International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

A review on blockchain impact on in cybersecurity: Current applications, challenges and future trends

Mani Gopalsamy *

Louisville, KY, USA- 40220.

International Journal of Science and Research Archive, 2022, 06(02), 325–335

Publication history: Received on 22 May 2022; revised on 24 July 2022; accepted on 27 July 2022

Article DOI: https://doi.org/10.30574/ijsra.2022.6.2.0146

Abstract

The potential for blockchain to transform several industries, including cybersecurity, has piqued the interest of many different sectors. This abstract delves into the relationship between blockchain and cybersecurity, showcasing how the two may work together to strengthen data security. The present cybersecurity scenario prompted this study to examine existing blockchain-based security solutions. In this study, we looked at the ways blockchain technology maintains the security triangle. The results show that blockchain has a lot of promise for solving current cybersecurity problems, especially with IoT, data ownership and integrity, and network security. However, high-cost complexity, regulatory barriers, and technology immaturity all hinder wider implementation. As a result, using blockchain-based solutions in cybersecurity requires careful consideration of how well they apply to the particular requirements of an organisation, as well as the establishment of precise implementation objectives and the navigation of potential obstacles. This pertinent systematic review sheds light on several subjects that should be explored further as fields for cyber and blockchain security research, education, and practice, including blockchain security in the IoT, blockchain security for AI data, and sidechain security.

Keywords: Cybersecurity; Blockchain technology; Cybersecurity through blockchain technology; Challenges and future trends

1. Introduction

Many industries, including healthcare, banking, and Industry 4.0, have found blockchain technology to be a safe and efficient solution. An immutability, decentralisation, and transparency of blockchain technology have made it a popular choice for loyalty program administration [1]. Blockchain technology (BT) is a decentralised system for managing transactions and data that offers security, privacy, and data integrity without requiring a third-party organisation to be involved in the transaction process[2]. By using electronic invoicing ledgers, BT has control over equity for online transactions. BT is also seeing use in industries such as e-commerce, supply chain management, gaming, gambling trade, and finance. The BT behind the BT system is a digital ledger that records every transaction ever made[3].

In addition, the distributed blockchain network's nodes (users) are all capable of managing the shared ledger. Assembled blocks form chains, with the bottom block serving as the base of each stack. The building blocks of the chain are interconnected[4]. A cryptographic hash method is used to create a unique hash for each block. It is possible for a block to have more than one child block and only one parent block in a chain[5]. A block's header links it to its parent blocks in a chain; it's composed of a unique hash of those blocks. Genesis blocks are the first building blocks of a cryptocurrency network; the first Bitcoin block was generated in 2009. In contrast to conventional centralised database systems, the BT system keeps an ever-expanding list of transaction records digitally, serving as a record of ownership. From an accessibility and organisation standpoint, there are three main types of BT-related activities:

* Corresponding author: Mani Gopalsamy

- The first-generation public blockchain,
- The second-generation public blockchain,
- The third-generation private blockchain [6].

Deep association analysis at the finer levels and mining of big, disparate, diversified security datasets are both within its capabilities [7][8]. Security analysts rely on cybersecurity knowledge graphs to get a more intuitive grasp of the present security condition and to decipher intricate patterns of network attacks from threat information[9]v. Security entity identification, connection extraction, and attribute extraction are the core components of cybersecurity knowledge graph creation technology[10]. Cybersecurity knowledge graphs are built on top of security entity recognition technologies[11][12].

The proliferation of cryptocurrencies has increased the technology's profile, but it has other potential uses outside of the financial industry as well. A simple definition of a blockchain would be a network of interconnected cryptographically secured blocks [13]. An information structure's "blocks" are made up of three pieces: data, the hash of the block that came before it, and the hash of both. Thus, to guarantee the complete[14][15]. Blockchain's integrity, there is a dependence order between blocks. Any modification to the contents of any block will also affect its hash. The hashes of the blocks that follow will also become invalid as a result of this domino effect. This is the reason why Blockchain transactions cannot be changed. Problem areas with cybersecurity, like the IoT, networks, and data storage and transmission, may benefit greatly from this architecture [16].

Examining the present uses, difficulties, and potential future trends of blockchain technology as it pertains to cybersecurity is the primary goal of this study. By exploring the integration of blockchain in areas such as data integrity, decentralised identity management, and secure transactions, the study aims to demonstrate how blockchain enhances security and privacy in various sectors. Additionally, it addresses the challenges posed by quantum computing, interoperability, and evolving cryptographic standards while also identifying future opportunities for leveraging blockchain technology to strengthen cybersecurity frameworks and systems.

- The study highlights the use of BT for enhancing data integrity and cybersecurity through its immutable ledger and decentralised framework.
- It explores blockchain’s application in decentralised identity management, decreasing a risks of identity theft and data breaches.
- The study demonstrates how blockchain can facilitate secure transactions and ensure transparency by eliminating a need for intermediaries.
- It presents blockchain as a solution for improving supply chain security and preventing tampering in industries like pharmaceuticals and luxury goods.
- The study discusses blockchain's potential for decentralised cybersecurity solutions, such as decentralised VPNs and peer-to-peer networks, improving resilience against cyber threats.

