International Journal of Advanced Digital Systems
and Multidisciplinary Studies (IJADSMS),
Volume - 1, Issue - 4 pp. 11–15, 2026

Blockchain Technology: Architectures, Security Challenges, and Emerging Applications

Mr. Ajit Kumar[1], Ms. Kumari Puja[2], Mr. Abhishek Kumar [3] , Ms. Lakshmi Kumari [4], Mr. Ashok Singh Gaur[5], Mr. Sachin Kashyap[6]

[1]Assistant Professor, Department of Information Technology, Amity University, Ranchi, Jharkhand,

[2,3,4,5,6]Assistant Professor, School of Computer Applications, Noida Institute of Engineering & Technology, Greater Noida

Abstract

This paper presents a comprehensive review of blockchain technology, encompassing its fundamental architectural designs, prevalent security challenges, and burgeoning application domains. It delineates the intricate layered structure of blockchain, providing a foundational framework for understanding its operational complexities and vulnerabilities. Furthermore, it explores how various security threats can undermine the integrity and reliability of blockchain systems, offering a novel taxonomy for classifying existing research on vulnerability detection within this rapidly evolving technological landscape. It also provides an in-depth analysis of prominent attack vectors encountered within the blockchain ecosystem, accompanied by an exploration of existing defense mechanisms and a discussion of future research directions to enhance system robustness. This comprehensive analysis aims to dissect the intricate ecosystem of blockchain, offering readers a nuanced understanding of its multifaceted security landscape.

Keywords: Blockchain, distributed ledger technology, cryptography, consensus algorithms, security, attacks, vulnerabilities, applications.

Introduction

Blockchain technology, a decentralized and distributed ledger system, has garnered significant attention across various sectors due to its inherent security features and potential to revolutionize digital interactions [1]. This technology fundamentally redefines trust, security, and efficiency by providing a transparent and immutable framework for transactions and data management [2]. Initially recognized for its role in cryptocurrencies like Bitcoin, blockchain's applicability now extends far beyond digital currency, promising transformative impacts on numerous industries by offering a secure, transparent, and tamper-resistant method for recording and verifying transactions [3]. Its foundational strength lies in its innovative utilization of established cryptographic and networking principles to create a novel database system where interconnected blocks form a chain [3]. Each block within this chain contains a cryptographic hash of the preceding block, a timestamp, and transaction data, thereby ensuring the integrity and chronological order of the ledger [4]. This architecture facilitates a trustless environment, enabling participants to transfer value and information across networks without requiring a central authority or intermediary [3]. The integration of diverse computer technologies, including cryptography, consensus mechanisms, and peer-to-peer networks, enables the creation of a decentralized and tamper-resistant public ledger where data and transactions are securely stored through cryptographic methods [5]. This distributed ledger technology ensures data integrity and prevents tampering by replicating the ledger across a network of computers, thereby making it exceedingly difficult for any single entity to alter records surreptitiously [6]. This comprehensive review delves into the fundamental architecture of blockchain, exploring its core technical components including distributed consensus algorithms, cryptographic principles, and smart contract functionality that enable its unique properties [7].

