World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Blockchain as a Backbone for Cybersecurity: From Data Integrity to Decentralized Trust

Prajakta Sudhir Khade [1,*], Aarushi Santosh Gode [1] and Rajeshkumar U. Sambhe [2]

[1] *Department of Computer Science and Engineering, Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, Maharashtra, India.*
[2] *Department of Mechanical Engineering, Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, Maharashtra, India.*

World Journal of Advanced Research and Reviews, 2025, 28(01), 2014-2023

Publication history: Received on 05 August 2025; revised on 14 September 2025; accepted on 16 October 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.1.3215

Abstract

The exponential rise of cyber threats has revealed the vulnerabilities of centralized security systems, including susceptibility to insider attacks, single points of failure, and regulatory inefficiencies. This paper investigates blockchain as a transformative backbone for cybersecurity, focusing on its potential to ensure data integrity, decentralize trust, and mitigate advanced cyber risks. Beginning with a comprehensive literature review, the study examines the fundamentals of blockchain technology—distributed ledgers, consensus mechanisms, and cryptographic primitives—that enable tamper-proof, transparent, and secure digital ecosystems. The challenges of centralized systems are contrasted with blockchain's resilience, highlighting its role in eliminating bottlenecks and enhancing trust. Applications across identity management, IoT security, supply chains, and e-governance are analyzed alongside a proposed methodology that integrates blockchain with artificial intelligence, IoT, and quantum-resilient models. Real-world case studies demonstrate blockchain's adoption in healthcare, government, and industrial systems, while challenges such as scalability, interoperability, and compliance are critically assessed. Collectively, this study underscores blockchain's pivotal role in shaping next-generation cybersecurity architectures.

Keywords: Blockchain; Cybersecurity; Data Integrity; Decentralized Trust; Smart Contracts

1. Introduction

In the digital era, the sophistication of cyberattacks has increased drastically, exposing the weaknesses of conventional security infrastructures. Centralized models, while widely adopted, are increasingly criticized for their reliance on trusted third parties and single points of failure. Once compromised, these centralized systems can lead to catastrophic data breaches, insider abuse, and financial losses, as seen in recent high-profile cyber incidents [1]. This rising threat landscape necessitates a paradigm shift towards distributed and tamper-resistant security frameworks.

Blockchain technology has emerged as a promising candidate to address these challenges. With its immutable, transparent, and decentralized ledger structure, blockchain enhances data integrity, ensures secure audit trails, and minimizes unauthorized manipulation [2]. Unlike conventional databases, blockchain does not depend on a central authority, thereby reducing vulnerabilities associated with trust dependency. This makes blockchain particularly relevant for industries such as finance, healthcare, government, and energy, where secure and verifiable data exchange is paramount [3].

* Corresponding author: Prajakta Sudhir Khade

Beyond its role as a secure transaction ledger, blockchain also introduces new paradigms for cybersecurity when combined with artificial intelligence (AI) and machine learning. Such integration enables predictive threat detection, anomaly recognition, and automated incident response, ultimately creating sustainable and adaptive security ecosystems [4]. In addition, blockchain can support decentralized identity management systems, empowering users with control over their credentials while minimizing identity theft and fraud [5]. Applications in smart cities, critical infrastructure, and the Internet of Things (IoT) further highlight blockchain's ability to secure large-scale, heterogeneous networks where centralized solutions often fall short.

Despite its transformative potential, blockchain adoption in cybersecurity is not without limitations. Issues related to scalability, interoperability between blockchain platforms, energy consumption of consensus mechanisms, and regulatory compliance continue to pose barriers [6]. Moreover, concerns regarding the integration of blockchain into legacy systems and the challenges of balancing privacy with transparency warrant further research. Nevertheless, scholars and practitioners alike view blockchain as an essential component of the next generation of cybersecurity frameworks, especially as digital ecosystems expand into cloud computing, the metaverse, and edge computing environments [7].

By reimagining trust as a decentralized construct, blockchain offers not just incremental improvements but a foundational shift in how cybersecurity can be achieved. This study investigates blockchain as a backbone for cybersecurity, focusing on its role in ensuring data integrity and establishing decentralized trust across multiple domains.

