Jurnal ELTIKOM :
Jurnal Teknik Elektro, Teknologi Informasi dan Komputer

Vol. 9, No. 2, December 2025, page. 196-205
ISSN 2598-3245 (Print), ISSN 2598-3288 (Online)
DOI: http://doi.org/10.31961/eltikom.v9i2.1701
Available online at http://eltikom.poliban.ac.id

THE SYNERGY OF BLOCKCHAIN AND CYBERSECURITY: BUILDING TRUST IN DIGITAL ENVIRONMENTS

Hewa Majeed Zangana[1*], Zina Bibo Sallow[2], Firas Mahmood Mustafa[3], Mamo Muhamad Husain[1]

[1)] IT Department, Duhok Technical College, Duhok Polytechnic University, Duhok, Iraq
[2)] Computer System Department, Ararat Technical Private Institute, Kurdistan Region, Iraq
[3)] Chemical Engineering Dept., Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq
e-mail: hewa.zangana@dpu.edu.krd, zina.salo@araratpti.edu.krd, firas.mahmoud@dpu.edu.krd, mamo.husain@dpu.edu.krd

Received: 29 June 2025 – Revised: 5 August 2025 – Accepted: 12 August 2025

ABSTRACT

The rapid expansion of digital ecosystems has intensified concerns about data security, privacy, and trust. Blockchain technology, characterized by its decentralized, immutable, and transparent nature, of-fers a transformative approach to strengthening cybersecurity. This paper examines the synergy between blockchain and cybersecurity, emphasizing how blockchain's cryptographic foundations, consensus mechanisms, and smart contracts can mitigate cyber threats, enhance authentication, and ensure data integrity. By analyzing emerging trends, challenges, and real-world applications, this study underscores the potential of blockchain to reinforce digital trust and resilience across diverse sectors. The findings contribute to the ongoing discourse on secure digital environments by proposing an integrated framework for blockchain-based cybersecurity solutions

Keywords*: blockchain, cryptography, cybersecurity, digital trust, smart contracts.*

I. INTRODUCTION

THE increasing reliance on digital infrastructures has amplified concerns about cybersecurity threats, data breaches, and identity fraud. Traditional security mechanisms, although effective to some extent, often fail to counter sophisticated cyberattacks, necessitating the exploration of innovative solutions. Blockchain technology has emerged as a potential game-changer in the cybersecurity domain, offering decentralized, immutable, and transparent security frameworks [1]. By leveraging cryptographic techniques, consensus mechanisms, and smart contracts, blockchain enhances data integrity, access control, and secure communication [2], [3].

The integration of blockchain and cybersecurity is gaining momentum across various industries, including financial services, healthcare, supply chain management, and critical infrastructure protection [4]. This synergy is particularly relevant in addressing challenges such as data tampering, unauthorized access, and distributed denial-of-service (DDoS) attacks [5], [6]. The decentralized nature of blockchain reduces single points of failure, mitigating risks associated with centralized data storage and strengthening trust in digital environments [7].

Despite its potential, blockchain-based cybersecurity solutions face persistent challenges, including scalability, energy consumption, and regulatory uncertainties [8]–[12]. Moreover, while blockchain can strengthen cybersecurity, it remains vulnerable to issues such as smart contract exploits and 51% attacks [13], [14]. Therefore, a comprehensive approach is required to integrate blockchain technology effectively within cybersecurity frameworks while addressing its inherent limitations [15].

Although several studies have examined blockchain applications in cybersecurity, most focus on technical aspects or isolated sectoral use cases without providing a consolidated synthesis. Furthermore, there is a lack of integrative frameworks analyzing the interplay among blockchain mechanisms, industry adoption, regulatory influences, and future innovations. This literature review seeks to fill this

