International Journal of Advanced Digital Systems and Multidisciplinary Studies (IJADSMS),
Vol. 1, Issue 2, pp. 1–9, (2026)
Published: February 2026

Blockchain Security Architecture, Platforms, and Applications: A Comprehensive Review

Mr. Ajit Kumar[1], Ms. Lakshmi Kumari[2], Ms. Ku ma r i P uja [3] , Mr. Abhishek Kumar[4] , Mr. Samant Kumar[5], Ms. Anupama[6]
1 Assistant Professor , Amity Institute of Information Technology (AIIT), Amity University Jharkhand, Ranchi
2,3,4,6 Assistant Professor ,School of Computer Applications, Noida Institute of Engineering and Technology (NIET) Greater Noida
5 Assistant Professor ,Masters of computer Applications, Parul University, Vadodara, Gujrat
akumar7@rnc.amity.edu [1], lakshmi1051999@gmail.com[2], gkp2910@gmail.com[3],abhishek.kumar@niet.co.in[4] , samant91@gmail.com[5], anupama0140@gmail.com[6]

Abstract

Blockchain technology has emerged as a transformative paradigm for secure, decentralized data management across diverse domains, extending far beyond its origins in cryptocurrency. Despite its inherent attributes of decentralization, transparency, and immutability, the rapid evolution and widespread deployment of blockchain systems have introduced complex security challenges that demand systematic investigation. This paper presents a comprehensive review of blockchain security architecture, platforms, and applications through a structured analysis of existing literature. It examines the layered security model encompassing data, network, consensus, incentive, smart contract, and application layers, identifying critical vulnerabilities and attack vectors such as 51% attacks, Sybil attacks, smart contract exploits, and network-level threats. The study further evaluates major blockchain platforms—including public, private, and consortium models—highlighting their security mechanisms, trade-offs, and suitability for different use cases. Additionally, the review explores real-world applications in finance, healthcare, supply chain, IoT, and digital ownership, emphasizing domain-specific security implications and mitigation strategies. By synthesizing findings across multiple research dimensions, this work identifies prevailing challenges, emerging trends, and research gaps, underscoring the need for enhanced cryptographic methods, secure development practices, and governance frameworks. The paper contributes a holistic understanding of blockchain security and provides insights to guide future research toward building resilient and trustworthy blockchain ecosystems.

Keywords

Blockchain Security; Distributed Ledger Technology; Security Architecture; Smart Contracts; Consensus Mechanisms; Cybersecurity Threats; Blockchain Platforms; Permissioned and Permissionless Systems; Systematic Literature Review; Blockchain Applications

Introduction

Blockchain technology, initially conceptualized by Satoshi Nakamoto in 2008 as the foundational component of Bitcoin, has rapidly evolved into a transformative force across various sectors, moving beyond digital currencies to impact diverse fields such as finance, healthcare, supply chain management, and cybersecurity [1], [2], [3]. Its core characteristics—decentralization, immutability, transparency, and enhanced security through cryptographic techniques—offer significant advantages over traditional centralized systems [1], [3], [4]. Blockchain aims to solve problems of multi-party trust in transactions, reduce costs, and mitigate risks in traditional industries, potentially triggering an industrial revolution akin to the internet's impact [2].

Despite its promising potential and widespread adoption, the rapid development and expanding application scenarios of blockchain technology have brought forth a significant increase in security vulnerabilities and unique challenges [2], [3], [5]. While much research has focused on blockchain applications and the technology itself, less attention has been given to its security aspects [2]. Issues like smart contract flaws, 51% attacks, Sybil attacks, and other sophisticated cyber threats can undermine the integrity and trustworthiness of blockchain applications, leading to substantial economic losses [2], [6], [7]. The security of blockchain is still in its nascent stages, requiring continuous problem-solving and ongoing research to mature [2]. New demands for security and privacy protection in data storage, transmission, and applications continually emerge,

challenging existing solutions and authentication mechanisms [2].

This comprehensive review aims to bridge this gap by systematically analyzing the security threats, defense technologies, diverse platforms, and expansive applications of blockchain. We will delve into the layered security architecture of blockchain, examining vulnerabilities and potential attacks at the application, smart contract, incentive, consensus, network, and data layers [2], [8], [9]. Furthermore, the paper will explore various blockchain platforms, discussing their inherent security models, privacy features, and suitability for different applications [10], [11], [12], [13]. Finally, we will investigate the broad spectrum of blockchain applications across industries, highlighting how security considerations are addressed in practice and outlining the ongoing challenges and future research directions required to enhance the robustness and reliability of this groundbreaking technology [2], [14], [15].

Literature Review

The emergence of blockchain technology, since its inception with Bitcoin in 2008, has catalyzed a paradigm shift across numerous industries, moving beyond its initial application in digital currencies to encompass a broad spectrum of fields including finance, healthcare, supply chain management, and the Internet of Things [1], [2], [15]. This distributed ledger technology is characterized by decentralization, immutability, transparency, and robust security mechanisms, offering significant advantages over conventional centralized systems [1], [3], [4]. These inherent features aim to foster multi-party trust, reduce operational costs, and mitigate risks, thereby driving an industrial revolution similar to the impact of the internet [2]. Researchers and practitioners alike acknowledge the transformative potential of blockchain, with studies detailing its birth, development, and diverse applications [2].

