


The Role of Blockchain Technology in Enhancing Cybersecurity: Emerging Trends and Future Perspective

^{1*} Mustafa Abdulhadi Ben Hmada 

¹ *Higter Institute for Sciences & Technology-Misrata, Libya.*

*Corresponding Author: BOFA_benhmada@uahoo.com

Information of Article

Article history:

Received: Feb 2023

Revised: Mar 2023

Accepted: May 2023

Available online: Jun 2023

Keywords:

Blockchain Technology

Cybersecurity Enhancement

Digital Security Innovations

Decentralized Data Protection

Future Trends in Cybersecurity

ABSTRACT

This paper delves into the pivotal role of blockchain technology in enhancing cybersecurity, addressing its emerging trends and future perspectives. The main objective is to investigate how blockchain can be leveraged to fortify digital security in an era of escalating cyber threats. Employing a comprehensive literature review and qualitative analysis, the study analyzes academic research, case studies, and expert interviews to offer a multifaceted understanding of the subject. Key findings reveal that blockchain's decentralization, immutability, and transparency provide robust solutions to various cybersecurity challenges, including data breaches, fraud, and unauthorized access. The technology finds application across diverse sectors, enhancing the security of digital transactions and personal data. However, the study also identifies significant challenges in blockchain implementation, such as scalability, integration complexities, and ethical considerations surrounding data privacy. Future perspectives suggest an optimistic outlook for blockchain in cybersecurity, with advancements poised to overcome existing limitations and pave the way for innovative applications, particularly in conjunction with AI and IoT technologies. The long-term impact of blockchain is projected to be transformative, significantly altering cybersecurity practices by providing more resilient and trustworthy digital infrastructures. Conclusively, the paper underscores blockchain's potential as a game-changer in cybersecurity, while also acknowledging the hurdles and ethical implications that need addressing. It serves as a comprehensive resource for understanding the current state and future potential of blockchain in enhancing cybersecurity, offering valuable insights for researchers, industry professionals, and policymakers.

1.0 Introduction

Blockchain technology, first introduced as the underlying framework for Bitcoin, has rapidly evolved into a cornerstone of modern digital infrastructure. Its relevance extends beyond cryptocurrencies, impacting various sectors including finance, healthcare, and government operations. As Catalini (2018) notes, blockchain's immutable and decentralized nature offers groundbreaking possibilities in digital transactions and data management, reshaping the landscape of digital economy and cybersecurity. This technology, characterized by its robustness against tampering and fraud, is becoming increasingly important in an era marked by frequent cyber-attacks and data breaches.

The current digital landscape is besieged with challenges in cybersecurity, ranging from data breaches and identity theft to advanced persistent threats and state-sponsored cyber-attacks. The increasing sophistication of cyber-attacks, as illustrated by d BH, T., Lehar, F., & Sarajevo, B. H. (2022), requires innovative and robust security solutions (d BH et al., 2022). Traditional cybersecurity measures are often centralized, creating single points of failure that can be exploited by attackers. Furthermore, the surge in IoT devices and the advent of 5G networks, as discussed by Han et al. (2021), have expanded the attack surface, making conventional security protocols insufficient (Han et al., 2021).

This study aims to explore how blockchain technology can address these burgeoning cybersecurity challenges. With its inherent properties of decentralization, transparency, and immutability, blockchain presents a paradigm shift in cybersecurity approaches. The study investigates the application of blockchain in enhancing data integrity, securing digital transactions, and safeguarding against unauthorized access, as highlighted by Demirkan, Demirkan, and McKee (2020) in the context of business cybersecurity (Demirkan et al., 2020). Additionally, the study examines how

blockchain can be integrated with other technologies like AI and IoT to fortify cybersecurity defenses, as suggested by Salam and Salam (2020) (Salam & Salam, 2020).

The scope of this paper encompasses an in-depth analysis of blockchain technology in cybersecurity, covering emerging trends and future perspectives. It delves into the innovative uses of blockchain in various cybersecurity applications, the integration with other cutting-edge technologies, and the challenges and limitations associated with its deployment. The paper also provides a forward-looking perspective on the potential impacts and future developments in blockchain technology, as discussed by Sharin, F. H., Hernandez, M. S., & Sentosa, I. (2023) and Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023), predicting how it could revolutionize cybersecurity practices in the long term (Sharin et al., 2023; Wenhua et al., 2023). Through this comprehensive exploration, the paper aims to provide a holistic view of blockchain's role in enhancing cybersecurity and its implications for the future of digital security.

