Review

Leveraging Blockchain Technology for Cyber Security: A Comprehensive Review

Md. Badiuzzaman Biplob * , Tasnia Zannat , Arif Ahmed , Mahmuda Samia Konika , Kazi Mohammad Moinul Ahsan

Posted Date: 5 September 2024

doi: 10.20944/preprints202409.0407.v1

Keywords: blockchain; decentralization; immutability; transparency; systematic; survey; cryptocurrency; security

Article

Leveraging Blockchain Technology for Cyber Security: A Comprehensive Review

Md. Badiuzzaman Biplob [a,*], Tasnia Zannat [b], Arif Ahmed [b], Mahmuda Samia Konika [b] and Kazi Mohammad Moinul Ahsan [b]

[a] Computer Science and Engineering Department, Chittagong University of Engineering and Technology, Bangladesh
[b] Computer Science and Engineering Department, Daffodil Institute Of IT, Bangladesh
* Correspondence: biplob.cse45@gmail.com

Abstract. Blockchain is a shared, unchangeable, decentralized ledger that allows transactions to be recorded securely and transparently via a network of computers. In addition to its significant contributions to cryptocurrencies, blockchain technology has shown promise as a game-changing advancement in cyber security. This study offers a thorough analysis of how blockchain technology is strongly linked to defending against cyber security risks in the modern world. This research clarifies the primary mechanisms of decentralization, immutability, transparency, and cryptographic security by which blockchain improves cyber security through a review of the literature and case studies. Furthermore, the study addresses the difficulties and constraints associated with incorporating blockchain technology into cybersecurity frameworks and proposes potential directions for future research.

Keywords: blockchain; decentralization; immutability; transparency; systematic; survey; cryptocurrency; security

1. Introduction

The recent explosion of digital technology has presented previously unheard of chances to boost innovation capabilities and generate efficiencies. As digital technology has advanced, so too have the number of digital attacks or cyber security concerns, which are increasingly prevalent. This is a global issue at the moment that is really concerning. The demand for the technology employed in cyber security systems as well as the amount of money invested in its services are rising due to cyber security dangers. The old approaches to cyber security are insufficient to address the dynamic and complex character of contemporary cyber threats. It must contend with a number of issues, such as manipulation, illegal access and vital infrastructure. A viable paradigm for addressing these issues, boosting cyber security resilience and lowering the frequency of cyber-attacks is blockchain technology.

Blockchain is a decentralized ledger that makes data transparent and unchangeable. Distribution network architecture, consensus processes, and cryptography are used to solve cyber security issues like fraud, data breaches, and identity theft. This thorough analysis shows that blockchain technology helps mitigate modern cyber security threats. This study analyses existing literature, case studies, and practical implementations to determine how blockchain technology improves cyber security resilience and trust while building a resilient digital ecosystem against malicious actors. The next section of this research paper discusses blockchain technology's decentralization, immutability, transparency, and cryptographic security. Then, the study examines cyber security threats and the frequency and effects of cyberattacks in many markets and sectors. It examines blockchain's supply chain security, decentralized identity management, and safe data storage applications in cyber security.

This paper also looks at the difficulties and constraints associated with incorporating blockchain technology into current cyber security systems. Through a critical assessment of the advantages and

 doi:10.20944/preprints202409.0407.v1

disadvantages of blockchain based cyber security solutions, we hope to pinpoint possible directions for future innovation in research and collaboration in this expanding sector.

2. Review of Literature

The concepts from recent research articles on the effect of blockchain technology on cyber security form the basis of this ongoing paper. The researchers examined a wide range of earlier publications examining the cyber security flaws and possible attack vectors of blockchain technology in the research article **[1]**, which is accessible by reference. The report also suggested several other potential options. In their article, they go into great detail on POW and offer a robust security solution. Researchers examine and describe a novel distributed intrusion detection system (IDS) that employs fog computing to identify denial-of-service attacks (DDOS) in article **[2,3]**. This study evaluates the distributed fog nodes performance using Random Forest (RF) and an update gradient. The tree boosting method (XG boot) is used one after the other. Additionally, they present a novel example of federated learning enabled by blockchain technology in this work. They talk about the concept of fusing blockchain technology and the Internet of Things in a research paper **[4]**. This study takes into consideration a number of blockchain and IoT research studies. Examining the document **[5]** reveals that the study emphasizes the prospects for further research in the area of cyber security outside of the Internet of Things. This study also finds peer-reviewed literature discussing the application of blockchain to cyber security. The research article **[6]** examines the possible and present applications of blockchain technology in the fields of accounting and cyber security in business. Because of the significance of cyber security development, this paper examines the Department of Homeland Security's plans for cyber security over the next few years to understand what the US government is planning to do. Paper **[7]** fills the cyber security vacuum left by the smart grid by providing a thorough survey on blockchain. As a result, the study offers the most recent understandings of the theories, plans and techniques associated with applying blockchain technology to cyber security in smart grids. Due to its inability to address certain issues like centralized control, adversary attacks, security and privacy, the research paper **[8]** proposed Deep Block IoT Net. This is a secure deep learning method that uses blockchain for IoT networks, where deep learning operations are carried out in a secure, decentralized manner between edge nodes at the edge layer. In order to improve security by monitoring voltage and current in smart DC-MG, the Hilbert-Huang transform method with blockchain based laser technology is utilized in article **[9]** to identify false data injection attack (FDIAS) in an MG system. A blockchain framework supporting cyber security measures for smart home installations was presented in Paper **[11]**. This framework allows for dynamic and immutable administration of blacklisted malicious IPs in addition to providing necessary smart contract support to guarantee the integrity of smart house gateways and IoT devices. Conversely, the study **[12]** examines and identifies the major obstacles to closing the knowledge gap regarding the adoption, promotion and use of blockchain technology among SMEs, corporations, organizations, businesses, government agencies and the general public. As demonstrated in the publication **[13]**, researchers identify two main unresolved issues for blockchain enabled CPS development excessive consensus building time and low through put and suggest future lines of inquiry. The application of blockchain technology to security solutions for BOT ecosystems is reviewed in Paper **[16]**. In order to improve grid security, Paper **[19]** looks into the usage of blockchain technology. It also suggests a symmetric encryption method based on random sequences that shares decryption keys via a secure blockchain platform. As demonstrated in the publication **[20]**, this study categorizes the various cyber security concerns in BCT and examines the breadth of the existing research.