Blockchain Security Architecture and Challenges

Despite the widespread adoption and rapid development of blockchain, the technology faces a growing number of security vulnerabilities and unique challenges [2], [3], [5]. Much of the existing literature has concentrated on the application and technological aspects of blockchain, often leaving its critical security dimensions underexplored [2]. The security landscape of blockchain is still in its nascent stages, necessitating continuous problem-solving and research to achieve maturity [2]. The escalating popularity of blockchain also introduces new demands for data storage, transmission, and application security and privacy, posing challenges to established security solutions, authentication protocols, and information regulation [2].

A comprehensive security analysis of blockchain typically considers a layered architecture, encompassing the application layer, smart contract layer, incentive layer, consensus layer, network layer, and data layer [2], [8], [9]. Each layer presents distinct security concerns. For instance, the application layer, particularly centralized nodes like cryptocurrency exchanges, is a frequent target for attackers due to the substantial funds they manage [2].

Vulnerabilities and Attack Vectors

Blockchain systems, while designed for security, are susceptible to various attacks that can compromise their integrity and lead to significant financial losses. The integrity of cryptographic primitives, such as SHA256 and elliptic curve cryptography, is crucial, and their long-term security, especially against advancements like quantum computing, is a subject of ongoing discussion [2]. If these fundamental cryptographic elements are compromised, the entire security framework of the blockchain could collapse [2]. Economic losses from blockchain security incidents have been substantial, with approximately $2.1 billion reported in 2018 alone due to digital currency theft and exchange hacks [2]. Attacks such as 51% attacks, double-spending, and smart contract vulnerabilities are frequently observed in real-world deployments, severely impacting the security and stability of blockchain systems [6], [16], [17].

Common consensus mechanisms like Proof of Work, Proof of Stake, and Delegated Proof of Stake are integral to blockchain operation but are not immune to attacks such as Bribe Attack, Long-Range Attack, Accumulation Attack, Precomputing Attack, and Sybil Attack [2]. Research indicates the need for more secure and faster consensus mechanisms that can withstand these threats [2]. The network layer, which facilitates information transmission via peer-to-peer (P2P) networks, also introduces vulnerabilities. The necessity for nodes to expose their IP addresses makes them susceptible to attacks, especially if individual nodes have weak security, potentially threatening the entire network [2]. Malicious information attacks, involving the insertion of harmful content into the blockchain, pose a unique challenge due to the data's immutable nature [2].

Security Measures and Defense Technologies

The growing threat landscape has spurred extensive research into enhancing blockchain security. Existing literature reviews highlight the importance of understanding attacks and implementing preventive measures [3]. Countermeasures discussed in various studies include advancements in consensus mechanisms, robust cryptographic techniques, and secure smart contract development practices [6], [16]. The implementation of formal verification methods, enhanced consensus protocols, and international collaboration are proposed to mitigate risks effectively [6].

Surveys in the field emphasize the need for continued research in blockchain anonymity and upper-level security, particularly for smart contract and application layers [2]. Solutions for securing smart contracts involve code analyzers and the development of secure smart contract libraries [18]. Furthermore, security practices extend to integrating blockchain with existing cybersecurity measures, advocating for multi-tiered approaches that include frequent security audits and network monitoring [10]. The evolution of security measures must continuously adapt to new attack vectors [3].

Blockchain Platforms and Their Security Features

Various blockchain platforms cater to different industrial needs, each with specific architectural designs, security models, and privacy features. These platforms can be broadly categorized into permissionless (public) and permissioned (private/consortium) blockchains. Permissionless platforms, such as Bitcoin and Ethereum, generally rely on computationally intensive consensus processes like PoW and allow any node to join the network [10], [11]. While offering high decentralization, they may face scalability issues and specific privacy challenges [10], [18].

Permissioned blockchain platforms, such as Hyperledger Fabric and Corda, offer enhanced security through access control layers that manage permissions for authorized nodes [10], [11]. These platforms are often preferred for enterprise solutions where greater control over participants and transactions is required. A comparative analysis of various platforms considers metrics such as security, performance, and specific features tailored for different applications [19], [20]. Research also delves into the suitability of these platforms for specific applications, such as IoT, by examining their architectures, security, privacy, and performance [11].

Applications and Security Implications

Blockchain technology's characteristics of decentralization, trust elimination, tamper-resistance, safety, and reliability have led to its wide adoption across numerous domains. These applications include financial services, credit and ownership management, trade management, cloud storage, user-generated content, copyright protection, advertising, and gaming [2]. Blockchain addresses challenges related to multi-party trust in transactions and helps reduce costs and risks in traditional industries [2].