1.1. Structure of the Paper

The article is structured as follows: an introduction to blockchain and cybersecurity ideas is provided at the beginning. Section II introduces the concept of blockchain technology, while Section III delves into its potential uses in the information security industry. Key issues and weaknesses in blockchain security are addressed in Section IV. The article features a summary and future directions in Section VI, after which Section V delves into real-world use cases.

2. Overview of Cybersecurity

Furthermore, there is a tendency for public discourse to erroneously conflate cybersecurity with concepts such as privacy, information sharing, intelligence collection, and monitoring. The ability to control who has access to one's private information is fundamental to the idea of privacy. In an electronic world, privacy may, therefore, be safeguarded by effective cybersecurity[17][18]. On the other hand, material shared to enhance cybersecurity initiatives could sometimes include details that some onlookers would regard as private. Cybersecurity is a way to prevent unauthorised people from spying on your information system and stealing sensitive data. On the other hand, these kinds of actions might be beneficial to cybersecurity when directed towards possible cyberattack vectors[19][20]. Figure 1 shows the cyber security tools and techniques.

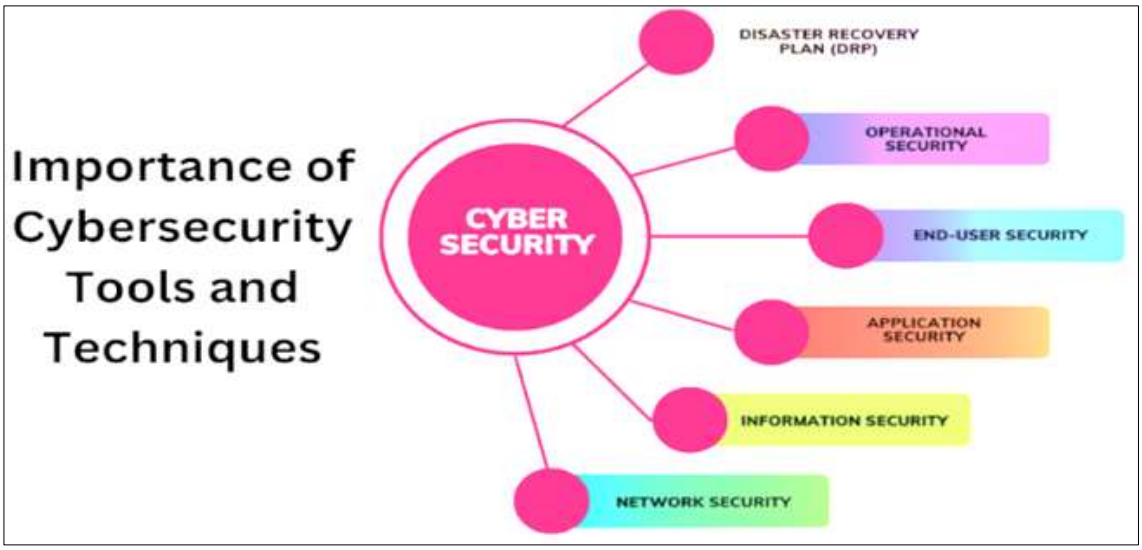

Figure 1 Cyber Security tools and techniques

Cybersecurity is necessary because many institutions, including those in the military, business, financial, and medical sectors, keep vast quantities of sensitive information on vulnerable networks[21][22]. Illegal access or acquisition of the data stored on these systems might have wide-ranging and detrimental consequences for individuals or potentially the whole planet[23]. The chairman, president, and CEO of IBM, Gini Rometty, has said that cybercrime poses the biggest risk to all businesses worldwide[24][25].

The majority of cyberattacks follow a standard, multi-stage procedure. Collecting information on a particular target network is known as surveillance and is the first stage in this process[26]. Port scans and ping scans are two ways to discover the existence of hosts and the services they provide. Remote exploitation of vulnerabilities linked to the services discovered in the first step constitutes the second phase. It is possible to make use of internal trust connections in the context of cybersecurity development, as seen in Figure 2:

