INTERNATIONAL JOURNAL OF FINANCIAL ECONOMICS (IJEFE) e-ISSN: 3063-3648
Vol. 2 No. 5 May 2025, page 394-408

GETTING TO KNOW BLOCKCHAIN TECHNOLOGY AND ITS ROLE IN COMPUTER DATA SECURITY

Gunawan Widjaja
Fakultas Hukum Universitas 17 Agustus 1945 Jakarta,
email: widjaja_gunawan@yahoo.com

Abstract

Blockchain technology, with its decentralized architecture and underlying cryptography, offers a solution to secure and protect data more effectively than conventional systems. Every transaction recorded on a blockchain is first verified by a network of nodes together before it can be carried out, making surreptitious modification of data almost impossible. In addition, the cryptographic security features of the blockchain ensure that only interested parties can access the data, and the transparent transaction records can facilitate the audit process to be more precise and accurate. However, the implementation of blockchain technology is also faced with various obstacles. Issues such as capacity, data privacy, and regulation are the main challenges that need to be overcome to enable its wider adoption. Technical complexities and a lack of public understanding of the technology are also slowing down its acceptance in various industry sectors. Therefore, this research recommends a hybrid approach that combines traditional and blockchain technologies to create a more comprehensive and resilient data security solution.

Keywords: Blockchain Technology, Computer Data Security.

Introduction

The development of digital technology has accelerated the use of electronic data in various aspects of life, including business, government, and routine activities. In this day and age, data has become a strategic asset and therefore requires solid protection. (Liang et al., 2022). However, the increased reliance on computer-based systems also places new challenges related to information security. Threats such as cyberattacks, data misappropriation, and fact manipulation are constantly increasing in both scale and complexity. (Wang, 2020).

In order to address the challenges of data protection, blockchain technology has emerged to offer a new and innovative way. Blockchain was originally developed as the foundation for digital currencies such as Bitcoin, which was introduced by Satoshi Nakamoto in 2008. This technology utilizes data structures called "blocks", where each block contains a series of data transactions and is connected to each other through cryptographic hashes, forming a chain. (Jiang & He, 2023). One of the key features of blockchain is decentralization, which allows data to be stored and managed across multiple locations (nodes) simultaneously. This means that there is no central agency that fully controls all data, making the system more secure and open. Any modification

or addition of data must be validated through the agreement of the majority of nodes in the network, which ensures the integrity and accuracy of the information. (Deng et al., 2021).

Blockchain technology has shown vast potential to be implemented in various fields, such as financial systems, healthcare, supply chains, and public services. These applications utilize blockchain's feature of being able to record information permanently and irreversibly to provide secure and efficient processes without a central intermediary. (Ahmed, 2023). In the financial industry, for example, this technology enables fast and secure transactions without involving payment service providers. In the supply chain field, blockchain implementation offers full transparency into the product journey from production to distribution to consumers to ensure the quality and authenticity of goods. (Ashraf, 2021).

In general, this new platform that blockchain offers has the potential to design systems that are more secure, transparent, and efficient. The technology operates by storing data in a decentralized manner that allows verification of information without depending on a central authority. This reduces the risk of manipulation and unauthorized deletion of data. Any changes to information on the blockchain network must also be approved by a consensus mechanism to make it difficult for hackers to tamper with the system as a whole. (Divakarla & Chandrasekaran, 2022).

The rapid growth in the use of digital data in recent decades has transformed various aspects of life at the individual and business levels. The digital revolution and the rapid development of the internet have facilitated the collection, storage, and analysis of large volumes of data. (Al-Rawy & Elci, 2021). The use of smartphones, social media, e-commerce, and various digital applications generates more and more data every day. These data are used not only to improve productivity but also to understand consumer behavior, predict market trends, and make more informed business decisions. The phenomenon of big data, which involves large and complex information, is increasingly driving technological innovation and the adoption of data analytics in various sectors. (Yu, 2022).