2.1. Papers Screening

Initially about sixty papers were gathered for examination. The IEEE, Google Scholar, ResearchGate and ScienceDirect databases were searched for peer-reviewed articles. A few duplicate articles were discovered and eliminated. This article contains a total of 41 papers for review. Of them, 24 focused on the use of blockchain technology in cyber security, while the remaining 17 publications examined its application in various other domains.

 doi:10.20944/preprints202409.0407.v1

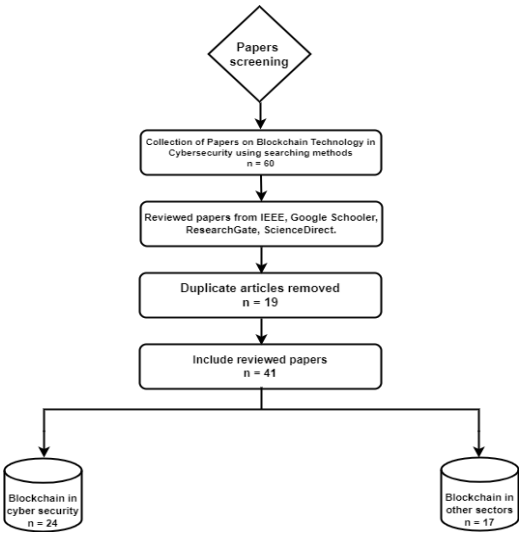

Figure 1. Diagram of screening paper.

2.2. Papers Collection

Numerous research papers on the development of blockchain technology have been published in recent years. The articles published between 2018 and 2024 are reviewed in this report. In light of this, an example is given in which 10% of the articles published in 2024, 14% in 2023, 3% in 2022, 4% in 2021, 6% in 2020, 4% in 2019 and 2% in 2018 papers have been collected and included in this research paper.

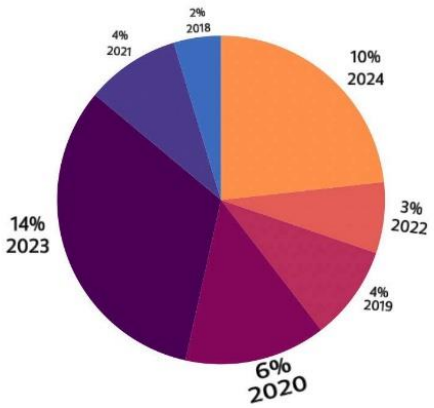

Figure 2. Papers collection towards blockchain in cyber security.

3. Background

Blockchain technology is a decentralized digital ledger that records all computer transactions immutably. Thus, this immutable ledger cannot change or remove transactions. Blockchain spreads the network system among all parties, preventing monopolization. This gives everyone access to the same data. To prevent data loss, each block references the previous block's records. Blockchain technology offers such strong data security that criminals cannot alter it. Thus, encrypted data cannot be changed. Blockchain technology is also gaining popularity due to smart contracts, cryptography, and consensus mechanisms.