Specific examples of blockchain applications include digital currency systems like Bitcoin, which demonstrate autonomous and reliable global real-time transactions [2]. Financial institutions are actively exploring blockchain to simplify transaction processes and reduce settlement costs in global securities trading [2]. Furthermore, blockchain is being utilized for ownership and copyright management, tracking valuables, and digital publications [2]. Securing these diverse applications requires addressing domain-specific challenges, including data privacy, identity management, and the protection of sensitive information, particularly in sectors like healthcare [21]. The integration of blockchain with other technologies, such as AI and cloud computing, also necessitates robust security frameworks for digital ecosystems [22]. The ongoing evolution of blockchain technology continues to present challenges and opportunities for improving security across its ever-expanding application landscape [23].

Methodology

This comprehensive review employs a Systematic Literature Review methodology to systematically identify, evaluate, and synthesize existing research on blockchain security architecture, platforms, and applications. This approach ensures a rigorous, transparent, and reproducible process for gathering and analyzing the vast body of literature, aligning with established guidelines for conducting comprehensive reviews [22], [24], [25], [26], [27].

1. Research Questions

To guide this comprehensive review, the following primary research questions were formulated:

- RQ1: What are the prevalent security architectures and mechanisms employed within blockchain technologies?
- RQ2: What are the key features, advantages, and limitations of various blockchain platforms concerning security, scalability, and application suitability?
- RQ3: How is blockchain technology being applied across different sectors, and what are the specific security considerations and challenges within these applications?
- RQ4: What are the current and emerging security threats to blockchain systems, and what mitigation strategies are proposed in the literature?

2. Search Strategy

A multi-database search strategy was executed across prominent academic databases to capture a broad and representative spectrum of relevant literature. The selected databases include IEEE Xplore, ACM Digital Library, Scopus, Web of Science, SpringerLink, and Google Scholar [28]. The search was conducted using a combination of keywords and their synonyms, structured with Boolean operators. The primary search terms included:

- "Blockchain" OR "Distributed Ledger Technology" OR "DLT"
- "Security Architecture" OR "Security Model" OR "Security Mechanisms" OR "Threats" OR "Vulnerabilities" OR "Attacks" OR "Cybersecurity"
- "Platforms" OR "Frameworks" OR "Ecosystems" OR "Protocols"
- "Applications" OR "Use Cases" OR "Implementations" OR "Sectors"
- "Review" OR "Survey" OR "Comprehensive Analysis" OR "State-of-the-Art"

The search was refined to include publications primarily from 2016 onwards, reflecting the significant acceleration of blockchain research following its initial applications, and extending to the most current available research [24].

3. Study Selection Criteria

The identified studies were subjected to a rigorous two-stage selection process based on predefined inclusion and exclusion criteria [24].

Inclusion Criteria:

- Peer-reviewed journal articles, conference papers, and comprehensive review articles.
- Publications written in English.

- Studies focusing on blockchain technology, distributed ledger technology, or related cryptographic systems.
- Research addressing security aspects (vulnerabilities, threats, architectures, countermeasures), different platforms (public, private, consortium), and real-world applications of blockchain.
- Papers that provide empirical, theoretical, or review-based insights relevant to the research questions.

Exclusion Criteria:

- Non-academic publications (e.g., blog posts, news articles, whitepapers without academic rigor).
- Studies primarily focusing on cryptocurrency economics or market analysis without significant technical or security discussions.
- Duplicate publications.
- Papers not directly relevant to blockchain security, architecture, platforms, or applications.

The initial search results were screened based on titles and abstracts. Subsequently, the full text of potentially relevant articles was retrieved and reviewed against the inclusion and exclusion criteria to ensure the selection of highly pertinent studies.

4. Data Extraction and Synthesis

For each selected study, relevant data were systematically extracted, organized, and categorized. The extracted data points included:

- Publication details (authors, year, venue).
- Blockchain type (public, private, consortium).
- Security features and mechanisms discussed.
- Identified vulnerabilities, threats, and attack vectors.
- Proposed countermeasures and mitigation strategies.
- Specific blockchain platforms analyzed.
- Application domains and use cases.
- Challenges and future research directions.

The extracted information was then synthesized using a thematic analysis approach. This involved identifying recurring themes, categorizing security vulnerabilities by blockchain layer, mapping platform features to security properties, and consolidating insights regarding blockchain applications and their security implications. Comparative tables and conceptual models were developed to illustrate key findings, contrasting different approaches to blockchain security, platform designs, and application-specific challenges. This systematic process ensured that the review comprehensively addressed the formulated research questions and provided a holistic understanding of the current landscape of blockchain security architecture, platforms, and applications.

Results

The systematic literature review yielded significant insights into the intricate landscape of blockchain security architecture, the diverse array of platforms, and their varied applications, alongside the persistent challenges and proposed mitigation strategies. The findings are structured to address the research questions posed in the methodology.

1. Blockchain Security Architecture and Threat Landscape

(RQ1: What are the prevalent security architectures and mechanisms employed within blockchain technologies? & RQ4: What are the current and emerging security threats to blockchain systems, and what mitigation strategies are proposed in the literature?)

Blockchain security is best understood through a layered architecture, where each layer presents distinct vulnerabilities and requires specific defense mechanisms. This review identifies six primary layers: data, network, consensus, incentive, smart contract, and application layers [2].