2.0 Literature Review

Recent literature has extensively explored the intersection of blockchain technology and cybersecurity, providing a comprehensive understanding of both the current state and potential future directions. Catalini (2018) delves into the implications of blockchain technology and cryptocurrencies in the digital economy and governmental sectors, emphasizing its transformative role. Similarly, Demirkan, Demirkan, and McKee (2020) discuss how blockchain technology could revolutionize business cybersecurity and accounting, suggesting its potential to enhance the integrity and transparency of digital transactions (Demirkan et al., 2020). Gad et al. (2022) present a thorough review of emerging trends in blockchain technology, highlighting its diverse applications and future outlook, particularly in enhancing cybersecurity (Gad et al., 2022). Ghosh et al. (2020) focus on the security of cryptocurrencies within blockchain technology, addressing the current state-of-art, challenges, and future prospects in this domain (Ghosh et al., 2020). Giannoutakis et al. (2020) propose a blockchain solution for bolstering the cybersecurity defense of IoT, demonstrating the technology's practical applicability in contemporary digital infrastructure (Giannoutakis et al., 2020). In the context of emerging technologies, Han et al. (2021) explore the potential of blockchain in 5G networks, particularly for drone operations, which is indicative of its broader applicability in next-generation networks (Han et al., 2021). Kumar and Mallipeddi (2022) investigate the impact of cybersecurity on operations and supply chain management, identifying emerging trends and future research directions that include blockchain as a key component (Kumar & Mallipeddi, 2022). Mahmood, Chadhar, and Firmin (2022) conduct a scoping review of cybersecurity challenges in blockchain technology, providing an overview of the current landscape and its complexities. Salam and Salam (2020) discuss the Internet of Things (IoT) in the context of sustainability, considering privacy and cybersecurity perspectives and the role of blockchain in addressing these concerns (Salam & Salam, 2020).

While existing research has made significant strides in understanding blockchain's role in cybersecurity, certain gaps remain unaddressed. There is a need for more empirical studies and real-world case analyses that demonstrate the practical implementation and effectiveness of blockchain in diverse cybersecurity scenarios. Additionally, much of the current literature focuses on theoretical frameworks and potential applications, but lacks in-depth analysis of the long-term sustainability and scalability of blockchain solutions in cybersecurity. There is also a notable gap in understanding the integration challenges of blockchain with existing cybersecurity infrastructures, especially in legacy systems. The ethical and legal implications of blockchain in cybersecurity are another underexplored area, requiring more comprehensive research to navigate the complexities of data privacy, regulatory compliance, and cross-border data security. Furthermore, while some studies like Sharin, Hernandez, and Sentosa (2023) and Wenhua et al. (2023) touch upon future trends, there is a need for more predictive analyses that can guide policymakers and practitioners in preparing for the evolving landscape of blockchain in cybersecurity (Sharin et al., 2023; Wenhua et al., 2023). Overall,

the literature indicates a growing interest in the application of blockchain technology in cybersecurity, but calls for further exploration and empirical validation of its practicality, effectiveness, and long-term impact in the field.

3.0 Blockchain Technology: An Overview

Blockchain technology, at its core, is a decentralized digital ledger that records transactions across multiple computers in a way that ensures security, transparency, and immutability. Catalini (2018) articulates that the fundamental components of blockchain include a distributed network, cryptographic algorithms, consensus mechanisms, and smart contracts. The distributed nature of blockchain means that no single entity controls the data, enhancing security and resilience against cyber threats, as highlighted by Taylor et al. (2020). Cryptography is crucial in blockchain for ensuring the security of transactions. Each block contains a cryptographic hash of the previous block, forming a chain that is virtually impossible to alter retroactively. This aspect is central to the security of cryptocurrencies in blockchain technology, as discussed by Ghosh et al. (2020). Consensus mechanisms, such as Proof of Work or Proof of Stake, are employed to validate transactions. These mechanisms ensure that all participants in the network agree on the validity of transactions, thus maintaining the integrity of the ledger, as explored by Gad et al. (2022). Lastly, smart contracts automatically execute transactions based on predefined rules, contributing to the efficiency and automation of processes on the blockchain, as noted by Giannoutakis et al. (2020) in the context of IoT cybersecurity.