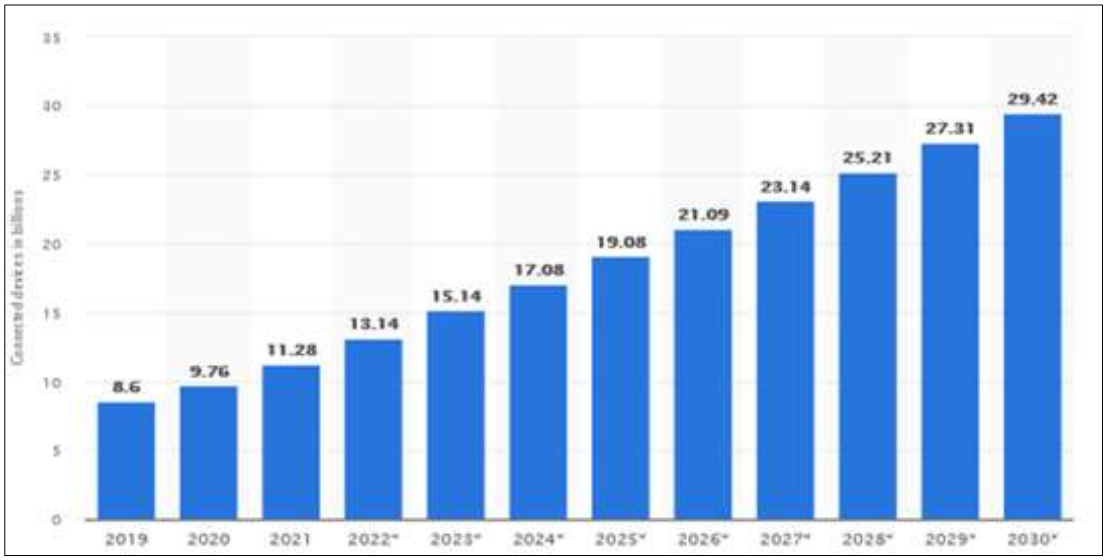

Figure 2 Growth of cybersecurity

2.1. Threats to cybersecurity

The failure to take adequate precautions, such as using only protected software or programs, allows the majority of cybercrimes to occur[27]. Cybercriminals launch their attacks on networks comprised of vulnerable computers and other electronic devices. All aspects of cyber must be considered for cyber security to be successful.

- Network security
- Data security
- Database and infrastructure security
- Cloud security
- Mobile Security
- Disaster recovery/business continuity planning End-use education.

2.2. Elimination of Human Factor

Businesses no longer have to worry about authenticating users and devices without passwords due to BT. Avoiding an attack technique becomes easier when human mistake is eliminated.

2.3. Secured Private Messaging

In order to complete tasks, communication inside an organisation about papers and other work-related data is essential. However, often, this material is sent across several messaging and social media applications, which increases the risk of content theft.

3. Overview of Blockchain Technology

A distributed network with several linked nodes is a feature of blockchain technology. The whole ledger, including all transactions from the very beginning, is replicated on each node [27][28]. Because the chain is peer-to-peer connected, no one individual has control over the whole network[21][29]. The majority of nodes must accept the transaction for it to function. Nobody is able to identify the voter due to the way blockchain operates [30].

The blockchain concept was first put out. Originally, it served as a distributed ledger that solely verified Bitcoin-related transactions[31]. Researchers began to pay attention to the enormous potential that Bitcoin has as its popularity increased. Figure 3 illustrates areas of blockchain technology.

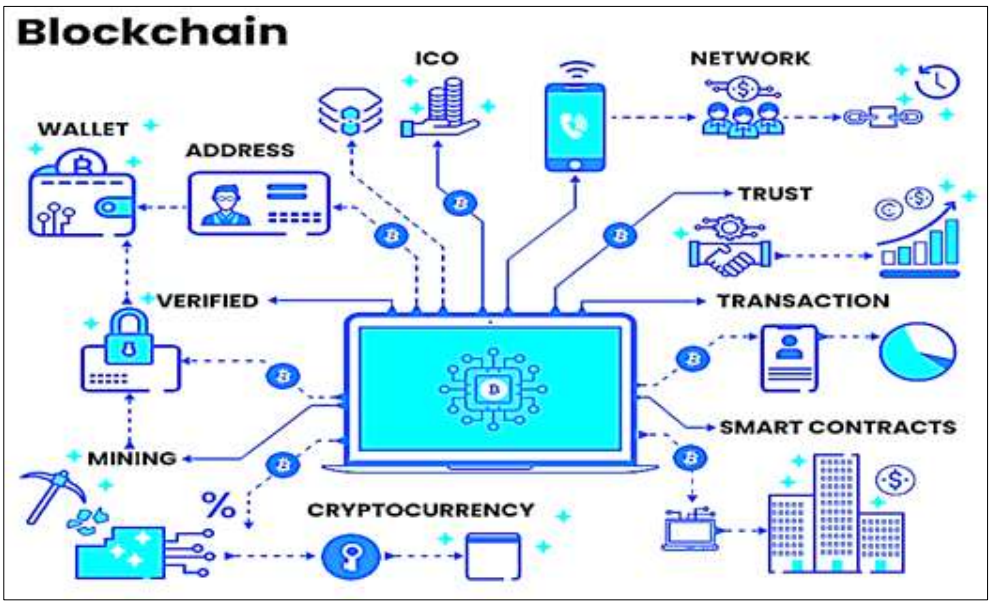

Figure 3 Blockchain Technology

Blockchain Technology Offers Benefits Over Traditional Client-Server Based Applications in A Number of ways:

The more blockchain nodes there are in a network, the more resistant it will be to cyberattacks, according to the distributed nature of blockchain technology.

- The blockchain database is copied across all nodes that are involved. Transparency between users who are not trusted is achieved by this configuration.

- To provide a complete record of all transactions, blockchain technology relies on an append-only ledger, which means that no one can alter or delete a transaction.
- The use of encryption ensures that no one has altered data stored in a blockchain, which makes the ledger verifiable and safe.
- A consensus process is used to generate and verify all blockchain transactions. Anyone prepared to put in the time and effort to keep a blockchain network running may participate in the open competition made possible by this new crowd-sourced transaction and verification procedure.

