Siber International Journal of Education Technology (SIJET)
E-ISSN : 2988-0084
P-ISSN : 2988-1595
https://review.e-siber.org/SIJET siberpublisher.info@gmail.com +62 812-1046-7572
DOI: https://doi.org/10.38035/gcir.v2i1

The Utilization of Blockchain Technology to Enhance Data Security

Karomah Alif Sabilla Rustam Sutoto[1], Ifan Sadewa[2], Harri Romadhona[3], Ridwan[4]
[1]Universitas Dinamika Bangsa, Jambi, Indonesia, abilsabilla13c@gmail.com
[2]Universitas Batanghari, Jambi, Indonesia, ifan.sadewa.81@gmail.com
[3]Stikom Dinamika Bangsa, Jambi, Indonesia, s3nobi@gmail.com
[4]STIE Dewantara, Bogor, Indonesia, ridwans70@gmail.com

Corresponding Author: ridwans70@gmail.com[4]

Abstract: The way governments and businesses operate globally is changing due to the worldwide trend of digital transformation. By implementing blockchain technology to improve data security in day-to-day operations, Indonesia's government and private sector are hastening the country's digital transition. Numerous blockchain initiatives, including payment systems, medical data storage, and certificate verification and validation, have been implemented in Indonesia. Notwithstanding, there are still a number of obstacles that Indonesia must overcome before it can effectively use blockchain technology, including imprecise legislation, inadequate infrastructure, and a dearth of knowledge about the network. Consequently, for Indonesia to adopt blockchain technology more quickly, assistance from all parties is required. In order to maximize blockchain technology's potential and hasten Indonesia's digital revolution, more research and development should be done.

Keyword: Digital Transformation, Blockchain, Data Security, Technology

INTRODUCTION

Blockchain is a set of information largely pertaining to the application of cryptography. The usage of information technology is become more intricate and widespread in the present digital era. In the digital world, this leads to a number of difficulties and barriers in preserving data security. A increasing volume of data makes it necessary to find quick fixes for issues or instances of data corruption that could endanger a person or an organization. Blockchain technology is one tool that can be utilized to enhance data security in the digital era (Hakim et al., 2024).

Blockchain is a digital system that securely stores and manages private information using a distributed ledger. Consensus mechanisms and automatic data validation conducted by the relevant network provide the foundation for data security in blockchain technology (Maariz et al., 2024).

Data security can be enhanced by blockchain technology in a number of sectors, such as banking and healthcare. Furthermore, blockchain can be used to ensure data integrity and prevent unwanted data modifications (Elan Maulani et al., n.d.). There aren't many blockchain

developers in Indonesia, and even fewer companies are eager to integrate this technology into their operations. A government agency can process data using blockchain technology. The security of each and every one of the organization's data resources must be considered in the disciplines of economics and other data processing involving an organization or state-owned institution. According to earlier studies on encryption and data security, this encryption is still susceptible to manipulation, particularly when combined with more advanced computational methods that can decrypt data with bigger bytecode (Bahanan et al., n.d.).

It is now crucial to do study on how blockchain technology might improve data security in the digital era. This research can help individuals or organizations protect their data more effectively and efficiently by offering solutions to the increasingly complex data security concerns of the digital age (Rizkia Wardhani & Irwan Padli Nasution, n.d.).

METHOD

The research methodology is conducted using a qualitative descriptive approach. This research was conducted by analyzing data and information obtained from literature studies through journals, articles, and official sources related to digital transformation and the implementation of blockchain technology in Indonesia, carried out over a period of two months. Additionally, this research also involved interviews with experts and practitioners in the fields of technology and digital transformation in Indonesia (Waruwu, 2023).