Literature Review

This section provides a thorough examination of the foundational principles of blockchain technology, meticulously detailing its operational mechanisms, the critical role of consensus algorithms, and the profound implications of decentralization in fostering heightened security and operational efficiency across various domains [8]. A core tenet of this technology is the distributed, consensus ledger, which underpins its ability to create a secure, immutable data storage and management system [9]. Each block in this ledger is cryptographically linked to the previous one, forming an unbreakable chain that ensures data integrity and prevents unauthorized alterations [8], [10]. This immutability is further reinforced by the cryptographic hash functions and consensus mechanisms integral to the blockchain's operation, which together maintain the ledger's consistency and security across all network nodes [11], [12]. The decentralized nature of blockchain, facilitated by a peer-to-peer network where multiple participants, or nodes, maintain replicas of the ledger, inherently eliminates the need for a central authority, thereby bolstering resistance to censorship and single points of failure [13], [14]. This distributed architecture ensures that control is shared among all participants, rather than being concentrated in a single entity, which is a significant departure from traditional centralized systems [15]. Moreover, the implementation of sophisticated cryptographic algorithms within blockchain technology is paramount for safeguarding data integrity, authenticating transactions, and ensuring the privacy and authenticity of information stored on the blockchain through hash functions, digital signatures, and encryption [16]. This cryptographic underpinning ensures that all transactions are secured and verifiable, contributing significantly to the overall trustworthiness of the blockchain network [17]. The concept of decentralization is a cornerstone of blockchain technology, fundamentally distinguishing it from conventional centralized systems by distributing data across numerous nodes rather than housing it in a singular location [18]. This distributed structure not only enhances resilience against attacks and system failures but also promotes transparency and reduces the risk of data manipulation [19], [20]. This decentralized approach ensures that no single point of control exists, thereby mitigating the risks associated with centralized data storage, such as single points of failure and censorship [21], [22]. This inherent distribution across a network of computers, where each node holds a complete copy of the ledger, makes it exceptionally difficult for any single entity to tamper with the data, thereby safeguarding its integrity and ensuring transparency for all peer-connected nodes [23], [24]. This decentralized framework ensures that every participant possesses an identical copy of the ledger, thereby guaranteeing data integrity and significantly reducing reliance on any central authority [25], [26]. This decentralized architecture fundamentally distinguishes blockchain from traditional centralized databases, where a single entity holds absolute control over the data [27]. The replication of the entire ledger across all participating nodes ensures that any attempt to alter data on one node would be immediately evident to the rest of the network, thereby maintaining the immutability of recorded information [28], [29]. This distributed storage paradigm is pivotal, as it inherently mitigates the risks associated with centralized intermediaries, safeguarding against data compromise and manipulation [30].

Methodology

This section outlines the methodological approach employed in this review, detailing the systematic process of literature identification, selection, and synthesis to comprehensively analyze blockchain architectures, security challenges, and emerging applications. This review synthesizes findings from a diverse range of scholarly articles, conference proceedings, and industry reports to provide a holistic understanding of the technological landscape and its socio-economic implications. A rigorous analysis of existing research was conducted to identify key themes, controversies, and gaps in the current understanding of blockchain technology. The methodological approach included comprehensive search strategies across multiple databases, ensuring the inclusion of high-quality studies relevant to blockchain's potential in enhancing security and transparency across various sectors, particularly telecommunications [29]. The selection criteria focused on peer-reviewed publications from reputable journals and conferences, prioritizing those that offer empirical data, theoretical frameworks, or comprehensive surveys on blockchain implementations and their associated challenges. The synthesis process involved thematic analysis to categorize and consolidate information related to blockchain architectures, security mechanisms, and diverse application areas, highlighting both established knowledge and nascent research directions [29], [31]. This systematic approach allowed for a nuanced understanding of blockchain's evolution, from its origins as a decentralized digital currency [32] to its current expansive applications across various industries, emphasizing its capacity to address issues like data manipulation and censorship inherent in centralized systems [3]. This comprehensive review not only maps the technological advancements but also critically assesses the performance trade-offs, security vulnerabilities, and scalability limitations inherent in different blockchain storage architectures [33]. The systematic literature search utilized a broad array of scientific databases including IEEE Xplore, Elsevier, Springer, MDPI, Wiley, ACM, Taylor & Francis, and Emerald, with no single publisher being prioritized to ensure a balanced and comprehensive selection of studies [34]. The search queries incorporated keywords such as "blockchain architecture," "consensus mechanisms," "security challenges," "scalability solutions," "distributed ledger technology," and "decentralized applications" to capture a wide spectrum of relevant research [35], [36]. The systematic review process adhered to established guidelines, such as those by Kitchenham and Charters, ensuring the reproducibility and rigor of the methodology [37], [38]. Furthermore, the selection criteria specifically targeted studies published between 2018 and 2024 to capture the most recent advancements and discussions within the rapidly evolving field of blockchain technology [39]. This temporal constraint allowed for an in-depth examination of contemporary issues and solutions, moving beyond foundational concepts to explore cutting-edge developments and practical implementations [40].

