International Journal of Cyber and IT Service Management (IJCITSM) **p-ISSN: 2797-1325**
Vol. 3 No. 2 October 2023 **e-ISSN: 2808-554X**

Securing Enterprises: Harnessing Blockchain Technology Against Cybercrime Threats

Fallen Zidan[1], Dimas Nugroho[2], Baskara Adi Putra[3]
Informatics Engineering, Darmajaya Institute of Informatics and Business
Jl. ZA. Pagar Alam No.93, Gedong Meneng, Kec. Rajabasa, Bandar Lampung City, Lampung 35141
Indonesia
e-mail: fallen.zidan@darmajaya.ac.id[1], dimas@darmajaya.ac.id[2], baskaraadiputra@darmajaya.ac.id[3]

Author Notification
13 October 2023
Final Revised
29 October 2023
Published
31 October 2023

To cite this document:
Zidan, F. ., Nugroho, D. ., & Putra, B. A. . (2023). Securing Enterprises: Harnessing Blockchain Technology Against Cybercrime Threats. International Journal of Cyber and IT Service Management, 3(2), 168–173. Retrieved from https://iiast.iaic-publisher.org/ijcitsm/index.php/IJCITSM/article/view/120

DOI:
https://doi.org/10.34306/ijcitsm.v3i2.120

Abstract

In the face of increasingly sophisticated cybercrime threats, large companies now need innovative solutions to protect their data and interests. Blockchain technology, which is based on the principles of decentralization and strong encryption, offers great potential in improving corporate cybersecurity. This research investigates the implementation of blockchain technology in the context of enterprise security by developing a blockchain-based dynamic system model. These findings make an important contribution in changing the way audits and general accounting operations are carried out, presenting fundamental changes in the profession. This new approach integrates blockchain technology into various aspects of cybersecurity, embracing innovation and creativity in the face of current challenges. By creating accurate computer models, this research brings a breakthrough in understanding system responses to employee fraud in corporate environments that adopt blockchain technology. This research aims to explore the potential of blockchain technology in improving corporate cybersecurity by identifying security gaps and designing effective updates, creating a safe and trustworthy digital environment for companies in this digital era. The findings of this research highlight the importance of integrating blockchain technology in auditing and general accounting operations, creating a foundation for the development of robust cybersecurity systems. In the context of companies using blockchain technology, this research reveals improved system responsiveness to employee fraud, indicating positive potential in mitigating security risks. This research provides a solid foundation for further development in the field of enterprise cybersecurity, inspiring innovation in protecting businesses and digital assets in a rapidly evolving cyberspace.

Keywords*: Corporate Cybersecurity, Blockchain Technology, Digital Era, Cyber Crime*

1. Introduction

In the era of rapid digital revolution, large companies face complex challenges in maintaining cyber security [1]. Technological developments, especially in the context of blockchain technology, open up new opportunities to increase efficiency and change business paradigms [2]. However, this progress also raises serious concerns regarding the security of company data and information [3]. Increasingly sophisticated threats from cyberspace demand innovative and trusted solutions to protect sensitive data and corporate interests [4].

Copyright © 2023 Fallen Zidan[1], Dimas Nugroho[2], Baskara Adi Putra[3].
This work is licensed under a Creative Commons Attribution 4.0 (CC BY 4.0)

This research explores the potential of blockchain technology as a solution to secure companies from the threat of cybercrime [5]. By relying on the principles of decentralization and strong encryption, blockchain technology promises to be an effective solution in improving corporate cybersecurity [6]. Our focus is not only on exploring the current uses of blockchain technology, but also on its potential in the future, especially in the enterprise space [7]. We strive to identify existing security gaps and design efficient updates, creating a safe and trusted digital environment for companies in this digital era [8].