Because of its decentralized nature and security features, blockchain technology has been used in a number of industries. The blockchain has undergone a revolution thanks to its successful application. Blockchain is applied in a number of areas, including e-commerce, smart grid, healthcare, banking, agriculture and transportation. It's now well-liked. Numerous research articles on the

 doi:10.20944/preprints202409.0407.v1

subject have been written. Thus, it makes sense that blockchain technology has become essential to the modern world. Data security, patient privacy protection and safe medical record sharing have all been made possible by the application of blockchain technology in smart healthcare.**[27]** this research paper provides a thorough analysis to show the blockchain technology's importance for the healthcare industry from both an application and a technological standpoint. The article discusses how different application characteristics and blockchain applications relate to interoperability in the health care area. **[26]**a thorough literature review was done to investigate these processes, as can be seen in the research article. As demonstrated in the second aim, a high-level architecture for the entire process and its validation has been proposed via a domain specific language for particular smart contracts utilizing a model-driven engineering strategy. The financial system has had extraordinary success with blockchain technology. It makes financial transactions easier while enhancing security and reducing fraud. The research study **[28]** demonstrates how financial models based on blockchain technology can be used to leverage smart contracts to free labor from cumbersome and traditional company processes. This study report also discusses how blockchain may fully preserve the educational track by utilizing the financial sharing center concept and increase the credibility of students' learning outcomes when they apply for jobs. However, of the 12 most well-known blockchain technology platforms **[29]** covered in the research paper, only six platforms with a financial focus are given a detailed description. Thanks to this study, applications for blockchain based securities trading are well understood. This study paper's objective was to present the ecosystem's effects of blockchain technology on the current financial system. The study paper **[30]** goes into great length about the technical characteristics, benefits and drawbacks of blockchain technology as well as its possible uses in financial management. Furthermore, the supply chain system can now be more transparent and traceable thanks to blockchain technology, which guarantees authenticity and lowers counterfeiting. A research study **[31]** explores how supply chain systems might be made more trustworthy by using blockchain technology's tamperproof, reliable and traceable properties. In this research work, a systematic review that combines theme analysis of upcoming research trends with bibliometric analysis is presented. However, the disruptive features of blockchain technology in supply chain management are covered in a research article **[32]**. The technological use of supply chain management systems employing blockchain technology is reviewed in research paper **[33]**. Furthermore, this research compares and validates the efficacy of blockchain techniques in supply chain management systems using multiple security criteria. Blockchain technology is useful for agricultural management in addition to these domains. This study **[34]** used blockchain technology to track food sources and establish trustworthy food supply chains. The use of blockchain technology in the food supply chain, agricultural insurance, smart agriculture and agricultural commodities trade, among other topics, is covered in detail in this research paper. A research article **[35]** examined the problem of using blockchain technology to provide a permanent and transparent record of all agriculture management transactions and operations. Additionally, blockchain technology is still having a big impact on transportation networks. Researchers have examined the current difficulties, potential uses and long-term needs for transportation networks in study paper **[36]**. Blockchain technology reviews the promotion of innovation in transportation services and offers substantial prospects for smart city transportation systems. However, in a research paper **[37]**, Blockchain suggested a multi-keyword search protocol for transportation system data based on bloom filters, which preserves privacy while being efficient. The school sector has seen unparalleled success with the application of blockchain technology. This study **[38]** explores how using blockchain technology to apply visualization techniques enhances student teaching strategies and streamlines administrative processes. Additionally, it makes use of blockchain technology to securely verify testimonies and analyze data with open records. As the publication **[39]** demonstrates, the study provides a systematic examination of integrating blockchain applications with cutting-edge technology to execute Education Systems 4.0. Blockchain technology is used in e-commerce management in a way that is unmatched for safe and secure online transactions. Today's traditional business is conducted online due to the quick adoption of digitization. The e-commerce industry is continually changing as a result. A blockchain integrated enterprise e-commerce platform was

 doi:10.20944/preprints202409.0407.v1

created by the research paper **[40]** using the Power of Attorney consensus method to create and approve new blocks within the system.

3.1. Market Dynamics Overview

Global demand for blockchain technology is rising daily, according to an analysis of research articles **[41]**. The global blockchain technology market was projected to be worth $339.5 million in 2017, per the research document. That is, a graph chart is used in this research paper to illustrate the expansion of blockchain technology from 2017 to 2030 based on the paper's review. The market for blockchain technology is predicted to reach a valuation of $3.1 trillion by 2030, that having grown in $2.3 billion by 2021.

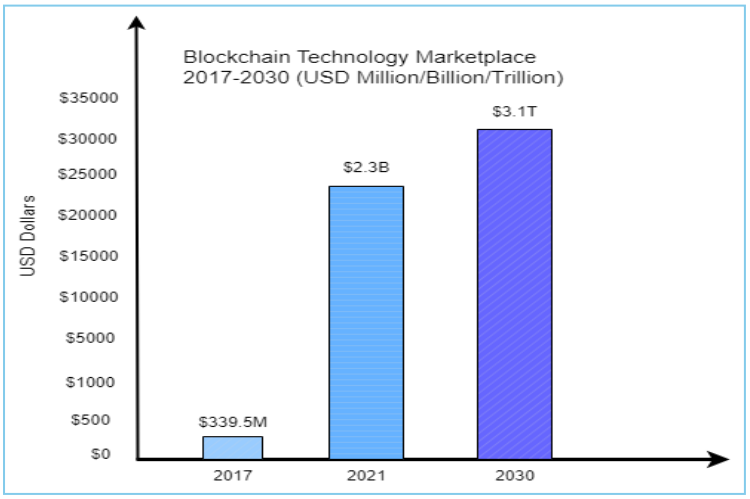

Figure 3. Navigating the Blockchain Marketplace Evolution (2017-2030).