Results

The systematic review process yielded a robust dataset of relevant publications, which were subsequently analyzed to synthesize key findings regarding blockchain architectures, prevalent security challenges, and emerging application trends [36], [41]. This section presents a detailed comparative analysis of the reviewed studies, categorizing them by consensus mechanisms, energy efficiency metrics, and architectural innovations, while also identifying barriers to widespread adoption [42]. Specifically, the analysis delves into the algorithmic trade-offs, scalability considerations, and security implications of various consensus mechanisms, providing comprehensive guidance for network design and implementation [41], [42]. The findings indicate that while energy-efficient mechanisms like Proof of Stake and Directed Acyclic Graphs significantly reduce energy consumption compared to Proof of Work by over 99%, they often introduce trade-offs concerning decentralization and security [42]. This systematic review corroborates that while these alternative mechanisms address the critical issue of high energy consumption associated with traditional blockchain networks, they often necessitate careful consideration of their impact on network resilience and resistance to attack [42].

Discussion

Beyond energy concerns, the findings also highlight critical challenges such as limited interoperability, where different blockchain networks struggle to communicate effectively, and scalability issues, with transaction speeds significantly lower than traditional payment systems [43]. Moreover, the nascent stage of Web 3.0 and Industry 4.0 technologies, such as Decentralized Finance and Non-Fungible Tokens, within certain sectors, like food supply chains, suggests a need for further interdisciplinary research to fully leverage blockchain's potential [38]. The integration of artificial intelligence and the Internet of Things with blockchain further complicates these dynamics, necessitating frameworks like Ai-Chain to manage secure and distributed sharing of learning outcomes across diverse network edges [44]. Furthermore, regulatory uncertainties, high initial costs, and the absence of industry-wide standards continue to impede broader adoption, necessitating coordinated stakeholder efforts to unlock blockchain's full potential [45].

Conclusion

This paper offers a comprehensive review of blockchain architectures, security challenges, and emerging applications, emphasizing its transformative potential across various sectors, especially in enhancing supply chain traceability and data integrity through decentralized and immutable record-keeping [44]. Despite these advancements, persistent technological hurdles, particularly scalability issues and high energy consumption associated with certain consensus mechanisms, alongside implementation barriers such as significant initial costs and the lack of robust regulatory frameworks, continue to impede widespread adoption [46]. Addressing these critical challenges through innovations in consensus mechanisms, improved interoperability solutions, and standardized regulatory frameworks is paramount for realizing blockchain's full potential across diverse industries [47], [48]. Future research should therefore focus on developing more energy-efficient and scalable blockchain solutions, exploring novel consensus algorithms, and fostering greater interoperability between disparate blockchain networks to overcome current limitations [49]. Moreover, the integration of advanced technologies like AI and IoT with blockchain presents a promising avenue for mitigating challenges such as data quality and real-time traceability, particularly in complex systems like food supply chains, despite existing limitations in their comprehensive implementation [50], [51]. The amalgamation of AI and blockchain, specifically, holds significant promise for enhancing data accuracy, system compatibility, and overall security in sensitive domains such as food safety and fraud prevention, by creating secure, irreversible, and decentralized systems for highly sensitive data [47], [51]. However, achieving seamless integration requires standardized protocols and interfaces, necessitating collaborative initiatives among industry stakeholders, technology providers, and policymakers to create a unified framework fostering smooth interaction between blockchain and AI components [52].

References

[1] M. An, Q. Fan, H. Yu, and H. Zhao, “Blockchain technology research and application: a systematic literature review and future trends,” *arXiv (Cornell University)* , Jan. 2023, doi: 10.48550/arxiv.2306.14802.