In the course of this research, we relate the application of blockchain technology to the cybersecurity challenges faced by companies today [9]. We believe that the integration of blockchain technology is not only a temporary solution, but also the starting point for a more robust corporate cybersecurity system [10]. Through our analytical and innovative approach, we strive to provide valuable guidance for companies in protecting their business and digital assets from the rapidly evolving threat of cybercrime [11].

This research not only addresses current cybersecurity challenges, but also explores the positive potential of blockchain technology in creating operational efficiency, reliability and trust in digital business environments [12]. We believe that the integration of blockchain technology is not only a preventive measure, but also a proactive step to shape an innovative and leading business environment in the future [13].

This research also attempts to fill a gap in the academic literature, combining practical findings and theoretical approaches [14]. Our hope is that the results of this research will not only provide new insights for academics in understanding the complexity of corporate cybersecurity in the digital era, but also provide concrete and applicable guidance for business stakeholders [15]. Through this research, we seek to stimulate broad discussion regarding the use of blockchain technology as an effective solution in facing the threat of cybercrime, as well as supporting sustainable and secure business development in this ever-changing era.

2. Research Method

This research method, which focuses on a case study approach, was carefully designed to gain an in-depth understanding of the implementation of blockchain technology in the context of enterprise security [16]. A case study approach was chosen because it allows for in-depth analysis of real cases across companies, providing rich and detailed insights into how blockchain technology is being used to address cybercrime threats. The following is a further development of the research methodology steps used in Figure 1.

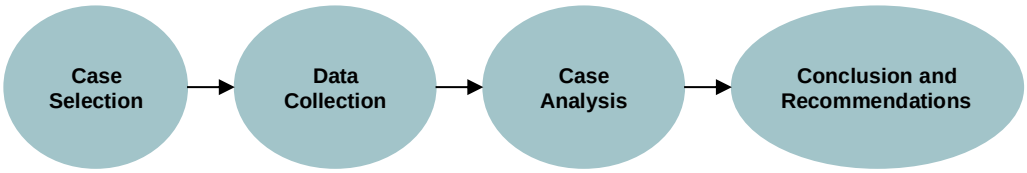

Figure 1. Research Method with a Case Study Approach

1. Case Selection

The selection of case study companies was careful, including representatives from a wide range of industries, scales, and levels of security complexity [17]. Through rigorous criteria, we selected companies that have successfully adopted blockchain technology and have significant experience in fighting the threat of cybercrime [18].

2. Data Collection

a. In-depth Interviews: The research team will conduct in-depth interviews with cybersecurity experts and technical staff at the selected companies [19]. This interview is designed to understand the blockchain implementation strategy, the challenges faced, and the real impact that has been achieved [20].

b. Document Analysis: Additionally, secondary data will be obtained from related literature, internal company documents, security reports, and other reliable sources [21]. An in-depth analysis will be conducted on these documents to understand the journey of blockchain technology implementation and changes in corporate cybersecurity [22].

3. Case Analysis

The collected data will be analyzed holistically. We will engage qualitative and quantitative analysis techniques to identify positive impacts, such as increased operational efficiency, reduced risk, and increased system reliability [23] . On the other hand, we will also examine the challenges and obstacles that companies may face during the process of implementing blockchain technology [24].

4. Conclusion and Recommendations

a. Conclusion: Based on the case analysis, we will draw in-depth conclusions about how blockchain technology has changed the cybersecurity landscape in the companies studied [25]. This will include understanding positive impacts, learning from mistakes, and aspects that require improvement [26].

b. Recommendations: The recommendations prepared will be practical and targeted. They will cover blockchain implementation optimization strategies, recommended security measures, and best practices for dealing with cybercrime threats. These recommendations will provide valuable guidance for other companies planning to adopt blockchain technology in an effort to combat cybersecurity threats.

Through this in-depth case study approach, this research will provide a comprehensive understanding of the role of blockchain technology in protecting companies from the threat of cybercrime, and in doing so, provide a solid foundation for innovation and cybersecurity in the digital business world.

