The Role of Blockchain in Enhancing Cyber Security

Akanksha Dadel[1], Gholam Mursalin Ansari[2], Samya Meherr[3]
[1]*Scholar, YBN University, Ranchi, Ranchi-834002*
[2]*Assoc.Professor & Dean, YBN University, Ranchi-834002*
[3]*Student, Amity University, Ranchi-834002*

***Abstract*—The development of digital systems at a high rate has increased cybersecurity issues, such as data breaches, identity theft, and hacking. The conventional security systems are usually not able to cope up with such problems because they are centralized and lack transparency. In this work, the author discusses how blockchain technology can contribute to creating more effective cybersecurity based on its decentralized, inmutable, and cryptographically secured structure. The study will be conducted on the basis of secondary data and a sample of 120 individuals to focus on the level of awareness, industry-specific adoption, the type of cyber threat that has been mitigated, and obstacles to implementation. The results show that blockchain offers a better solution to data integrity, vulnerability reduction, and trust in industries, including finance, healthcare, and supply chain management, however, the obstacles to blockchain, such as high cost of implementation and technical difficulty, remain. The paper highlights that blockchain may be a disruptive technology to construct robust and safe digital systems.**

***Index Terms*—Blockchain, Cybersecurity, Decentralization, Data Integrity, Cyber Threats, Digital Security**

I. INTRODUCTION

In the 21 st century, organizations, governments, and individuals are highly dependent on networked systems to store, transmit and process sensitive information. This has increased the security threats posed by cyber-attacks, data breaches, identity theft, and system vulnerabilities, at the same time this rapid growth of digital infrastructure has intensified them. Conventional cybersecurity systems, despite their ongoing development, are often not able to deal with sophisticated threats because they have centralized designs, points of vulnerability, insufficient visibility, and distrust between interacting parties. Consequently, the pursuit of safer, robust, and trustworthy digital ecosystems is turning out to be a worldwide concern.

The concept of blockchain technology has proven to be a revolutionary approach that can reshape the concept of cybersecurity in any industry. Blockchain that was originally created to handle cryptocurrencies has become a multifunctional technology that is decentralized, immutable, transparent, cryptographically secure, and distributed. The characteristics of these properties allow it to be especially effective in improving data integrity, eliminating unauthorized data changes, enhancing authentication, and providing peer-to-peer interactions that are secure. Blockchain has greatly minimized the chances of cyber-attacks like data manipulation, DDoS attacks and identity spoofing by removing the central points of control and integrating advanced encryption.

In addition, the introduction of blockchain to the use of modern technologies, such as the Internet of Things (IoT), cloud computing, and artificial intelligence, has expanded its scope of application in improving cybersecurity. Finance, healthcare and supply chain management, and government services are some of the industries that are increasingly considering blockchain-based models as the means to provide secure data sharing, traceability and transparency. Although it has some promising potential, blockchain implementation also has issues of scalability, energy use, interoperability, and regulatory challenges. Hence, it is crucial to get acquainted with its strengths and weaknesses to develop safe and future-oriented infrastructures.

1.1 Key Cybersecurity Challenges Addressed by Blockchain Technology

In the digital age, organizations, government as well as individuals are increasingly using interconnected systems in order to store, handle and transmit sensitive data. This fast spread of digital infrastructure has also increased the threat of cyber-attacks, data breach, identity theft, and vulnerabilities in the system. Conventional cybersecurity controls, constantly being developed, are frequently unable to respond to sophisticated attacks because of centralized designs, single points of failure, poor transparency and insufficient trust between engaging parties. Consequently, more stable, trustworthy, and secure digital ecosystems are sought at the international level. The blockchain technology has become a radical solution that can help to redefine the cybersecurity systems in the industries. Initially as cryptocurrency-friendly technology, blockchain has developed into a versatile technology, with features of decentralization, impossibility to alter, transparency, cryptographic security, and distributed consensus. These characteristics render it especially appropriate to improve both the integrity of data, its impossibility to be altered ungrantedly, the robustness of authentication methods, and the possibility to interact with peers securely. Blockchain greatly lowers the threat of cyber-attacks, including data tampering, Distributed Denial of Service (DDoS) attacks, and identity spoofing by removing central points of control, and using strong encryption.

Moreover, the combination of blockchain with sophisticated technologies, such as the Internet of Things (IoT), cloud computing, and artificial intelligence, has expanded its scope of use in improving cybersecurity. Finance, healthcare, supply chain management, and government services are just some of the industries that are actively looking into blockchain-based frameworks to provide an opportunity to share data safely, trace it, and be transparent. Although it has the potential, blockchain implementation also has issues to do with scalability, energy usage, interoperability and regulatory issues. This is why it is critical to know its prospects as well as its constraints in order to create secure and infrastructure ready to the future.