4. Cyber security Threat Landscape

The environment of cyber security threats is ever-changing. Recent patterns indicate that this has made a number of organizations more vulnerable. The advent of new cyber risks is accompanied by a shift in the danger environment. The threat environment for cyber security includes a broad spectrum of possible dangers, such as:

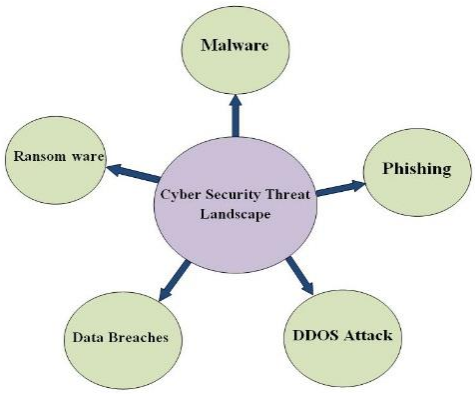

Figure 4. Threat to Cyber security.

- **Malware:** Malicious software is shortened to malware. This harmful software is intended to gain unauthorized access to computer systems. Malware comes in several forms, including ransomware, worms, trojan horses and spyware.
- **Ransomware:** This type of harmful software infiltrates the system, encrypts it completely and then demands a ransom to be paid in order to unlock it. At the moment, it is the cyber security

 doi:10.20944/preprints202409.0407.v1

danger that is most discussed. It has had an impact on numerous organizations worldwide. According to a report conducted by the Australian Cyber Security Center (ACSC), ransomware virus increased by 15% in the 2020–21 fiscal year. Blockchain technology that can withstand ransomware attacks has become a game-changer in lowering attack risk. Its numerous uses improve defenses against intruders' unlawful access.

- **Phishing:** Occasionally, emails containing startling offers show up in individual email accounts. We open and click on the names of banks, well-known companies and acquaintances. Personal information is stolen by phishing emails. Along with credit card fraud, data breaches also affect individuals and cause significant financial losses for a number of different corporations. It is therefore dangerous to open unfamiliar or questionable emails.
- **Data Breaches:** When unauthorized parties obtain sensitive or private information, such as personal or company data, this is referred to as a data breach. This has grown to be a major cyber security problem. Financial loss, reputational harm, identity theft and fraud are all possible outcomes of data breaches.
- **Distributed Denial of Service (DDOS) attack:** In a DDOS attack, an online website is brought offline and cut off from internet traffic. Deeds is the acronym for DDoS. In other words, the browser will not load the website. In order to accomplish this, a network comprising around 10,000 computers is linked to every other computer. A botnet is a website from which attempts are made to load webpages. A web page becomes offline as a result of being unable to handle so many loads at once. In order to achieve this, hackers It starts by identifying holes in the operating system of the computer and then notifies the user to install a variety of defective applications.

As per the examined research article, there has been a significant surge in malicious attacks that compromise cyber security in the past several years. A graphic representation shows the depressing rise in ransomware, phishing, DDoS assaults, malware and data breaches from 2018 to the present 2024.

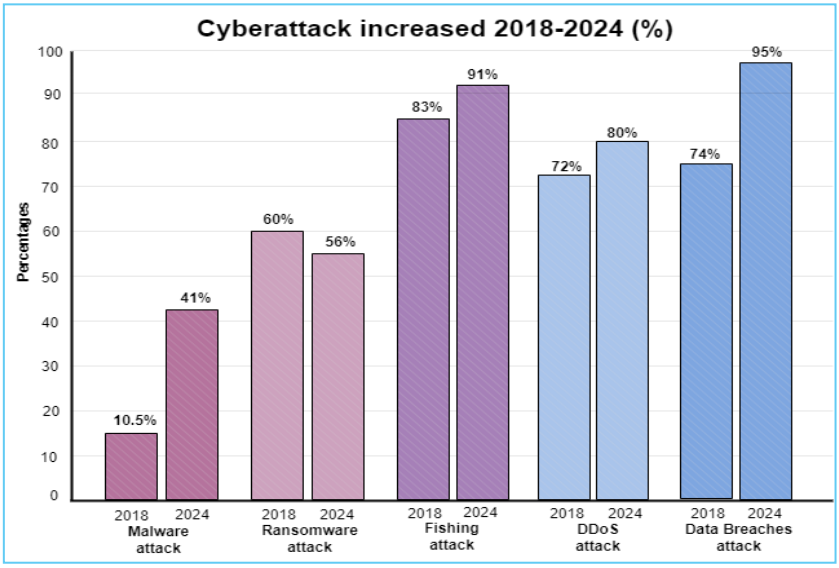

Figure 5. Exploring the Escalation of Cyberattacks (2018-2024).