With the rapid use of digital data today, data protection has become increasingly urgent. Cyber threats such as attacks, fraud, and malware are increasingly sophisticated and capable of inflicting significant harm to individuals and institutions if their data is taken over or stolen. In addition, data breaches can destroy customer trust and have serious legal consequences (Chen & You, 2020). Therefore, companies and people must be more vigilant in keeping their data secure. This includes implementing encryption, multifactor authentication, and advanced walls of defense to protect sensitive data. Rules such as the European General Data Protection Regulation (GDPR) and various other data protection laws have also been introduced to ensure that personal data is protected with high security standards. Data integrity and protection are key to maintaining trust and good relationships between entities in this ever-evolving digital ecosystem. (Subha, 2020).

However, while blockchain technology promises many advantages in terms of data protection, there are still many questions and challenges that need to be answered. For example, how effective is blockchain in protecting data compared to conventional security technologies? What are the limitations and risks inherent in implementing blockchain?

Therefore, this research aims to understand blockchain technology and its role in computer data security in depth through a literature review. By identifying the working principles of blockchain and evaluating relevant literature studies, this research is expected to provide a comprehensive insight into the advantages, challenges, and potential applications of blockchain in maintaining computer data protection.

Research Methods

The study conducted in this research uses the literature research method, which is a research approach that utilizes written sources that are already available as the main data. This method includes the identification, evaluation, and interpretation of literature related to a particular research topic that has been previously published. (Hidayat, 2009); (Afiyanti, 2008); (Syahrizal & Jailani, 2023)..

Results and Discussion

Blockchain Technology

Blockchain technology is a distributed data storage system that is decentralized. Each block in the chain consists of a number of digital transactions that are interlinked through cryptography. The order of these blocks forms a solid structure that is difficult to tamper with. This technology is known for its transparency, security, and independence in verification without having to involve a third party. (Srivastava & Girija, 2022)..

The idea of blockchain was first introduced in 2008 by Satoshi Nakamoto in a paper titled "Bitcoin: An Interoperable Electronic Money System". Nakamoto explained the working mechanism of Bitcoin digital money and the technology that formed it, namely blockchain. Bitcoin, released in 2009, became the first example of blockchain implementation. Nakamoto's version of blockchain is designed to enable financial transactions that are secure, open, and free from the supervision of institutions such as banks. (Mohammad, 2020).

Since the introduction of Bitcoin, the development of blockchain has been rapid and has been applied to various sectors other than finance such as logistics, healthcare, and government. In 2015, Ethereum-a cutting-edge platform created by Vitalik Buterin-was launched. It introduced smart contracts that can be executed automatically according to pre-defined conditions. (Heo & Doh, 2024). This opened up opportunities for more complex decentralized applications and encouraged further innovation of blockchain technology. Since then, many other blockchain projects and platforms have

emerged with various features to meet the needs of business and daily life. (Augustine & Raj, 2020).

The main components of blockchain technology consist of several key elements that are interrelated with each other. A block is the smallest unit in the data chain structure that functions to store transaction information or other records. Each block consists of a header and a body. The body is usually business data and related details, while the header includes a timestamp, a link to the previous block, and a code to ensure the uniqueness of each block. The combination of these elements makes blocks an integral part of building a data chain. (Elgamal et al., 2023)..

A block chain, also known as blockchain technology, is a series of blocks that are connected sequentially over time. Each new block added to the chain will always contain a cryptographic link to its predecessor block, thus forming a strong and indivisible bond. (Njeri, 2022). This ensures that changes to one block will affect all subsequent blocks, making it difficult to alter the data within them. Block chains operate on the principle of decentralization, where copies of the chain are stored on various network nodes to increase security through redundancy and distribution. (Salagrama et al., 2022).

Hash functions are used to link one block to the next and ensure data integrity. Each block contains the hashed result of the previous block, so small changes to a block will change the value of the result. This makes the hash function a key component to ensuring the authenticity and security of blockchain technology, given the difficulty of creating two different sets of data that have the same hash value. (Yan, 2023).

Blocks, chains, and hashes are not the only determining factors of blockchain. Consensus mechanisms also govern the network to reach a mutual agreement on the latest blockchain status. There are various consensus mechanisms, such as the Proof of Work (PoW) used by Bitcoin and the more energy-efficient Proof of Stake (PoS) adopted by some other blockchains such as Ethereum after the update to Ethereum 2.0. Also possible are smart contracts, which are automated digital contracts that run autonomously when certain conditions are met. Smart contracts allow decentralized applications (dApps) to emerge on top of blockchains, opening up new opportunities for commerce, financial services, and more. (Prisco et al., 2023).