2. Literature Review

The integration of blockchain into cybersecurity has been widely examined in contemporary scholarship, with systematic reviews and bibliometric analyses outlining both its promise and persistent challenges. A comprehensive review synthesizes the existing body of knowledge, concluding that blockchain's defining features—immutability, decentralization, and transparency—make it well-suited for enhancing trust and resilience in digital systems. However, the same study emphasizes limitations such as latency, interoperability difficulties, and concerns over data privacy leakage, which continue to hinder large-scale deployment [8].

One area of concentrated research is supplying chain security, where blockchain is recognized as a powerful tool for improving transparency, accountability, and cyber resilience. Literature shows that immutable transaction records within supply chains prevent fraud, reduce the risk of malicious interference, and enable trusted tracking of goods from origin to destination [9]. These findings highlight blockchain's capacity not only to secure operational environments but also to improve confidence among stakeholders.

Institutional cybersecurity governance has also become a key focus, with research incorporating blockchain into security maturity assessment frameworks. Studies report that the ability to generate tamper-proof audit trails and immutable compliance logs significantly enhances monitoring and regulatory accountability [10]. In parallel, anomaly detection in blockchain systems has been identified as an emerging research stream. Reviews emphasize that blockchain does not merely store data securely but also supports proactive mechanisms for identifying abnormal behaviors and potential attacks within decentralized networks [11].

Sector-specific investigations further enrich the literature. In energy systems, blockchain has been combined with artificial intelligence to secure smart grids and distributed energy infrastructures. The findings suggest that decentralization improves operational resilience while reducing vulnerabilities associated with centralized control structures [12]. Healthcare research similarly identifies blockchain as a foundation for identity management and data privacy protection. Frameworks developed in this domain demonstrate how blockchain can safeguard sensitive medical information, reduce data breaches, and ensure controlled access to health records [13].

Beyond sector-specific applications, scholars increasingly focus on blockchain's influence on organizational cybersecurity and governance. Bibliometric reviews in business contexts argue that blockchain adoption strengthens enterprise data management, prevents digital fraud, and enhances customer and partner trust in electronic transactions [14]. In the public sector, research highlights blockchain's disruptive impact on e-governance, particularly through secure voting systems, digital identity solutions, and tamper-resistant public record management [15].

Taken together, the literature positions blockchain as more than a complementary cybersecurity tool; it is widely regarded as a transformative backbone for future security architectures. Nonetheless, scholars repeatedly emphasize challenges related to scalability, consensus efficiency, interoperability across blockchain networks, and evolving

regulatory frameworks. These recurring themes underline the need for further innovation, interdisciplinary collaboration, and policy support to fully realize blockchain's potential in reshaping cybersecurity.

3. Fundamentals of Blockchain Technology

Blockchain technology is a distributed ledger system designed to ensure transparency, immutability, and trust in digital transactions without the need for centralized intermediaries. At its core, blockchain functions as a peer-to-peer network where participants maintain a shared database that is continuously updated and cryptographically secured [16]. Each block contains a set of validated transactions, linked through hash functions, creating an immutable chain resistant to tampering [17].

A key principle of blockchain is decentralization, which distributes authority across network participants rather than relying on a single trusted entity. This design eliminates single points of failure and strengthens resilience against cyberattacks. The consensus mechanism is central to blockchain's operation, as it ensures agreement among nodes on the validity of transactions. While Proof-of-Work (PoW) and Proof-of-Stake (PoS) are the most widely studied, recent work explores energy-efficient alternatives that balance scalability, security, and decentralization [18].

Another critical building block is cryptography. Public-key cryptography secures user identities, while digital signatures authenticate transactions. Hashing algorithms guarantee data integrity, ensuring that any attempt to alter recorded information is instantly detectable [19]. Together, these cryptographic primitives underpin blockchain's ability to act as a secure and tamper-resistant infrastructure.

Beyond basic transaction recording, smart contracts extend blockchain's utility by enabling automated execution of rules and agreements. These self-executing contracts, coded into the blockchain, reduce reliance on third-party enforcement and are being increasingly adopted in fields such as finance, supply chains, and digital identity management [20]. Furthermore, permissioned blockchains are gaining traction in enterprise settings, where controlled access and enhanced privacy are required while retaining the core features of distributed ledgers [21].