The evolution of blockchain technology traces back to its inception with the creation of Bitcoin in 2009, as a response to the need for a decentralized financial system. The original design by Satoshi Nakamoto introduced the first practical solution to the double-spending problem in digital currencies using a peer-to-peer network. This innovation is well articulated in the works of Catalini (2018), who emphasizes the initial role of blockchain in the digital economy and cybersecurity. Blockchain technology quickly transcended its initial application in cryptocurrencies, evolving into a platform for various decentralized applications. The introduction of Ethereum marked a significant milestone, as it expanded the capabilities of blockchain with smart contracts, enabling more complex and automated functionalities. This evolution is highlighted by Tezel et al. (2021), who discuss the opportunities and issues of blockchain in various sectors, including its role in trust, transparency, and cybersecurity.

Recent advancements in blockchain technology focus on enhancing scalability, speed, and energy efficiency, addressing some of the early limitations. Innovations like the development of blockchain 3.0 and 4.0 technologies, as noted by Sharin, Hernandez, and Sentosa (2023), signify the ongoing evolution and growing maturity of blockchain technology. These newer versions aim to integrate blockchain more seamlessly with emerging technologies like IoT, AI, and 5G networks, a trend explored by Han et al. (2021) and Salam and Salam (2020).

4.0 Blockchain in Cybersecurity

Blockchain technology is being increasingly recognized for its potential to significantly enhance cybersecurity across various sectors. Its inherent features of decentralization, transparency, and immutability make it a formidable tool against common cyber threats. Catalini (2018) discusses the implications of blockchain in creating secure and tamper-proof systems, particularly in digital transactions and government operations. One of the key applications of blockchain in cybersecurity is in securing Internet of Things (IoT) networks. As Giannoutakis et al. (2020) illustrate, blockchain can provide a secure framework for IoT devices, ensuring data integrity and preventing unauthorized access. In the realm of financial transactions, blockchain's role is crucial in preventing fraud and ensuring the security of digital currencies, as explored by Ghosh et al. (2020). Another significant application is in supply chain management, where

blockchain can offer transparent and secure tracking of goods, as detailed by Kumar and Mallipeddi (2022). Additionally, blockchain is being used to enhance identity management systems, providing a more secure and efficient way of handling personal and sensitive data, a trend highlighted by Taylor et al. (2020) in their systematic review of blockchain cybersecurity.

Healthcare Sector: Wenhua et al. (2023) discuss blockchain's application in healthcare for securing patient data and managing supply chains. A notable case study is the use of blockchain to ensure the integrity and confidentiality of patient records, thereby enhancing privacy and security in healthcare systems.

Government Operations: Catalini (2018) references the use of blockchain in government operations to secure sensitive data and enhance transparency in public services. For instance, Estonia's implementation of blockchain in their e-governance system serves as a pioneering example of enhancing cybersecurity and efficiency in government services.

Financial Services: The implementation of blockchain in financial services for secure transactions is well-documented by Ghosh et al. (2020). A notable example is the deployment of blockchain by major banks for cross-border payments, significantly reducing the risk of fraud and improving the security of financial transactions.

Supply Chain Management: As Kumar and Mallipeddi (2022) point out, blockchain has been effectively used in supply chain management to enhance cybersecurity. A case study involves its use by global shipping companies to securely track shipments and verify the authenticity of goods, thereby reducing the risk of counterfeit products.

IoT Security: The case of an IoT-based smart home system, as discussed by Giannoutakis et al. (2020), showcases blockchain's application in securing IoT devices. Here, blockchain was used to create a decentralized network that significantly reduced the risk of DDoS attacks and unauthorized access.

5.0 Emerging Trends

Blockchain technology is experiencing innovative applications in the field of cybersecurity, moving beyond its initial role in cryptocurrency security. One emerging trend, as highlighted by Demirkan, Demirkan, and McKee (2020), is the use of blockchain in business cybersecurity and accounting, offering a new layer of security against fraud and data breaches. In digital identity management, blockchain is being leveraged to create more secure and user-controlled identity verification processes. This application, discussed by Taylor et al. (2020), reduces the risk of identity theft and unauthorized access to personal data. Furthermore, Catalini (2018) notes the potential of blockchain in enhancing the cybersecurity of government systems, providing a secure infrastructure for e-governance and public record keeping. Another innovative use is in securing communications networks, particularly in areas prone to cyber-attacks. As Han et al. (2021) explore, blockchain can enhance the security of emerging 5G networks, ensuring secure and transparent communications. Additionally, in the context of IoT, Giannoutakis et al. (2020) demonstrate how blockchain can be used to secure IoT devices and networks against cyber threats, ensuring the integrity and confidentiality of IoT data.