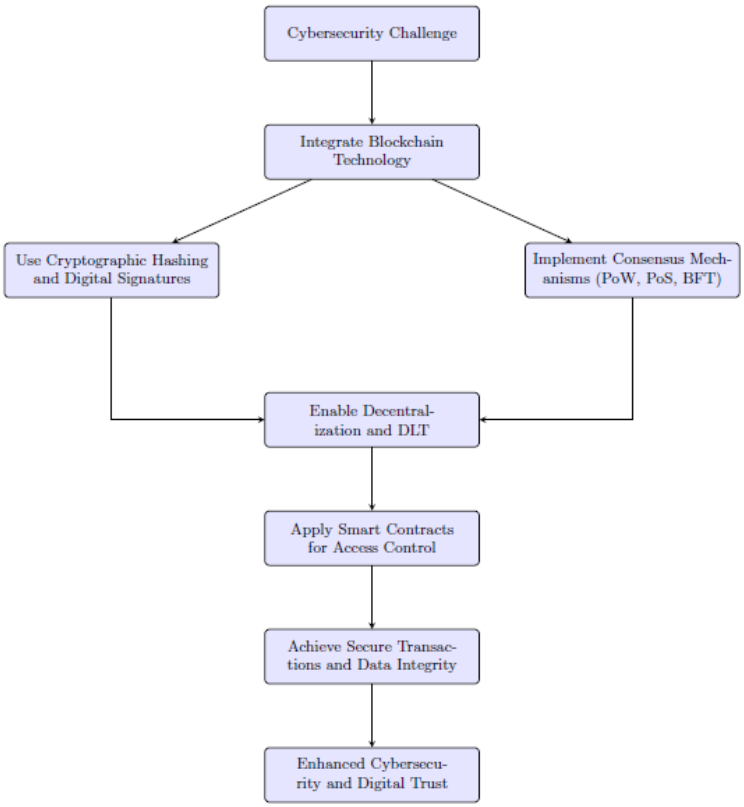

Figure 1. Blockchain-Based Cybersecurity Framework (Adapted and synthesized by the authors based on insights from [6], [7], [16], and [17])

gap by systematically analyzing peer-reviewed research, developing a conceptual taxonomy, and identifying sector-specific challenges and trends that inform future adoption.

This paper investigates the integration of blockchain into cybersecurity through the lens of a central research question: How can blockchain-based mechanisms enhance cybersecurity across critical sectors while addressing key challenges such as scalability and regulation? By answering this question, the study aims to synthesize existing literature and propose a conceptual taxonomy that consolidates key applications, limitations, and innovations in the field.

II. LITERATURE REVIEW

The intersection of blockchain and cybersecurity has been extensively explored in both academic and industry research. Blockchain is recognized for its capacity to enhance security through decentralization, cryptographic techniques, and consensus mechanisms. This section reviews existing literature on blockchain's role in cybersecurity, focusing on its applications, advantages, challenges, and future directions.

A. Blockchain for Cybersecurity

Blockchain technology has been proposed as a solution to multiple cybersecurity challenges, particularly in securing financial transactions, protecting identity management, and preventing data breaches [16], [17]. Antonyan [7] emphasize blockchain’s capacity to mitigate cyber threats by providing immutable records and decentralized control, thereby reducing the risk of data manipulation. Similarly, Hasanova [6] present a survey identifying blockchain vulnerabilities and countermeasures, demonstrating its resilience against common cyberattacks.

The integration of blockchain technology into cybersecurity follows a structured approach that enhances data protection, ensures secure transactions, and mitigates cyber threats. The flowchart below presents a blockchain-based cybersecurity framework, outlining key security features and mechanisms that safeguard digital environments.

Figure 1 illustrates a Blockchain-Based Cybersecurity Framework designed to address key digital threats through multiple structured layers. The framework begins with identifying a cybersecurity

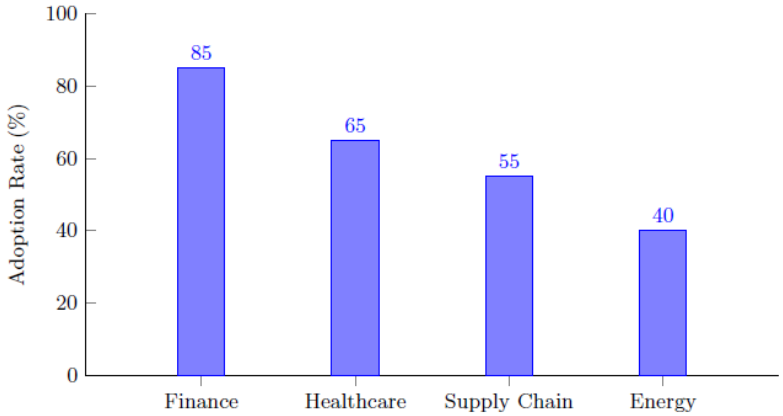

Figure 2. Blockchain Adoption in Different Industries for Cybersecurity (Data derived from synthesized findings across [13], [20], [21], [22], and [25], reflecting estimated adoption trends as of 2023)

challenge, followed by the integration of blockchain technology as a foundational defense. This includes the use of cryptographic hashing and digital signatures to protect data integrity and authenticity. Concurrently, implementing consensus mechanisms such as PoW, PoS, or BFT ensures trustless transaction validation. Together, these components enable decentralization and distributed ledger technology (DLT), eliminating single points of failure. Smart contracts are applied to automate access control and policy enforcement. These mechanisms collectively achieve secure transactions and data integrity, resulting in enhanced cybersecurity and stronger digital trust.