The layered architecture of blockchain is also a defining characteristic. At the network layer, peer-to-peer communication ensures synchronization. The data layer organizes blocks and chains, while the application layer enables decentralized applications (Dapps) to operate atop the ledger [22]. Together, these layers create a modular yet integrated framework that facilitates innovation across industries.

Recent scholarship emphasizes the blockchain trilemma, which refers to the difficulty of simultaneously achieving scalability, decentralization, and security. Proposed solutions such as consortium blockchains and hybrid consensus models aim to balance these competing goals, providing a foundation for secure large-scale applications [23].

Overall, blockchain's fundamentals—distributed consensus, cryptography, smart contracts, and layered architecture—establish the technological backbone for exploring its role in cybersecurity. A deeper understanding of these principles is essential before analyzing blockchain's transformative role in ensuring data integrity and decentralized trust.

4. Cybersecurity Challenges in Centralized Systems

Centralized architectures remain the dominant design for many organizations, yet they present critical vulnerabilities that make them increasingly unsuitable for securing modern digital infrastructures. The following challenges have been widely reported in the literature:

4.1. Single Point of Failure

Centralized systems depend on one controlling authority or database. If this authority is compromised, the entire system collapses, exposing all data and services. Attackers frequently exploit these points of concentration through denial-of-service (DoS) attacks, ransomware, or direct breaches, often resulting in catastrophic losses for organizations [24].

4.2. Regulatory Mismatches

Cybersecurity frameworks for centralized systems often lag behind the rapid evolution of threats. Regulatory and compliance structures designed for static, centralized architectures fail to adapt to highly distributed, dynamic attack

vectors such as botnets or cross-border intrusions. This mismatch reduces the effectiveness of policies and leaves organizations exposed to systemic risks [25].

4.3. Vulnerability of Government Systems

Centralized government databases store sensitive personal and financial records. Once breached, attackers can gain unauthorized access to millions of records at once. Moreover, insider threats are amplified in centralized public administration, as system administrators often have broad access privileges that can be misused without adequate monitoring [26].

4.4. Rigid Incident Response

Centralized cybersecurity governance structures rely on hierarchical decision-making. This rigidity delays response times to threats such as zero-day exploits and advanced persistent threats (APTs). By the time approvals move through bureaucratic chains, attackers may have already escalated privileges or exfiltrated data, leaving organizations with limited recovery options [27].

4.5. Overdependence on Centralized Monitoring

Many organizations rely on centralized security information and event management (SIEM) systems. While effective at aggregating logs, these systems create overdependence. Once adversaries breach or disable the monitoring center, organizations lose visibility into network activity, rendering them blind to ongoing threats [28].

4.6. IoT Security Weaknesses

The rise of IoT has intensified vulnerabilities in centralized models. Centralized control servers often become bottlenecks, causing latency in authentication and patch updates. Attackers exploit these inefficiencies by compromising poorly secured IoT devices, then using them as backdoors into core systems. The Mirai botnet is a well-documented case, and recent research suggests that similar exploits remain viable due to the weaknesses of centralized IoT security frameworks [29].

4.7. Industrial and Energy Sector Risks

In industrial control systems (ICS) and critical energy infrastructures, centralized control introduces cascading risks. A single compromised control center can disrupt power grids, oil pipelines, or manufacturing processes. This lack of redundancy makes centralized infrastructures prime targets for state-sponsored cyberattacks, which can escalate into national security threats [30].

5. Blockchain as a Backbone for Cybersecurity

Blockchain is increasingly recognized as a foundational technology for modern cybersecurity, offering decentralized trust, immutability, and data integrity as core features. Unlike centralized systems, blockchain distributes authority across a network of nodes, which eliminates single points of failure and makes attacks significantly harder to execute. Recent studies emphasize that this decentralized architecture is highly resistant to fraud, data tampering, and denial-of-service attacks, providing a robust foundation for digital trust [31].

One of blockchain's primary contributions to cybersecurity is enhancing data integrity. Every transaction is cryptographically linked to the previous one, forming an immutable chain where unauthorized modifications are nearly impossible. This ensures that sensitive data, whether financial, governmental, or healthcare-related, remains trustworthy and verifiable over time [32]. Beyond integrity, blockchain strengthens transaction security through consensus mechanisms that validate actions collectively, reducing the risks of insider threats and unauthorized manipulation [33].