1.1 Layered Security Model and Vulnerabilities

- Data Layer: This foundational layer relies heavily on cryptographic primitives like SHA256 hash functions and elliptic curve cryptography to ensure data integrity and immutability [2]. However, the immutability of data also poses a challenge as malicious information, once written, is difficult to remove, potentially leading to the spread of illegal or undesirable content [2]. The long-term security of current cryptographic algorithms against future threats, such as quantum computing, remains a topic of discussion [2].
- Network Layer: Blockchain networks operate on a peer-to-peer (P2P) model, where information transmission exposes nodes' IP addresses, making them susceptible to attacks. Common threats include Eclipse attacks, where a node is isolated by hostile peers, and BGP hijacking, which can allow attackers to control a significant portion of network traffic [2]. Distributed Denial of Service attacks are also a significant concern, capable of disrupting services and causing substantial downtime, as seen in past exchange attacks [2].
- Consensus Layer: The consensus mechanism is critical for validating transactions and maintaining the blockchain's integrity. While mechanisms like Proof of Work, Proof of Stake, and Delegated Proof of Stake are widely used, they are vulnerable to various attacks. These include 51% attacks, where an entity gains control of more than half of the network's hash power, potentially monopolizing mining rights and disrupting the credit system [2], [29], [30]. Other attacks comprise Bribe Attack, Long-Range Attack, Accumulation Attack, Precomputing Attack, and Sybil Attack [2].
- Incentive Layer: This layer is designed to encourage node participation in security verification. However, if the cost of participation (e.g., computing resources, electricity) outweighs the rewards, nodes may withdraw, potentially

leading to centralization problems and reducing overall network security [2].

- Smart Contract Layer: Smart contracts, while offering automated execution, introduce new vulnerabilities. Identified attack vectors include reentrancy attacks (e.g., The DAO hack), transaction-ordering dependence, integer overflow/underflow, and unauthorized access due to improper function visibility or insufficient permission checks [2], [9], [31]. The open-source nature of many smart contracts can lower the cost for attackers to identify and exploit flaws [29].

- Application Layer: Security issues at this layer often stem from centralized components, such as cryptocurrency exchanges, which manage large funds and are frequent targets for attacks. These can include unauthorized access to exchange servers, leading to data breaches (e.g., Mt.Gox attack), and user-centric attacks like phishing [2].

1.2 Mitigation Strategies

A multi-faceted approach is required to address the diverse threats.

- Network Layer: Enhanced P2P network security and robust network authentication mechanisms, including reliable encryption algorithms for data transmission and necessary verification for important operations [2]. Diversifying node connections and implementing secure peer detection protocols can counter eclipse attacks [29].

- Consensus Layer: Adopting alternative consensus mechanisms like PoS can reduce susceptibility to 51% attacks compared to PoW systems [29]. Ongoing research is necessary to explore more secure and faster consensus mechanisms [2].

- Smart Contract Layer: Developers must conduct thorough security tests before deployment, perform regular code audits, monitor deployed contracts for abnormal behavior, and adhere to secure coding practices [2], [3]. Utilizing standard mathematical libraries can mitigate overflow/underflow issues [9].

- Application Layer: Application developers must ensure software is free of known vulnerabilities and rigorously tested. Centralized entities like trading platforms require real-time system health monitoring and protected methods like data encryption storage. User education on secure account and key management, and distinguishing true from false information, is crucial against phishing [2].

- General Measures: Collaborative security solutions are urgent to improve overall blockchain system security [2]. Further research into strengthening privacy protection through anonymous protection mechanisms or new blockchain designs (e.g., Zerocash) is also important [2]. Quantum-resistant cryptographic algorithms are also being explored [32].

2. Analysis of Blockchain Platforms

(RQ2: What are the key features, advantages, and limitations of various blockchain platforms concerning security, scalability, and application suitability?)

Blockchain platforms are generally categorized into public (permissionless) and private/consortium (permissioned) blockchains, each offering distinct characteristics impacting their security, scalability, and suitability for different applications [2].

- Public Blockchains:

  - Characteristics: Open access (anyone can join, send transactions, and validate), high decentralization, participants' anonymity, and complete data transparency [2], [33], [34]. Examples include Bitcoin and Ethereum.

  - Security: Offer a high level of security due to extensive decentralization and consensus protocols, making it difficult for any single attacker to tamper with information [34], [35]. Cryptographic security ensures data immutability and non-repudiation [33].

  - Limitations: Can suffer from scalability issues (e.g., transaction throughput), privacy concerns due to public ledgers, and high energy consumption (especially PoW-based) [10], [18], [36]. Vulnerable to 51% attacks if a single entity gains majority control [30], [37].

  - Suitability: Ideal for scenarios requiring maximum decentralization, transparency, and trust minimization among unknown participants, such as cryptocurrencies [35].

- Private/Permissioned Blockchains:

  - Characteristics: Restricted access (only authorized participants can join and write transactions), greater control over participants and data, and varying degrees of transparency (public or limited reading rights) [2], [33], [38]. Examples include Hyperledger Fabric and Corda.