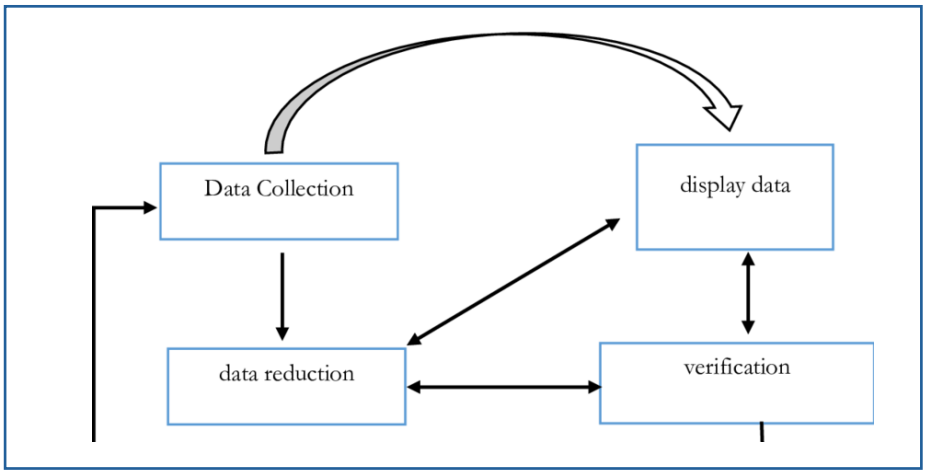

Figure 1: Data analysis flow

Gathering and studying relevant material on digital transformation and blockchain technology in Indonesia, as well as examining policies and plans from the Indonesian government about blockchain adoption, comprised the first phase of the research. Following that, in order to obtain a more comprehensive and in-depth understanding of the application of blockchain technology in Indonesia, the researcher spoke with practitioners and experts in the domains of technology and digital transformation (Putri et al., 2022).

Following an analysis and compilation of the research findings, a conclusion was reached about the potential and difficulties of integrating blockchain technology into Indonesia's digital transformation. Additionally, suggestions for how the public and private sectors could work together to optimize the advantages of blockchain technology in Indonesia's digital transformation were also made (Damanik et al., 2024).

RESULTS AND DISCUSSION

Blockchain is a technology that started with the concept that, because it is decentralized, digital data might be safely transferred and kept without being subject to manipulation or

hacking. The goal of information security is to shield data and information against tampering, loss, or unwanted access. Information data security has grown in significance in the digital age as more data is transmitted and kept via digital means.

Blockchain and cryptography are two methods that businesses and other entities use to protect their data. The study of guaranteeing message security is called cryptography. (text message). A further definition of cryptography is the science of studying mathematical methods connected to data integrity, confidentiality, and authentication, among other aspects of computer security (Febriana & Aji, 2017).

Cryptography is the science that studies how to keep our messages or documents safe, so they cannot be read by unauthorized parties. There are two types of cryptographic algorithms based on the type of key, namely (Wachid Hidayatulloh et al., 2023) :

1) Symmetry Algorithm

Also known as conventional algorithms, these are algorithms that use the same encryption key as their decryption key. Symmetric algorithms are often referred to as secret key algorithms, single key algorithms, or one-key algorithms.

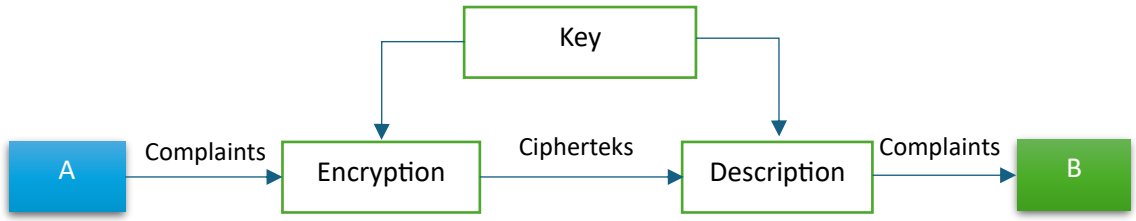

Figure 2. Symmetric Cryptography Process

2) Algoritma Asimetri

Designed in such a way that the key used for encryption is different from the key used for decryption, the key for encryption is not secret, hence it is also called a public key, while the key for decryption is secret, thus it is called a private key