[2] G. Nagar and A. Manoharan, “BLOCKCHAIN TECHNOLOGY: REINVENTING TRUST AND SECURITY IN THE DIGITAL WORLD,” *International Research Journal of Modernization in Engineering Technology and Science* , Jun. 2024, doi: 10.56726/irjmets23989.

[3] A. B. Baftijari and L. Nakov, “The architecture of Blockchain technology and Beyond,” in *IntechOpen eBooks* , IntechOpen, 2024. doi: 10.5772/intechopen.1004138.

[4] Z. Baracskai, D. Vukovic, and J. Janjusevic, “Economic and social development: 73rd International Scientific Conference on Economic and Social Development - ‘Sustainable Tourism in Post-pandemic World’: book of proceedings.” Oct. 21, 2021.

[5] K. Dwivedi, A. Agrawal, A. Bhatia, and K. Tiwari, “A Novel Classification of Attacks on Blockchain Layers: Vulnerabilities, Attacks, Mitigations, and Research Directions,” *arXiv (Cornell University)* , Apr. 2024, doi: 10.48550/arxiv.2404.18090.

[6] P. Alhat, “Blockchain Technology,” *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT* , vol. 8, no. 4, p. 1, Apr. 2024, doi: 10.55041/ijsrem30694.

[7] A. P. Singh, “Blockchain Technology: Core Mechanisms, Evolution, and Future Implementation Challenges,” 2025, doi: 10.48550/ARXIV.2505.08772.

[8] P. O. Shoetan and B. T. Familoni, “BLOCKCHAIN’S IMPACT ON FINANCIAL SECURITY AND EFFICIENCY BEYOND CRYPTOCURRENCY USES,” *International Journal of Management & Entrepreneurship Research* , vol. 6, no. 4, p. 1211, Apr. 2024, doi: 10.51594/ijmer.v6i4.1032.

[9] F. Anwar, B. U. I. Khan, M. L. M. Kiah, N. A. Abdullah, and K. W. Goh, “A Comprehensive Insight into Blockchain Technology: Past Development, Present Impact and Future Considerations,” *International Journal of Advanced Computer Science and Applications* , vol. 13, no. 11, Jan. 2022, doi: 10.14569/ijacsa.2022.01311101.

[10] A. Anyanwu, S. O. Dawodu, A. Omotosho, O. J. Akindote, and S. K. Ewuga, “Review of blockchain technology in government systems: Applications and impacts in the USA,” *World Journal of Advanced Research and Reviews* , vol. 20, no. 3, p. 863, Dec. 2023, doi: 10.30574/wjarr.2023.20.3.2553.

[11] S. Narkedimilli, R. A. Kumar, N. Kumar, R. P. Reddy, and C. P. Kumar, “FL-DECO-BC: A Privacy-Preserving, Provably Secure, and Provenance-Preserving Federated Learning Framework with Decentralized Oracles on Blockchain for VANETs,” *arXiv (Cornell University)* , Jul. 2024, doi: 10.48550/arxiv.2407.21141.

[12] S. R. Addula and A. Ali, “A Novel Permissioned Blockchain Approach for Scalable and Privacy-Preserving IoT Authentication,” *Journal of Cyber Security and Risk Auditing* , vol. 2025, no. 4, p. 222, Jan. 2025, doi: 10.63180/jcsra.thestap.2025.4.3.

[13] M. Ghaly, E. Elbeltagi, A. Elsmadony, and M. A. Tantawy, “Integration of Blockchain-Enabled Smart Contracts in Construction: SWOT Framework and Social Network Analysis,” *Civil Engineering Journal* , vol. 10, no. 5, p. 1662, May 2024, doi: 10.28991/cej-2024-010-05-020.

[14] K. Zhu, “Blockchain Technology: Applications, Opportunities, Challenges, and Countermeasures,” in *Advances in economics, business and management research/Advances in Economics, Business and Management Research* , Atlantis Press, 2023, p. 460. doi: 10.2991/978-94-6463-298-9_50.

