point of failure, it entails dispersing data across many network nodes. A decentralised network is more impervious to censorship and threats because no one organisation controls the whole blockchain. Additionally, even in the event that certain nodes malfunction or are hacked, the network will continue to function thanks to this division of control.

C. Blockchain security challenges

- **51% Attack:** The 51% attack is among the most well-known dangers to blockchain networks. In this case, a malevolent actor takes over over 50% of a Proof-of-Work (PoW) blockchain's processing capacity. This gives them the ability to possibly alter transactions and interfere with network functions, compromising the blockchain's integrity [12].
- **Smart Contract Vulnerabilities:** Despite their revolutionary nature, smart contracts are not impervious to flaws. Attackers may modify data, steal money, or even bring down the whole network by taking advantage of flaws or mistakes in smart contract programming. The dependability and security of blockchain applications depend heavily on the security of smart contracts [13].
- **Phishing and Social Engineering Attacks:** Social engineering schemes and phishing efforts may fool people into disclosing their digital wallets or private keys, which is why blockchain users are vulnerable to them. These assaults may jeopardise the blockchain network's security and result in unlawful access to money [14].
- **Sybil Attacks:** In order to interfere with voting or consensus procedures, sybil attacks include the creation of several fictitious identities on the network. Through the manipulation of the network's decision-making process, assailants can compromise its integrity by controlling multiple identities.
- **Routing Attacks:** The blockchain network's ability to operate may be hampered by malicious actors targeting internet service providers (ISPs) to obstruct communication between nodes. Attacks on routing may interfere with information flow and jeopardise the network's security and dependability.
- **Insider Threats:** Blockchain networks are at serious danger from insider threats as bad actors within a company who have access to private keys or blockchain systems may steal money or alter data for their own benefit. Insider attacks emphasise the need of strong monitoring systems and access constraints.

D. Future Trends in Blockchain Security

Blockchain security is an area that is always changing. Here are some trends to look out for in the future:

- **Quantum-Resistant Cryptography:** One important field of study is creating cryptography methods that are resistant to assaults by quantum computing. Current encryption techniques

might be broken by quantum computers, therefore creating quantum-resistant solutions is crucial.

- **AI and Machine Learning:** An increasing trend is the use of machine learning and artificial intelligence to improve security protocols and identify potential risks. By detecting trends and irregularities in blockchain networks, artificial intelligence (AI) may enhance danger detection and reaction.
- **Interoperability:** Another significant development is making sure that various blockchain networks may safely communicate with one another. The primary objective of interoperability solutions is to facilitate the seamless exchange of data and communication between separate blockchain systems.

2 Literature Review

(Liang, 2025) [15] The decentralisation, transparency, and immutability of blockchain technology have shown to be very beneficial in a variety of industries, including public administration, healthcare, logistics, and finance. But this technology also has a number of performance and security issues. The actual economy and blockchain technology are becoming more and more integrated. Security risk barriers have progressively surfaced throughout the investigation of blockchain application deployment. Despite the fact that blockchain technology offers trustworthy security assurances, attackers may still identify security flaws in the system and launch attacks. Every year, more and more damages are brought on by network assaults. While concentrating on the main attack techniques and summarising the current defence mechanisms against these risks, this article recounts the evolution and fundamental ideas of blockchain technology.

(Chen et al., 2023) [16] want to provide a full-stack architectural security solution to address security threats in blockchain services. We also suggest a formal representation of security concerns and defence strategies from a full-stack security viewpoint, as well as a formal specification of the full-stack security architecture for blockchain-based services. We do a property-based testing formal verification experiment for smart contracts using Concert. We have chosen and listed the security flaws in blockchain services that are listed in the China Nation Vulnerability Database (CNVD) and Common Vulnerabilities and Exposures (CVE). Additionally, an experimental technique replicates three genuine attack events at the contract layer. The security issues and defence strategies are examined and studied using Hyperledger Fabric's Identity Mixer and Alibaba's blockchain services as a case study. Finally, suggestions for future study paths are made.

(Verma et al., 2023) [17] Data security concerns have experienced a substantial rise in recent years, primarily due to the increasing frequency and complexity of intrusions and data breaches. The goal of this research study is to examine and evaluate blockchain technology's security features in detail. We will look at the many cryptographic approaches that blockchain uses, evaluate its resistance against various assaults, and discuss the advantages and disadvantages of blockchain in terms of data security. In addition, we will examine real-world applications and case studies to gain a comprehensive understanding of the practical implementation of blockchain security and to identify potential

vulnerabilities and development opportunities. This study aims to add to the current discussion on how to properly safeguard data in the digital era by offering a thorough review of blockchain security.