To advance the originality and analytical depth of this study, a conceptual taxonomy is proposed to outline the integration of blockchain into cybersecurity practices across domains, and this taxonomy is structured along three dimensions: the Security Layer, which emphasizes core features such as decentralization, immutability, and cryptographic integrity; the Application Layer, which focuses on sector-specific implementations including finance, healthcare, energy, and supply chains; and the Integration Layer, which addresses emerging synergies with AI, IoT, and quantum-resilient technologies. This taxonomy provides a unified framework through which blockchain's cybersecurity contributions can be critically evaluated and compared across diverse use cases and domains. It also establishes a foundation for future empirical investigations and technical assessments.

B. Applications in Various Sectors

Several studies have examined the integration of blockchain across different industries to strengthen cybersecurity. In the financial sector, blockchain enhances the security of banking transactions and supports fraud prevention [13]. The healthcare industry also benefits from blockchain through secure patient data sharing and integrity verification [18]. In supply chain management, [19] discuss blockchain's role in ensuring the authenticity of food products, minimizing cyber risks. The energy sector likewise benefits, as [20] analyze blockchain's role in protecting next-generation smart grids from cyber threats.

Blockchain adoption differs across industries, with financial services leading due to the demand for secure transactions and fraud prevention. The healthcare sector follows, leveraging blockchain to protect patient data, while supply chain management applies it for traceability and verification. The bar chart below visualizes blockchain adoption rates across various industries.

Figure 2 presents an overview of blockchain adoption across major industries as of 2023, based on a synthesis of recent studies. The financial sector shows the highest adoption rate (approximately 85%) due to its early utilization of blockchain for secure transactions, fraud mitigation, and regulatory compliance, as seen in platforms such as Ripple and JPMorgan's blockchain systems. The healthcare sector follows with an estimated 65% adoption, mainly involving pilot projects for secure patient data exchange. Supply chain sectors report around 55% adoption, using blockchain for traceability and anti-counterfeiting, while the energy sector demonstrates roughly 40% adoption, primarily in smart grid protection initiatives. These figures represent general trends reported in the literature rather than data

from a single statistical source and should be interpreted as indicative of relative maturity across industries.

C. Challenges in Blockchain-Based Cybersecurity

Despite its benefits, blockchain technology faces several challenges. [8] provide a scoping review of cybersecurity issues related to blockchain, including scalability, high energy consumption, and regulatory concerns. [21] discusses how these limitations hinder the widespread adoption of blockchain in cybersecurity applications. Another significant challenge lies in smart contract vulnerabilities, which have been exploited in several blockchain-based systems [14]. Similarly, [1] highlights privacy concerns, particularly in public blockchains where transaction data remains visible to all participants.

D. Emerging Trends and Future Directions

Several emerging trends indicate that blockchain will continue to play a significant role in cybersecurity. The integration of blockchain with artificial intelligence (AI) and machine learning is being investigated to improve threat detection and incident response [9]. Research also suggests that blockchain can enhance drone cybersecurity by ensuring secure data transmission and mission integrity [22]. Furthermore, the development of private and permissioned blockchains may help address scalability and regulatory challenges, as noted by [15].

E. Summary

The reviewed literature highlights blockchain as a promising tool for enhancing cybersecurity through transparency, data integrity, and decentralized security frameworks. However, challenges related to scalability, energy consumption, and regulatory compliance must be resolved to enable broader adoption. Future research should focus on optimizing blockchain's integration with existing cybersecurity frameworks to build more resilient digital infrastructures [23], [24].

While many studies have surveyed blockchain applications in cybersecurity, such as [25] and [26], this review distinguishes itself by integrating a thematic synthesis with a conceptual taxonomy spanning multiple sectors and technological layers. In contrast to prior SLRs that concentrate narrowly on technical mechanisms or single-industry applications, this study bridges technical, regulatory, and application-oriented perspectives to provide a comprehensive view of the blockchain–cybersecurity nexus.

III. Research Method

This section describes the methodology used to investigate the integration of blockchain technology in cybersecurity. The study follows a structured process that includes a systematic literature review, data collection, analytical procedures, and evaluation criteria.

A. Research Approach

The study adopts a qualitative research design, employing a systematic literature review (SLR) to synthesize existing research on blockchain-based cybersecurity solutions. This approach enables a comprehensive understanding of the topic by evaluating peer-reviewed journal articles, conference proceedings, and industry reports. The review adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to maintain transparency and methodological rigor.