Comparative analyses between traditional and blockchain-based cybersecurity approaches highlight blockchain's superiority in transparency and resilience. While centralized frameworks struggle with latency and bottlenecks, blockchain systems provide distributed consensus and autonomous verification, ensuring scalability alongside security [34]. Moreover, blockchain does not function in isolation—it integrates with emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT) to create adaptive and intelligent security systems capable of real-time threat detection and mitigation [35].

In addition, the layered architecture of blockchain allows it to serve as a backbone for digital ecosystems beyond cryptocurrency. Applications in financial infrastructures, decentralized identity management, and smart city ecosystems demonstrate how blockchain not only secures data but also provides a trust layer for coordinating complex, multi-stakeholder environments [36]. Collectively, these findings affirm blockchain's role as a transformative backbone for cybersecurity, capable of addressing longstanding vulnerabilities of centralized systems while paving the way for decentralized trust in critical infrastructures.

6. Applications of Blockchain in Cybersecurity

Blockchain technology has evolved beyond cryptocurrencies to become a cornerstone of modern cybersecurity. Its decentralized, immutable, and transparent nature makes it highly suitable for addressing long-standing security challenges across industries. The following applications illustrate blockchain's transformative role in cybersecurity:

6.1. Identity and Access Management

Blockchain enables decentralized identity systems where individuals control their credentials without relying on centralized authorities. This prevents identity theft and unauthorized access while offering secure digital identities across healthcare, finance, and e-governance [37].

6.2. Data Privacy and Confidentiality

By encrypting, timestamping, and immutably recording sensitive data, blockchain enhances confidentiality while ensuring accountability. Every data access attempt can be verified, reducing risks of unauthorized modifications in critical systems [38].

6.3. IoT and Zero-Trust Security

Blockchain integrates seamlessly with IoT environments to provide decentralized authentication. Zero-trust models combined with blockchain strengthen IoT defenses by validating each device independently and preventing malicious entry points [39].

6.4. Threat Detection and Anomaly Prevention

Blockchain combined with AI can provide real-time anomaly detection in critical networks. Immutable audit trails improve forensic analysis, allowing organizations to trace attack origins and design effective countermeasures [40].

6.5. Secure Data Management for Businesses

Organizations use blockchain to protect data across distributed supply chains and industrial operations. Immutable smart contracts reduce insider threats while automating compliance processes and enhancing resilience [41].

6.6. Secure Communication and Data Sharing

In multi-party environments such as defense, finance, and smart cities, blockchain ensures tamper-proof communication. Studies highlight how blockchain-backed smart contracts prevent interception and manipulation of sensitive communications [42].

7. Proposed Methodology

The proposed methodology aims to establish a blockchain-driven cybersecurity framework that enhances data integrity, strengthens identity management, and mitigates cyber threats through decentralized mechanisms. The framework is structured into four key stages:

7.1. Framework Design and Architecture

The methodology begins with designing a multi-layered blockchain architecture integrated with AI for adaptive cybersecurity. Hybrid frameworks such as AI-blockchain systems for smart grids demonstrate how decentralized consensus can be paired with intelligent anomaly detection to proactively counter threats [43].

7.2. Integration with IoT and SDN Ecosystems

IoT networks and software-defined networking (SDN) systems form critical environments for cyber defense. The proposed framework integrates blockchain with SDN and deep learning models to ensure secure routing, real-time monitoring, and dynamic reconfiguration under potential cyberattacks [44].

7.3. Threat Intelligence and Data Analysis

AI and blockchain are combined to analyze attack patterns, identify anomalies, and sustain resilience against ransomware and supply chain attacks. Literature reviews highlight how integrating blockchain into threat intelligence pipelines leads to stronger detection mechanisms [45].

7.4. Sustainability and Ethical Considerations

Beyond technical security, the methodology considers ethical AI alignment and sustainable digital ecosystems. Studies suggest that blockchain can ensure transparency in AI decisions, while promoting digital trust and reducing biases in security applications [46].

7.5. Quantum-Resilient Trust Models

To address future threats, particularly quantum computing risks, the framework adopts trust-enhanced blockchain methodologies. Quantum trust and consultative transaction-based models demonstrate secure validation for sensitive sectors such as healthcare [47].