2.2 Literature Review

2.2.1 Blockchain Technology as a Basis for Corporate Security

Blockchain is a decentralized digital ledger consisting of blocks of transactions between the parties involved. Blockchain is defined as “a distributed database, or public ledger because all transactions or digital events are completed and shared between the parties involved.” Blockchain is decentralized and has great potential for various industries. The high level of security in this technology comes from the fact that in order to change anything in the blockchain, the majority of all parties involved in transactions in subsequent blocks in the chain must agree to the change, and blockchain uses advanced mathematics and innovative software technology that difficult to manipulate. This makes blockchain technology attractive and attention-grabbing as it simplifies the verification process, which speeds up the overall transaction process.

The development of blockchain technology can be divided into three stages: Blockchain 1.0, 2.0, and 3.0. Blockchain 1.0 is the first stream that is generally considered the most popular, mainly involving cryptocurrencies such as Bitcoin, Litecoin, and Ethereum. Blockchain 2.0 includes distributed ledger agreements as well as other underlying technologies such as smart contracts and other protocols. Blockchain 3.0 represents “the future of blockchain,” reflecting what more this technology can do for society. The use of this technology will have various impacts on human life, including but not limited to domain names, digital identity, electronic government, and smart contracts.

2.2.2 Cybersecurity and Blockchain as a Security Framework

Cybersecurity attacks today are so common that it is no longer a matter of "if they will happen," but rather "when they will happen." Many theories have been proposed to explain individuals' security intentions and actual behavior in information technology environments, such as general deterrence theory, protection motivation theory, planned behavior theory, rational

choice theory, and naturalization theory. All of these models and theories focus on extrinsic or perceived factors, rather than intrinsic factors such as decision-making style, which can also explain behavior that may be important. Despite this understanding, in both their personal and professional lives, businesses and individuals continue to be unprepared for these types of cyberattacks. According to a survey conducted by a cybersecurity company, 86 percent of businesses admit that their current cybersecurity systems are not ready to deal with potential threats that may occur now or in the future.

To protect themselves from cybercriminals, businesses must be better prepared. These criminals attack companies to get whatever information they can from the company in hopes of gaining profit from it. Many banks and other financial institutions are currently investigating and implementing blockchain security systems to reduce risks, cybersecurity threats and fraud. NASDAQ recently announced plans to launch a blockchain-based digital ledger that will allow them to enhance their equity management capabilities. Researchers in the fields of blockchain and cybersecurity view it in the context of financial markets, cryptocurrencies, the Internet of Things, and electronic money. They address issues such as malware, data protection, authentication, and peer-to-peer networks that arise in these areas because they require robust information protection methods. Cyberattacks against blockchain technology have shown that this technology is not immune to cyberattacks. However, all these cyber attacks have resulted in improvements to bitcoin technology through Blockchain 1.0–3.0. Blockchain 1.0, which includes Bitcoin, is not a single system

3. Findings

The findings of this research underline that blockchain technology is able to provide a solid solution in facing the threat of cybercrime. In situations of information theft, data manipulation, and unauthorized access, the use of blockchain has proven to be very effective. The uniqueness of the blockchain system lies in its ability to record every activity and transaction transparently and irreversibly. In this way, blockchain creates irrefutable digital proof, providing an additional layer of security that ensures data integrity and eliminates the potential for data alteration by unauthorized parties.

Through risk analysis, researchers found that systems that adopt blockchain technology have a lower level of risk when compared to traditional information systems. Blockchain's reliability in maintaining data integrity and transaction security provides significant advantages in protecting sensitive company information. However, researchers would like to emphasize that the success of blockchain technology is highly dependent on thoughtful access policies. If unrestricted access is granted to users, the potential security risk remains high, regardless of the technology used. Therefore, implementing strict access policies and regular monitoring of activity logs is critical in maintaining enterprise cybersecurity.

