Blockchain Frontier Technology (B-Front)
Vol. 2 No. 1 July 2022

P-ISSN: 2808-0831
E-ISSN: 2808-0009

Blockchain Technology in the Future of Enterprise Security System from Cybercrime

Siti Maesaroh[1], Handy Januar Permana[2], Pipit Dirgayusa Febrianaga[3], Noviyanti[4], Renhad Andreas Pardosi[5]
University of Raharja, Indonesia[1,2,3,4,5]
Modern, Jl. Jenderal Sudirman No.40, RT.002/RW.006, Cikokol, Kec. Tangerang, Kota Tangerang, Banten 15117
e-mail: siti.maesaroh@raharja.info[1], handy.permana@raharja.info[2], pipit.dirgayusa@raharja.info[3], noviyanti.novi@raharja.info[4], Renhad@raharja.info[5]

Author Notification
30 May 2022
Final Revised
24 June 2022
Published
29 June 2022

Maesaroh, S. ., Permana, H. J. ., Dirgayusa Febrianaga, P., Noviyanti, & Pardosi, R. A. . Blockchain technology in the future of Enterprise Security System from Cybercrime. Blockchain Frontier Technology. Retrieved from
DOI: https://journal.pandawan.id/b-front/article/view/88

Abstract

This study looks into the current, and potential uses of Blockchain technology in business, specifically in the security system of enterprise. The goal of this study is to use modern blockchain technology to address the problem of enhancing the degree of cybersecurity in huge corporations. Enterprises that have seen examples of cyber fraud perpetrated not only by hackers but also by business personnel have evaluated the urgency of the matter. The authors have developed a blockchain-based system dynamic model of the company's cybersecurity system. The use of this modeling tool enables the creation of a computer model of a complicated cybersecurity system, which can then be used to design the suggested update more effectively. We show how Blockchain affects auditing in a variety of ways that will fundamentally alter the profession. We also believe that blockchain technology should be integrated into other parts of cybersecurity, including auditing and general accounting operations. The findings have allowed researchers to draw conclusions about the increased system response in cases of employee fraud in the context of a company's automated information system that uses blockchain technology.

Keywords: *Blockchain, Cybersecurity, Enterprise, Business, System*

1. Introduction

The world of technology is moving at an unparalleled rate. This is a trend that will only accelerate in the coming years as brilliant brains continue to invent new ways to make everyday living easier and more accessible to all. Change will be prevalent not only in everyday life, but also in the corporate world as a whole, if this trend continues. Technology has already exploded, allowing firms to reach new heights of profitability and competitiveness [1]. While technological advancements, particularly blockchain technologies, have allowed the enterprise to grow and, in the process, establish blockchain-based practices as a possible future for business information systems, they have also raised concerns for many different companies about overall cybersecurity [2] [3]. Most businesses face a problem with decreased reliability of the cyber security system, which leads to vulnerabilities in enterprise corporate information systems and violations of data confidentiality, integrity, and availability. In today's world, such issues typically result in the loss of information, and as a result, businesses lose customers, money, and reputation [4]. Enterprise employees with unlimited access rights, using remote access, mobile applications, and cloud technologies, are frequently involved in

cybercrime cases [5] [6]. As a result, businesses are eager to develop an effective cybersecurity system that will reduce the number of incidents and prevent cyber threats.

The practice demonstrates that, despite increasing investment in cybersecurity system development, current data protection solutions do not meet the needs of the business. This was the conclusion reached by 81 percent of respondents polled by Dell Technologies. The primary reason is the increased amount of information owned by businesses. In 2019, its volume increased by nearly 40% over 2018, with a total cost of data loss of more than $1 billion per organization. The problem of increasing the efficiency of enterprise cybersecurity systems is a global one. In June 2019, the average financial loss from information leaks for medium-sized businesses worldwide was approximately $3.92 million. As a result, businesses are interested in attracting cutting-edge technology to ensure information reliability and security.

As a result, in this paper, we investigate the current and potential applications of Blockchain technology in business, specifically in enterprise, and we discuss related Cybersecurity issues. We also relate Blockchain uses to current cybersecurity concerns. Despite advancements in blockchain technology in the cybersecurity area in practice, we believe there is a gap in the literature from a more academic perspective, which may impede academics from leading the way and proposing policies to the practice and further development of blockchain technologies in business.