4. Cyber Security Through Blockchain Technology

Initially, a blockchain was only a growing list of blocks. The data of transactions that have taken place, together with a timestamp and a hash, make up each block. Blockchain is a distributed ledger system that efficiently and, more importantly, permanently records all transactions in a verifiable manner. The immutability of data once entered into the blockchain ledger is its defining characteristic [32]. Figure 4 shows Blockchain use cases in cybersecurity.

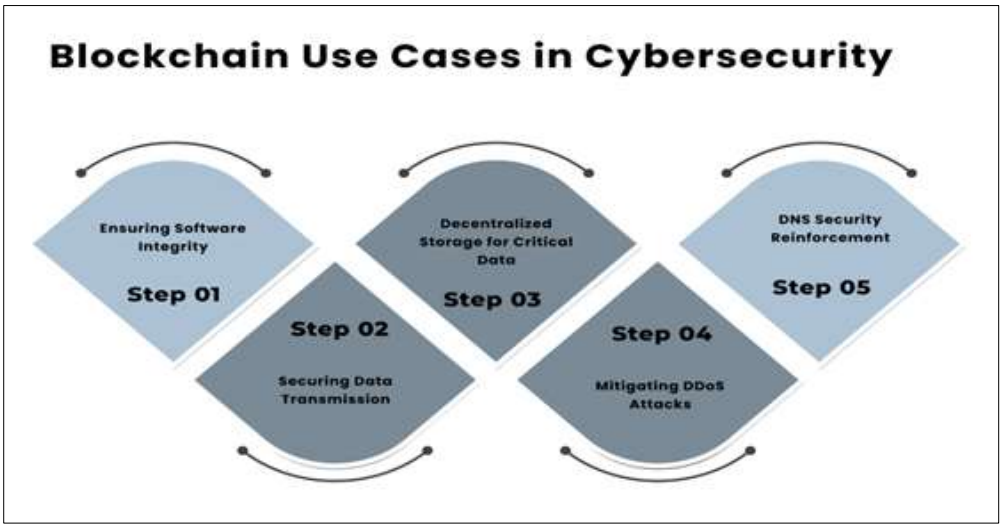

Figure 4 Blockchain use cases in cybersecurity

Current ballot-based voting has a number of issues that the blockchain plan on electronic voting can fix[33][34]. Since it is impossible to publicly verify vote manipulation in the existing system, blockchain's permanent nature may put an end to it [35][4]. It is possible to reduce other inconsistencies, such as the lack of verification of vote tallying, computer manipulation, manual vote tallying, and bullying throughout the voting process. An examination of blockchain technology reveals its promise to improve the trustworthiness of voting systems [36].

The domains like smart cities and the IoT. Table 1 below shows the following subsections that show how blockchain is used in smart cities and the IoT[5]:

Table 1 Blockchain In IOT

IoT Challenges	Blockchain-based solutions
Security	There is no central point of failure with blockchain, which makes it a secure option for the IoT.
Privacy	A key component of blockchain technology is its ability to maintain user anonymity.
Trust	A key component of the IoT ecosystem is trust, which blockchain's immutability capability ensures.
	The decentralised nature of blockchain technology lowers IoT implementation costs by keeping out undesirable third parties.

Attacks on information and communication technology systems are carried out by unauthorised individuals, often with the goal of committing theft, disruption, destruction, or other unlawful acts [37]. Over the next years, a lot of analysts predict that both the quantity and intensity of cyberattacks will rise.1 The process of protecting ICT systems and the

data they hold is known as cybersecurity. Figure 5 illustrates how cybersecurity, a broad and maybe somewhat nebulous topic, can be valuable but resists a clear definition.

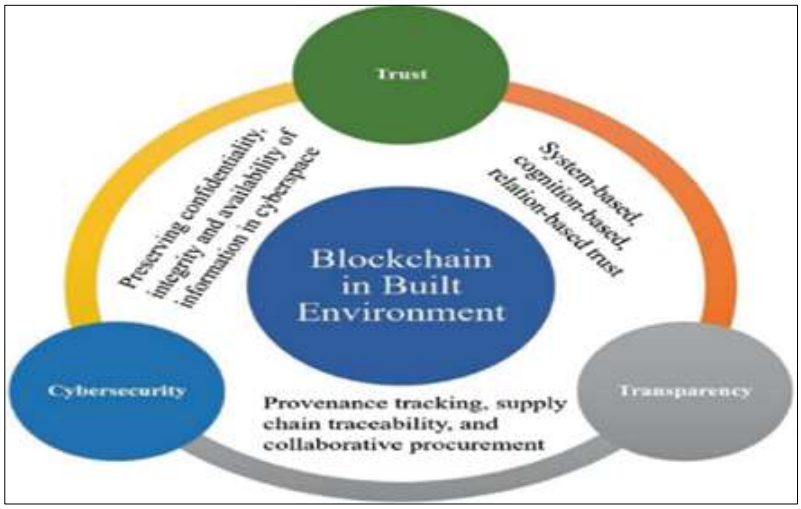

Figure 5 Blockchain in Built Environment

It usually refers to one or more of three things:

Cybersecurity is the practice of taking extra measures to prevent unauthorised access to, or alteration of, data stored on, transmitted by, or connected with computers, networks, and related hardware and software, as well as other cyberspace components.[38].