The role of blockchain technology in securing companies from the threat of cybercrime is very vital. However, to maximize its potential, it is important for companies to integrate blockchain technology with careful access policies and ongoing security monitoring. With this holistic approach, companies can optimize the benefits of blockchain technology, create a secure and reliable environment, and protect their digital assets from cyber threats in a more efficient and effective way in this digital era.

In continuing this research, researchers also found that the successful implementation of blockchain technology does not only depend on technical factors alone. Human aspects, such as user awareness and skills, also play a crucial role in mitigating the threat of cybercrime. Therefore, it is important for companies to provide training and education to their employees regarding good cybersecurity practices and how to use blockchain technology correctly.

In addition, researchers highlight the importance of collaboration between companies and cyber security institutions in facing the threat of cybercrime. Exchanging information about emerging attack methods can help companies prepare and take preventive action more efficiently. This collaboration can also lead to the development of industry security standards that can be applied broadly, creating a safer business environment overall.

Finally, researchers emphasize the need for effective regulations to support the use of

blockchain technology in the context of corporate security. Clear and strict regulations will provide clear guidance for companies in properly implementing blockchain technology and ensuring compliance with established security standards. Strong regulation could also provide additional encouragement for companies to invest in cybersecurity and leverage blockchain technology as a reliable solution against the threat of cybercrime.

Thus, through the combination of advanced blockchain technology, adequate education, inter-company cooperation, and strict regulations, companies can build a robust and effective defense against the threat of cybercrime. A deep understanding of cybersecurity and judicious application of blockchain technology not only protects a company's digital assets, but also creates a strong foundation for business growth and sustainability in this digital era.

4. Conclusion

This research confirms that blockchain technology is a powerful solution in fighting the threat of cybercrime, especially in situations of information theft, data manipulation and unauthorized access. The use of blockchain has proven to be very effective because it is able to record every activity and transaction transparently and irreversibly. The uniqueness of this system creates irrefutable digital evidence, providing an additional layer of security to ensure data integrity and prevent data modification by unauthorized parties.

Risk analysis shows that systems that implement blockchain technology have a lower level of risk compared to traditional information systems. Blockchain's reliability in maintaining data integrity and transaction security provides significant protection for sensitive company information. However, the success of blockchain technology relies heavily on thoughtful access policies. By enforcing strict access policies and regularly monitoring activity logs, companies can maintain their cybersecurity and maximize the potential of blockchain technology.

It is important for companies to integrate blockchain technology with thoughtful access policies, employee training, and cooperation between companies and cybersecurity agencies. Collaboration and exchange of information on emerging attack methods allows companies to prepare and take preventive action more efficiently. Effective regulation is also essential, providing clear guidelines and supporting the use of blockchain technology in confronting the threat of cybercrime. With this holistic approach, companies can build a strong defense and ensure the continuity of their business in this digital era.

References

[1] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, and A. H. Gandomi, “The revolution of blockchain: State-of-the-art and research challenges,” *Arch. Comput. Methods Eng.*, vol. 28, pp. 1497–1515, 2021.

[2] L. Koh, A. Dolgui, and J. Sarkis, “Blockchain in transport and logistics–paradigms and transitions,” *International Journal of Production Research*, vol. 58, no. 7. Taylor & Francis, pp. 2054–2062, 2020.

[3] H. Tabrizchi and M. Kuchaki Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, 2020.

[4] J. R. Biden, “Interim national security strategic guidance,” *The White House*, p. 8, 2021.

[5] A. Bayramova, D. J. Edwards, and C. Roberts, “The role of blockchain technology in augmenting supply chain resilience to cybercrime,” *Buildings*, vol. 11, no. 7, p. 283, 2021.

[6] P. Zhuang, T. Zamir, and H. Liang, “Blockchain for cybersecurity in smart grid: A comprehensive survey,” *IEEE Trans. Ind. Informatics*, vol. 17, no. 1, pp. 3–19, 2020.

[7] D. Levis, F. Fontana, and E. Ughetto, “A look into the future of blockchain technology,” *PLoS One*, vol. 16, no. 11, p. e0258995, 2021.