  - Security: Enhanced security through access control layers, which manage permissions for authorized nodes. They can be configured to comply with specific regulations (e.g., HIPAA, GDPR) [30]. Lower number of nodes can make them more susceptible to control by malicious actors compared to highly decentralized public chains [34].

  - Limitations: Less decentralized than public blockchains, which can lead to higher risks of hacking and data manipulation if not properly secured, as fewer nodes mean easier control for bad actors [34]. May lack the same level of cryptographic security as public chains, depending on their design [33].

  - Suitability: Preferred for enterprise solutions requiring greater control, privacy, and performance, such as internal company database management, auditing, and regulated industries [2], [11].

- Consortium Blockchains:

  - Characteristics: A hybrid model where the consensus process is controlled by a pre-selected group of nodes (e.g., multiple financial institutions) [2]. They combine features of both public and private blockchains [34].

- Security: Offer a balance between decentralization and control, with security mechanisms often tailored to the specific consortium's needs.
- Suitability: Suitable for inter-organizational collaborations where multiple parties need to share data and processes securely, but with defined governance [2].

3. Applications and Security Considerations

(RQ3: How is blockchain technology being applied across different sectors, and what are the specific security considerations and challenges within these applications?)

Blockchain's intrinsic features like decentralization, immutability, and tamper-resistance have driven its adoption across numerous sectors, each presenting unique security considerations.

- Financial Services: Blockchain supports autonomous and reliable real-time transactions, simplifying processes and reducing settlement costs in global securities trading [2]. Security here focuses on protecting large fund holdings, preventing cyberattacks on exchanges (e.g., DDoS), and ensuring the integrity of financial data [2].
- Supply Chain Management: Blockchain enhances traceability, transparency, and trust among supply chain participants [29], [36]. Key security challenges include scalability limitations, interoperability barriers across diverse platforms, high implementation costs, and data privacy concerns, particularly when sensitive operational or commercial information is shared [36], [39]. Solutions often involve off-chain data storage for large datasets (e.g., IPFS) to reduce transaction costs and improve scalability, while storing hashes on-chain for integrity verification [39].
- Healthcare: Blockchain offers potential for secure data sharing, patient record management, and drug traceability. However, ensuring patient data privacy is paramount, necessitating compliance with regulations like HIPAA and GDPR [30], [40]. Public blockchains are generally unsuitable for sensitive healthcare data due to their public nature; permissioned or consortium blockchains are often preferred to manage access and permissions [41]. Vulnerabilities like 51% attacks and data integrity threats remain a concern [40], [42].
- Internet of Things: Blockchain can secure IoT ecosystems by providing a decentralized and tamper-proof ledger for device interactions and data. Security concerns include data integrity attacks (e.g., data tampering, rogue data injection), confidentiality attacks (e.g., packet sniffing), and availability threats like distributed denial of sleep attacks on embedded devices [43]. Interoperability among diverse IoT platforms and blockchain solutions is also a challenge [43].
- Ownership and Copyright Management: Blockchain can track valuables and manage digital publications, offering inherent data security and effective privacy protection [2]. The security here focuses on preventing unauthorized access and ensuring the integrity of ownership records.

Across these applications, a common theme is the need to balance the benefits of blockchain (e.g., decentralization, immutability) with practical considerations such as scalability, privacy, and integration with existing systems. The shift from theoretical models to practical implementations continues to uncover new security challenges that require ongoing research and robust mitigation strategies.

Discussion

This comprehensive review has elucidated the multifaceted landscape of blockchain security, architecture, platforms, and their applications, revealing a dynamic interplay between technological innovation and persistent challenges. The findings underscore that while blockchain offers unprecedented opportunities for secure, decentralized systems, its successful deployment hinges on a deep understanding and proactive mitigation of its inherent vulnerabilities.

Blockchain technology is often lauded as "trustless," implying that it eliminates the need for trusted third parties. However, our findings suggest a more nuanced understanding of trust in these systems. Instead of eliminating trust, blockchain fundamentally redistributes it, shifting reliance from human intermediaries to the underlying cryptographic protocols, consensus mechanisms, and the collective community that maintains the network [44], [45]. This shift brings algorithmic trust to the forefront, yet the integrity of this trust is constantly tested by vulnerabilities at various layers. Security incidents, whether due to smart contract flaws or network attacks, can significantly erode user and institutional confidence, directly impacting adoption rates and the perceived legitimacy of blockchain systems [2], [46]. Therefore, fostering a truly trustworthy blockchain ecosystem requires not only robust technical safeguards but also transparent governance models and effective incident response strategies.