4.1. The Constraints of Cybersecurity Solutions

In order to safeguard digital systems, networks, data and programs against cyberthreats, cyber security solutions are crucial. Cyber security solutions are built using a variety of methods to guard against data breaches, cyberattacks and unauthorized access.

- **Intrusion Detection Systems (IDS) and firewalls:** firewalls keep an eye on and regulate all incoming and outgoing network traffic. Firewalls regulate unlawful access barriers and examine data packets as they travel across the network. Firewalls cannot, however, identify internal threats. In other words, preventing internal risks cannot be achieved by concentrating on managing exterior traffic. Contrarily, intrusion detection and surveillance (IDS) security systems

 doi:10.20944/preprints202409.0407.v1

are made to look into unusual activity rather than policy infractions. IDS is unable to identify novel or complex attacks that diverge from typical patterns of network traffic.

- **Software for antivirus protection and endpoint detection and response (EDR):** These two elements are crucial to any contemporary cyber security plan. However, the background apps and real-time scanning of antivirus software can drain system resources and degrade system performance. Furthermore, it cannot identify sophisticated threats. The cyber security technology known as endpoint detection and response (EDR), on the other hand, continuously watches and examines endpoint activity in order to identify, look into and address security incidents and threats. Nevertheless, EDR can be difficult to set up and maintain and it was unable to identify new threats.
- **Multi-factor authentication (MFA):** MFA, sometimes referred to as two-factor authentication (2FA) or two-step verification, is an authentication method. It's a kind of security system where users have to authenticate themselves using two or more different methods before they can access a system or application. Consequently, security is enhanced. However, because of how difficult it is to manage, people may find it inconvenient.
- **Email Security Gates (SEG):** SEGs are a type of security solution that guards against ransomware, spam, phishing and other malicious email threats for a variety of enterprises. SEGs identify and filter unsolicited mass emails using sophisticated algorithms and heuristics. But the sophistication of phishing assaults is rising to the point that different people and organizations are becoming targets of email attacks.

5. Blockchain in Cyber security

The article goes into detail on how blockchain technology may be used in a variety of ways to greatly enhance cyber security, including through the use of its inherent decentralization, transparency and immutability qualities.

- **Decentralization:** Decentralization removes authority, control, and power from a central body. The system is not controlled by one entity. Decentralization reduces a single point of failure and prevents centralized institutions from censoring or manipulating data, improving data security, privacy, and resilience. It prevents cybercriminals from attacking directly by creating an impenetrable barrier. Multiple nodes receive information from decentralization. A ledger system stores data in each node. Cybercriminals cannot attack multiple nodes simultaneously. Data security remains unaffected.
- **Transparency:** One of the main characteristics of blockchain technology that is crucial for cyber security is transparency. Increased openness makes data that has been kept safe and permanent. Additionally, as blockchain technology makes every access accessible, transparency and accountability are clear. Each block of data in blockchain technology is connected to the one before it via a cryptographic hash. As a result, its genesis block can incorporate a clear audit trail. Blockchain technology increases the dependability of cyber security by ensuring authenticity, trust and transparency to stop data fraud and manipulation.
- **Immutability:** An attribute of blockchain technology, immutability essentially implies that once an item is entered into the blockchain, it cannot be altered or removed in any way. To preserve data immutability, numerous sophisticated cryptographic approaches and consensus procedures are used. In order to treat blockchains as immutable ledgers, proof of work is utilized. Moreover, every blockchain block is connected to every other block in a chain through the process of cryptographic hashing. Because of this, hackers are unable to alter the data of a block without also altering the data of every other block. However, blockchain's immutability renders it immune to manipulation, censorship and unauthorized changes.
- **Decentralized Storage:** Using blockchain technology to store data over a dispersed network of blockchain nodes instead of depending on a centralized server or data center is known as decentralized storage. In cyber security, this strategy helps to preserve data security, resilience and privacy. Data can therefore be shielded from unwanted access. Decentralized storage solutions, on the other hand, guarantee data availability and access by dividing up data copies among several network nodes.

 doi:10.20944/preprints202409.0407.v1

- **Smart Contract:** In the context of blockchain technology, a smart contract is a self-executing agreement with terms encoded directly into the code. Smart contracts have various uses in cyber security, with the main goals being to improve automation, security and transparency. Smart contracts guarantee that only authorized users have access to sensitive data or systems by enforcing access control regulations based on predetermined guidelines and criteria. Additionally, vulnerability disclosure programs and bug bounties in cyber security can be managed via smart contracts.