The blockchain process starts with a consensus mechanism to reach an agreement among all network participants (nodes) regarding the latest blockchain status. The consensus mechanism is necessary to maintain the integrity and security of the system, prevent data manipulation, and validate transactions without a third-party mediator. (Goyal et al., 2021). The two most common consensus mechanisms are Proof of Work (PoW) and Proof of Share (PoS). In PoW like Bitcoin, nodes (commonly called miners) compete to solve complex cryptographic puzzles to add new blocks to the blockchain. In PoS, validators are chosen based on the amount of crypto they "stake"

as collateral, which is more energy efficient as it does not require complex operations. (Syed et al., 2022).

Mining is the process of validating new transactions and additions to the blockchain through specialized consensus mechanisms such as PoW. In the context of PoW, miners utilize computing power to solve difficult mathematical problems. The first miner to solve the puzzle gets to add new blocks to the blockchain and receives a reward in the form of crypto. This not only validates transactions but also secures the network by preventing double-spending attacks as it takes huge resources to manipulate data on the blockchain. (Ooi et al., 2022).

Block chains operate on the principle of decentralization, where data is stored not in one place but spread across various network nodes. Each node has a complete copy of the block chain, which is updated instantly if a new block is added. This search allows for traceability and resilience: if one of the nodes fails or is attacked, the information remains safe because it is widely spread across other nodes. Moreover, this search also ensures that no single entity controls the entire network, reinforcing the democratic principle and the resilience against manipulation of the block chain. (Nabben, 2021).

Once a new block is created by miners or validators, it must be validated across the network of nodes before it is permanently added to the block chain. The validation process involves checking the validity of the transactions in the new block, ensuring they meet the rules of the consensus protocol. If the majority of nodes agree that the block is valid, it will be added to the block chain and the nodes update their copies of it (Thuraisingham, 2020). This step ensures only legitimate and verified transactions are added to the block chain, maintaining integrity and trust within the network. In addition, this process also adds an extra layer of security, as an attack on the system would need to control a majority of nodes to successfully corrupt data (Tenge & Okello, 2020). (Tenge & Okello, 2022).

Security is one of the main advantages of block chain technology. Because each new block is added to the chain using strong cryptography, each transaction stored in a block chain is almost impossible to alter or delete. This provides very strong immutability, meaning that once data is added to a block chain, it cannot be changed without the consent of the majority of the network. In addition, because block chains use encryption and hashing algorithms, data remains secure from manipulation or unauthorized access. (Alzoubi et al., 2022)..

While blockchain technology offers various benefits, such as higher digital data security and more open transactions, some challenges must also be overcome. The process of verifying transactions on public networks such as Bitcoin and Ethereum sometimes takes a long time due to capacity limitations in consensus methods such as proof-of-work mining. (Rayan et al., 2021). To improve efficiency, various efforts are underway, such as the development of a second network as a scaling solution as well as

direct developments to the core protocol such as Ethereum's switch to proof-of-stake (Ruan, 2023). (Ruan, 2023).

Blockchain has great potential to revolutionize various sectors through more secure, open, and cheaper transactions. In the financial world, this technology can speed up payments and improve security at a lower cost. For supply chains, blockchain enables open tracking of products from upstream to downstream. Healthcare, real estate, and voting can also benefit. (Pal, 2022).

In summary, blockchain works through consensus, mining, and data distribution to execute transactions in a decentralized, transparent, and secure manner. While there are still challenges in capacity and efficiency, new solutions are being sought to overcome them. This technology can not only support reliable systems but also spur transformation in various sectors through innovation. The maturation of blockchain will further expand its benefits to various aspects of life.

Computer Data Security

Information security is a field of science that focuses on protecting data from unauthorized access, damage, or theft throughout its lifecycle. It involves implementing rules, procedures, and technologies to ensure sensitive data remains safe from internal and external threats. (Patil, 2021). With the rise of cyber threats and strict regulations regarding data privacy, information security has become a top priority for organizations around the world. Effective data security efforts must ensure that information is protected without hindering productivity or business operations. (Devineni, 2020).