7.6. Implementation and Validation

The final phase includes validating the framework using real-world cybersecurity datasets, leveraging blockchain consensus for data immutability. Empirical evaluations of AI–blockchain models confirm enhanced robustness and resilience in critical systems [48].

This methodology provides a comprehensive roadmap for deploying blockchain in cybersecurity contexts, balancing technical resilience with ethical, scalable, and sustainable approaches.

8. Case Studies

The adoption of blockchain in cybersecurity has moved well beyond theoretical models, with several real-world case studies highlighting its impact across critical domains. In healthcare, blockchain has been deployed to address longstanding concerns regarding patient data security and integrity. Solutions such as blockHealthSecure demonstrate how blockchain can ensure tamper-proof electronic health records, secure medical IoT devices, and streamline data-sharing between hospitals while minimizing the risk of cyber intrusions. This approach has proven vital in post-pandemic healthcare systems, where the secure handling of sensitive information has become a global priority [49]. Similarly, a case study of UK local council health services revealed how blockchain-enhanced cybersecurity frameworks enabled stronger anomaly detection and faster recovery from cyber incidents, reinforcing trust in digital health infrastructures [50].

In the public sector, blockchain has been integrated into e-government ecosystems, ensuring accountability, transparency, and protection against tampering with sensitive citizen data. Governments adopting blockchain for digital services have achieved a higher degree of resilience against cyberattacks while enabling secure cloud interoperability. By leveraging blockchain with AI and cloud computing, modern e-governance frameworks enhance citizen trust and protect critical services from internal and external threats [51]. Beyond governance, blockchain has also been employed in smart city and precision agriculture projects, where unified frameworks that combine blockchain, AI, IoT, and cryptography deliver security across urban infrastructure and food supply systems. These initiatives highlight how blockchain is capable of protecting distributed environments from both insider and outsider cyber risks [52].

The Internet of Things (IoT) has emerged as a particularly vulnerable domain where blockchain applications have shown great promise. Studies indicate that blockchain enhances IoT cybersecurity by decentralizing authentication, securing communication channels, and preventing unauthorized device interactions. For example, blockchain-based IoT models applied to smart manufacturing and logistics have improved trust across devices and reduced the likelihood of network-wide breaches [53]. On a broader scale, reviews of blockchain adoption reveal its transformative potential across finance, healthcare, and supply chains. These analyses stress that blockchain not only mitigates privacy and

security risks but also strengthens governance and data accountability, though scalability and energy efficiency remain ongoing challenges [54].

Collectively, these case studies reinforce that blockchain is more than a theoretical tool—it is already reshaping digital security frameworks across healthcare, government, IoT ecosystems, and industrial applications. By providing tamper-proof data management, enhancing resilience against cyberattacks, and fostering decentralized trust, blockchain is positioning itself as a cornerstone of cybersecurity in the digital era.

9. Challenges

While blockchain offers groundbreaking opportunities for cybersecurity, its adoption is not without critical challenges. These limitations need to be carefully addressed to enable broader integration into real-world systems.

9.1. Scalability and Performance Limitations

One of the primary concerns with blockchain-based cybersecurity frameworks lies in scalability. As cyber environments generate massive volumes of data, blockchain's consensus mechanisms often face bottlenecks in transaction throughput and latency. This makes it difficult to apply blockchain efficiently in high-speed, large-scale environments like IoT ecosystems and financial networks. Research emphasizes that although blockchain improves trust and data immutability, the slow pace of consensus remains a major obstacle to achieving real-time cyber defense [55].

9.2. Interoperability and Integration Barriers

Another pressing issue is interoperability. Existing cybersecurity infrastructures—spanning IoT devices, cloud services, and AI-powered systems—often rely on legacy architectures that cannot seamlessly integrate with blockchain protocols. This leads to fragmented adoption, inconsistent security enforcement, and difficulty in building unified defense mechanisms. Recent studies highlight that interoperability remains a daunting vision for digital systems, where policy misalignment and lack of standardized blockchain protocols create major obstacles for cross-platform security integration [56].

9.3. Energy Consumption and Sustainability

Many blockchain systems still rely on energy-intensive consensus mechanisms such as Proof of Work. While alternatives like Proof of Stake are emerging, the high energy demands of blockchain limit its feasibility in resource-constrained environments like IoT or mobile cybersecurity. This poses significant concerns for sustainability, especially in large-scale deployments.