- The condition or attribute of being shielded from certain dangers.
- The wide range of actions aimed at putting such plans into action and raising their quality.

The concept is similar to, but not necessarily the same as, information security, which is defined by federal law as the prevention of loss, misuse, alteration, or destruction of data or computer systems in order to ensure the following:

- Integrity includes protecting against unauthorised information alteration or deletion and guaranteeing the validity and nonrepudiation of information.;
- Confidentiality, meaning that approved controls on disclosure and access must be maintained, along with methods for safeguarding private information and intellectual property; and
- Availability, meaning that data must be accessible and used reliably and in a timely manner.

5. Applications of Cybersecurity Through Blockchain Technology

There are a number of novel uses for blockchain technology in cybersecurity.

Data Integrity and Verification: Blockchain's immutable ledger ensures that data cannot be altered retroactively. Particularly helpful for checking the authenticity of private information like bank records or social security numbers [39].

5.1. Here are some key areas where it can enhance security:

- **Decentralized Identity Management:** Users may take ownership of their own identification data by using blockchain technology to establish safe, decentralised identity systems. The likelihood of data breaches and identity theft is lessened as a result[35].
- **Secure Transactions:** Automation and security of transactions devoid of middlemen are possible with smart contracts on blockchain. As a result, there is less opportunity for fraud and more clarity in financial dealings.
- **Supply Chain Security:** Through the use of blockchain technology, the origin of items can be traced, providing assurance that products have been handled with integrity all the way through the supply chain. This is vital for industries like pharmaceuticals and luxury goods[40].

- **Access Control and Authentication:** Blockchain can facilitate secure access control systems by storing and managing user credentials in a decentralised manner, reducing the risks associated with centralised databases.
- **Threat Intelligence Sharing:** Organizations can use blockchain to share threat intelligence data securely and transparently. This collaborative approach helps in identifying and mitigating cybersecurity threats more effectively[41].
- **Secure Voting Systems:** By using blockchain technology, voting methods may be made transparent and impenetrable, increasing election security and public confidence in democratic processes[12].
- **Incident Response and Forensics:** Blockchain can provide a secure, auditable trail of events leading up to a cybersecurity incident, aiding in forensic investigations and incident response.
- **Data Sharing and Privacy:** By using cryptographic techniques, blockchain allows secure sharing of data while maintaining user privacy. This is important for sectors like healthcare, where sensitive information needs to be shared securely[42].
- **Decentralized Cybersecurity Solutions:** Blockchain can support decentralised security applications, such as decentralised VPNs or security-focused peer-to-peer networks, reducing reliance on single points of failure.

These applications highlight how blockchain can complement existing cybersecurity measures, offering enhanced protection, transparency, and user control.

6. Challenges and Future Trends

Here are some challenges and future trends in blockchain technology that could impact cybersecurity[43][44]:

6.1. Advanced Cryptography

- **Quantum-Resistant Algorithms:** As quantum computing advances, the need for quantum-resistant cryptographic techniques will become critical to protect blockchain systems from potential vulnerabilities.

6.2. Decentralized Identity Solutions

- **Self-Sovereign Identity:** Users will increasingly manage their own identities on blockchain, reducing reliance on centralised authorities and minimising identity theft risks.

6.3. Interoperability Standards

- **Cross-Chain Solutions:** Development of robust interoperability protocols will facilitate secure communication between different blockchains, reducing the risk of vulnerabilities in cross-chain transactions.

6.4. Automated Security Audits

- **AI and Machine Learning:** Leveraging AI for continuous security monitoring and automated auditing of smart contracts will help identify vulnerabilities before they can be exploited.

6.5. Privacy-Enhancing Technologies

- **Zero-Knowledge Proofs:** These technologies will gain traction, allowing for transaction validation without revealing sensitive information, enhancing user privacy while maintaining security.

6.6. Regulatory Frameworks

- **Standardization and Compliance:** As blockchain adoption grows, regulatory bodies will establish clearer guidelines, prompting organisations to enhance their security measures to comply with legal requirements.

6.7. Decentralized Finance (Defib) Security Enhancements

- **Insurance and Risk Management Solutions:** As Defib evolves, insurance products for smart contract failures and hacks will become more prevalent, providing users with added security against losses.

6.8. Integration with IoT and AI

- **Secure IoT Deployments:** Combining blockchain with IoT can enhance device security through tamper-proof data logging, while AI can help identify and mitigate threats in real time.

7. Literature Review

This section provides a literature review of Blockchain Impact on Cybersecurity: Current Applications, Challenges and Future Trends shown in Table 2:

In this study, Liu, (2020) explores how blockchain technology has altered the field of internal auditing. This article investigates and builds the operating mode of "blockchain + internal auditing," then examines the application problems around it, by analysing the features of BT and how these features are applicable to internal auditing. Additionally, it delves into how internal auditing functions are reshaped within this framework[45].