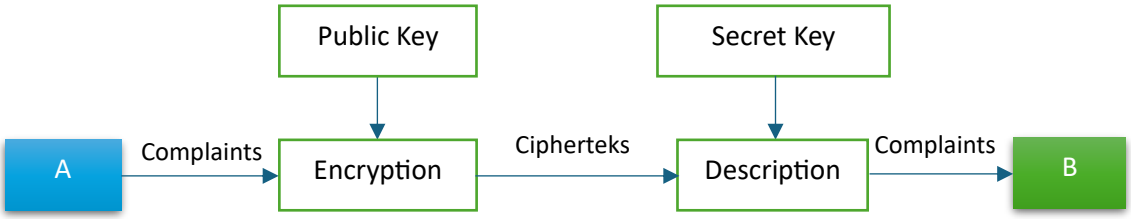

Figure 3. Asymmetric Cryptography Process

In the research written by Tito Wira Eka Suryawijaya, it discusses the efforts to implement blockchain technology, which is essentially aimed at optimizing data security systems (Wira & Suryawijaya, 2023). This step is seen as an important effort to embrace the rapidly advancing digital transformation in Indonesia.

The research aims to determine the security of the system in protecting user data, minimizing execution errors from the system, and reducing the risk of errors in the system, so that the login system can be used safely. The results of the research indicate that the conclusion that can be drawn is that the login system has been successfully developed. By using blockchain technology, user data is kept confidential.

The testing was conducted using Burp Suite. The data sent is in the form of hash blocks and is encrypted, ensuring its security. The security testing of this login system has been successfully carried out accurately, making the system more secure than before. The data

username and password are converted into ciphertext so that attackers cannot access the user's information (Khozindani et al., 2023).

In the research conducted by Azra Hita Dahayu Putri, Aisyatul Muhdiyyah, and Raya Rambu Anarki, the discussion revolves around web server security as one of the important aspects in the world of web application development. As time goes by, Web Server technology continues to advance, as do the security attacks that threaten the system. It is important for organizations and web developers to implement methods that can enhance the security of their web server systems. The purpose of this journal is to analyze several methods that can be used to improve web server security, taking into account their effectiveness and suitability in different contexts (Hita et al., 2024)

In the research conducted by Wasriyono, it discusses the Innovation of Utilizing Blockchain in Enhancing the Security of Intellectual Property in Education, particularly in higher education institutions. Blockchain is a significant factor in higher education, as demonstrated by this study's author, who examines how blockchain can be used to monitor various university systems using computing solutions and IT infrastructure in an effort to improve, preserve, or rebuild educational systems. of an endeavor to advance, preserve, or rebuild the educational system of a university. It's been claimed that privacy and security concerns in higher education are growing yearly, especially with regard to degrees and certificates (Wasriyono et al., 2022).

The development and frequent use of this technology illustrate its rapid growth in popularity and demand. The emerging need for blockchain technology for more and better applications aims to facilitate its use in providing better solutions compared to traditional approaches in the tech world (Bahanan et al., n.d.). The final findings of this research are consistent with other studies, which have found that because Blockchain Technology is immutable, secure, transparent, and distributed, it has many advantages and can be applied to streamline university operations.

Reduced counterfeiting of genuine university documents, including transcripts and other official university documents, is another benefit of this technology. The results of the FGD are consistent with business practices and critical domains that require Blockchain technology security in order to guarantee the integrity of student data. The prototype application was demonstrated to participants and provided with an explanation. Attendance records are one of the crucial academic tasks that must be addressed as part of the learning process in order to support further study. The education industry can benefit greatly from the expansion of blockchain technology's potential services (Sinsuw & Najoan, 2013).

One of the main focuses of blockchain technology is its data security. Data on the blockchain is protected by several layers of secondary technology such as hashes, hash chains, private-public keys, and P2P data distribution. This makes blockchain ideal for storing public data that is vulnerable to manipulation. For example, consider the data of residents' identities. Resident identity data is vulnerable to manipulation and hacking, so it must be stored with a high level of security. However, at the same time, it should also be easily accessible to the public for various purposes, such as data validation. This makes blockchain ideal for storing such data (Hita et al., 2024).

In general, blockchain technology still has limitations, including:

1) Data yang tidak portable

Blockchain is a technology that underlies the creation of various systems. However, each system built using blockchain technology is separate from one another. When a user utilizes a blockchain system, it will be difficult or even impossible to integrate or transfer data between one system and another. This is primarily due to the absence of standards underlying blockchain technology, resulting in each system implementing it differently. The data recorded in the blockchain is also permanent, as deleting one block of data will affect the subsequent

blocks. This is good for preventing data manipulation, but it can become a problem for various systems.