The PRISMA guidelines provide a standardized framework for conducting and reporting systematic literature reviews. They consist of a 27-item checklist and a flow diagram that together promote clarity, completeness, and reproducibility. PRISMA ensures that essential elements, including research objectives, eligibility criteria, data sources, study selection procedures, and synthesis methods, are clearly documented. By following PRISMA, this review upholds methodological rigor and facilitates peer evaluation and replication. The current study applies the PRISMA 2020 framework, which incorporates updated guidance reflecting advances in systematic review methodology and digital research practices [27].

B. Data Collection

The literature review was conducted using reputable academic databases, including IEEE Xplore, SpringerLink, ScienceDirect, and the ACM Digital Library. The search focused on studies published

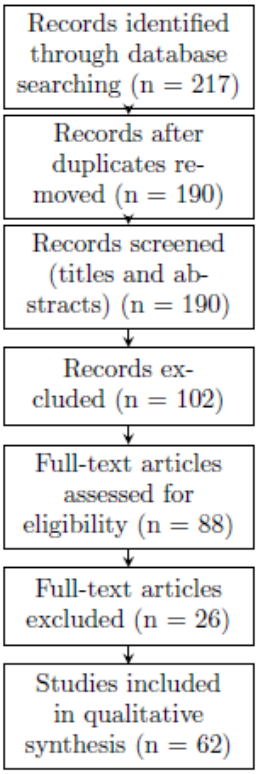

Figure 3. PRISMA Flow Diagram for Study Selection

between 2016 and 2024 to capture recent advancements in blockchain and cybersecurity. The selection detail is shown in Figure 3. The selection criteria were as follows:

1) Keywords: The search employed terms such as "blockchain cybersecurity," "blockchain for data protection," "blockchain-based security models," and "decentralized security solutions."
2) Inclusion Criteria:
   - Peer-reviewed journal articles and conference papers
   - Studies examining blockchain's role in preventing cyber threats
   - Research highlighting blockchain's impact across various industries
   - Publications written in English
3) Exclusion Criteria:
   - Studies unrelated to cybersecurity applications of blockchain
   - Non-peer-reviewed articles, such as blog posts or opinion pieces
   - Duplicate studies

C. Data Analysis

A thematic analysis approach was used to categorize findings into key themes, including blockchain security mechanisms, industry applications, emerging challenges, and future directions. Thematic coding was performed using NVivo software to identify recurring patterns and relationships among the selected studies.

1) Blockchain Security Mechanisms: Studies were grouped based on cryptographic methods, consensus protocols, and immutability features that strengthen security [6], [7].
2) Industry Applications: Literature was classified according to blockchain adoption in sectors such as finance [13], healthcare [18], and energy [20].
3) Challenges and Limitations: Articles discussing blockchain scalability, regulatory issues, and smart contract vulnerabilities were analyzed separately [8], [21].
4) Emerging Trends: Studies addressing innovations such as AI-enhanced blockchain security and permissioned blockchain frameworks were explored [9], [15].

The literature search initially identified 217 studies, of which 62 met the inclusion criteria and were analyzed. The PRISMA flow diagram below summarizes the screening and selection process.

D. Evaluation Criteria

To ensure the reliability and validity of the findings, the study applied the following evaluation criteria.

1) Relevance: Each selected study was assessed for its direct connection to blockchain-based cybersecurity.
2) Credibility: Only peer-reviewed sources and reputable industry reports were included.
3) Recency: Emphasis was placed on recent publications (2019–2024) to capture the latest developments in blockchain technology.
4) Comparative Analysis: Findings were compared across industries to identify both commonalities and unique applications.

E. Summary

Through the use of a systematic literature review and thematic analysis, this study provides a structured and comprehensive examination of blockchain's role in cybersecurity. The methodological design enhances the credibility of the findings, offering a solid foundation for understanding blockchain's potential and limitations in securing digital ecosystems.

IV. Results and Discussion

This section presents the study's findings, analyzing the impact of blockchain technology on cybersecurity. The results are categorized into four main areas: blockchain security mechanisms, industry applications, challenges and limitations, and future directions. The findings are supported by tables summarizing data extracted from the reviewed literature.

A. Blockchain Security Mechanisms

Blockchain offers multiple mechanisms that enhance data integrity, authentication, and network security. Analysis of the selected studies identified four primary security mechanisms:

1) Cryptographic Security – Blockchain uses cryptographic hashing (SHA-256, ECC) and digital signatures to ensure data confidentiality and authenticity [6], [7].
2) Decentralization and Distributed Ledger Technology (DLT) – Eliminates single points of failure, increasing resistance to cyberattacks [16], [17].
3) Consensus Mechanisms – Algorithms such as Proof of Work, Proof of Stake, and Byzantine Fault Tolerance strengthen network reliability [3], [4].
4) Smart Contracts – Automated security rules and identity management enhance the security of digital transactions [2], [23].