2. Literature review

2.1Blockchain Technology

A blockchain is essentially a decentralized digital ledger made up of blocks of transactions between parties. Blockchain is defined as a "distributed database of records, or public ledger because of all transactions or digital events completed and shared among participating parties." Blockchain is decentralized and has enormous potential benefits for many industries [7]. This high level of security stems from the fact that in order to change anything in a blockchain, a majority of all parties to transactions in subsequent blocks within the chain must agree to the change, and blockchains employ sophisticated math and innovative software technologies that are generally difficult to manipulate [8]. This makes blockchain technology appealing and interesting because it simplifies the verification process, which speeds up the overall transaction process.

Blockchain development can be divided into three stages: Blockchain 1.0, 2.0, and 3.0. Blockchain 1.0 is the first stream, which most people would consider to be the most popular. It is mostly made up of cryptocurrencies, such as Bitcoin, Litecoin, and Ethereum. Blockchain 2.0 includes distributed ledger agreements as well as other foundational technologies such as smart contracts and other protocols. Blockchain 3.0 is the "future of the blockchain," implying what else it might be able to do for us as a society. The application of this technology will have a wide range of effects on human life. Blockchain 3.0 goes beyond 1.0 and 2.0 and includes applications such as domain names, digital identities, eGovernment, and smart contracts [9] [10] [11].

2.2 Cybersecurity

Cyber security attacks are now so common that it is no longer a question of "if it will happen," but rather "when will it happen." Many theories have been proposed to explain individual security intentions and actual behaviors in the information technology environment, such as general deterrence theory, protection motivation theory, theory of planned behavior, rational choice theory, and naturalization theory. All of these models and theories are focused on extrinsic or perceived factors, rather than intrinsic factors such as decision styles, which may also explain the behaviors that would be essential [12] [13]. Even with this as the mindset of people in their personal and professional lives, businesses and people continue to be unprepared for these types of cyber-attacks. In a survey conducted by a cyber-security company, 86 percent of businesses admitted to feeling and knowing that their current cybersecurity system was unprepared for what could happen in the present or in the future.

Businesses must be better prepared to defend themselves against cybercriminals. These people who will engage in cybercrime are attacking companies in order to obtain any information they can from the company in order to potentially profit from it. Many banks and other financial institutions are currently investigating and implementing blockchain security systems to reduce risk, cyber threats, and fraud. The NASDAQ recently announced a plan to launch a Blockchain based digital ledger which allows them to boost their equity management capabilities.

Blockchain and cybersecurity researchers look at them in the context of financial markets, cryptocurrencies, the Internet of things, and electronic money. They address the issues of malware, data protection, authentication, and peer-to-peer networks that arise in these areas because they necessitate powerful information protection methods. Cyberattacks on blockchain technology have demonstrated that this technology is not immune to cyber-attacks [11]. However, all cyberattacks have resulted in improvements to bitcoin technology via Blockchain 1.0–3.0. Blockchain 1.0, which includes Bitcoin, is not a perfectly fungible system because some coins may be linked to accounts used for fraudulent activities [14]. However, as systems evolve, newer systems can address these concerns by incorporating "mixer" networks to conceal transaction history [15]. While Hyperledger fabric has since been built on later technologies, it still requires moderate attention based on the risk profile, initial security concerns, and other vulnerabilities identified at the point of engagement, and it may not be indestructible [16] [14].

2.3 Blockchain as a cybersecurity framework

Blockchain is emerging as one of the more dependable and powerful cyber security technologies. The norm today, as it has been for years, is that when dealing with information exchange or the transfer of money and assets via online transactions via the internet, we will use a trusted intermediary. The intermediaries are in charge of ensuring the secure exchange and are therefore liable for any problems that arise during the transaction, including security breaches. Given future cybersecurity concerns and the plans that the US government hopes to implement over the next five years, businesses may turn to blockchain as part of their security framework. While there is no agreement on how much companies should invest in cybersecurity, industry experts suggest that robust investments in cybersecurity should not be less than three percent of a company's total capital expenditures. Companies should approach cybersecurity policies and technologies in the same way they would any other investment: fluid, long-term, performance-driven, and with quantifiable goals. Cybersecurity is something that can be developed in the future for businesses as blockchain technologies are implemented. "Blockchain is being promoted as a technology that can provide a robust and powerful cybersecurity solution, as well as a high level of privacy protection.