Conclusion

In conclusion, while blockchain technology presents a transformative paradigm with its core attributes of decentralization, immutability, and transparency [1], [2], [3], [4], its secure and widespread adoption is critically dependent on addressing its multifaceted security challenges. This review underscores that vulnerabilities are inherent across its layered architecture—from cryptographic primitives and consensus mechanisms susceptible to attacks like 51% threats [2], [29], [30], to smart contracts prone to reentrancy and other exploits requiring rigorous formal verification [2], [9], [31], [47], [48], [49]. The diverse landscape of blockchain platforms, encompassing public and private implementations, reveals a fundamental trade-off among decentralization, security, and scalability, often termed the "blockchain trilemma" [50], [51], [52]. Furthermore, the application of blockchain across vital sectors such as finance, supply chain, healthcare, and IoT introduces distinct security and privacy demands [2], [30], [36], [39], [40], [41], [43], indicating that no single security solution is universally applicable. Ultimately, the successful evolution of blockchain necessitates a nuanced understanding of trust redistribution

[44], [45], [46], continuous advancements in cryptography and formal methods [47], [48], [53], [54], [55], and robust governance frameworks [56], [57], [58] to ensure its resilience and integrity in an ever-evolving digital landscape [2], [23].

References

[1] A. N. S. Putro, S. Mokodenseho, N. A. Hunawa, M. Mokoginta, and E. R. M. Marjoni, "Enhancing Security and Reliability of Information Systems through Blockchain Technology: A Case Study on Impacts and Potential," West Science Information System and Technology , vol. 1, no. 1, p. 35, Aug. 2023, doi: 10.58812/wsist.v1i01.166.

[2] X. Yun, W. Wen, B. Lang, H. Yan, L. Ding, J. Li, and Y. Zhou, Eds., Cyber Security: 15th International Annual Conference, CNCERT 2018, Beijing, China, Aug. 14–16, 2018, Revised Selected Papers, Communications in Computer and Information Science, vol. 970. Singapore: Springer, 2019.

[3] B. Saha, Md. M. Hasan, N. Anjum, S. Tahora, A. Siddika, and H. Shahriar, "Protecting the Decentralized Future: An Exploration of Common Blockchain Attacks and their Countermeasures," arXiv (Cornell University) , Jun. 2023, doi: 10.48550/arxiv.2306.11884.

[4] B. Y. Supriya et al. , "Advancement and Innovation in Blockchain and Cryptography: A Comparative Analysis of Traditional Systems and Emerging Solutions," International Journal for Research in Applied Science and Engineering Technology , vol. 12, no. 11, p. 2119, Nov. 2024, doi: 10.22214/ijraset.2024.65466.

[5] K. Dwivedi, A. Agrawal, A. Bhatia, and K. Tiwari, "A Novel Classification of Attacks on Blockchain Layers: Vulnerabilities, Attacks, Mitigations, and Research Directions," 2024, doi: 10.48550/ARXIV.2404.18090.

[6] U. Ahsan and M. Zafar, "Blockchain Security: Vulnerabilities and Protective Measures," World Journal of Advanced Research and Reviews , vol. 25, no. 3, p. 1056, Mar. 2025, doi: 10.30574/wjarr.2025.25.3.0791.

[7] M. Javadi, "BLOCKCHAIN IN SECURITY: EVOLUTION,
PPLICATIONS AND CHALLENGES," International Journal of Advanced Research in Computer Science , vol. 13, no. 5, p. 18, Oct. 2022, doi: 10.26483/ijarcs.v13i5.6913.

[8] J. Das, S. A. A. Tasin, Md. F. Rabbi, and M. S. Ferdous, "Analysing Attacks on Blockchain Systems in a Layer-based Approach," arXiv (Cornell University) , Sep. 2024, doi: 10.48550/arxiv.2409.10109.

[9] 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.

[10] W. S. Khorseed and A. H. Hamad, "Inter and Intra Domain DDoS Attack Mitigation for Software Defined
Network Based on Hyperledger Fabric Blockchain Technology," Ingénierie des systèmes d information , vol. 29, no. 1, p. 301, Feb. 2024, doi: 10.18280/isi.290130.

[11] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance," Computer Networks , vol. 191, p. 108005, Mar. 2021, doi: 10.1016/j.comnet.2021.108005.

[12] T. Bayan, R. Banach, A. Nurbekov, M. M. Galy, A. Sabyrbayev, and Z. Nurbekova, "Blockchain-enhanced Integrity Verification in Educational Content Assessment Platform: A Lightweight and Cost-Efficient Approach," arXiv (Cornell University) , Sep. 2024, doi: 10.48550/arxiv.2409.19828.

[13] K. Saito et al. , "Requirement Analyses and Evaluations of Blockchain Platforms per Possible Use Cases," arXiv (Cornell University) , Mar. 2021, Accessed: Mar. 2025. [Online]. Available: http://arxiv.org/abs/2103.03209

[14] M. Pandey, M. S. Velmurugan, G. Sathi, A. R. Abbas, N. Zebo, and T. Sathish, "Blockchain Technology: Applications and Challenges in Computer Science," E3S Web of Conferences , vol. 399, p. 4035, Jan. 2023, doi: 10.1051/e3sconf/202339904035.

[15] A. M. Alqahtani and A. Algarni, "A Survey on Blockchain Technology Concepts, Applications and Security," International Journal of Advanced Computer Science and Applications , vol. 14, no. 2, Jan. 2023, doi: 10.14569/ijacsa.2023.0140296.

[16] K. Kumar, D. Kumar, S. Baghel, and K. Arora, "Blockchain Security: Threats, Vulnerabilities and Countermeasures -A Review," SSRN Electronic Journal , Jan. 2025, doi: 10.2139/ssrn.5221226.