9.4. Privacy and Compliance Conflicts

Blockchain's immutability, while beneficial for ensuring data integrity, also creates challenges when data must be erased or modified to comply with regulations such as GDPR. This tension between immutability and compliance raises legal and ethical dilemmas for industries like healthcare and finance, where privacy is paramount.

9.5. Emerging Quantum Threats

The rise of quantum computing threatens to undermine blockchain's cryptographic foundations. Algorithms that secure today's blockchain transactions could be rendered obsolete by quantum attacks, making the development of quantum-resistant blockchain protocols an urgent research direction.

10. Conclusion

Blockchain has emerged as a paradigm-shifting technology in cybersecurity, redefining how trust, data integrity, and resilience are achieved in digital ecosystems. Unlike centralized systems, which suffer from inherent vulnerabilities, blockchain introduces decentralization, transparency, and immutability, making it a robust foundation for secure infrastructures. This study explored blockchain's core principles, reviewed its integration across multiple domains, and proposed a comprehensive methodology for its implementation. Case studies confirmed its effectiveness in healthcare, e-governance, IoT, and industrial systems, proving that blockchain is not merely theoretical but already transforming critical sectors. Nevertheless, significant challenges remain, particularly in scalability, interoperability, regulatory compliance, and sustainability. Addressing these issues through energy-efficient consensus models, standardized frameworks, and quantum-resistant security solutions will be crucial for large-scale adoption. As the digital landscape continues to expand with AI, IoT, and emerging technologies, blockchain stands as a cornerstone for building adaptive,

resilient, and trustworthy cybersecurity frameworks. Ultimately, blockchain does not just enhance cybersecurity—it redefines it for the decentralized future.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict-of-interest to be disclosed.

References

[1] Shreemali J. Assessing business prospects for the role of blockchain technology and addressing cybersecurity challenges in explainable artificial intelligence. In: Emerging Technologies in Business. Taylor and Francis; 2025. p. 221–40.

[2] Mohamed S. AI and blockchain in cybersecurity: A sustainable approach to protecting digital assets. Informatech J. 2025;4(2):45–59. doi:10.69533/1hh4he43.

[3] Bătușaru CM, Moro N. Blockchain and cryptocurrencies as emerging security threats: A bibliometric analysis of global concerns. Sciendo. 2025;33(1):87–105.

[4] Dey S. Analysis and quantification of different security issues in deploying AI and blockchain: Cybersecurity perspective. In: AI-Driven Security Solutions. IGI Global; 2025. p. 93–114.

[5] Denis A, Thomas A, Robert W, Samuel A, Kabiito SP. A survey on artificial intelligence and blockchain applications in cybersecurity for smart cities. SHIFRA J. 2025;1(1):14–29. doi:10.70470/SHIFRA/2025/001.

[6] Sindiramutty SR, Jhanjhi NZ, Ray SK. Blockchain in cybersecurity: Enhancing data integrity and transaction security. In: Next-Generation Security Frameworks. IGI Global; 2025. p. 67–88.

[7] Radanliev P. Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. Front Blockchain. 2024;7:1359130. doi:10.3389/fbloc.2024.1359130.

[8] Magalhães J. Of blockchain: A systematic literature review. J Blockchain Res. 2025;12(1):55–73.

[9] Yüksel M, Demirci H. The role of blockchain technology in supply chain and logistics sector: A literature review for the period 2015–2024. DUBİTED. 2025;14(2):201–16.

[10] Brezavšek A, Baggia A. Recent trends in information and cyber security maturity assessment: A systematic literature review. Systems. 2025;13(1):44. doi:10.3390/systems13010044.

[11] Shevchuk R, Martsenyuk V, Adamyk B. Anomaly detection in blockchain: A systematic review of trends, challenges, and future directions. Appl Sci. 2025;15(15):6789. doi:10.3390/app15156789.

[12] Shevchuk R, Martsenyuk V, Adamyk B. Anomaly detection in blockchain: A systematic review of trends, challenges, and future directions. Appl Sci. 2025;15(15):6789. doi:10.3390/app15156789.

[13] Ahmed W. Blockchain applications in cybersecurity: Exploring use cases in identity management, data privacy, and threat mitigation. Premier J Sci. 2025;4(2):101–15.