2) The Absence of Regulations and Standards

Due to the technology still being very young, there are no appropriate regulations that can govern blockchain. Without regulations or implementation standards, it is only a matter of time before issues related to blockchain arise.

3) Security of the Private Key

The application of public-private key encryption makes data on the blockchain very secure because no single party has absolute access to the data. However, on the flip side, when a user loses their private key, they permanently lose access, as there is no way to regenerate the lost private key. This makes blockchain carry a high risk for users.

In the journal titled "Blockchain-based Trust, Transparent, Traceable Modeling on the Learning Recognition System of Kampus Merdeka," it discusses that the existence of mechanisms involving various actors within it makes Kampus Merdeka have many new outputs that must be recognized by all stakeholders who need them. Blockchain technology and smart contracts offer the ability to build trust among all actors in the Merdeka Campus activities due to their transparent nature and reliable, immutable data storage capabilities.

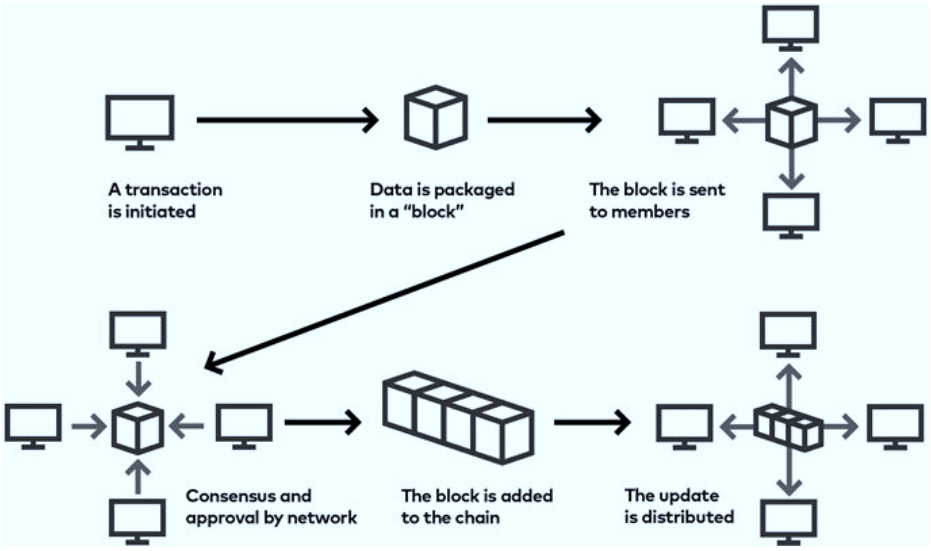

Figure 4. Illustration of the Blockchain Framework

Every stage that occurs within it can be traced from upstream to downstream. This research aims to design a blockchain architecture model for the Merdeka Campus learning recognition system. This uses analytical studies to identify potential issues and the stakeholders involved, and to design the proposed model solutions (Wibowo, 2022).

Blockchain technology is built using several existing technologies. The main technologies that build blockchain are asymmetric key encryption, hash functions & hash chains, and peer-to-peer networks. Hashing is the process of transforming any input into an output consisting of a random arrangement of characters with a predetermined length, which can be defined as unique characters for each piece of data that has been processed. Unlike encryption, data that has been converted into hash form typically cannot be reverted to its original form (Deyani, 2018).

An example of a hash function is modulo, where all integer numbers that are infinite in sum can be divided by a constant integer, and the remainder of this division is the hash value from the modulo function. Blockchain is essentially a hashchain within a global hashchain. In

other words, a blockchain is a global hashchain with the data in its blocks consisting of an internal hashchain. The hashchain is then distributed to the computers owned by the users of a blockchain system. A peer-to-peer (P2P) network is a network concept that allows computer systems to interact with each other without intermediaries or instructions from a central or parent computer. In a P2P network, all computers have equal status and interact based on mutually agreed-upon rules, eliminating the need for a central computer to manage or provide instructions. For that reason, the P2P system is decentralized.