(Wenhua et al., 2023) [18] The data structure offered by blockchain technology has built-in security features including consensus, decentralisation, and cryptography that guarantee transaction trust. Without third-party guarantees, blockchain technology offered a decentralised solution to trust-less problems between distrusting parties. However, the technology's "trust-less" security was readily misinterpreted and hindered the security distinctions between public and private blockchains. The aforementioned advantages and disadvantages of blockchain technology served as an incentive for us to conduct a thorough and comprehensive investigation into its potential applications. By contrasting and evaluating current security procedures, this study identifies the security threats in the six levels of blockchain technology with an emphasis on healthcare security. Additionally, it describes and investigates the many security threats and difficulties that arise while using blockchain technology, which encourages the creation of strong security protocols and theoretical study in the distributed work environment of today and the future.

(Alfaw et al., 2022) [19] Assess the blockchain systems' security risk, examine the vulnerabilities that have been exploited, and pinpoint current security issues the blockchain is facing. Notwithstanding the security risks associated with the blockchain system, there are various research on the subject, but no thorough analysis of the issue has been conducted. This study used an observational research style. Numerous studies on the risks and weaknesses of blockchain technology have been produced using this technique. Identifying the most significant security threats that the blockchain is currently facing and taking into account the most recent security vulnerabilities are the primary objectives of this research. Examined are procedures and strategies for managing security concerns.

(Guo & Yu, 2022) [20] We first conduct a more thorough analysis of blockchain technology in this paper, focussing on its history, quantitative comparisons of consensus algorithms, public key cryptography details, zero-knowledge proofs, blockchain hash functions, and a detailed list of blockchain applications. Additionally, this article focusses on the security of the blockchain itself. Specifically, we use risk analysis to evaluate blockchain security in order to create thorough risk categories, examine actual assaults and defects on the blockchain, and compile the most current security updates for the blockchain. In order to create blockchain systems that are more safe and scalable for large-scale deployments, the research trends and obstacles are finally discussed.

(Singh et al., 2021) [21] Significant progress has been made in distributed systems as a result of the development of IoT technology across several fields. The blockchain idea necessitates a decentralised data management solution for network data and transaction sharing and storage. In addition to discussing the blockchain idea and pertinent variables, this article offers a thorough examination of possible security threats and current solutions that may be implemented as defences against them. By highlighting important ideas that may be used to create different blockchain systems and security tools that address security flaws, this article also offers options for enhancing blockchain security. The study concludes by outlining unresolved problems and potential avenues for future blockchain-IoT system research.

3 Conclusion

This review paper presents a comprehensive analysis of blockchain security, encompassing risk categorization, real-world attack case studies, and recently developed defense mechanisms. By reproducing three notable security incidents, we demonstrate common vulnerabilities in the blockchain application ecosystem. Through formal verification using ConCert and property-based testing, we identify and validate a smart contract vulnerability, emphasizing the need for rigorous contract auditing. Our findings highlight that while blockchain offers inherent advantages in ensuring data integrity and decentralization, it is still vulnerable to numerous threats such as 51% attacks, smart contract bugs, Sybil attacks, phishing, ISP targeting, insider threats, and future quantum threats. The study underscores the importance of continuous innovation in security measures, including quantum-resistant cryptography, AI-based anomaly detection, and enhanced interoperability. Particularly in the healthcare sector, where data security is paramount, blockchain adoption is hindered by unresolved security issues and limited regulatory oversight. Thus, future development in blockchain security must focus on technological advancements, deeper application integration, and robust supervision systems. Ultimately, securing blockchain networks requires a holistic approach combining technical, procedural, and human-centric strategies to safeguard assets and uphold trust in decentralized systems. This paper aims to guide future research and application development by illuminating critical vulnerabilities and outlining practical defense solutions.

References

[1] A. Shukla, P. Jirli, A. Mishra, and A. K. Singh, “An overview of blockchain research and future agenda: Insights from structural topic modeling,” *J. Innov. Knowl.*, vol. 9, no. 4, 2024, doi: 10.1016/j.jik.2024.100605.

[2] M. Hasnain, I. Ghani, D. Smith, A. Daud, and S. R. Jeong, “Cybersecurity Challenges in Blockchain-based Social Media Networks: A Comprehensive Review,” *Blockchain Res. Appl.*, 2025, doi: 10.1016/j.bcra.2025.100290.