[17] X. Li et al. , "Blockchain Security Threats and Collaborative Defense: A Literature Review," Computers, materials & continua/Computers, materials & continua (Print) , vol. 76, no. 3. p. 2597, Jan. 01, 2023. doi: 10.32604/cmc.2023.040596.

[18] B. Bellaj, A. Ouaddah, E. Bertin, N. Crespi, and A. Mezrioui, "SOK: A Comprehensive Survey on Distributed Ledger Technologies," in 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) , May 2022, p. 1. doi: 10.1109/icbc54727.2022.9805533.

[19] C. Connors and D. Sarkar, "Comparative Study of Blockchain Development Platforms: Features and Applications," arXiv (Cornell University) , Oct. 2022, doi: 10.48550/arxiv.2210.01913.

[20] S. D. Angelis, F. Lombardi, G. Zanfino, L. Aniello, and
V. Sassone, "Security and dependability analysis of blockchain systems in partially synchronous networks with Byzantine faults," International Journal of Parallel Emergent and Distributed Systems , p. 1, Oct. 2023, doi: 10.1080/17445760.2023.2272777.

[21] R. D. Garcia et al. , "A Survey of Blockchain-Based Privacy Applications: An Analysis of Consent

Management and Self-Sovereign Identity Approaches," arXiv (Cornell University) , Nov. 2024, doi: 10.48550/arxiv.2411.16404.

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

[23] A. Tariq, T. Qayyum, S. Alrabaee, and M. A. Serhani, "Blockchain and Distributed Ledger Technologies for Cyberthreat Intelligence Sharing," arXiv (Cornell University) , Apr. 2025, doi: 10.48550/arxiv.2504.02537.

[24] 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.

[25] W. Charles et al. , "Blockchain-Based Dynamic Consent: Protocol for an Integrative Review of Applications for Patient-Centric Research and Health Information Sharing (Preprint)," JMIR Research Protocols , vol. 13, Dec. 2023, doi: 10.2196/50339.

[26] H. K. Alay, "Evaluating Research Trends on The Emerging Blockchain Technology In The Fields of Business And Management: A Systematic Review," DergiPark (Istanbul University) . Istanbul University, Sep. 15, 2022. Accessed: Oct. 2025. [Online]. Available: https://dergipark.org.tr/tr/pub/joeep/issue/69748/117569 6

[27] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PLoS ONE , vol. 11, no. 10. Public Library of Science, Oct. 03, 2016. doi: 10.1371/journal.pone.0163477.

[28] D. Liu, J. Zhang, Y. Wang, H. Shen, Z. Zhang, and T. Ye, "Blockchain Smart Contract Security: Threats and Mitigation Strategies in a Lifecycle Perspective," ACM Computing Surveys , vol. 58, no. 4, p. 1, Sep. 2025, doi: 10.1145/3769013.

[29] 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.

[30] N. E. Madhoun and B. Hammi, "Blockchain Technology in the Healthcare Sector: Overview and Security Analysis," in 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) , Jan. 2024, p. 439. doi: 10.1109/ccwc60891.2024.10427731.

[31] W. Haouari, A. Hafid, and M. Fokaefs, "Vulnerabilities of smart contracts and mitigation schemes: A Comprehensive Survey," arXiv (Cornell University) , Apr. 2024, doi: 10.48550/arxiv.2403.19805.

[32] K. Kumar, D. Kumar, S. Baghel, and K. Arora, "Blockchain Security: Threats, Vulnerabilities and Countermeasures - A Review." Jan. 01, 2025. doi: 10.2139/ssrn.5066915.

[33] S. R. Fahim, S. K. Rahman, and S. Mahmood, "Blockchain: A Comparative Study of Consensus Algorithms PoW, PoS, PoA, PoV," International Journal of Mathematical Sciences and Computing , vol. 9, no. 3, p. 46, Aug. 2023, doi: 10.5815/ijmsc.2023.03.04.

[34] M. Xiao, C. Xiao-bo, M. Wang, Y. Han, and X. XU, "Application decision model of blockchain technology in construction supply chain," Research Square (Research Square) , Apr. 2024, doi: 10.21203/rs.3.rs-4133660/v1.

[35] G. Llambías, L. González, and R. Ruggia, "Blockchain Interoperability: a Feature-based Classification Framework and Challenges Ahead," CLEI electronic journal , vol. 25, no. 3, Mar. 2023, doi: 10.19153/cleiej.25.3.4.

[36] M. Khatun and T. Darwish, "Unlocking Blockchain's Potential in Supply Chain Management: A Review of Challenges, Applications, and Emerging Solutions," Network
, vol. 5, no. 3. Multidisciplinary Digital Publishing Institute, p. 34, Aug. 26, 2025. doi: 10.3390/network5030034.

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

[38] N. Gupta and A. K. Jain, "RSA Based Consensus Algorithm for Lightweight Private Blockchain Network," ITM Web of Conferences , vol. 54, p. 3003, Jan. 2023, doi: 10.1051/itmconf/20235403003.