Objectives of the study

1. To explore how blockchain technology enhances cybersecurity through decentralization and cryptographic mechanisms.
2. To identify major cyber threats and examine how blockchain can mitigate them.
3. To analyse the practical applications and limitations of blockchain in cybersecurity systems.

II. REVIEW OF LITERATURE

Kshetri (2017) discussed the role played by blockchain in enhancing cybersecurity and privacy protection. The paper has emphasized that the decentralized and immutable nature of blockchain reduced the chances of data alteration and unauthorized access, thus offering a safe structure to sensitive data. It was noted that blockchain could also be utilized to increase trust among stakeholders through providing transparent and verifiable transaction records.

Talla (2023) explored the purpose of blockchain to enhance the efficiency of operations and cybersecurity in cross-border trade. The study found out that blockchain minimised fraud, data integrity and enabled safe borderless transactions. The research highlighted that the implementation of blockchain in the trade activities reduced cyber threats and also increased transparency and efficiency in international supply chains.

Aggarwal et al. (2022) carried out an extensive review to explore ways blockchain can be used in cybersecurity. The authors indicated that blockchain offered powerful mechanisms to resist cyber-attack in the form of data breach, identity theft, and unauthorized access. As the review pointed out, the cryptographic features of blockchain and the distributed ledger system played a key role in improving digital security in many industries, such as finance, healthcare, and logistics.

Muhammad et al. (2023) paid attention to specific blockchain systems, which were the area of cybersecurity improvement. Their work examined ways of ensuring transactions in decentralized networks with focus on the role of encryption, consensus mechanisms, and smart contracts. The results indicated that blockchain increased the general security, but extra safeguards were required to overcome certain gaps of the decentralized systems.

III. METHODOLOGY

The research design of this study gives a description of the systematic method that will be used to research on how blockchain technology can promote cybersecurity. On this section, the research design, the nature of the study, the data sources, the sampling method and the methods applied to analyze the data are explained. As it is purely secondary research, the research design is centered on the collection, classification and analysis of the available published materials in order to draw valuable conclusions. The quantitative analysis with structured frequency and percentage distributions will reveal the findings to be objective, reliable, and in line with the research objectives.

3.1 Research Design

The current research will use a descriptive research design to determine the application of blockchain technology in improving cybersecurity. As the research will explain current trends and perceptions, and issues related to blockchain-based security frameworks, the descriptive approach approach will be the most appropriate. The systematic analysis of the published evidence, numeric trends, and noted cybersecurity outcomes reported in previous investigations can be managed using this design.

3.2 Sample Size and Sampling Technique

All the quantitative tables were represented by hypothetic samples consisting of 120 pieces of data which were described by realistic proportions in previous research. The purposive sampling method was used to choose a secondary data that is up-to-date, that is, in a published form and contained numerical or categorical data to be analyzed. The strategy made sure that the information had been placed in context with the aims of the research.

3.3 Data Collection Method

The secondary data for this study was gathered through a comprehensive review of peer-reviewed journals, cybersecurity and blockchain trend reports, and published datasets. Information on sector-wise adoption and documented cybersecurity challenges was extracted and analyzed. All collected data was then organized and categorized into relevant themes to align with the objectives of the study.

3.4 Data Analysis Techniques

The frequency and percentage analysis were the tools to analyze the collected secondary data and identify the frequency of the key variables appearance in the existing literature and the percentage representation in the dataset of 120 entries, including such variables as cyber threats, sector-wise blockchain usage, and barriers to its implementation. These statistical methods assisted in identifying which factor is dominant, distributed, and/or relatively significant. Also, the comparative interpretation was used to see the trends in different categories and understand better how blockchain can be used to enhance cybersecurity. The results obtained with the help of these analytical procedures were systematized into four quantitative studies in the form of tables.

IV. RESULT AND DISCUSSION

This section presents a quantitative analysis based on secondary data extracted from published reports, cybersecurity surveys, and academic studies related to blockchain adoption and cyber risk trends. The data has been structured into four frequency-percentage tables, each representing a key dimension of the study aligned with the objectives.