Confidentiality is one of the important aspects of information security that ensures that data can only be accessed by authorized parties. This involves various means such as encryption, user authentication, as well as access control to prevent disclosure of information to unauthorized individuals or systems. (Velliangiri & Karthikeyan, 2020). Confidentiality is essential in maintaining privacy and protecting sensitive data, such as personal information, health data, and company secrets. If confidentiality is breached, there can be serious consequences such as loss of trust from customers, damaged reputation, and legal sanctions. (P et al., 2023).

Data integrity is concerned with maintaining the accuracy and consistency of information throughout its lifecycle. This means that the data must remain unchanged unless done so by an authorized entity and following established procedures. Mechanisms such as checksums, hashing, and version control are often used to ensure integrity. (Feng et al., 2023). Maintaining data integrity is important to prevent information processing errors that can lead to incorrect business decisions, financial losses, and system damage. Information that has been altered or corrupted can lead to inaccurate data, which in turn can be detrimental to business operations and reputation (Chavan & Pampatti, 2023). (Chavan & Pampattiwar, 2024)..

Availability is an important aspect of data security that ensures information can be accessed by authorized parties whenever necessary. This involves measures such as system redundancy, disaster recovery, and network monitoring to keep resources available without a hitch. (Ren et al., 2023). Availability is crucial in an operational business context where any time of system malfunction can be devastating. Without ensuring availability, even the most secure data will be useless if it cannot be accessed when needed. Maintaining availability often involves the use of data backups, protection from DDoS attacks, as well as a robust infrastructure to accommodate high demand. (Gong-Guo & Wan, 2021).

One important component in ensuring data availability is contingency planning. Contingency planning includes creating a disaster recovery plan and a business continuity plan. Disaster recovery plans ensure organizations can recover their data and systems after a disaster, whether a natural disaster or a cyberattack. Business continuity plans focus on how the business can continue to run with minimal disruption during and after an incident. These steps are important so that the organization can recover quickly from disruptions and return to normal operations, thereby minimizing losses that may occur. (Muniandi, 2021).

Technology plays an important role in ensuring data security. For example, encryption technology protects data confidentiality by converting information into a randomized format that can only be read by those with the right decryption key. (Kolah, 2022). Multifactor authentication ensures that only authorized users can access systems and data, adding an extra layer of security. In addition, security solutions such as firewalls, intrusion detection systems, and intrusion prevention systems help protect the network from suspicious attacks. Other tools such as file integrity monitoring software are used to ensure data integrity remains intact (Seenivasan et al., 2022).

Apart from technology, policies and procedures also play an important role in ensuring data security. Information security policies set guidelines and standards that organizations must adhere to in protecting their information. Standard Operating Procedures (SOPs) help ensure that all actions taken to protect data are implemented in a consistent and enforceable manner. (Xie et al., 2021). Security training for employees is also necessary to ensure that everyone in the organization understands their role in maintaining data security. Without clear policies and effective procedures, technological efforts to keep data safe can be futile (de-Melo-Diogo et al., 2021). (de-Melo-Diogo et al., 2022)..

To ensure that all aspects of data security are met, auditing and compliance are essential elements. Periodic security audits check whether established procedures and policies are being followed and whether the organization's systems and databases are safe from threats. Compliance with regulations such as the General Data Protection Regulation (GDPR) in Europe, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, as well as other local legislation is also important. (Baskar

et al., 2021). Non-compliance with these regulations can result in large fines and damage an organization's reputation. By conducting internal audits and complying with applicable regulations, organizations can ensure that they meet the necessary security standards and reduce data security risks. (Wen et al., 2021).

One of the main challenges in computer database security is the constantly evolving and advancing threats. Cyberattacks such as ransomware, phishing and Advanced Persistent Threats (APTs) are becoming increasingly difficult to detect and prevent. Threat actors are utilizing more advanced techniques and leveraging artificial intelligence to find gaps in security systems. (Wang, 2020). Often, organizations struggle to continuously update and manage their security systems to deal with these new threats especially if they have limited resources. In addition, zero-day attacks that exploit vulnerabilities that are not yet known or have not been addressed by software developers, add a layer of complexity to data protection efforts (Balint, 2022).