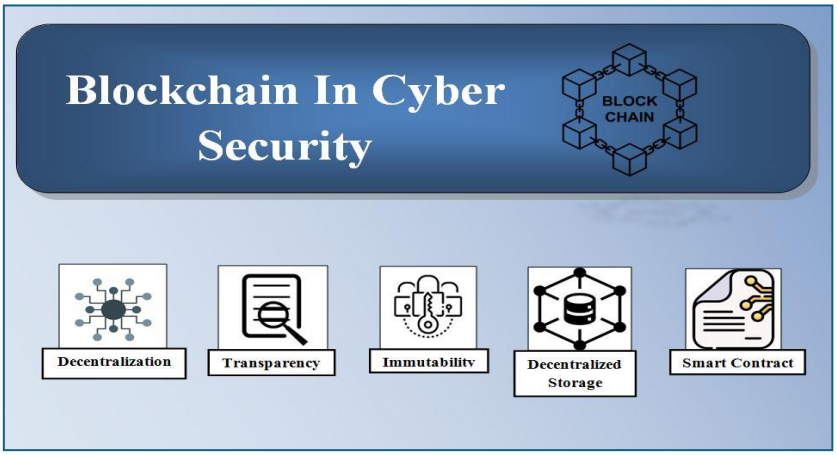

Figure 6. Blockchain in Cyber security.

6. Case Studies

Blockchain technology is being used more and more in cyber security to safeguard digital assets and enhance security procedures that offer creative fixes. Blockchain technology has significantly improved the integrity of cryptocurrencies by guaranteeing safe transactions and thwarting fraud. Blockchain technology is being used in healthcare data security to safeguard patient health records and ensure that private medical data is unchangeable and secure. Blockchain technology keeps hackers from being able to access any identifiable information in a patient's medical record. Blockchain technology can enhance porous security. Secure data encryption powers the entire system, effectively putting a wall between hackers and personally identifying information. Publicly accessible ledgers, decentralized information storage and encrypted data could create a new set of government cyber security priorities. For the military, defense contractors and space organizations that handle the most sensitive data, blockchain is seen as a viable data protection solution. These defense and military organizations enhance data security and maximize privacy by utilizing blockchain's encryption and decentralization techniques. Additionally, as IoT device security has grown, blockchain technology is being utilized to protect IoT devices from cyber-attacks, collect and transfer data and guarantee data integrity. The demand for more advanced cyber security solutions is growing along with the IoT device market. Blockchain offers a safe framework for data transfers between devices that prevents malevolent parties from getting involved. IoT devices can provide audit trails and tracking systems for product registration and consumption thanks to decentralized control.

6.1. Successes & Challenges

The application of blockchain technology has helped us succeed greatly in many different sectors. Because of its immutability, decentralization, and cryptographic encryption, blockchain-based solutions provide increased security and are impervious to tampering and unwanted access. Furthermore, blockchain technology is more resistant to hackers because to its distributed nature. The transparent ledger of blockchain enables real-time data tampering monitoring and aids in the early identification of cyberthreats. Stakeholders can also use it to confirm the accuracy of data and transactions. Blockchain lowers costs, simplifies procedures, boosts efficiency, and does away with

 doi:10.20944/preprints202409.0407.v1

the need for middlemen in transactions. By lowering the possibility of fraud and raising accountability, it also strengthens participant trust. Not with standing its success, blockchain technology application is not without its difficulties. Integrating blockchain technology into current systems, or integration, can be costly and time-consuming. As the volume of transactions rises, blockchain networks may encounter scalability issues that could result in longer processing times and more expenses. Since blockchain technology is still relatively new and there aren't many specialists who can properly deploy it, cost and resources also present a big issue. Consequently, businesses must spend money on expert recruiting or employee training, which can be expensive. Privacy issues provide still another significant obstacle. Privacy concerns stem from the public nature of blockchain networks, where all transactions are visible to all participants, notwithstanding the transparency that blockchain offers. Furthermore, the smooth integration and communication of blockchain-based solutions may be impeded by interoperability problems among various blockchain platforms and protocols.

7. Future Directions

First things first, the difficulties in keeping blockchain technology operational must be resolved. Technology, politics and industry collaboration are all necessary components of a comprehensive strategy to addressing issues like scalability, privacy, regulation and interoperability. The ability to scale One kind of protocol that uses blockchain technology to boost transaction capacity is called a layer 2 scaling solution. Sharding is the technique of splitting a database into smaller, quicker, easier-to-manage parts so that transactions can happen in parallel. Another name for it is shard. Time spent validating transactions and energy usage may be decreased as a result. In addition, network upgrades refer to the ongoing enhancement of network protocols and infrastructure in order to manage growing transaction volumes. The regulatory framework can be maintained by adhering to protocols including explicit guidelines, compliance programs, transparent governance, regulatory engagement, regulatory sandbox and smart contract compliance. Blockchain technology offers a variety of privacy-preserving techniques that can be used, including encryption, privacy coins, Secure Multiparty Computation (MPC) and Zero-Knowledge Proofs (ZKPs). Integrating zero-knowledge proofs to guarantee the legitimacy of private transactions is known as zero-knowledge proofing. Without disclosing the underlying data, encrypted data can be computed using the MPC protocol. Lastly, during transaction verification, data privacy can be preserved by utilizing sophisticated encryption techniques. Cross-chain communication protocols, which allow information to be transferred and exchanged between multiple blockchain networks with ease, can be designed to guarantee interoperability in blockchain technology.

Furthermore, these approaches combine legislative and technological advancements to help overcome obstacles and open the door for broader acceptance and more effective use of blockchain technology and other interconnected systems.