The integration of blockchain with other cutting-edge technologies like AI, IoT, and big data analytics is creating synergistic effects in enhancing cybersecurity. Gad et al. (2022) discuss how the combination of blockchain and AI can lead to advanced security protocols capable of learning and adapting to new cyber threats. This convergence is particularly potent in combating advanced cyber-attacks, where AI's predictive capabilities and blockchain's immutability can significantly enhance threat detection and response. In the realm of IoT, Salam and Salam (2020) explore the integration of blockchain with IoT devices, providing a secure and transparent framework for device-to-

device communication and data exchange. This integration is crucial in mitigating the inherent security vulnerabilities of IoT networks, as it ensures data integrity and prevents unauthorized access. Another exciting development is in the field of supply chain management, where blockchain's integration with big data analytics and IoT is transforming how supply chains are monitored and secured. Kumar and Mallipeddi (2022) highlight how this integration can lead to more transparent, traceable, and secure supply chains, reducing the risk of fraud and improving overall cybersecurity. Moreover, the use of blockchain in secure cloud storage, as indicated by Tezel et al. (2021), represents another integration point. By combining blockchain with cloud technologies, it's possible to create decentralized and secure data storage solutions, enhancing data privacy and protection against breaches.

6.0 Challenges and Limitations

6.1 Technical Challenges

Implementing blockchain for cybersecurity, while promising, comes with its set of technical hurdles. One of the primary challenges is scalability. As blockchain networks grow in size and complexity, the resources required to maintain them also increase significantly. This issue is particularly evident in public blockchains where the number of transactions can severely impact processing times and costs, as discussed by Ghosh et al. (2020). Another challenge lies in the integration of blockchain with existing systems. As noted by Demirkan, Demirkan, and McKee (2020), integrating blockchain into current business structures, especially those with legacy systems, can be complex and resource-intensive. This integration often requires significant architectural changes and can present compatibility issues. Energy consumption is also a significant concern, especially for blockchains using proof-of-work (PoW) consensus mechanisms. The energy-intensive nature of PoW can lead to sustainability concerns, as highlighted by Sharin, Hernandez, and Sentosa (2023). Additionally, maintaining the security of blockchain networks is an ongoing challenge, as attackers continuously develop new strategies to exploit vulnerabilities, a concern raised by Taylor et al. (2020).

6.2 Ethical and Legal Considerations

The use of blockchain in cybersecurity also raises various ethical and legal issues. Data privacy is a primary concern, especially with the immutable nature of blockchain. As Salam and Salam (2020) point out, once data is entered into a blockchain, it cannot be altered or deleted, which might conflict with laws like the General Data Protection Regulation (GDPR) that allow individuals to request data deletion. Another legal challenge is the jurisdictional ambiguity in blockchain transactions. Since blockchain networks can span multiple countries, determining the applicable legal framework for transactions and data handling can be complex, as discussed by Catalini (2018). This issue becomes particularly pertinent in cross-border transactions or disputes. Moreover, there are concerns about the ethical implications of blockchain in surveillance and monitoring. The transparency and traceability of blockchain, while beneficial for security, also raise concerns about user anonymity and the potential for misuse in surveillance and data collection, an issue explored by Mahmood, Chadhar, and Firmin (2022). The decentralization of blockchain also poses a regulatory challenge. Since there is no central authority, it can be difficult to enforce regulations and standards across the network. This lack of regulation can lead to ethical dilemmas, particularly in sectors like finance and healthcare, where data sensitivity is high, as noted by Wenhua et al. (2023).

7.0 Methodology

The methodology employed in this study is a combination of a comprehensive literature review and qualitative analysis, aimed at thoroughly understanding the role and potential of blockchain technology in enhancing cybersecurity. Initially, a systematic literature review was conducted following the guidelines similar to those outlined by Taylor et al. (2020). This involved identifying relevant research papers through academic databases using specific keywords and selecting them based on set inclusion and exclusion criteria. The selected literature was then subjected to a thematic analysis, as described by Mahmood, Chadhar, and Firmin (2022), categorizing the content into themes such as applications, challenges, and future trends of blockchain in cybersecurity. This approach facilitated an organized synthesis of the collected data. Additionally, a comparative analysis, akin to the method used by Ghosh et al. (2020), helped in drawing parallels and contrasts between the applications and challenges of blockchain technology across various sectors. To add a practical dimension to the study, case studies, similar to those discussed by Giannoutakis et al. (2020) and Han et al. (2021), were meticulously analyzed. These case studies provided concrete examples of blockchain applications in real-world cybersecurity scenarios.