[3] K. Duan, G. Pang, and Y. Lin, “Exploring the current status and future opportunities of blockchain technology adoption and application in supply chain management,” *J. Digit. Econ.*, vol. 2, 2023, doi: 10.1016/j.jdec.2024.01.005.

[4] A. Baran, “CONCEPT OF E-CURRENCY: A BROADER VIEW ON A WIDER CANVAS,” *Int. J. Innov. Sci. Eng. Manag.*, vol. 3, pp. 108–114, 2024.

[5] P. S. Aithal, A. Aithal, and E. Dias, “Blockchain Technology - Current Status and Future Research Opportunities in Various Areas of Healthcare Industry,” *Int. J. Heal. Sci. Pharm.*, vol. 5, no. 1, 2021, doi: 10.47992/ijhsp.2581.6411.0070.

[6] N. Li *et al.*, “Blockchain Cross-Chain Bridge Security: Challenges, Solutions, and Future Outlook,” *Distrib. Ledger Technol. Res. Pract.*, vol. 4, no. 1, 2025, doi: 10.1145/3696429.

[7] E. Kesavan, “Internet of Things (IoT): A Review of Security Challenges and Solutions,” *Int. J. Innov. Sci. Eng. Manag.*, vol. 2, no. 4, 2023, doi: 10.69968/ijisem.2023v2i465-71.

[8] M. Abdelhamid, L. Sliman, R. Ben Djemaa, and G. Perboli, “A Review on Blockchain Technology, Current Challenges, and AI-Driven Solutions,” *ACM Comput. Surv.*, vol. 57, no. 3, 2024, doi: 10.1145/3700641.

[9] S. Chandra, “A STUDY ON BLOCKCHAIN SECURITY ISSUES AND CHALLENGES,” *Int. J. Nov. Res. Dev.*, vol. 3, no. 5, 2018, doi: 10.22214/ijraset.2018.3143.

[10] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: a survey,” *Int. J. web grid Serv.*, vol. 14, no. 8, 2018, doi: 10.54648/ecta2019011.

[11] S. Makridakis and K. Christodoulou, “Blockchain: Current Challenges and Future Prospects/Applications,” *Futur. Internet*, vol. 11, 2019, doi: 10.1201/9781032684819-27.

[12] N. Moosavi and H. Taherdoost, “Blockchain Technology Application in Security: A Systematic Review,” *Blockchains*, vol. 1, no. 2, pp. 58–72, 2023, doi: 10.3390/blockchains1020005.

[13] T. Kukman and S. Gričar, “Blockchain for Quality: Advancing Security, Efficiency, and Transparency in Financial Systems,” *FinTech*, vol. 4, no. 1, pp. 1–19, 2025, doi: 10.3390/fintech4010007.

[14] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, “Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing,” *Futur. Internet*, vol. 14, no. 11, 2022, doi: 10.3390/fi14110341.

[15] X. Liang, “Security Challenges and Defense Strategies in Blockchain Systems,” *Int. Conf. Mechatronics Smart Syst.*, 2025, doi: 10.54254/2755-2721/2025.21087.

[16] H. Chen, X. Luo, L. Shi, Y. Cao, and Y. Zhang, “Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective,” *Blockchain Res. Appl.*, vol. 4, no. 3, 2023, doi: 10.1016/j.bcra.2023.100135.

[17] S. Verma, M. Srivastava, S.- Fatima, and S. K. Mishra, “Enhancing Security In Blockchain Technology: A Comprehensive Study,” *J. Reatt. Ther. Dev. Divers.*, vol. 6, no. 8, 2023, doi: 10.53555/jrtdd.v6i8s.2910.

[18] Z. Wenhua, F. Qamar, T. A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, “Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends,” *Electron.*, vol. 12, no. 3, 2023, doi: 10.3390/electronics12030546.

[19] A. Alfaw, W. Elmedany, and M. S. Sharif, “Blockchain Vulnerabilities and Recent Security Challenges: A Review Paper,” *2022 Int. Conf. Data Anal. Bus. Ind. ICDABI 2022*, 2022, doi: 10.1109/ICDABI56818.2022.10041611.

[20] H. Guo and X. Yu, “A survey on blockchain technology and its security,” *Blockchain Res. Appl.*, vol. 3, no. 2, 2022, doi: 10.1016/j.bcra.2022.100067.

[21] S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, “Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network,” *IEEE Access*, vol. 9, 2021, doi: 10.1109/access.2021.3051602.