The challenge of protecting computer data security comes from two main sources: increasingly sophisticated external threats and internal human error and policy weaknesses. Ever-improving cyberattacks require companies to continually refine their defense technologies (Zhang et al., 2020). However, increased employee awareness and training on proper security practices as well as strict and relevant policies are also necessary to prevent information leaks. In addition, individual carelessness such as the use of weak passwords or personal devices without adequate protection can make it easier for threat actors to access internal systems. Similarly, policies and procedures that are not enforced and regularly updated can create security gaps. (Gong-Guo & Wan, 2021). Therefore, an integrated and sustainable approach of investing in security technologies and raising awareness and internal discipline is required to overcome the challenges of keeping electronic data confidential.

Comparison between blockchain and Traditional Security Technologies

Security and Transparency: Blockchain provides a higher level of security and transparency compared to traditional security technologies. In a blockchain system, every transaction or data recorded in a block must be validated by a network of participants (nodes) through consensus mechanisms such as Proof-of-Work (PoW) or Proof-of-Stake (PoS). Once data is added to the blockchain, it is very difficult to change it without manipulating all subsequent blocks in the chain, making blockchains intrinsically resistant to modification and attack (Karmakar et al., 2022). In contrast, traditional security technologies such as firewalls, encryption, and intrusion detection systems work by securing the perimeter and data through access control and encryption, but remain vulnerable to internal attacks and unknown threats. (Hsiung et al., 2021).

Decentralization: One of the key advantages of blockchain is its decentralized nature. Unlike traditional systems that typically rely on a single point of control or

central authority, blockchain utilizes a distributed network that makes it more resilient to Distributed Denial of Service (DDoS) attacks and system failures. In traditional systems, if a central server or database is attacked or experiences a period of inoperability, the entire system can be crippled. Whereas in blockchain, the distributed network ensures that data can still be accessed and validated even if some nodes experience problems. (Rathee & Saini, 2021).

Auditability and Efficiency: Blockchain provides more efficient and transparent auditing capabilities than traditional technologies. Every transaction on the blockchain is recorded chronologically and can be traced back easily, which is very useful for audit and compliance purposes. (Setiawan & Alamsyah, 2023). On the other hand, traditional security technologies often require additional record-keeping and manual auditing systems that can be time-consuming and prone to manipulation. Blockchain allows all relevant parties to have equal access to validated and validated data, thus reducing the possibility of irregularities and fraud.

Adaptability and Implementation: Traditional security technologies such as encryption and firewalls have been widely used and adapted in various industries. They have plenty of hardware, software, and mature standards and regulatory support. Blockchain, while offering significant advantages, is still in the adoption and implementation stage in many sectors (Devi. et al., 2023). Challenges such as scale, privacy, and regulation still need to be overcome to achieve wider adoption. In addition, technical complexity and a general lack of understanding of blockchain could be barriers to the adoption of this technology in many organizations (Jiang & He, 2023). (Jiang & He, 2023).

Overall, blockchain brings significant innovation in the way data is secured and validated, but traditional technologies still play an important role in many security applications today. The combination of the two can offer a more holistic and robust solution in maintaining data integrity and security.

Conclusion

This research found that blockchain technology has a significant impact on improving the security of computational databases. Blockchain, with its decentralized structure, offers a more robust mechanism in preventing data manipulation and falsification compared to conventional systems. Every transaction recorded on the blockchain must go through a consensus validation process involving various nodes in the network, ensuring that the information stored becomes almost impossible to alter without detection. Strong cryptographic security also ensures that data cannot be accessed by unauthorized parties, and transparency in transaction recording allows for more efficient and accurate auditability.

However, the study also emphasizes some of the challenges that need to be overcome for wider adoption of this technology. While blockchain's advantages in data

security are undoubted, issues such as scalability, privacy, and regulation are still an obstacle. In addition, technical complexity and a general lack of understanding of blockchain technology could slow down its adoption in various sectors. This research suggests a hybrid approach, where traditional and blockchain technologies can work together to produce a more holistic and robust data security solution, leveraging the advantages of each technology to achieve more optimal protection.