To further enrich the research, interviews with subject matter experts in blockchain and cybersecurity were conducted. These interviews offered valuable industry insights and up-to-date information, complementing the findings from the literature review. The primary sources of data for this study were peer-reviewed academic journals and conference papers from reputable sources like the Georgetown Journal of International Affairs, Journal of Management Analytics, and Journal of Network and Computer Applications. The inclusion of expert interviews provided an additional layer of depth to the study, ensuring a comprehensive understanding of the current state and future potential of blockchain technology in cybersecurity. This blend of systematic academic research and practical insights from industry professionals forms the backbone of the study's methodology

8.0 Analysis and Discussion

8.1 Interpretation of Findings

The analysis of data and case studies in this research underscores the significant role of blockchain technology in enhancing cybersecurity. The findings align with Catalini's (2018) assertion on blockchain's potential in securing digital transactions and government operations, showcasing its utility in creating tamper-proof systems that are crucial for protecting sensitive data. Furthermore, the case studies analyzed, including those in IoT security as discussed by Giannoutakis et al. (2020), demonstrate blockchain's practical effectiveness in preventing unauthorized access and ensuring data integrity across various digital platforms. In the context of business cybersecurity and accounting, as explored by Demirkan, Demirkan, and McKee (2020), blockchain emerges as a transformative technology. It not only enhances the security of financial transactions but also introduces a new paradigm in maintaining transparent and immutable records, thereby mitigating risks associated with data breaches and fraud. This is further corroborated by the analysis of blockchain's application in supply chain management, where it significantly reduces the risk of counterfeit products and ensures the traceability of goods, as highlighted by Kumar and Mallipeddi (2022).

8.2 Correlation with Existing Literature

The findings from this research are in harmony with the existing literature, but they also bring new insights to the forefront. The literature review, as in the works of Taylor et al. (2020), emphasizes blockchain's potential in cybersecurity; however, the analyzed case studies provide practical examples that demonstrate how this potential is

being realized in various sectors. For instance, the use of blockchain in enhancing the cybersecurity of 5G networks, as explored by Han et al. (2021), represents an emerging trend not extensively covered in earlier literature but is crucial in understanding the future scope of blockchain applications. Additionally, while the challenges and limitations of blockchain in cybersecurity, such as those identified in the scoping review by Mahmood, Chadhar, and Firmin (2022), are acknowledged in the literature, this research offers a more nuanced view by analyzing how these challenges are being addressed in practical scenarios. For example, the evolving solutions to scalability and energy consumption issues in blockchain networks present a more optimistic future than previously suggested. In conclusion, this research not only supports the assertions made in existing literature about the benefits of blockchain in enhancing cybersecurity but also extends the understanding by providing empirical evidence and real-world applications. It highlights the evolving nature of blockchain technology and its increasing relevance in securing digital infrastructures against a backdrop of growing cyber threats

9.0 Future Perspectives

The future of blockchain in cybersecurity is poised for significant advancements, shaped by evolving technological landscapes and growing cyber threats. One key area of development, as suggested by Catalini (2018), is the integration of blockchain with emerging digital economies and governmental operations. This involves blockchain becoming a fundamental part of national cybersecurity strategies, providing a resilient framework against cyber attacks and data breaches. Advancements in blockchain technology are expected to address current limitations such as scalability and energy consumption, as highlighted by Sharin, Hernandez, and Sentosa (2023). Innovations like Proof of Stake (PoS) consensus mechanisms and sharding are likely to enhance the efficiency and sustainability of blockchain networks. Furthermore, the integration of blockchain with artificial intelligence (AI) and machine learning (ML) could lead to more sophisticated cybersecurity solutions capable of predictive threat detection and automated response, a trend that aligns with the perspectives shared by Gad et al. (2022). In the realm of Internet of Things (IoT), as discussed by Salam and Salam (2020), blockchain is expected to play a crucial role in securing the vast networks of connected devices. By leveraging blockchain, IoT systems can ensure data integrity, user privacy, and secure device-to-device communication.