The blockchain is a secure alternative for allowing these transactions to take place while eliminating the middleman. Once approved by the exchange participants, the transaction is added to the blockchain and cannot be edited, altered, or removed without the approval of all parties in the chain. The blockchain is a system that cannot be reversed. Because the ledger is constantly synchronized across all participants, using blockchain not only reduces business costs but also eliminates the possibility of information loss due to a single point of failure by one of the parties involved. This is why blockchain is such an incredible technology for cyber security and reliability when it comes to replacing the current transactional status quo. The blockchain is capable of ensuring privacy and security at all times. Blockchain technology is rapidly evolving in many directions, but there is insufficient practice history of making business decisions for executives. One area where blockchain technology will be used in business is in supply chain management, which will make transactions easier, more secure, and more accurate for the purpose of reporting [17] [18]. Every link in the supply chain can be tracked, and the sources of insecurity can be easily identified. Knowing the public availability of blockchain, it can be deduced that it could easily be used to effectively track down recalled products more efficiently than the current process that companies use when a product appears to be prone to virus problems [10] [19]. If a product is released and it is later discovered that it is vulnerable to malware attacks, having the blockchain as part of your supply chain allows

you to easily track where all of those products went and where they are located, allowing your company to easily remove them from the market, effectively ending the cyber-attack. With this as an example, it shows what blockchain is able to do as a security framework being used to its potential [6] [20].

3. Method

The system-dynamic modeling method was chosen for the study. Its main advantage is the ability to model system behavior at a high level, based on information and logical structure, and using a data-flow approach. The stages of the research methodology are as follows:

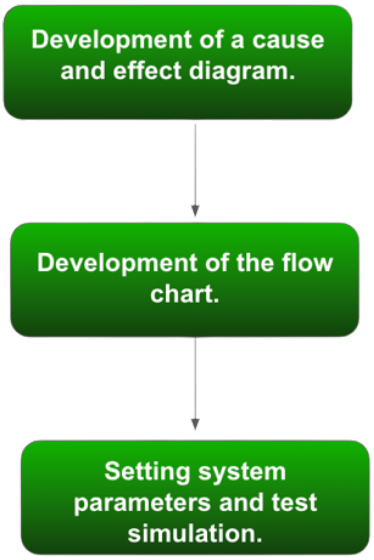

Figure 1. Method Syste Dynamic Modelling

- **Development of A Cause and Effect Diagram.**

  The following system elements were identified for this purpose: a person's intention to commit cybercrime; human actions for committing cybercrime; influencing factors for increasing or decreasing cybercrime; data recording in the Blockchain. Cause and effect relationships were established between the main elements, which, along with other elements, formed the system parameters. A cause and effect relationship is positive if an increase (decrease) in the parameter affects the increase (decrease) of the affected parameter, and negative if an increase (decrease) in the parameter affects the decrease (increase) of the affected parameter.

- **Development of the Flow Chart**

  Levels were identified at this stage, which are parameters that are influenced by a larger number of other parameters, taking into account both positive and negative effects. Special parameters, i.e. those that cause the corresponding level to increase or decrease, were considered. In addition, additional variables and constants were used. An equation was created for each variable.

- **Setting System Parameters and Test Simulation.**

  Changes are required for the following parameters: a prohibition on

downloading information, a prohibition on opening and launching unknown files, a prohibition on the use of external media, limited access, hardware errors, database openness, and remote access. If necessary, the appropriate levels are debugged. The simulation is then run, yielding a visualization of the system's behavior when there are potential cybercrime intentions; the system's reactions are determined in the case of recording data in the blockchain and in the case of using a traditional information system.

4. Result

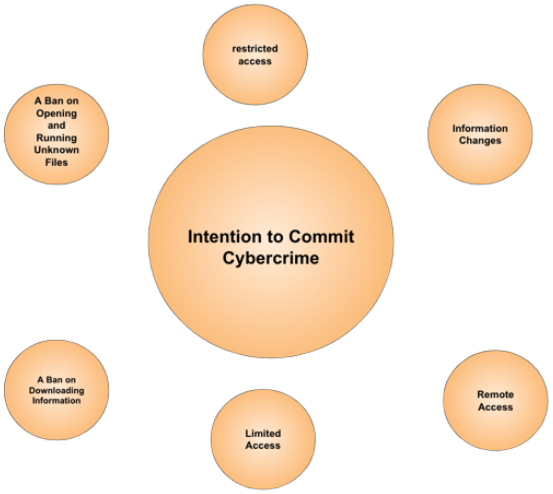

Figure 2. Step 1 Cause & Effect

The model assumes that a cybercriminal intends to steal information by copying it, or to destroy data or change information, or to perform intentional non-saving, unauthorized access, or to distort information by making mistakes. These are the most common illegal activities that contribute to the emergence of vulnerabilities in a system and reduce its level of cybersecurity. When blockchain technology is implemented in a business, all actions are recorded in the blockchain and are not subject to change. As a result, blockchain data can quickly provide information about user behavior and, as a result, detect violations when used in conjunction with an artificial intelligence system. The model assumes that the recording takes place in a traditional information system, but if the information is updated, the system recording may not be saved. To detect violations, the cybersecurity system will need to check activity logs for quite some time. Depending on the results, a flow chart Blockchain protected cybercrime was obtained.