[15] F. E. Adediran, B. A. Okunade, R. E. Daraojimba, O. E. Adewusi, O. B. A, and J. C. Igbokwe, “Blockchain for

social good: A review of applications in humanitarian aid and social initiatives," *International Journal of Science and Research Archive* , vol. 11, no. 1. p. 1203, Feb. 05, 2024. doi: 10.30574/ijsra.2024.11.1.0184.

[16] J. Liu *et al.* , "Enhancing Trust and Privacy in Distributed Networks: A Comprehensive Survey on Blockchain-based Federated Learning," *arXiv (Cornell University)* , Mar. 2024, doi: 10.48550/arxiv.2403.19178.

[17] X. Zhang, Y. Sheng, and Z. Liu, "Using expertise as an intermediary: Unleashing the power of blockchain technology to drive future sustainable management using hidden champions," *Heliyon* , vol. 10, no. 1, Dec. 2023, doi: 10.1016/j.heliyon.2023.e23807.

[18] J. A. B. Moya, "Blockchain for Academic Integrity: Developing the Blockchain Academic Credential Interoperability Protocol (BACIP)," *arXiv (Cornell University)* , Jun. 2024, doi: 10.5281/zenodo.12527471.

[19] P. Kowalski and L. Esposito, "The Role of Blockchain Technology in Enhancing Supply Chain Transparency in Europe," *Journal of Procurement & Supply Chain* , vol. 7, no. 2, p. 11, Jul. 2023, doi: 10.53819/81018102t2179.

[20] K. K. Vaigandla, "Quantum-Secure IoT Networks for the 6G Era: Post-Quantum Cryptography, Blockchain Integration, and Trust Architectures - A Comprehensive Review," *Journal of Sensors, IoT & Health Sciences (JSIHS).* , vol. 3, no. 3. Oxford University Press, p. 44, Sep. 30, 2025. doi: 10.69996/jsihs.2025014.

[21] M. I. Hossain, T. Steigner, M. I. Hussain, and A. Akther, "Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach," *arXiv (Cornell University)* , May 2024, doi: 10.48550/arxiv.2405.04837.

[22] M. Ghorbian and M. Ghobaei-Arani, "Key Concepts and Principles of Blockchain Technology," *arXiv (Cornell University)* , Jan. 2025, doi: 10.48550/arxiv.2501.11707.

[23] P. Rajbhandari, G. Giri, H. Verma, and Prof. K. Soni, "Blockchain Technology for Intelligent transportation Systems: A Systematic Literature Review," *International Journal for Research in Applied Science and Engineering Technology* , vol. 11, no. 4, p. 1993, Apr. 2023, doi: 10.22214/ijraset.2023.50304.

[24] F. Rabia, S. Arezki, and T. Gadi, "A Review of Blockchain-Based E-Voting Systems: Comparative Analysis and Findings," *International Journal of Interactive Mobile Technologies (iJIM)* , vol. 17, no. 23. kassel university press, p. 49, Dec. 12, 2023. doi: 10.3991/ijim.v17i23.45257.

[25] S. Islam and K. U. Apu, "DECENTRALIZED VS. CENTRALIZED DATABASE SOLUTIONS IN BLOCKCHAIN: ADVANTAGES, CHALLENGES, AND USE CASES," *Global mainstream journal of innovation, engineering & emerging technology.* , vol. 3, no. 4, p. 58, Aug. 2024, doi: 10.62304/jieet.v3i04.195.

[26] M. Ivasenko, "Blockchain as a Tool to Strengthen the State's Financial Security," *Business Inform* , vol. 1, no. 564, p. 219, Jan. 2025, doi: 10.32983/2222-4459-2025-1-219-229.

[27] A. Al-Jabra, H. Alnuhait, S. Almanasra, and H. A. Al-Khawaja, "A Vision Towards the Future of Cryptocurrencies Rooting, its Financial Significance, and Legal Challenges in its Use," *Information Sciences Letters* , vol. 12, no. 8, p. 2545, Aug. 2023, doi: 10.18576/isl/120811.