This study, Alkhalifah et al., (2019) classify against the most important blockchain cybersecurity flaws, as the number of attacks has been on the rise recently, likely caused by the absence of adequate security measures in the digital currency exchange and the underlying weaknesses in smart contracts. This report surveyed 80 research articles with an emphasis on blockchain security concerns. This review article covers prominent studies on blockchain ecosystems, blockchain division, blockchain implementation, security concerns, and blockchain problems[46].

In this study, Taylor et al., (2020) conducts an exhaustive analysis of the most popular blockchain security applications and identifies scholarly works that seek to use blockchain technology to achieve objectives related to cyber defence. Our study indicates that the IoT, networks, ML, public-key cryptography, online applications, certification programs, and the secure storage of PII might all be very beneficial for future blockchain applications[47].

In this, Vance and Vance, (2019) study aimed to assess the evolution of blockchain technology, assess its present uses in the energy industry, and suggest future uses by reviewing blockchain research published between 2015 and 2019. Blockchain-based cybersecurity research and applications have grown at an average yearly pace of 169% in the energy sector since 2015. This rise has been attributed to an increased emphasis on IoT and Smart Grid infrastructures, as shown by quantitative analysis. The study and use of IoT and Smart Grids are expected to grow further, according to computed forecasts[48].

In this, Maleh et al., (2020) Blockchain technology and its applications in cybersecurity are the primary topics of this book. Learn about blockchain's many uses in healthcare and the IoT for security purposes. Included in the book's extensive examination of the key subjects are: Aspects of blockchain design and obstacles Risks and Exposures in the Blockchain Potential future use cases and blockchain security Using blockchain technology to protect IoT devices Encryption using blockchain technology in healthcare Blockchain technology for enhancing the privacy and security of financial transactions[44].

Table 2 Literature Review Summary for Blockchain Impact on Cybersecurity

Study	Focus	Study	Key Findings	Limitations	Future Work
[45]	Impact of blockchain on internal auditing	Analysis of blockchain characteristics	Constructs the operation mode of 'blockchain + internal auditing'; discusses transformative potential for auditing functions.	Limited empirical data on practical applications of blockchain in auditing requires further validation of proposed models.	Explore real-world case studies to assess the effectiveness of blockchain in various auditing environments.
[46]	Cybersecurity vulnerabilities in blockchain	Review of 80 research papers	Identifies an upward trend in attacks; highlights security gaps in digital currency exchanges and smart contracts.	Focus on vulnerabilities may overlook broader systemic issues in blockchain security; limited geographic scope.	Investigate additional security frameworks and their applicability to diverse blockchain implementations.
[47]	Cybersecurity vulnerabilities in blockchain	Systematic literature review	Analyses frequent blockchain security applications; suggests integration	Limited focus on specific applications may not encompass all potential use	Expand research to include more industries, particularly emerging

			with IoT, public-key cryptography, and secure storage of PII.	cases across industries.	sectors like AI and machine learning integration.
[48]	Blockchain in the energy sector	Quantitative and qualitative analysis	Reports 169% annual growth in blockchain-based cybersecurity research; emphasises IoT and Smart Grid applications.	Analysis confined to studies published up to 2019; potential for significant developments post-2019.	Conduct updated analyses to track the evolution of blockchain applications in cybersecurity beyond 2019.
[44]	Fundamentals and challenges of blockchain for cybersecurity.	Comprehensive literature review and case studies	Covers architectures, threats, and use cases in IoT and healthcare; provides a resource for various stakeholders in the field.	Generalisations may overlook niche challenges specific to certain applications (e.g., healthcare vs. IoT).	Delve deeper into sector-specific challenges and tailor solutions for distinct industries; consider interdisciplinary approaches.

8. Conclusion

Blockchain technology has shown that it can transform cybersecurity by providing improved security, privacy, and transparency across a range of applications. From decentralised identity management to secure voting systems, blockchain provides an immutable and verifiable way to protect sensitive data. Its decentralised nature eliminates many risks associated with traditional, centralised systems, making it a robust solution for a huge range of cybersecurity challenges. However, as blockchain technology continues to evolve, it will face new challenges, including quantum computing threats, interoperability issues, and the need for more advanced cryptographic techniques.

Future research in this field should concentrate on building more decentralised identification solutions, developing quantum-resistant algorithms, and fusing blockchain technology with cutting-edge innovations like AI and the IoT to build more effective and safe cybersecurity systems. Additionally, establishing regulatory frameworks will be critical to ensuring that blockchain implementations remain secure and compliant with legal requirements.

References

[1] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, H. A. Pham, N. H. Tuong, and E. Dutkiewicz, "Blockchain-based Secure platform for coalition loyalty program management," in *IEEE Wireless Communications and Networking Conference, WCNC*, 2021. doi: 10.1109/WCNC49053.2021.9417501.