P-ISSN: 2808-0831
E-ISSN: 2808-0009

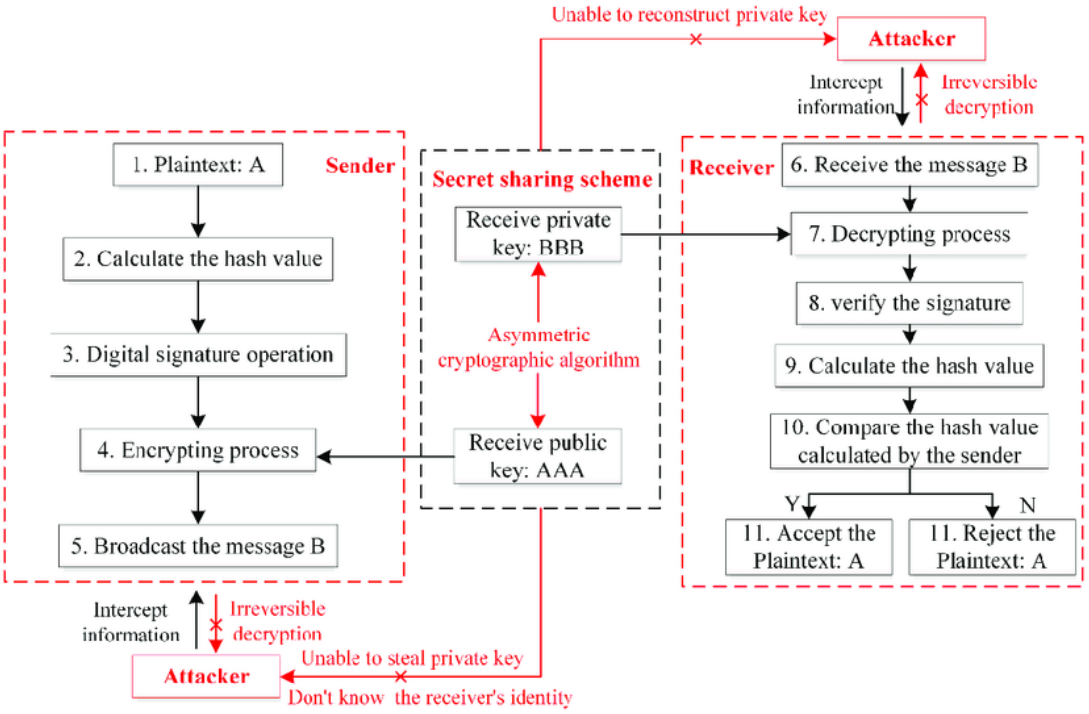

Figure 3. Flowchart

The flow diagram demonstrates the level of risk determined by a system that uses blockchain technology and a traditional information system. According to the implemented method, in almost all cases, a blockchain-based system is less risky than a traditional information system. Cases where both systems have a risk level of one are when the company does not establish a ban and allows users unlimited access, i.e. this is an option when all security measures are missing. As a result, no technology can have a positive impact on the cyber security system in this case.

4. Conclusion

As a result, the issues associated with cybersecurity system reliability violations are relevant. Financial resources, customer trust, and reputation and competitiveness may all suffer as a result. As a result, cyber security experts must respond quickly in the event of new types of cyber threats or an increase in the likelihood of system vulnerabilities. There are no one-of-a-kind tools that can completely solve cyber security issues. As a result, it should be a collection of measures that contribute to the effectiveness and dependability of the defense system. Some experts criticize most companies for increasing their investment in the use of modern technologies.