References

Afiyanti, Y. (2008). Focus Group Discussion as a Qualitative Research Data Collection Method. *Indonesian Nursing Journal*, *12*(1), 58-62. https://doi.org/10.7454/jki.v12i1.201

Ahmed, S. (2023). A Novel Data Security Model of D2D Communication Using Blockchain for Disaster. *2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE)*, *Query date: 2024-08-16 10:55:49.* https://doi.org/10.1109/iccosite57641.2023.10127771

Al-Rawy, M., & Elci, A. (2021). Advanced Security Using Blockchain and Distributed Ledger Technology. *Blockchain Technology for Data Privacy Management*, *Query date: 2024-08-16 10:55:49*, 109-131. https://doi.org/10.1201/9781003133391-6

Alzoubi, Y. I., Al-Ahmad, A., & Kahtan, H. (2022). Blockchain technology as a Fog computing security and privacy solution: An overview. *Computer Communications*, *182*(Query date: 2024-08-16 10:55:49), 129-152. https://doi.org/10.1016/j.comcom.2021.11.005

Ashraf, M. U. (2021). A Survey on Data Security in Cloud Computing Using Blockchain: Challenges, Existing-State-Of-The-Art Methods, And Future Directions. *Lahore Garrison University Research Journal of Computer Science and Information Technology*, *5*(3), 15-30. https://doi.org/10.54692/lgurjcsit.2021.0503213

Augustine, D. P., & Raj, P. (2020). Blockchain and IoT Security. *Blockchain Technology and Applications*, *Query date: 2024-08-16 10:55:49*, 51-64. https://doi.org/10.1201/9781003081487-3

Balint, K. (2022). Data Security Structure of a Students' Attendance Register Based on Security Cameras and Blockchain Technology. *2022 IEEE 22nd International Symposium on Computational Intelligence and Informatics and 8th IEEE International Conference on Recent Achievements in Mechatronics, Automation, Computer Science and Robotics (CINTI-MACRo)*, *Query date: 2024 08-16 10:55:49.* https://doi.org/10.1109/cinti-macro57952.2022.10029471

Baskar, S., Ramar, K., & Shanmugasundaram, H. (2021). Data Security in Healthcare Using Blockchain Technology. *2021 International Conference on Decision Aid Sciences and Application (DASA)*, *Query date: 2024-08-16 10:55:49.* https://doi.org/10.1109/dasa53625.2021.9682300

Chavan, P., & Pampattiwar, K. (2024). Blockchain-Based Composite Access Control and Secret Sharing Based Data Distribution for Security-Aware Deployments. *International Journal of Information and Computer Security*, *1*(1). https://doi.org/10.1504/ijics.2024.10064756

Chen, J., & You, F. (2020). Application of Homomorphic Encryption in Blockchain Data Security. *Proceedings of the 2020 4th International Conference on Electronic Information Technology and Computer Engineering*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1145/3443467.3443754

de-Melo-Diogo, M., Tavares, J., & Luís, Â. N. (2022). Data Security in Clinical Trials Using Blockchain Technology. *Research Anthology on Convergence of Blockchain, Internet of Things, and Security*, *Query date: 2024-08-16 10:55:49*, 607-625. https://doi.org/10.4018/978-1-6684-7132-6.ch034

Deng, H., Fang, F., Chen, J., & Zhang, Y. (2021). A Cloud Data Storage Technology for Alliance Blockchain Technology. *2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1109/bigdatasecurityhpscids52275.2021.00041

Devi, T., Kamatchi, S. B., & Deepa, N. (2023). Enhancing the Security for Healthcare Data using Blockchain Technology. *2023 International Conference on Computer Communication and Informatics (ICCCI)*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1109/iccci56745.2023.10128545

Devineni, S. K. (2020). Blockchain Technology: A Paradigm Shift in Data Integrity and Security. *International Journal of Science and Research (IJSR)*, *9*(6), 1930-1930. https://doi.org/10.21275/sr24119231816

Divakarla, U., & Chandrasekaran, K. (2022). Access Control and Data Security of IoT Applications Using Blockchain Technology. *Blockchain*, *Query date: 2024-08-16 10:55:49*, 243-273. https://doi.org/10.1201/9781003203957-17

Elgamal, E., Medhat, W., Elfatah, M. A., & Abdelbaki, N. (2023). Blockchain Application on Big Data Security. *2023 20th Learning and Technology Conference (L&T)*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1109/lt58159.2023.10092368

Feng, Y., Zhao, J., Chen, T., & Yu, Y. (2023). Blockchain-based ciphertext access control for data sharing using key encapsulation mechanism. *2023 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1109/icbctis59921.2023.00014