[8] M. H. P. Rizi and S. A. H. Seno, “A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city,” *Internet of Things*, vol. 20, p. 100584, 2022.

[9] S. Mahmood, M. Chadhar, and S. Firmin, “Cybersecurity challenges in blockchain technology: A scoping review,” *Hum. Behav. Emerg. Technol.*, vol. 2022, pp. 1–11, 2022.

[10] E. Toufaily, T. Zalan, and S. Ben Dhaou, "A framework of blockchain technology adoption: An investigation of challenges and expected value," *Inf. Manag.*, vol. 58, no. 3, p. 103444, 2021.
[11] R. Dillon, P. Lothian, S. Grewal, D. Pereira, and A. Kuah, "Cyber Security: Evolving Threats in an Ever Changing World," in *Digital Transformation in a Post-Covid World: Sustainable Innovation, Disruption and Change*, CRC Press, 2021, pp. 129–154.
[12] A. Tezel, E. Papadonikolaki, I. Yitmen, and M. Bolpagni, "Blockchain Opportunities and Issues in the Built Environment: Perspectives on Trust, Transparency and Cybersecurity," in *Industry 4.0 for the Built Environment: Methodologies, Technologies and Skills*, Springer, 2021, pp. 569–588.
[13] J. Leng *et al.*, "Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey," *Renew. Sustain. energy Rev.*, vol. 132, p. 110112, 2020.
[14] C. Huang, F. T. S. Chan, and S. H. Chung, "Recent contributions to supply chain finance: towards a theoretical and practical research agenda," *Int. J. Prod. Res.*, vol. 60, no. 2, pp. 493–516, 2022.
[15] F. Alfiana *et al.*, "Apply the Search Engine Optimization (SEO) Method to determine Website Ranking on Search Engines," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 65–73, 2023.
[16] S. Balasubramanian, V. Shukla, J. S. Sethi, N. Islam, and R. Saloum, "A readiness assessment framework for Blockchain adoption: A healthcare case study," *Technol. Forecast. Soc. Change*, vol. 165, p. 120536, 2021.
[17] S. Fedushko and T. Ustyianovych, "E-commerce customers behavior research using cohort analysis: A case study of COVID-19," *J. Open Innov. Technol. Mark. Complex.*, vol. 8, no. 1, p. 12, 2022.
[18] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, p. 102248, 2021.
[19] N. Huaman *et al.*, "A {Large-Scale} Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 1235–1252.
[20] J. Lohmer and R. Lasch, "Blockchain in operations management and manufacturing: Potential and barriers," *Comput. Ind. Eng.*, vol. 149, p. 106789, 2020.
[21] D. R. E. Ewim *et al.*, "Survey of wastewater issues due to oil spills and pollution in the Niger Delta area of Nigeria: a secondary data analysis," *Bull. Natl. Res. Cent.*, vol. 47, no. 1, p. 116, 2023.
[22] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transp. Res. part e Logist. Transp. Rev.*, vol. 142, p. 102067, 2020.
[23] K. Kano and E. Dolan, "Data Compression Analysis of Multimedia Video on Demand and DEMAND TV Broadcast Systems on the Network," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 48–53, 2023.
[24] C. Öztürk and A. Yildizbaşi, "Barriers to implementation of blockchain into supply chain management using an integrated multi-criteria decision-making method: a numerical example," *Soft Comput.*, vol. 24, pp. 14771–14789, 2020.
[25] A. Shahaab, I. A. Khan, R. Maude, C. Hewage, and Y. Wang, "Public service operational efficiency and blockchain–A case study of Companies House, UK," *Gov. Inf. Q.*, vol. 40, no. 1, p. 101759, 2023.
[26] A. Fernanda, M. Huda, and A. R. F. Geovanni, "Application of Learning Cloud Computing Technology (Cloud Computing) to Students in Higher Education," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 32–39, 2023.