[28] J. A. B. Moya, "Blockchain for Academic Integrity: Developing the Blockchain Academic Credential Interoperability Protocol (BACIP)," *arXiv (Cornell University)* , Jun. 2024, doi: 10.48550/arxiv.2406.15482.

[29] S. O. Folorunsho, O. A. Adenekan, C. Ezeigweneme, I. C. Somadina, and P. A. Okeleke, "Enhancing security and transparency in telecommunications through blockchain technology implementation," *Engineering Science & Technology Journal* , vol. 5, no. 8, p. 2520, Aug. 2024, doi: 10.51594/estj.v5i8.1442.

[30] N. Arshadi, "Perspective Chapter: Reexamining Coase's Transaction Costs Paradigm in the Context of Blockchain Technology and Smart Contracts," in *IntechOpen eBooks* , IntechOpen, 2024. doi: 10.5772/intechopen.1005348.

[31] S. Abdulrahman and M. Useng, "Blockchain and Distributed Ledger Technologies for IoT Security: A Survey paper," *Mesopotamian Journal of Computer Science* , p. 5, Apr. 2022, doi: 10.58496/mjcsc/2022/006.

[32] H. M. Marhoon, N. Basil, and A. Ma'arif, "Exploring Blockchain Data Analysis and Its Communications Architecture: Achievements, Challenges, and Future Directions: A Review Article," *International Journal of Robotics and Control Systems* , vol. 3, no. 3. p. 609, Sep. 06, 2023. doi: 10.31763/ijrcs.v3i3.1100.

[33] H. Eren, Ö. Karaduman, and M. T. Gençoğlu, "Security Challenges and Performance Trade-Offs in On-Chain and Off-Chain Blockchain Storage: A Comprehensive Review," *Applied Sciences* , vol. 15, no. 6. Multidisciplinary Digital Publishing Institute, p. 3225, Mar. 15, 2025. doi: 10.3390/app15063225.

[34] Ö. Karaduman and G. Gülhas, "Blockchain-Enabled Supply Chain Management: A Review of Security, Traceability, and Data Integrity Amid the Evolving Systemic Demand," *Applied Sciences* , vol. 15, no. 9. Multidisciplinary Digital Publishing Institute, p. 5168, May 06, 2025. doi: 10.3390/app15095168.

[35] M. M. Yakubu *et al.* , "A Systematic Literature Review on Blockchain Consensus Mechanisms' Security: Applications and Open Challenges," *Computer Systems Science and Engineering* , vol. 48, no. 6, p. 1437, Jan. 2024, doi: 10.32604/csse.2024.054556.

[36] A. Chandan, V. Potdar, and M. John, "Systematic Literature Review of Blockchain Technology's Technical Challenges: A Tertiary Study," *Information* , vol. 15, no. 8, p. 475, Aug. 2024, doi: 10.3390/info15080475.

[37] B. Bellaj, A. Ouaddah, E. Bertin, N. Crespi, and A. Mezrioui, "Drawing the Boundaries Between Blockchain and Blockchain-Like Systems: A Comprehensive Survey on Distributed Ledger Technologies," *Proceedings of the IEEE* ,

vol. 112, no. 3, p. 247, Mar. 2024, doi: 10.1109/jproc.2024.3386257.

[38] R. M. Ellahi, L. C. Wood, and A. E. A. Bekhit, “Blockchain-Based Frameworks for Food Traceability: A Systematic Review,” *Foods* , vol. 12, no. 16. Multidisciplinary Digital Publishing Institute, p. 3026, Aug. 11, 2023. doi: 10.3390/foods12163026.

[39] U. V. R. Kumari, “USING BLOCK CHAIN FOR SEED TRACEABILITY: A SYSTEMATIC LITERATURE REVIEW,” *ShodhKosh Journal of Visual and Performing Arts* , vol. 5, no. 6, Jun. 2024, doi: 10.29121/shodhkosh.v5.i6.2024.6332.