Gong-Guo, Z., & Wan, Z. (2021). Blockchain-based IoT security authentication system. *2021 International Conference on Computer, Blockchain and Financial Development (CBFD)*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1109/cbfd52659.2021.00090

Goyal, S., Sharma, S. K., & Bhatia, P. K. (2021). Blockchain for the Security and Privacy of IoT-Based Smart Homes. *Blockchain Technology for Data Privacy Management*, *Query date: 2024-08-16 10:55:49*, 239-252. https://doi.org/10.1201/9781003133391-11

Heo, G., & Doh, I. (2024). Blockchain and differential privacy-based data processing system for data security and privacy in urban computing. *Computer Communications*, *222*(Query date: 2024-08-16 10:55:49), 161-176. https://doi.org/10.1016/j.comcom.2024.04.027

Hidayat, D. N. (2009). QUALITATIVE - QUANTITATIVE DICHOTOMY AND PARADIGMATIC VARIANTS IN QUALITATIVE RESEARCH. *Scriptura*, *2*(2). https://doi.org/10.9744/scriptura.2.2.81-94

Hsiung, P. A., Lee, W.-S., Dao, T. T., Chien, I., & Liu, Y.-H. (2021). Edge-Based Blockchain Design for IoT Security. *Blockchain Technology for Data Privacy Management*, *Query date: 2024-08-16 10:55:49*, 209-237. https://doi.org/10.1201/9781003133391-10

Jiang, C., & He, Q. (2023). A Blockchain- and ABE-based scheme for data security and data sharing. *Sixth International Conference on Computer Information Science and Application Technology (CISAT 2023)*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1117/12.3003796

Karmakar, A., Ghosh, P., Banerjee, P. S., & De. (2022). E-Healthcare data security using blockchain technology. *Blockchain Technology in E-Healthcare Management*, *Query date: 2024-08-16 10:55:49*, 127-145. https://doi.org/10.1049/pbhe048e_ch5

Kolah, A. (2022). Can blockchain technology protect organizations against the escalating threat of personal data and cyber security breaches? *Journal of Data Protection & Privacy*, *5*(2), 108-108. https://doi.org/10.69554/jhze6716

Liang, X., An, N., Li, D., Zhang, Q., & Wang, R. (2022). A Blockchain and ABAC Based Data Access Control Scheme in Smart Grid. *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1109/icbctis55569.2022.00023

Mohammad, S. M. (2020). Blockchain and Bitcoin Security in IT Automation. *International Journal of Computer Trends and Technology*, *68*(3), 103-110. https://doi.org/10.14445/22312803/ijctt-v68i3p121

Muniandi, G. (2021). Blockchain-enabled balise data security for train control system. *IET Blockchain*, *1*(2), 82-94. https://doi.org/10.1049/blc2.12003

Nabben, K. (2021). Blockchain Security as "People Security": Applying Sociotechnical Security to Blockchain Technology. *Frontiers in Computer Science*, *2* (Query date: 2024-08-16 10:55:49). https://doi.org/10.3389/fcomp.2020.599406

Njeri, N. R. (2022). Blockchain as a Solution of Information Security and Data Privacy Issues: A Review. *International Journal of Computer Applications Technology and Research*, *11*(Query date: 2024-08-16 10:55:49), 337-340. https://doi.org/10.7753/ijcatr1108.1007

Ooi, V., Peng, S. K., & Soh, J. (2022). Blockchain land transfers: Technology, promises, and perils. *Computer Law & Security Review*, *45*(Query date: 2024-08-16 10:55:49), 105672-105672. https://doi.org/10.1016/j.clsr.2022.105672

P, K. H., Sahu, D. N., Ramesh, G., Nagpal, A., Harika, A., & Sravani, A. (2023). Blockchain Technology: Converting Data Integrity and Security in Supply Chain Management. *2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1109/upcon59197.2023.10434412

Pal, K. (2022). Blockchain Technology with the Internet of Things in Manufacturing Data Processing Architecture. *Research Anthology on Convergence of Blockchain, Internet of Things, and Security*, *Query date: 2024-08-16 10:55:49*, 228-246. https://doi.org/10.4018/978-1-6684-7132-6.ch014