[14] Barcellos-Paula L, Gil-Lafuente AM, Merigó JM. Research on cybersecurity and business: A bibliometric review (2004–2023). Univ Basque Country. 2025; Working Paper.

[15] Lubis S, Ahmad J, Mustanir A, Jabbar A. Blockchain and e-governance: Insights from bibliometric analysis and systematic review. In: Emerging trends in digital governance. IGI Global; 2025. p. 77–96.

[16] Li H, Wang H. Fundamentals of blockchain. IEEE Press; 2025.

[17] Maldonado-Ruiz D, Torres J, Madhoun NE. Fundamentals of blockchain technology. Cham: Springer; 2022. 241 p.

[18] Jha AK, Obaidat MS. Energy-efficient consensus mechanisms in blockchain systems: A survey. IEEE Access. 2023;11:45678–701. doi:10.1109/ACCESS.2023.3267891.

[19] Salah K, Rehman MHU, Jayaraman R. Blockchain for cybersecurity and privacy: Architectures, applications, and future trends. Future Gener Comput Syst. 2023;139:307–24. doi:10.1016/j.future.2023.03.009.

[20] Zhang J, Zhou Q. Smart contracts and their applications in blockchain systems: A review. J Syst Archit. 2023;142:102–58. doi:10.1016/j.sysarc.2023.102958.

[21] Sharma P, Bawa S. Permissioned blockchain architectures and their role in enterprise security. J Netw Comput Appl. 2024;236:103754. doi:10.1016/j.jnca.2023.103754.

[22] Gupta R, Bansal A, Kumar N. Blockchain layered architecture: Concepts and applications. Comput Stand Interfaces. 2023;85:103643. doi:10.1016/j.csi.2023.103643.

[23] Chen Y, Xu L. Addressing the blockchain trilemma: A review of scalability, security, and decentralization solutions. ACM Comput Surv. 2024;56(1):1–36. doi:10.1145/3571744.

[24] Barros P, Agupugo CP, Ejichukwu E, Ogunmoye KA. Decentralized energy security: Cybersecurity challenges and opportunities in distributed renewable energy. Energies. 2025;18(5):2176. doi:10.3390/en18052176.

[25] Sisoyan A. New cybersecurity challenges: Digital transformation and the political implications of their implementation. J Political Sci. 2025;33(2):77–95.

[26] Sani A, Olajide A, Ogunsanya V, Oyebode D. Cybersecurity challenges in digitizing government administration. Gov Inf Q. 2025;42(1):102725. doi:10.1016/j.giq.2024.102725.

[27] Jaber A. Cybersecurity governance and political structures: Comparing centralized and decentralized approaches to cyber defense. Def Secur Anal. 2025;41(2):145–61. doi:10.1080/14751798.2025.1157263.

[28] Svete U. Cybersecurity between technological determinism, political governance, and national security challenges. J Civil Prot. 2025;5(1):33–49.

[29] Hassan A, Hadullo K, Tole K. Advances in cybersecurity: A literature review. Inf Secur J. 2025;34(2):111–29.

[30] Zhukabayeva T, Zholshiyeva L, Karabayev N, Khan S. Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. Sensors. 2025;25(1):122. doi:10.3390/s25010122.

[31] Prashanth MS, Karnati R, Velpuru MS. Blockchain in cyber security: A comprehensive review. In: Blockchain and emerging technologies. Cham: Springer; 2023. p. 201–22.

[32] Aiden MK, Sabharwal SM, Chhabra S. AI and blockchain for cyber security in cyber-physical systems. In: Blockchain for CPS. Cham: Springer; 2023. p. 139–58.

[33] Alam MA, Sarna SA. Strengthening cybersecurity protocols to safeguard US financial infrastructure against emerging threats. Adv Eng Financ Sci. 2025;3(2):59–73.

[34] Patil S. Comparative study of traditional vs blockchain-based cybersecurity approaches. Anuvallabh J Inf Secur. 2025;4(1):22–35.

[35] Bhumichai D, Smiliotopoulos C, Benton R. The convergence of artificial intelligence and blockchain: The state of play and the road ahead. Information. 2024;15(5):201. doi:10.3390/info15050201.

[36] Sharma SR, Kshetri N. BCT4C4: Blockchain technology for cybersecurity, cyber data, and cyber communication in today's cyber world. In: Cyber data and communication. Taylor and Francis; 2025. p. 311–29.