B. Industry Applications of Blockchain in Cybersecurity

Blockchain technology is increasingly applied across industries to mitigate cybersecurity risks. The reviewed literature highlights its use in finance, healthcare, energy, and supply chain security.

1) Finance – Banks and financial institutions employ blockchain for secure transactions and fraud detection [13], [28].
2) Healthcare – Blockchain enhances the security of patient data, minimizing the risk of breaches [18], [20].
3) Energy Sector – Blockchain protects smart grid networks from cyber threats through decentralized authentication [20].
4) Supply Chain Security – It improves traceability and reduces counterfeiting in logistics operations [19].

Despite promising use cases, real-world deployment of blockchain in cybersecurity remains inconsistent. The financial sector has achieved measurable progress, as demonstrated by platforms such as Ripple and JPMorgan's Onyx, which enhance secure payments and fraud prevention. In contrast, applications in healthcare and supply chain management are largely limited to pilot projects or conceptual models, hindered by interoperability and legal challenges. Within the energy sector, blockchain adoption has primarily focused on smart grid pilots, with large-scale implementation still constrained. A more nuanced understanding of industry readiness is essential for identifying where blockchain can be deployed most effectively. Factors such as regulatory clarity, stakeholder maturity, and technical feasibility significantly influence the degree of adoption across sectors.

TABLE 1
BLOCKCHAIN SECURITY MECHANISMS AND THEIR BENEFITS

Security Mechanism	Description	Benefits	Key References
Cryptographic Security	Uses hashing & encryption to secure transactions	Ensures confidentiality, integrity, authentication	[6], [7]
Decentralization & DLT	Stores data across multiple nodes, reducing attack risk	Eliminates single points of failure and enhances resilience	[16], [17]
Consensus Mechanisms	Validates transactions without a central authority	Prevents fraud and unauthorized alterations	[3], [4]
Smart Contracts	Automates security protocols and access control	Strengthens identity verification and secure transactions	[2], [23]

TABLE 2
INDUSTRY APPLICATIONS OF BLOCKCHAIN FOR CYBERSECURITY

Industry	Use Case	Benefits	Key References
Finance	Fraud prevention and secure transactions	Reduces financial fraud and enhances transaction integrity	[13], [28]
Healthcare	Patient data security	Protects medical records and prevents unauthorized access	[18], [20]
Energy	Smart grid security	Prevents cyberattacks on critical infrastructure	[20]
Supply Chain	Product authentication	Ensures traceability and reduces counterfeiting	[19]

TABLE 3
CHALLENGES OF BLOCKCHAIN IN CYBERSECURITY

Challenge	Description	Impact	Key References
Scalability Issues	Slow transaction speed due to network limitations	Reduces adoption in high-volume industries	[8], [21]
Regulatory Uncertainty	Lack of clear policies on blockchain usage	Causes legal and compliance challenges	[1], [3]
High Energy Consumption	PoW-based blockchain networks require large power usage	Increases operational costs and environmental impact	[6]
Smart Contract Vulnerabilities	Code flaws can be exploited by hackers	Poses risks to financial and business transactions	[23], [29]

TABLE 4
FUTURE DIRECTIONS FOR BLOCKCHAIN CYBERSECURITY

Future Trend	Description	Expected Impact	Key References
Scalable Blockchain	Layer 2 solutions for faster transactions	Increases blockchain adoption	[30], [31]
AI and Blockchain Security	AI-driven anomaly detection	Enhances threat prevention and detection	[9]
Quantum-Resistant Cryptography	Post-quantum encryption for blockchain	Protects against future quantum attacks	[18]
Regulatory Frameworks	Global standards for blockchain security	Improves compliance and legal clarity	[1]

C. Challenges and Limitations of Blockchain in Cybersecurity

Despite its advantages, blockchain faces significant challenges, including scalability issues, regulatory uncertainty, high energy consumption, and smart contract vulnerabilities.

1) Scalability Issues – Limited transaction processing speed hinder large-scale adoption [8], [21].
2) Regulatory Uncertainty – Governments vary in their regulations on blockchain implementation [1], [3].
3) Energy Consumption – Proof of Work (PoW) mechanisms consume excessive energy, raising environmental concerns [6].
4) Smart Contract Vulnerabilities – Bugs in smart contracts can be exploited by attackers [23], [29].

Although blockchain offers robust cybersecurity advantages, it continues to face significant obstacles, including limited scalability, regulatory ambiguity, and energy inefficiency. The pie chart below illustrates the proportional distribution of the most common challenges that hinder widespread adoption of blockchain in cybersecurity.