[2] V. Kumar and F. T. S. Chan, "A superiority search and optimisation algorithm to solve RFID and an environmental factor embedded closed loop logistics model," *Int. J. Prod. Res.*, vol. 49, no. 16, 2011, doi: 10.1080/00207543.2010.503201.

[3] A. Razaque *et al.*, "Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled cybersecurity awareness system," *Appl. Sci.*, 2021, doi: 10.3390/app11177880.

[4] J. Thomas and V. Vedi, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 9, 2021.

[5] J. Thomas, K. V. Vedi, and S. Gupta, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–879, 2021.

[6] H. Hasanova, U. jun Baek, M. gon Shin, K. Cho, and M. S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *Int. J. Netw. Manag.*, 2019, doi: 10.1002/nem.2060.

[7] Y. Fang, Y. Zhang, and C. Huang, "CyberEyes: Cybersecurity Entity Recognition Model Based on Graph Convolutional Network," *Comput. J.*, 2021, doi: 10.1093/comjnl/bxaa141.

[8] S. G. Kumud Dixit, Priya Pathak, "SECURE LOCATION SELECTION USING TRUSTED AUTHORITY OR RSU IN AODV BASED VANET," *IJCCER*, vol. 4, no. 1, pp. 10–14, 2016.

[9] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey," *IEEE Trans. Ind. Informatics*, 2021, doi: 10.1109/TII.2020.2998479.

[10] V. K. Yarlagadda and R. Pydipalli, "Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity," *Eng. Int.*, vol. 6, no. 2, pp. 211–222, 2018.

[11] V. K. Y. Nicholas Richardson, Rajani Pydipalli, Sai Sirisha Maddula, Sunil Kumar Reddy Anumandla, "Role-Based Access Control in SAS Programming: Enhancing Security and Authorization," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 6, no. 1, pp. 31–42, 2019.

[12] P. Pathak, A. Shrivastava, and S. Gupta, "A survey on various security issues in delay tolerant networks," *J Adv Shell Program.*, vol. 2, no. 2, pp. 12–18, 2015.

[13] S. G. Darshan Meena, Priya Pathak, "Crytography Bases Solution FOR Distributed Denial of Service Attack in Manet," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 6, pp. 219–234, 2016.

[14] S. Dixit, P. Pathak, and S. Gupta, "A novel approch for gray hole and black hole detection and prevention," in *2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016*, 2016. doi: 10.1109/CDAN.2016.7570861.

[15] R. Goyal, "THE ROLE OF REQUIREMENT GATHERING IN AGILE SOFTWARE DEVELOPMENT: STRATEGIES FOR SUCCESS AND CHALLENGES," *Int. J. Core Eng. Manag.*, vol. 6, no. 12, pp. 142–152, 2021.

[16] A. R. Mathew, "Cyber security through blockchain technology," *Int. J. Eng. Adv. Technol.*, 2019, doi: 10.35940/ijeat.A9836.109119.

[17] V. V. Kumar, F. T. S. Chan, N. Mishra, and V. Kumar, "Environmental integrated closed loop logistics model: An artificial bee colony approach," in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.

[18] V. Kumar, V. V. Kumar, N. Mishra, F. T. S. Chan, and B. Gnanasekar, "Warranty failure analysis in service supply Chain a multi-agent framework," in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.

[19] V. V. Kumar, A. Sahoo, and F. W. Liou, "Cyber-enabled product lifecycle management: A multi-agent framework," in *Procedia Manufacturing*, 2019. doi: 10.1016/j.promfg.2020.01.247.

[20] M. M. Alani, "Big data in cybersecurity: a survey of applications and future trends," *J. Reliab. Intell. Environ.*, 2021, doi: 10.1007/s40860-020-00120-3.

[21] M. Gopalsamy, "Artificial Intelligence (AI) Based Internet-ofThings (IoT)-Botnet Attacks Identification Techniques to Enhance Cyber security," *Int. J. Res. Anal. Rev.*, vol. 7, no. 4, pp. 414–420, 2020.

[22] M. Gopalsamy, "Advanced Cybersecurity in Cloud Via Employing AI Techniques for Effective Intrusion Detection," *Int. J. Res. Anal. Rev.*, vol. 8, no. 01, pp. 187–193, 2021.

[23] M. Gimenez-Aguilar, J. M. de Fuentes, L. Gonzalez-Manzano, and D. Arroyo, "Achieving cybersecurity in blockchain-based systems: A survey," *Futur. Gener. Comput. Syst.*, 2021, doi: 10.1016/j.future.2021.05.007.

[24] R. Goyal, "THE ROLE OF BUSINESS ANALYSTS IN INFORMATION MANAGEMENT PROJECTS," *Int. J. Core Eng. Manag.*, vol. 6, no. 9, pp. 76–86, 2020.

[25] V. V. Kumar, M. K. Pandey, M. K. Tiwari, and D. Ben-Arieh, "Simultaneous optimization of parts and operations sequences in SSMS: A chaos embedded Taguchi particle swarm optimization approach," *J. Intell. Manuf.*, 2010, doi: 10.1007/s10845-008-0175-4.