The blockchain system uses the concept of a P2P network, allowing each computer to send data blocks, the status of the blockchain, and whenever a new block is created. This makes every user a supervisor and guarantor of the validity of each data block. Users can check the validity of a data block at any time, and any changes affect the overall structure of the blockchain. Therefore, blockchain does not require a central entity to manage and operate this system.

By utilizing blockchain technology in data processing, it can help systems make data more secure and transparent. Due to the rampant cybercrime involving data manipulation that harms individuals or groups, data security measures need to be implemented.

CONCLUSION

In the digital age, blockchain technology can be utilized to improve data security. Blockchain technology is a decentralized, unchangeable system that may be used to make transaction records that are transparent and safe.

The security of blockchain is based on strong cryptographic algorithms and consensus mechanisms used to verify and validate each transaction on the network. Every transaction made on the blockchain is recorded permanently and cannot be altered or deleted without the approval of the majority of network users.

In many cases, blockchain technology can be used to provide better data security than traditional centralized systems. This is because the blockchain system does not have the same weaknesses as traditional centralized systems.

Blockchain technology is not without its own drawbacks, though. For many blockchain applications, for instance, scalability and transaction costs continue to be challenges. Furthermore, even if the blockchain system is hard to hack, a 51% attack can still be executed if one party controls a large portion of the network's processing power.

Despite these challenges, blockchain technology continues to evolve and improve. Developers are constantly working on solutions to address scalability issues and reduce transaction costs. Additionally, efforts are being made to decentralize control over the network in order to prevent the possibility of a 51% attack. As more businesses and industries adopt blockchain technology, its potential benefits in terms of security and transparency are becoming increasingly apparent. With ongoing advancements and innovations in the field, blockchain technology is poised to revolutionize the way data is stored and transactions are conducted in the digital age.

One of the key challenges facing blockchain technology is the issue of scalability. As the number of transactions on the network continues to grow, the current infrastructure may struggle to keep up with the demand. However, there are a number of potential solutions being explored to address this issue. One approach is to implement off-chain scaling solutions, such as the Lightning Network, which allow for faster and more cost-effective transactions. Another option is to increase the block size or implement sharding, which involves splitting the blockchain into smaller, more manageable sections. By exploring these and other potential solutions, developers are working to ensure that blockchain technology remains a viable and efficient option for businesses and industries around the world.

These solutions aim to improve scalability, reduce transaction fees, and increase the overall speed of transactions on the blockchain network. Additionally, ongoing research and development efforts are focused on optimizing consensus mechanisms, enhancing security protocols, and improving interoperability between different blockchain networks. By continuously innovating and adapting to meet the growing demands of users and businesses, the blockchain ecosystem is poised to revolutionize various industries and drive widespread adoption in the years to come.

In conclusion, blockchain technology can be used as a solution to enhance data security in the digital age. However, the implementation of blockchain technology must be carefully considered and measured against existing challenges and limitations to achieve optimal results.

REFERENSI

Bahanan, M., Al-Utsmani Bondowoso, S., & Wahyudi, M. (n.d.). *Analisis Pengaruh Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Pada Perbankan Syariah*.

Damanik, D. F., Negeri, U. I., & Utara, S. (2024). Analisis Penggunaan Teknologi Blockchain Dalam Pengelolaan Keamanan Data Pada Big Data Muhammad Irwan Padli Nasution. *Jurnal Ilmiah Nusantara (JINU)*, *1*(4), 3047–7603. https://doi.org/10.61722/jinu.v1i4.18892

Deyani, R. A. (2018). *Simulasi Cryptocurrency Menggunakan Elliptic Curve Cryptography*.

Elan Maulani, I., Herdianto, T., Febri Syawaludin, D., & Oga Laksana, M. (n.d.). Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi. *Medika Oga Laksana Jurnal Sosial Dan Teknologi (SOSTECH)*, *3*(2), 2023.

Febriana, I., & Aji, G. (2017). *PENERAPAN TEKNIK KRIPTOGRAFI PADA KEAMANAN SMSANDROID* (Vol. 1, Issue 1).