D. Future Directions for Blockchain and Cybersecurity

The future of blockchain-based cybersecurity centers on scalable architectures, AI integration, quantum-resistant cryptography, and standardized regulatory frameworks.

1) Scalable Blockchain Solutions – Layer 2 technologies (e.g., Lightning Network) enhance transaction speed and scalability [30], [31].
2) AI and Blockchain Integration – AI strengthens blockchain security by enabling real-time anomaly detection [9].

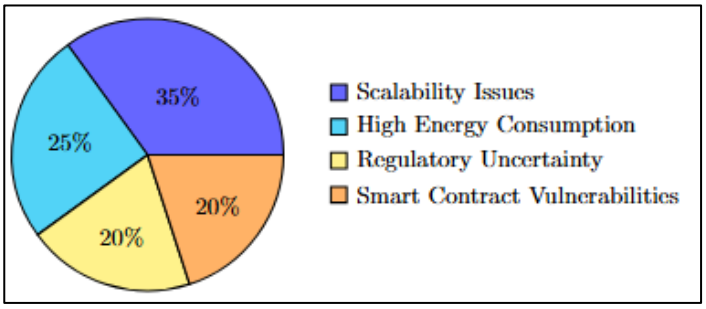

Figure 4. Challenges in Blockchain-Based Cybersecurity

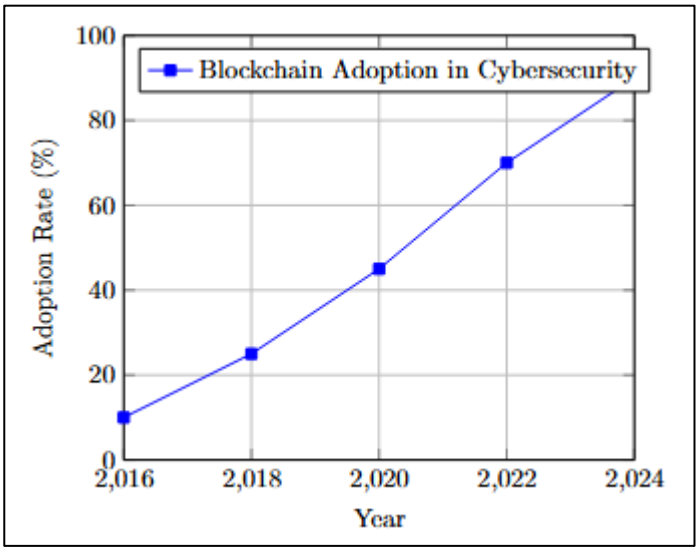

Figure 5. Growth of Blockchain Adoption in Cybersecurity (2016-2024)

3) Quantum-Resistant Cryptography – Future blockchain systems are expected to adopt post-quantum cryptographic techniques to counter potential quantum-based attacks [18].
4) Standardized Regulatory Frameworks – Governments and international organizations are developing global regulatory guidelines to support blockchain adoption in cybersecurity [1].

Although this review synthesizes key themes qualitatively, future research could benefit from incorporating bibliometric or scientometric analyses. Such approaches would allow for a quantitative assessment of publication volume, citation impact, and thematic clustering within blockchain–cybersecurity research. By mapping publication trends, identifying leading authors or institutions, and revealing underexplored subtopics, bibliometric tools can provide a more objective understanding of the field's development. Software such as VOSviewer and CiteSpace could be used to conduct keyword co-occurrence or citation network analyses, helping to identify research gaps and emerging areas of innovation.

The use of blockchain in cybersecurity has expanded considerably in recent years, with growing research output and practical applications across multiple industries. The line graph below illustrates the steady increase in blockchain implementations for cybersecurity between 2016 and 2024.

E. Discussion

The results indicate that blockchain significantly enhances cybersecurity through cryptographic security, decentralization, and smart contract automation. It has been widely adopted in industries such as finance, healthcare, and supply chain management, improving data integrity and reducing exposure to cyber threats. However, challenges related to scalability, regulatory uncertainty, and smart contract vulnerabilities continue to limit its widespread adoption.

While cryptographic security, decentralization, consensus algorithms, and smart contracts each play a critical role, their effectiveness is highly interdependent. For instance, consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) preserve ledger integrity but introduce trade-offs in energy consumption and latency, affecting scalability. Smart contracts automate security policies but rely on the robustness of both the consensus mechanism and code quality, creating risks if vulnerabilities

exist. Likewise, decentralization enhances system resilience but complicates compliance within centralized regulatory frameworks. These interdependencies suggest that blockchain-based cybersecurity systems must be holistically designed, accounting for both technical trade-offs and operational constraints. A single point of failure, such as a flawed contract logic, can cascade across the system and compromise overall security.