The long-term impact of blockchain on cybersecurity practices is expected to be transformative. Blockchain's ability to provide a secure, transparent, and immutable ledger will enhance trust in digital transactions and communications, as noted by Tezel et al. (2021) in the context of the built environment. This increased trust will be crucial for industries like finance, healthcare, and government, where data security and privacy are paramount. Blockchain's impact on cybersecurity will also be evident in the way data breaches and cyber attacks are managed. With blockchain, the ability to tamper with data or create fraudulent transactions will be significantly reduced, leading to a decrease in the frequency and severity of these incidents. This aligns with the findings of Kumar and Mallipeddi (2022), who discuss the impact of cybersecurity on operations and supply chain management. Moreover, the decentralized nature of blockchain will democratize data security, moving away from centralized models that are often vulnerable to single points of failure. This shift will empower individuals and businesses to have greater control over their data, enhancing personal privacy and security, as explored by Mahmood, Chadhar, and Firmin (2022) in their review of cybersecurity challenges in blockchain technology.

10.0 Conclusion

This paper has provided an extensive exploration of the role of blockchain technology in enhancing cybersecurity, highlighting its potential, challenges, and future prospects. Through a detailed examination of current research, case studies, and expert insights, it is evident that blockchain technology holds transformative potential for cybersecurity practices. Blockchain's inherent characteristics of decentralization, immutability, and transparency make it an ideal solution to many of the cybersecurity challenges faced in today's digital landscape. The technology's application spans various sectors, offering enhanced security in digital transactions, data management, and identity verification. Case studies across industries, from healthcare to finance, demonstrate blockchain's practical effectiveness in mitigating risks associated with data breaches, fraud, and cyber-attacks. However, the implementation of blockchain in cybersecurity is not without its challenges. Technical limitations such as scalability, energy consumption, and integration with existing systems pose significant hurdles. Moreover, the ethical and legal considerations around data privacy and regulatory compliance present areas that require further exploration and consensus. Looking forward, the potential long-term impact of blockchain on cybersecurity is substantial. The anticipated advancements in blockchain technology, including its integration with AI and IoT, promise to address current limitations and open new avenues for secure and efficient digital ecosystems. These developments are expected to fundamentally alter the cybersecurity landscape, offering more robust defenses against increasingly sophisticated cyber threats.

References

- Catalini, C. (2018). Blockchain technology and cryptocurrencies: Implications for the digital economy, cybersecurity, and government. *Georgetown journal of international affairs*, 19, 36-42.
- d BH, T., Lehara, F., & Sarajevo, B. H. (2022). Cyber Security Perspective of Top Future Technologies. *Building Cyber Resilience against Hybrid Threats*, 61, 85.
- 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.
- Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. *Journal of King Saud University-Computer and Information Sciences*, 34(9), 6719-6742.
- Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *Journal of Network and Computer Applications*, 163, 102635.
- Giannoutakis, K. M., Spathoulas, G., Filelis-Papadopoulos, C. K., Collen, A., Anagnostopoulos, M., Votis, K., & 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.
- Han, T., Ribeiro, I. D. L., Magaia, N., Preto, J., Segundo, A. H. F. N., de Macêdo, A. R. L., ... & de Albuquerque, V. H. C. (2021). Emerging drone trends for blockchain-based 5G networks: Open issues and future perspectives. *IEEE Network*, 35(1), 38-43.
- Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, 31(12), 4488-4500.
- Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies*, 2022, 1-11.

- Salam, A., & Salam, A. (2020). Internet of things for sustainability: perspectives in privacy, cybersecurity, and future trends. *Internet of things for sustainable community development: wireless communications, sensing, and systems*, 299-327.
- Sharin, F. H., Hernandez, M. S., & Sentosa, I. (2023, May). Future trends of blockchain technology in the technological fields. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 1307-1313). IEEE.
- Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, 6(2), 147-156.
- Tezel, A., Papadonikolaki, E., Yitmen, I., & Bolpagni, M. (2021). Blockchain Opportunities and Issues in the Built Environment: Perspectives on Trust, Transparency and Cybersecurity. In *Industry 4.0 for the Built Environment: Methodologies, Technologies and Skills* (pp. 569-588). Cham: Springer International Publishing.
- Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, 12(3), 546.