Hakim, N., Bakri, A. A., & Wahyudi, F. (2024). Use Of Blockchain Technology In Data Distribution System Security. *International Journal of Social and Education (INJOSEDU)*, *1*(6), 1715–1727.

Hita, A., Putri[1], D., Muhdiyyah[2], A., & Anarki[3], R. R. (2024). ANALISIS METODE-METODE PENINGKATAN KEAMANAN WEB SERVER. In *Jurnal Ilmiah Sains dan Teknologi* (Vol. 2, Issue 8).

Khozindani, A. A., Muhyidin, Y., & Agus Sunandar, M. (2023). Perbandingan Kinerja Tools Wireshark Dan Burpsuite Untuk Penyerangan Website Dengan Metode Sniffing. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 7, Issue 3).

Maariz, A., Wiputra, M. A., & Armanto, M. R. D. (2024). Blockchain Technology: Revolutionizing Data Integrity and Security in Digital Environments. *International Transactions on Education Technology (ITEE)*, *2*(2), 92–98. https://doi.org/10.33050/itee.v2i2.435

Putri, O. A., Hariyanti, S., & Kediri, I. (2022). *Review Artikel: Transformasi Digital Dalam Bisnis Dan Manajemen*. https://jurnalfebi.iainkediri.ac.id/index.php/proceedings

Rizkia Wardhani, P., & Irwan Padli Nasution, M. (n.d.). *Peran Teknologi Blockchain dalam Keamanan dalam Privasi Data*.

Sinsuw, A., & Najoan, X. (2013). Prototipe Aplikasi Sistem Informasi Akademik Pada Perangkat Android. *E-Journal Teknik Elektro Dan Komputer*. http://developer.android.com/guide/developing/devi

Wachid Hidayatulloh, N., Tahir, M., Amalia, H., Afdlolul Basyar, N., Prianggara, A. F., & Yasin, M. (2023). Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data. *Digital Transformation Technology (Digitech) | e*, *3*(1). https://doi.org/10.47709/digitech.v3i1.2293

Waruwu, W. (2023). Pendekatan Penelitian Pendidikan: Metode Penelitian Kualitatif, Metode Penelitian Kuantitatif dan Metode Penelitian Kombinasi (Mixed Method). *Jurnal Pendidikan Tambusai*, *7*(1).

Wasriyono, W., Apriliasari, D., & Seno, B. A. P. S. (2022). Inovasi Pemanfaatan Blockchain dalam Meningkatkan Keamanan Kekayaan Intelektual Pendidikan. *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi*, *1*(1), 68–76. https://journal.pandawan.id/mentari/article/view/142

Wibowo, S. A. (2022). Penerapan Smart Contract dalam Sistem Blockchain pada Pengakuan Sistem Kredit Semester Kampus Merdeka. *ITN Malang*, *3*.

Wira, T., & Suryawijaya, E. (2023). *Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia Strengthening Data Security through Blockchain Technology: Exploring Successful Implementations in Digital Transformation in Indonesia*. *2*(1), 55–67. https://doi.org/10.21787/jskp.2.2023.55-67

Isnawati, I., & Ali, H. (2024). Pengaruh Pendidikan, Informasi dan Komunikasi terhadap Internet of Things. *JURNAL MANAJEMEN PENDIDIKAN DAN ILMU SOSIAL*, *5*(3), 312-319.

Mangalindung, G. H., & Ali, H. (2023). Pengaruh Teknologi Informasi, Kualitas Informasi dan Dukungan Manajemen Puncak terhadap Sistem Informasi Keuangan. *Jurnal Manajemen dan Pemasaran Digital*, *1*(4), 232-238.

Sabarini, N. E., & Ali, H. (2024). Pengaruh Teknologi Informasi, Pemanfaatan Blog dan Database terhadap Sistem Informasi. *JURNAL MANAJEMEN PENDIDIKAN DAN ILMU SOSIAL*, *5*(3), 383-389.

Primawanti, E. P., & Ali, H. (2022). Pengaruh Teknologi Informasi, Sistem Informasi Berbasis Web Dan Knowledge Management Terhadap Kinerja Karyawan (Literature Review Executive Support Sistem (Ess) for Business). *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(3), 267-285.