[37] Sharma V. Blockchain-based identity management systems for financial institutions. SSRN Electron J. 2025. doi:10.2139/ssrn.5348871.

[38] Bako NZ, Ozioko CN, Sanni IO, Oni O. The integration of AI and blockchain technologies for secure data management in cybersecurity. ResGate. 2025.

[39] Aleisa MA. Blockchain-enabled zero trust architecture for privacy-preserving cybersecurity in IoT environments. IEEE Access. 2025;13:132457–69. doi:10.1109/ACCESS.2025.10839415.

[40] R S, Katiravan J. Enhancing anomaly detection and prevention in internet of things (IoT) using deep neural networks and blockchain-based cybersecurity. Sci Rep. 2025;15(1):4164. doi:10.1038/s41598-025-04164-4.

[41] Salama R, Altrjman C, Al-Turjman F. An overview of future cybersecurity applications using AI and blockchain technology. Future Trends Cybersecurity. 2024;20:211–27.

[42] Lomotey RK, Barker KL. Blockchain-enabled secure data sharing for cybersecurity applications. Future Gener Comput Syst. 2023;148:482–94. doi:10.1016/j.future.2023.06.018.

[43] Ghadi YY, Mazhar T, Shahzad T, Jaghdam IH. A hybrid AI-blockchain security framework for smart grids. Sci Rep. 2025;15(1):5257. doi:10.1038/s41598-025-05257-w.

[44] Alotaibi J. A hybrid software-defined networking approach for enhancing IoT cybersecurity with deep learning and blockchain in smart cities. Peer Peer Netw Appl. 2025;18:1935–47. doi:10.1007/s12083-025-01935-8.

[45] Alshammari B, Singh MM. A systematic literature review on tackling cyber threats for cyber logistic chain and conceptual frameworks for robust detection mechanisms. IEEE Access. 2025;13:44122–39. doi:10.1109/ACCESS.2025.10933978.

[46] Neulinger A, Sparer L, Roshanaei M, Ostojić D. Is blockchain the future of AI alignment? Developing a framework and a research agenda based on a systematic literature review. Digital. 2025;5(3):50. doi:10.3390/digital5030050.

[47] Selvarajan S, Mouratidis H. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. Sci Rep. 2023;13:34354. doi:10.1038/s41598-023-34354-x.

[48] Chaibi H, Darbali A, Quadar N, El Rharras A. Enhancing cybersecurity through AI and blockchain: An analysis using the cybersecurity threat dataset. In: Advances in cybersecurity research. Cham: Springer; 2024. p. 553–63.

[49] Pokharel BP, Kshetri N, Sharma SR, Paudel S. blockHealthSecure: Integrating blockchain and cybersecurity in post-pandemic healthcare systems. Information. 2025;16(2):133. doi:10.3390/info16020133.

[50] Igboko UA, Temitope OA. Securing public health in the digital age: A cybersecurity case study of UK local council health services. Int J Sci Manag Res. 2025;7(4):98–115.

[51] Almutairi B. Integrating AI, blockchain, and cloud computing for enhanced e-government solutions. In: Digital government innovation. IGI Global; 2025. p. 213–28.

[52] Prosper J. A unified framework for securing digital ecosystems: Integrating cryptography, blockchain, AI, and IoT across smart cities, healthcare, and precision agriculture. ResGate. 2025.

[53] Ahakonye LAC, Nwakanma CI, Kim DS. Tides of blockchain in IoT cybersecurity. Sensors. 2024;24(10):3111. doi:10.3390/s24103111.

[54] Wylde V, Rawindaran N, Lawrence J. Cybersecurity, data privacy and blockchain: A review. SN Comput Sci. 2022;3(6):1020. doi:10.1007/s42979-022-01020-4.

[55] Zhang P, Zheng B, Ding H. Cybersecurity: Challenges, technologies and future trends. IEEE Access. 2025;13:11298–313. doi:10.1109/ACCESS.2025.11099896.

[56] Adegoke K, Adegoke A, Dawodu D, Bayowa A. Interoperability in digital healthcare: Enhancing consumer health and transforming care systems. Preprints. 2025. doi:10.20944/preprints202502.1774.v1.