Future developments are expected to focus on scalability improvements, AI integration, and quantum-resistant cryptography, making blockchain a more robust cybersecurity solution. Regulatory advancements will also play a crucial role in supporting secure and ethical blockchain implementations.

This study contributes to the expanding body of knowledge on blockchain-based cybersecurity and provides valuable insights into potential directions for future research.

While the literature demonstrates the potential of blockchain in cybersecurity, it is essential to position these solutions alongside existing alternatives such as Public Key Infrastructure (PKI), intrusion detection systems (IDS), and conventional access control models. Compared with these methods, blockchain provides greater transparency and resistance to tampering but may perform less efficiently in terms of speed and energy usage. Moreover, limited empirical evidence is currently available to quantify blockchain's effectiveness. Future research should prioritize comparative case studies and real-world performance indicators, such as breach reduction rates and operational efficiency improvements, to evaluate the actual performance and return on investment (ROI) of blockchain-based security systems.

Cross-sector case comparisons also reveal how regional factors influence adoption. For example, Estonia's X-Road platform and the UAE's Emirates Blockchain Strategy 2021 demonstrate how supportive regulatory environments and government leadership facilitate implementation. In contrast, fragmented regulations across state and federal levels in the United States have hindered standardization and slowed integration. Comparative studies across regions can therefore help identify how legal and governance frameworks either accelerate or restrict blockchain adoption in cybersecurity.

V. CONCLUSION

Blockchain technology has emerged as a transformative solution for enhancing cybersecurity across diverse domains. Through its foundational principles of decentralization, cryptographic security, and smart contract automation, blockchain strengthens data integrity, authentication, and transaction protection. The findings of this study indicate that blockchain is increasingly applied in industries such as finance, healthcare, energy, and supply chain management, where it mitigates cyber threats and promotes transparency. However, despite its advantages, blockchain continues to face scalability challenges, regulatory uncertainty, high energy consumption, and smart contract vulnerabilities that must be addressed for broader adoption.

The study also underscores the pivotal role of consensus mechanisms in securing blockchain networks. While Proof of Work (PoW) and Proof of Stake (PoS) remain dominant, alternative models such as Byzantine Fault Tolerance (BFT) and Directed Acyclic Graphs (DAGs) show potential for improving both efficiency and security. Furthermore, AI-driven anomaly detection and quantum-resistant cryptography are expected to reshape blockchain-based cybersecurity, ensuring resilience against emerging threats.

Looking ahead, the convergence of blockchain with artificial intelligence, cloud computing, and quantum security will define the next phase of cybersecurity innovation. Researchers and industry professionals must collaborate to develop scalable architectures, robust security frameworks, and standardized regulations that support the seamless adoption of blockchain solutions. Governments and regulatory bodies will likewise play a crucial role in establishing legal frameworks that balance security, privacy, and compliance while fostering technological advancement.

In conclusion, while blockchain is not a universal solution, its potential to secure digital ecosystems is considerable. This review demonstrates that blockchain strengthens cybersecurity through cryptographic protection, decentralization, and automated contract enforcement. However, its adoption beyond the financial sector remains limited due to challenges such as regulatory constraints, interoperability issues, and scalability concerns. To move from potential to practical implementation, future research should focus on empirical validation, comparative case studies, and the design of interoperable architectures.

A proposed roadmap includes establishing regulatory sandboxes for secure experimentation, integrating blockchain with AI-driven threat detection systems, conducting large-scale pilot projects in

healthcare and supply chain sectors, and expanding quantitative research through bibliometric and meta-analytical methods. By aligning academic research with industry priorities and regulatory frameworks, blockchain can evolve into a cornerstone of next-generation cybersecurity solutions.