[40] I. Iswahyudi, D. Hindarto, and R. E. Indrajit, “Digital Transformation in University: Enterprise Architecture and Blockchain Technology,” *SinkrOn* , vol. 8, no. 4, p. 2501, Oct. 2023, doi: 10.33395/sinkron.v8i4.12977.

[41] J. Singh *et al.* , “A Systematic Review of Blockchain, AI, and Cloud Integration for Secure Digital Ecosystems,” *The International journal of networked and distributed computing* , vol. 13, no. 2. Springer Nature, Oct. 27, 2025. doi: 10.1007/s44227-025-00072-1.

[42] A. Zimba, K. O. Phiri, M. Mulenga, and G. Mukupa, “A systematic literature review of blockchain technology and energy efficiency based on consensus mechanisms, architectural innovations, and sustainable solutions,” *Discover Analytics* , vol. 3, no. 1, Sep. 2025, doi: 10.1007/s44257-025-00041-6.

[43] Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, “From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges.” Jun. 2021. doi: 10.1109/TII.2020.3003910.

[44] M. R. A. Rashid *et al.* , “Transforming agri-food value chains in Bangladesh: A practical application of blockchain for traceability and fair pricing,” *Heliyon* , vol. 10, no. 21, Nov. 2024, doi: 10.1016/j.heliyon.2024.e40091.

[45] M. F. M. S. Mustafa, N. Navaranjan, and A. Demirovic, “Food cold chain logistics and management: A review of current development and emerging trends,” *Journal of Agriculture and Food Research* , vol. 18. Elsevier BV, p. 101343, Aug. 05, 2024. doi: 10.1016/j.jafr.2024.101343.

[46] A. Varma, N. Dixit, S. Ray, and J. Kaur, “Blockchain technology for sustainable supply chains: A comprehensive review and future prospects,” *World Journal of Advanced Research and Reviews* , vol. 21, no. 3. GSC Online Press, p. 980, Mar. 13, 2024. doi: 10.30574/wjarr.2024.21.3.0804.

[47] I. Abrar and J. A. Sheikh, “Current trends of blockchain technology: architecture, applications, challenges, and opportunities,” *Discover Internet of Things* , vol. 4, no. 1, Jul. 2024, doi: 10.1007/s43926-024-00058-5.

[48] M. K. Pawar and P. Patil, “Scalability Enhancement for Blockchains by Dynamic Difficulty Level Adjustment: A Machine Learning Approach,” *Engineering Technology & Applied Science Research* , vol. 15, no. 5, p. 26440, Oct. 2025, doi: 10.48084/etasr.10526.

[49] O. I. Oriekhoe, B. I. Ashiwaju, K. C. Ihemereze, U. Ikwue, and C. A. Udeh, “BLOCKCHAIN TECHNOLOGY IN SUPPLY CHAIN MANAGEMENT: A COMPREHENSIVE REVIEW,” *International Journal of Management & Entrepreneurship Research* , vol. 6, no. 1. Fair East Publishers, p. 150, Jan. 13, 2024. doi: 10.51594/ijmer.v6i1.714.

[50] S. A. Burburi, A. Gaddi, R. Battur, M. C. Elemmi, and V. Hiremath, “Role of AI and Blockchain Technology in Enhancing Performance in Agri-Food Supply Chain System,” *ITM Web of Conferences* , vol. 79, p. 1006, Jan. 2025, doi: 10.1051/itmconf/20257901006.

[51] M. Vasileiou *et al.* , “Digital Transformation of Food Supply Chain Management Using Blockchain: A Systematic Literature Review Towards Food Safety and Traceability,” *Business & Information Systems Engineering* , Jun. 2025, doi: 10.1007/s12599-025-00948-0.

[52] S.-Y. Kim and A. A. AlZubi, “Blockchain and Artificial Intelligence for Ensuring the Authenticity of Organic Legume Products in Supply Chains,” *Legume Research - An International Journal* , Jan. 2024, doi: 10.18805/lrf-786.