Blockchain technology is becoming more popular, and its range of applications is expanding. As a result, it has a good chance of being used to improve the reliability of enterprise cyber security systems. The system-dynamic modeling enables assumptions about the benefits of this technology over traditional information systems to be made. First, this technology will not replace the existing one, but rather supplement it, because its primary function is to store information in its original form without changes, allowing deviations to be detected when attempting to implement changes. It is planned to expand the proposed model in the future by taking into account other parameters, such as increasing the number of activities, particularly by external users, and taking into account the impact factors at the local level.

References

[1] L. Chandra, Amroni, B. Frizca, Q. Aini, and U. Rahardja, "Utilization Of Blockchain Decentralized System In Repairing Management Of Certificate Issuance System," *J. Adv. Res. Dyn. Control Syst.*, vol. 12, no. 2, pp. 1922–1927, 2020, doi: 10.5373/JARDCS/V12I2/S20201235.

[2] S. Sudaryono, Q. Aini, N. Lutfiani, F. Hanafi, and U. Rahardja, "Application of Blockchain Technology for iLearning Student Assessment," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 14, no. 2, pp. 209–218.

[3] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *J. Manag. Anal.*, vol. 7, no. 2, pp. 189–208, 2020.

[4] Q. Aini, U. Rahardja, M. R. Tangkaw, N. P. L. Santoso, and A. Khoirunisa, "Embedding a Blockchain Technology Pattern Into the QR Code for an Authentication Certificate," *J. Online Inform.*, vol. 5, no. 2, 2020.

[5] I. Handayani, D. Supriyanti, G. Maulani, and N. Lutfiani, "The ilearning journal center: Education startup to enhance lecturer research," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 4, pp. 4678–4682, 2020, doi: 10.30534/ijatcse/2020/70942020.

[6] M. I. Sanni and D. Apriliasari, "Blockchain Technology Application: Authentication System in Digital Education," *Aptisi Trans. Technopreneursh.*, vol. 3, no. 2, pp. 37–48, 2021.

[7] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, p. 1788, 2019.

[8] A. Alam, S. M. Z. U. Rashid, M. A. Salam, and A. Islam, "Towards blockchain-based e-voting system," in *2018 International Conference on Innovations in Science, Engineering and Technology (ICISET)*, 2018, pp. 351–354.

[9] U. Rahardja, A. N. Hidayanto, N. Lutfiani, D. A. Febiani, and Q. Aini, "Immutability of Distributed Hash Model on Blockchain Node Storage," *Sci. J. Informatics*, vol. 8, no. 1, pp. 137–143, 2021.

[10] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[11] M. Warkentin and C. Orgeron, "Using the security triad to assess blockchain technology in public sector applications," *Int. J. Inf. Manage.*, vol. 52, p. 102090, 2020.

[12] B. Rawat, A. S. Bist, U. Rahardja, C. Lukita, and D. Apriliasari, "The Impact Of Online System on Health During Covid 19: A Comprehensive Study," *ADI J. Recent Innov.*, vol. 3, no. 2, pp. 195–201, 2022.

[13] A. Tapscott and D. Tapscott, "How blockchain is changing finance," *Harv. Bus. Rev.*, vol. 1, no. 9, pp. 2–5, 2017.

[14] R. Sabillon, J. J. Cano, V. Cavaller Reyes, and J. Serra Ruiz, "Cybercrime and cybercriminals: A comprehensive study," *Int. J. Comput. Networks Commun. Secur. 2016, 4*, 2016.

[15] P. A. Sunarya, U. Rahardja, L. Sunarya, and M. Hardini, "The Role Of Blockchain As A Security Support For Student Profiles In Technology Education Systems," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 2, pp. 13–17, 2020.

[16] M. Prawira, H. T. Sukmana, V. Amrizal, and U. Rahardja, "A Prototype of Android-Based Emergency Management Application," *2019 7th Int. Conf. Cyber IT Serv. Manag. CITSM 2019*, 2019, doi: 10.1109/CITSM47753.2019.8965337.

[17] R. Anderson *et al.*, "Measuring the cost of cybercrime," in *The economics of information security and privacy*, Springer, 2013, pp. 265–300.

[18] 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.

[19] N. Diallo *et al.*, "eGov-DAO: A better government using blockchain based decentralized autonomous organization," in *2018 International Conference on eDemocracy & eGovernment (ICEDEG)*, 2018, pp. 166–171.

[20] Q. Aini, N. Lutfiani, N. P. L. Santoso, S. Sulistiawati, and E. Astriyani, “Blockchain For Education Purpose: Essential Topology,” *Aptisi Trans. Manag.*, vol. 5, no. 2, pp. 112–120, 2021.