REFERENCES

[1] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecomm Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.
[2] A. Banafa, *Blockchain technology and applications*. River Publishers, 2022.
[3] C. Catalini, "Blockchain technology and cryptocurrencies: Implications for the digital economy, cybersecurity, and government," *Georgetown journal of international affairs*, vol. 19, pp. 36–42, 2018.
[4] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics*, vol. 7, no. 2, pp. 189–208, 2020.
[5] A. Alkhalifah, A. Ng, M. J. M. Chowdhury, A. S. M. Kayes, and P. A. Watters, "An empirical analysis of blockchain cybersecurity incidents," in *2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, IEEE, 2019, pp. 1–8.
[6] H. Hasanova, U. Baek, M. Shin, K. Cho, and M. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, vol. 29, no. 2, p. e2060, 2019.
[7] E. A. Antonyan and O. S. Rybakova, "Blockchain technologies for security against cyber attacks," *Вестник Национальной академии наук Республики Казахстан*, no. 4 (386), p. 21, 2020.
[8] S. Mahmood, M. Chadhar, and S. Firmin, "Cybersecurity challenges in blockchain technology: A scoping review," *Hum Behav Emerg Technol*, vol. 2022, no. 1, p. 7384000, 2022.
[9] M. Omar and H. M. Zangana, *Redefining Security With Cyber AI*. IGI Global, 2024.
[10] H. M. Zangana and M. Omar, "Introduction to Quantum-Aware Cybersecurity: The Need for LLMs," in *Leveraging Large Language Models for Quantum-Aware Cybersecurity*, IGI Global Scientific Publishing, 2025, pp. 1–28.
[11] M. Omar and H. M. Zangana, *Application of Large Language Models (LLMs) for Software Vulnerability Detection*. IGI Global, 2024.
[12] H. M. Zangana, Z. B. Sallow, and M. Omar, "The Human Factor in Cybersecurity: Addressing the Risks of Insider Threats," *Jurnal Ilmiah Computer Science*, vol. 3, no. 2, pp. 76–85, 2025.
[13] M. M. Rahman, A. Elshamly, S. U. Rehman, Z. Jameel, and R. Hameed, "Blockchain Technology And Its Impact On European Bank's Cyber Security And Data Integrity," *Journal of Namibian Studies: History Politics Culture*, vol. 34, pp. 1796–1813, 2023.
[14] I. A. Shah, N. Z. Jhanjhi, and A. Laraib, "Cybersecurity and blockchain usage in contemporary business," in *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, IGI Global, 2023, pp. 49–64.
[15] 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. 01, pp. 35–43, 2023.
[16] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in *2016 2nd international conference on contemporary computing and informatics (IC3I)*, IEEE, 2016, pp. 463–467.
[17] K. J. Smith and G. Dhillon, "Assessing blockchain potential for improving the cybersecurity of financial transactions," *Managerial Finance*, vol. 46, no. 6, pp. 833–848, 2020.
[18] A. Tezel, E. Papadonikolaki, I. Yitmen, and M. Bolpagni, "Blockchain opportunities and issues in the built environment: Perspectives on trust, transparency and cybersecurity," in *Industry 4.0 for the Built Environment: Methodologies, Technologies and Skills*, Springer, 2021, pp. 569–588.
[19] N. Etemadi, Y. G. Borbon, and F. Strozzi, "Blockchain technology for cybersecurity applications in the food supply chain: A systematic literature review," *Proceedings of the XXIV Summer School "Francesco Turco"—Industrial Systems Engineering, Bergamo, Italy*, pp. 9–11, 2020.
[20] N. Mengidis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Blockchain and AI for the next generation energy grids: cybersecurity challenges and opportunities," *Information & Security*, vol. 43, no. 1, pp. 21–33, 2019.
[21] A. R. Mathew, "Cyber security through blockchain technology," *Int. J. Eng. Adv. Technol*, vol. 9, no. 1, pp. 3821–3824, 2019.
[22] A. Ossamah, "Blockchain as a solution to drone cybersecurity," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, IEEE, 2020, pp. 1–9.
[23] V. Wylde *et al.*, "Cybersecurity, data privacy and blockchain: A review," *SN Comput Sci*, vol. 3, no. 2, p. 127, 2022.
[24] F. Zidan, D. Nugroho, and B. A. Putra, "Securing enterprises: harnessing blockchain technology against cybercrime threats," *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 167–172, 2023.
[25] H. Hasanova, U. Baek, M. Shin, K. Cho, and M. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, vol. 29, no. 2, p. e2060, 2019.
[26] V. Wylde *et al.*, "Cybersecurity, data privacy and blockchain: A review," *SN Comput Sci*, vol. 3, no. 2, p. 127, 2022.
[27] O. V. Kuzmenko, H. M. Yarovenko, and M. Sadigov, "Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system," 2021.
[28] R. Prakash, V. S. Anoop, and S. Asharaf, "Blockchain technology for cybersecurity: A text mining literature analysis," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100112, 2022.
[29] V. P. Sriram *et al.*, "Enhancing Cybersecurity Through Blockchain Technology," in *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, IGI Global, 2023, pp. 208–224.
[30] M. Sadigov, O. Kuzmenko, and H. Yarovenko, "Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system," *Economic and Social Development: Book of Proceedings*, pp. 399–408, 2020.
[31] O. V. Kuzmenko, H. M. Yarovenko, and M. Sadigov, "Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system," 2021.