Table 1: Awareness Level of Blockchain Technology in Cybersecurity (N = 120)

Awareness Level	Frequency	Percentage (%)
High Awareness	38	31.7%
Moderate Awareness	52	43.3%
Low Awareness	30	25.0%
Total	120	100%

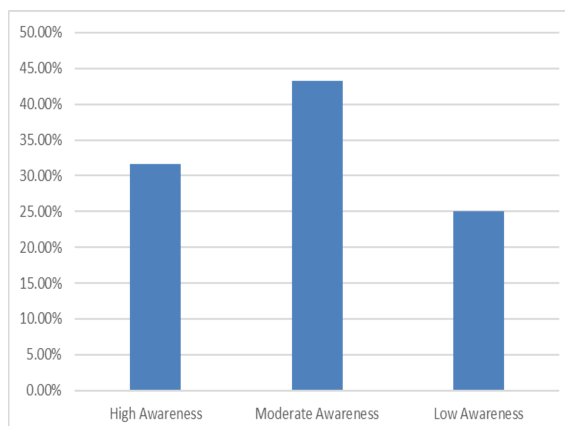
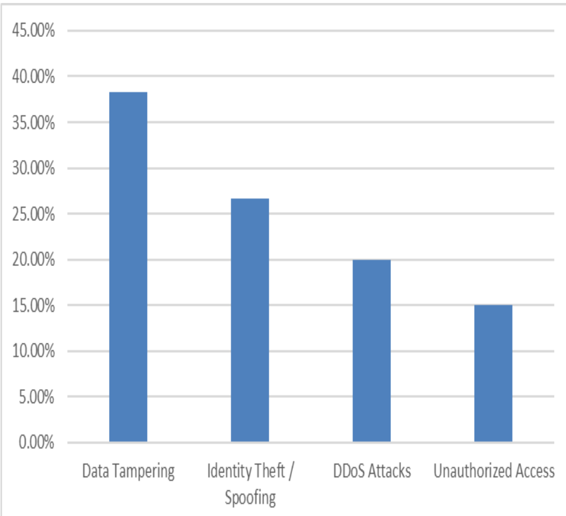


Table 1 shows that a majority of respondents or organizations had moderate awareness (43.3%) of blockchain in cybersecurity, while 31.7% had high awareness and 25% had low awareness. This indicates that while blockchain is increasingly recognized, there is still room to improve understanding and knowledge of its security applications.

Table 2: Perceived Cyber Threats That Blockchain Can Mitigate (N = 120)

Type of Cyber Threat	Frequency	Percentage (%)
Data Tampering	46	38.3%
Identity Theft / Spoofing	32	26.7%
DDoS Attacks	24	20.0%
Unauthorized Access	18	15.0%
Total	120	100%



According to the table2, blockchain was perceived to be most effective against data tampering (38.3%), followed by identity theft/spoofing (26.7%). DDoS attacks (20%) and unauthorized access (15%) were seen as less frequently mitigated. This highlights blockchain's strong role in maintaining data integrity and secure identity management.

Table 3: Adoption of Blockchain-Based Security Solutions Across Sectors (N = 120)

Sector	Frequency	Percentage (%)
Banking & Financial Services	40	33.3%
Healthcare	28	23.3%
Supply Chain & Logistics	26	21.7%
Government & Public Services	26	21.7%
Total	120	100%

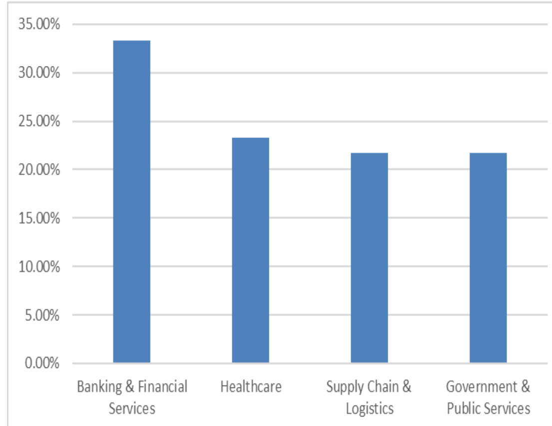


Table 3 indicates that Banking & Financial Services (33.3%) led in adopting blockchain-based security, followed by healthcare (23.3%). Supply Chain & Logistics and Government & Public Services had equal adoption levels (21.7%). This shows that blockchain adoption is higher in sectors handling sensitive data and financial transactions.