[26] A. P. A. Singh, "Streamlining Purchase Requisitions and Orders : A Guide to Effective Goods Receipt Management," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 5, pp. g179–g184, 2021.

[27] K. Patel, "Quality Assurance In The Age Of Data Analytics: Innovations And Challenges," *Int. J. Creat. Res. Thoughts*, vol. 9, no. 12, pp. f573–f578, 2021.

[28] Mani Gopalsamy, "Enhanced Cybersecurity for Network Intrusion Detection System Based Artificial Intelligence (AI) Techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 12, no. 01, pp. 671–681, Dec. 2021, doi: 10.48175/IJARSCT-2269M.

[29] V. K. Yarlagadda, "Harnessing Biomedical Signals: A Modern Fusion of Hadoop Infrastructure, AI, and Fuzzy Logic

in Healthcare," *Malaysian J. Med. Biol. Res.*, vol. 2, no. 2, pp. 85–92, 2021.

[30] A. Khandelwal, "Blockchain implimentation on E-voting System," in *Proceedings of the International Conference on Intelligent Sustainable Systems, ICISS 2019*, 2019. doi: 10.1109/ISS1.2019.8907951.

[31] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, "Assessment and improvement of intelligent controllers for elevator energy efficiency," in *IEEE International Conference on Electro Information Technology*, 2012. doi: 10.1109/EIT.2012.6220727.

[32] Y. Wang, G. Gou, C. Liu, M. Cui, Z. Li, and G. Xiong, "Survey of security supervision on blockchain from the perspective of technology," *J. Inf. Secur. Appl.*, 2021, doi: 10.1016/j.jisa.2021.102859.

[33] V. V Kumar, "An interactive product development model in remanufacturing environment : a chaos-based artificial bee colony approach," 2014.

[34] S. K. R. Anumandla, V. K. Yarlagadda, S. C. R. Vennapusa, and K. R. V. Kothapalli, "Unveiling the Influence of Artificial Intelligence on Resource Management and Sustainable Development: A Comprehensive Investigation," *Technol. \& Manag. Rev.*, vol. 5, no. 1, pp. 45–65, 2020.

[35] V. V. Kumar, S. R. Yadav, F. W. Liou, and S. N. Balakrishnan, "A digital interface for the part designers and the fixture designers for a reconfigurable assembly system," *Math. Probl. Eng.*, 2013, doi: 10.1155/2013/943702.

[36] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees," *Technol. Forecast. Soc. Change*, vol. 158, p. 120166, Sep. 2020, doi: 10.1016/j.techfore.2020.120166.

[37] S. Pandey, "A COMPREHENSIVE FRAMEWORK FOR JOB DESCRIPTION MANAGEMENT: INTEGRATION OF WORKDAY, BOX, AND GREENHOUSE FOR ENHANCED COMPLIANCE AND EFFICIENCY," *Int. J. Bus. Quant. Econ. Appl. Manag. reseacrh*, vol. 7, no. 1, pp. 48–56, 2021.

[38] M. Z. Hasan, R. Fink, M. R. Suyambu, M. K. Baskaran, D. James, and J. Gamboa, "Performance evaluation of energy efficient intelligent elevator controllers," in *IEEE International Conference on Electro Information Technology*, 2015. doi: 10.1109/EIT.2015.7293320.

[39] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, 2019, doi: 10.1016/j.neucom.2019.02.056.

[40] A. S. Ramakrishna Garine, Rajeev Arora, Anoop Kumar, "Advanced Machine Learning for Analyzing and Mitigating Global Supply Chain Disruptions during COVID-19," *SSRN*, pp. 1–6, 2020.

[41] R. Bishukarma, "The Role of AI in Automated Testing and Monitoring in SaaS Environments," *IJRAR*, vol. 8, no. 2, 2021, [Online]. Available: https://www.ijrar.org/papers/IJRAR21B2597.pdf

[42] R. Arora, "Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based ERP Applications," *8th Int. Conf. "Computing Sustain. Glob. Dev.*, no. March, pp. 458–463, 2021.

[43] M. Yassine, M. Alazab, I. Romdhani, and M. Shojafar, *Blockchain for Cybersecurity and Privacy:Architectures,Challenges and applications*, 1st ed. Boca Raton: CRC Press, 2020.

[44] Y. Maleh, M. Shojafar, M. Alazab, and I. Romdhani, *Blockchain for Cybersecurity and Privacy*, 1st ed. Boca Raton: CRC Press, 2020. doi: 10.1201/9780429324932.

[45] R. Liu, "A Preliminary Study of the Impact of Blockchain Technology on Internal Auditing," in *Proceedings - 2020 2nd International Conference on Applied Machine Learning, ICAML 2020*, 2020. doi: 10.1109/ICAML51583.2020.00066.

[46] 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 2019*, 2019. doi: 10.1109/CSDE48274.2019.9162381.

[47] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*. 2020. doi: 10.1016/j.dcan.2019.01.005.

[48] T. R. Vance and A. Vance, "Cybersecurity in the blockchain era: A survey on examining critical infrastructure protection with blockchain-based technology," in *2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings*, 2019. doi: 10.1109/PICST47496.2019.9061242.