[39] E. K. Kambilo, I. Rychkova, N. Herbaut, and C. Souveyet, "Addressing Trust Issues in Supply-Chain Management Systems Through Blockchain Software Patterns," in Lecture notes in business information processing , Springer Science+Business Media, 2023, p. 275. doi: 10.1007/978-3-031-33080-3_17.

[40] A. Atadoga, O. A. Elufioye, T. T. Omaghomi, O. Akomolafe, I. P. Odilibe, and O. R. Owolabi, "Blockchain in healthcare: A comprehensive review of applications and security concerns," International Journal of Science and Research Archive , vol. 11, no. 1. p. 1605, Feb. 12, 2024. doi: 10.30574/ijsra.2024.11.1.0244.

[41] A. H. Allam, I. Gomaa, H. H. Zayed, and M. Taha, "IoT-based eHealth using blockchain technology: a survey," Cluster Computing , vol. 27, no. 6, p. 7083, Apr. 2024, doi: 10.1007/s10586-024-04357-y.

[42] J. Malla, H. Singathala, and V. M. Viswanatham, "An Analysis of the Blockchain Based E-Healthcare Systems using a Bibliometric Study," Research Square (Research Square) , Sep. 2023, doi: 10.21203/rs.3.rs-3330423/v1.

[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] E. Poll, "Engineering the trust machine. Aligning the concept of trust in the context of blockchain applications,"

Ethics and Information Technology , vol. 26, no. 2, Jun. 2024, doi: 10.1007/s10676-024-09774-6.

[45] É. Toufaily and T. Zalan, “In blockchain we trust? Demystifying the ‘trust’ mechanism in blockchain ecosystems,” Technological Forecasting and Social Change , vol. 206, p. 123574, Jul. 2024, doi: 10.1016/j.techfore.2024.123574.

[46] N. B. Truong, G. M. Lee, K. Sun, F. Guitton, and Y. Guo, “A Blockchain-based Trust System for Decentralised Applications: When trustless needs trust,” arXiv (Cornell University) , Feb. 2022, doi: 10.48550/arxiv.2101.10920.

[47] İ. Mustafa, A. McGibney, and S. Rea, “Smart contract life-cycle management: an engineering framework for the generation of robust and verifiable smart contracts,” Frontiers in Blockchain , vol. 6, Jan. 2024, doi: 10.3389/fbloc.2023.1276233.

[48] N. K. Singh, A. M. Fajge, R. Halder, and Md. I. Alam, “Formal verification and code generation for solidity smart contracts,” in Elsevier eBooks , Elsevier BV, 2023, p. 125. doi: 10.1016/b978-0-323-96146-2.00028-0.

[49] K. Bhargavan et al. , “Formal Verification of Smart Contracts,” p. 91, Oct. 2016, doi: 10.1145/2993600.2993611.

[50] N. Kannengießer, S. Lins, T. Dehling, and A. Sunyaev, “What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs,” in Proceedings of the ... Annual Hawaii International Conference on System Sciences/Proceedings of the Annual Hawaii International Conference on System Sciences , Jan. 2019. doi: 10.24251/hicss.2019.848.

[51] S. Reno and K. Roy, “Navigating the Blockchain Trilemma: A Review of Recent Advances and Emerging Solutions in Decentralization, Security, and Scalability Optimization,” Computers, materials & continua/Computers, materials & continua (Print) , vol. 84, no. 2. p. 2061, Jan. 01, 2025. doi: 10.32604/cmc.2025.066366.

[52] M. Aliyu, N. Kannengießer, and K. Braune, “From Concept to Measurement: A Survey of How the Blockchain Trilemma Is Analyzed,” arXiv (Cornell University) , Apr. 2025, doi: 10.48550/arxiv.2505.03768.

[53] M. Tarawneh, “Cryptography: Recent Advances and Research Perspectives,” in IntechOpen eBooks , IntechOpen, 2024. doi: 10.5772/intechopen.111847.

[54] S. Schwerin, “Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study,” The Journal of British Blockchain Association , vol. 1, no. 1, p. 1, Jun. 2018, doi: 10.31585/jbba-1-1-(4)2018.

[55] P. Feng et al. , “Mastering AI: Big Data, Deep Learning, and the Evolution of Large Language Models -- Blockchain and Applications,” arXiv (Cornell University) , Oct. 2024, doi: 10.48550/arxiv.2410.10110.

[56] Y. Liu, Q. Lu, L. Zhu, H.-Y. Paik, and M. Staples, “A systematic literature review on blockchain governance,” Journal of Systems and Software , vol. 197, p. 111576, Dec. 2022, doi: 10.1016/j.jss.2022.111576.

[57] P. D. Filippi, S. Cossar, S. Primavera, T. Nabben, J. Merk, and K. Nabben, “Report on Blockchain Governance Dynamics,” Centre National de la Recherche Scientifique, May 2024. doi: 10.1080/24701475.2023.218364.

[58] Y. Liu, Q. Lu, G. Yu, H.-Y. Paik, H. Perera, and L. Zhu, “A Pattern Language for Blockchain Governance,” p. 1, Jul. 2022, doi: 10.1145/3551902.3564802.