8. Conclusion

This essay highlights the huge potential for growing the use of blockchain technology for cyber security. It highlights the various applications and benefits that blockchain offers to increase cyber resilience. This ongoing project investigates how smart contracts, decentralization, immutability and transparency in blockchain technology might be used to lessen cyber security risks. Furthermore, this research paper endeavors to offer a rudimentary comprehension of the diverse cyber security environments that are present in contemporary society. According to the current research described in this overview, cyber security is headed in a promising way. Blockchain technology is being utilized to create decentralized threat intelligence sharing platforms and self-sovereign identity systems in order to address the growing challenges related to cyber security in an interconnected world. This paper seeks to give a brief summary of the cyber security challenges related to scalability, interoperability and privacy that blockchain technology faces, despite its enormous potential. In addition, by encouraging collaboration, creativity and continuous research, we may use blockchain's revolutionary potential to create a stronger and safer cyber environment in the future.

 doi:10.20944/preprints202409.0407.v1

References

1. Hasanova, H., Baek, U.J., Shin, M.G., Cho, K. and Kim, M.S., 2019. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), p.e2060.
2. Patel, Priyanka, Ruby Bhatt, Manish Joshi, Govinda Patil, Hemant Pal, and Abdul Razzak Khan Qureshi. "Blockchain-Enabled Decentralized Edge Computing in Cyber Security for Intrusion Detection." *International Journal of Intelligent Systems and Applications in Engineering* 12, no. 13s (2024): 28-40.
3. Patel P, Bhatt R, Joshi M, Patil G, Pal H, Qureshi AR. Blockchain-Enabled Decentralized Edge Computing in Cyber Security for Intrusion Detection. International Journal of Intelligent Systems and Applications in Engineering. 2024 Jan 29;12(13s):28-40.
4. Aggarwal, B.K., Gupta, A., Goyal, D., Gupta, P., Bansal, B. and Barak, D.D., 2022. A review on investigating the role of block-chain in cyber security. *Materials Today: Proceedings*, *56*, pp.3312-3316.
5. Taylor, Paul J., Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, and Kim-Kwang Raymond Choo. "A systematic literature review of blockchain cyber security." *Digital Communications and Networks* 6, no. 2 (2020): 147-156.
6. Demirkan, S., Demirkan, I. and McKee, A., 2020. Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), pp.189-208.
7. Zhuang, P., Zamir, T. and Liang, H., 2020. Blockchain for cybersecurity in smart grid: A comprehensive survey. *IEEE Transactions on Industrial Informatics*, *17*(1), pp.3-19.
8. Rathore, S. and Park, J.H., 2020. A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics*, *17*(8), pp.5522-5532.
9. Ghiasi, Mohammad, Moslem Dehghani, Taher Niknam, Abdollah Kavousi-Fard, Pierluigi Siano, and Hassan Haes Alhelou. "Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform." *Ieee Access* 9 (2021): 29429-29440.
10. Maulani, G., Gunawan, G., Leli, L., Nabila, E.A. and Sari, W.Y., 2021. Digital certificate authority with blockchain cybersecurity in education. *International Journal of Cyber and IT Service Management*, *1*(1), pp.136-150.
11. Giannoutakis, K.M., Spathoulas, G., Filelis-Papadopoulos, C.K., Collen, A., Anagnostopoulos, M., Votis, K. and Nijdam, N.A., 2020, November. A blockchain solution for enhancing cybersecurity defence of IoT. In *2020 IEEE international conference on blockchain (blockchain)* (pp. 490-495). IEEE.
12. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C. and Platts, J., 2022. Cybersecurity, data privacy and blockchain: A review. *SN computer science*, *3*(2), p.127.
13. Zhao, W., Jiang, C., Gao, H., Yang, S. and Luo, X., 2020. Blockchain-enabled cyber–physical systems: A review. *IEEE Internet of Things Journal*, *8*(6), pp.4023-4034.
14. Ameen, A.H., Mohammed, M.A. and Rashid, A.N., 2023. Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions. *Journal of Intelligent Systems*, *32*(1), p.20220267.
15. Akbarov, N., Akbarova, M. and Goipova, X., 2023, October. Blockchain Technology for Network Security: Advancements and Potential Applications. In *Conference on Digital Innovation:" Modern Problems and Solutions"*.
16. Sharma, G., Sharma, D.K. and Kumar, A., 2023. Role of cybersecurity and Blockchain in battlefield of things. *Internet Technology Letters*, *6*(3), p.e406.
17. Deepak, A., William, P., Dubey, R., Sachdeva, S., Vinotha, C., Masand, S. and Shrivastava, A., 2024. Impact of Artificial Intelligence and Cyber Security as Advanced Technologies on Bitcoin Industries. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(3s), pp.131-140.
18. Patel, P., Bhatt, R., Joshi, M., Patil, G., Pal, H. and Qureshi, A.R.K., 2024. Blockchain-Enabled Decentralized Edge Computing in Cyber Security for Intrusion Detection. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(13s), pp.28-40.
19. Shukla, D., Chakrabarti, S. and Sharma, A., 2024. Blockchain-based cyber-security enhancement of cyber–physical power system through symmetric encryption mechanism. *International Journal of Electrical Power & Energy Systems*, *155*, p.109631.
20. Mahmood, S., Chadhar, M. and Firmin, S., 2022. Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies*, *2022*, pp.1-11.
21. Alotaibi, B., 2019. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. *IEEE Sensors Journal*, *19*(23), pp.10953-10971.
22. Mathew, A.R., 2019. Cyber security through blockchain technology. *Int. J. Eng. Adv. Technol*, *9*(1), pp.3821-3824.
23. Hasanova, H., Baek, U.J., Shin, M.G., Cho, K. and Kim, M.S., 2019. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), p.e2060.
24. Axon, L., Goldsmith, M. and Creese, S., 2018. Privacy requirements in cybersecurity applications of blockchain. In *Advances in Computers* (Vol. 111, pp. 229-278). Elsevier.