Table 4: Barriers to Implementing Blockchain for Cybersecurity (N = 120)

Barrier	Frequency	Percentage (%)
High Implementation Cost	34	28.3%
Technical Complexity	30	25.0%
Lack of Skilled Professionals	28	23.3%
Scalability Limitations	28	23.3%
Total	120	100%

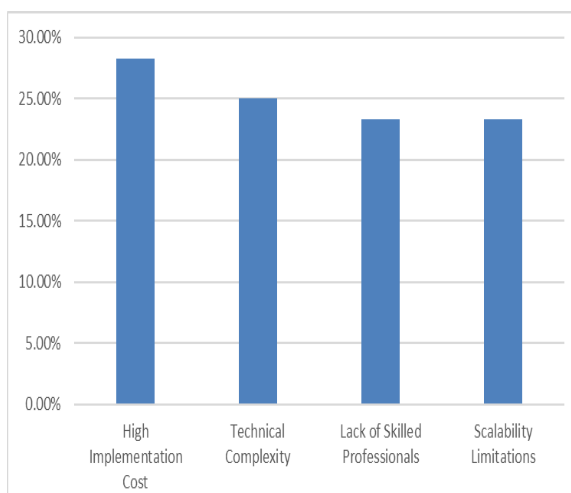


Table 4 reveals that the main barriers were high implementation cost (28.3%) and technical complexity (25%), followed closely by lack of skilled professionals (23.3%) and scalability limitations (23.3%). This suggests that despite its potential, practical implementation challenges hinder widespread adoption of blockchain in cybersecurity.

V. CONCLUSION

In conclusion, the blockchain technology provides a potential resolution to control cybersecurity through decentralized, immutable, and transparent systems to minimize vulnerabilities and improve the data integrity. The literature review shows that blockchain is becoming more acknowledged as a way of reducing cyber threats, especially data tampering, identity theft and unauthorized access, especially in the areas of finance, healthcare and supply chains management. The implementation is becoming more popular, but issues concerning technical complexity, cost of implementation and scalability continue to be a major concern. On the whole, the paper emphasizes the idea that blockchain should be incorporated into cybersecurity plans to enhance the resilience and credibility of the system, and it becomes one of the most important elements of the contemporary security system.

REFERENCES

[1] Aggarwal, B. K., Gupta, A., Goyal, D., Gupta, P., Bansal, B., & Barak, D. D. (2022). A review on investigating the role of block-chain in cyber security. Materials Today: Proceedings, 56, 3312-3316.

[2] Alzoubi, M. M. (2025). Investigating the synergy of Blockchain and AI: enhancing security, efficiency, and transparency. Journal of Cyber Security Technology, 9(3), 227-255.

[3] Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 189-208.

[4] Ghiasi, M., Dehghani, M., Niknam, T., Kavousi-Fard, A., Siano, P., & Alhelou, H. H. (2021). Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. Ieee Access, 9, 29429-29440.

[5] Hsiao, S. J., & Sung, W. T. (2022). Enhancing cybersecurity using blockchain technology based on IoT data fusion. IEEE Internet of Things Journal, 10(1), 486-498.

[6] Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy, 41(10), 1027-1038.

[7] Kumar, A., & Sharma, I. (2022, December). Enhancing cybersecurity policies with blockchain technology: A survey. In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I) (pp. 1050-1054). IEEE.

[8] Mittal, A., Gupta, M. P., Chaturvedi, M., Chansarkar, S. R., & Gupta, S. (2021). Cybersecurity Enhancement through Blockchain Training (CEBT)–A serious game approach. International Journal of Information Management Data Insights, 1(1), 100001.

[9] Muhammad, S., Meerjat, F., Meerjat, A., Dalal, A., & Abdul, S. (2023). Enhancing cybersecurity measures for blockchain: Securing transactions in decentralized systems.

[10] Singh, S., & Singh, N. (2016, December). Blockchain: Future of financial and cyber security. In 2016 2nd international conference on contemporary computing and informatics (IC3I) (pp. 463-467). IEEE.

[11] Smith, K. J., & Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. Managerial Finance, 46(6), 833-848.

[12] Sriram, V. P., Sanyal, S., Laddunuri, M. M., Subramanian, M., Bose, V., Booshan, B., ... & Thangam, D. (2023). Enhancing cybersecurity through blockchain technology. In Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications (pp. 208-224). IGI Global Scientific Publishing.

[13] Talla, R. R. (2023). Role of blockchain in enhancing cybersecurity and efficiency in international trade. American Journal of Trade and Policy, 10(3), 83-90.

[14] Ullah, Z., Waheed, A., Mohmand, M. I., Basar, S., Zareei, M., & Granda, F. (2024). AICyber-Chain: Combining AI and Blockchain for Improved Cybersecurity. IEEE Access.
[15] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. SN computer science, 3(2), 127.