 doi:10.20944/preprints202409.0407.v1

25. Hölbl, M., Kompara, M., Kamišalić, A. and Nemec Zlatolas, L., 2018. A systematic review of the use of blockchain in healthcare. *Symmetry*, *10*(10), p.470.
26. Villarreal, E.R.D., García-Alonso, J., Moguel, E. and Alegría, J.A.H., 2023. Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE Access*, *11*, pp.5629-5652.
27. Andrew, J., Deva Priya Isravel, K. Martin Sagayam, Bharat Bhushan, Yuichi Sei, and Jennifer Eunice. "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions." *Journal of Network and Computer Applications* (2023): 103633.
28. Chen, X. and Lai, P.C., 2023. The novel thinking exploration model for Blockchain Technology Financial Sharing Services. *JISTEM-Journal of Information Systems and Technology Management*, *20*, p.e202320005.
29. Wu, H., Yao, Q., Liu, Z., Huang, B., Zhuang, Y., Tang, H. and Liu, E., 2024. Blockchain for finance: A survey. *IET Blockchain*.
30. Karadag, B., Zaim, A.H. and Akbulut, A., 2024. Blockchain in Finance: A Systematic Literature Review.
31. Han, Yanhu, and Xiao Fang. "Systematic review of adopting blockchain in supply chain management: bibliometric analysis and theme discussion." *International Journal of Production Research* 62, no. 3 (2024): 991-1016.
32. Risso, L.A., Ganga, G.M.D., Godinho Filho, M., de Santa-Eulalia, L.A., Chikhi, T. and Mosconi, E., 2023. Present and future perspectives of blockchain in supply chain management: A review of reviews and research agenda. *Computers & Industrial Engineering*, p.109195.
33. Uddin, M., Selvarajan, S., Obaidat, M., Arfeen, S.U., Khadidos, A.O., Khadidos, A.O. and Abdelhaq, M., 2023. From hype to reality: Unveiling the promises, challenges and opportunities of blockchain in supply chain systems. *Sustainability*, *15*(16), p.12193.
34. Sajja, G.S., Rane, K.P., Phasinam, K., Kassanuk, T., Okoronkwo, E. and Prabhu, P., 2023. Towards applicability of blockchain in agriculture sector. *Materials Today: Proceedings*, *80*, pp.3705-3708.
35. Ordoñez, Cristian Camilo, Gustavo Ramírez Gonzales, and Juan Carlos Corrales. "Blockchain and agricultural." (2024).
36. Das, D., Banerjee, S., Chatterjee, P., Ghosh, U. and Biswas, U., 2023. Blockchain for intelligent transportation systems: Applications, challenges, and opportunities. *IEEE Internet of Things Journal*.
37. Jiang, S., Cao, J., Wu, H., Chen, K. and Liu, X., 2023. Privacy-preserving and efficient data sharing for blockchain-based intelligent transportation systems. *Information Sciences*, *635*, pp.72-85.
38. Ocheja, P., Flanagan, B., Ogata, H. and Oyelere, S.S., 2023. Visualization of education blockchain data: trends and challenges. *Interactive Learning Environments*, *31*(9), pp.5970-5994.
39. Haque, M., Kumar, V.V., Singh, P., Goyal, A.A., Upreti, K. and Verma, A., 2023. A systematic meta-analysis of blockchain technology for educational sector and its advancements towards education 4.0. *Education and Information Technologies*, *28*(10), pp.13841-13867.
40. Asaithambi, S., Ravi, L., Devarajan, M., Almazyad, A.S., Xiong, G. and Mohamed, A.W., 2024. Enhancing enterprises trust mechanism through integrating blockchain technology into e-commerce platform for SMEs. *Egyptian Informatics Journal*, *25*, p.100444.
41. AbdelSalam, F.M., 2023. Blockchain Revolutionizing Healthcare Industry: A Systematic Review of Blockchain Technology Benefits and Threats. *Perspectives in Health Information Management*, *20*(3)