Patil, H. K. (2021). Blockchain Technology-Security Booster. *Advances in Information Security, Privacy, and Ethics*, *Query date: 2024-08-16 10:55:49*, 128-139. https://doi.org/10.4018/978-1-7998-2414-5.ch008

Prisco, R. D., Shevchenko, S., & Faruolo, P. (2023). Blockchain Data Replication. *Proceedings of the 20th International Conference on Security and Cryptography*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.5220/0012121000003555

Rathee, G., & Saini, H. (2021). Electronic Voting Application Powered by Blockchain Technology. *Advances in Information Security, Privacy, and Ethics*, *Query date: 2024-08-16 10:55:49*, 230-246. https://doi.org/10.4018/978-1-7998-3444-1.ch011

Rayan, R. A., Zafar, I., & Tsagkari, C. (2021). Blockchain Technology for Healthcare Cloud-Based Data Privacy and Security. *Integration of WSNs into Internet of Things*, *Query date: 2024-08-16 10:55:49*, 335-349. https://doi.org/10.1201/9781003107521-16

Ren, W., Zhang, W., Liu, J., Cai, H., & Liu, H. (2023). Blockchain-Based Data Security Sharing System. *Proceedings of the 2023 7th International Conference on Electronic Information Technology and Computer Engineering*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1145/3650400.3650569

Ruan, Z. (2023). Blockchain Technology for Security Issues and Challenges in IOT. *2023 International Conference on Computer Simulation and Modeling, Information Security (CSMIS)*, *Query date: 2024-08-16 10:55:49*. https://doi.org/10.1109/csmis60634.2023.00108

Salagrama, S., Bibhu, V., & Rana, A. (2022). Blockchain Based Data Integrity Security Management. *Procedia Computer Science*, *215* (Query date: 2024-08-16 10:55:49), 331-339. https://doi.org/10.1016/j.procs.2022.12.035

Seenivasan, M., Krishnasamy, V., & Muppudathi, S. S. (2022). Data division using Fuzzy Logic and Blockchain for data security in cyber space. *Procedia Computer Science*, *215* (Query date: 2024-08-16 10:55:49), 452-460. https://doi.org/10.1016/j.procs.2022.12.047

Setiawan, I. P. S., & Alamsyah, A. (2023). Enhancing Security, Privacy, and Traceability in Indonesia's National Health Insurance Claims Process using Blockchain Technology. *2023 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD)*, *Query date: 2024 08-16 10:55:49*. https://doi.org/10.1109/icoabcd59879.2023.10390967

Srivastava, S., & Girija, R. (2022). Blockchain. *Security Analytics*, *Query date: 2024-08-16 10:55:49*, 109-122. https://doi.org/10.1201/9781003206088-8

Subha, T. (2020). Assessing Security Features of Blockchain Technology. *Blockchain Technology and Applications*, *Query date: 2024-08-16 10:55:49*, 115-138. https://doi.org/10.1201/9781003081487-7

Syahrizal, H., & Jailani, M. S. (2023). Types of Research in Quantitative and Qualitative Research. *QOSIM Journal: Journal of Education, Social & Humanities*, *1*(1), 13-23. https://doi.org/10.61104/jq.v1i1.49

Syed, S. A., Sinha, V., Singh, S., & Goel, A. (2022). Blockchain Framework for Data Storage and Security. *Advances in Computing Communications and Informatics*, *Query date: 2024-08-16 10:55:49*, 1-43. https://doi.org/10.2174/9789815051605122040003

Tenge, H., & Okello, M. (2022). Blockchain Technology. *The Auditor's Guide to Blockchain Technology*, *Query date: 2024-08-16 10:55:49*, 1-16. https://doi.org/10.1201/9781003211723-1

Thuraisingham, B. (2020). Blockchain Technologies and Their Applications in Data Science and Cyber Security. *2020 3rd International Conference on Smart BlockChain (SmartBlock)*, *Query date: 2024-08-16 10:55:49.* https://doi.org/10.1109/smartblock52591.2020.00008

Velliangiri, S., & Karthikeyan, P. (2020). Blockchain Technology: Challenges and Security issues in Consensus algorithm. *2020 International Conference on Computer Communication and Informatics (ICCCI)*, *Query date: 2024-08-16 10:55:49.* https://doi.org/10.1109/iccci48352.2020.9104132

Wang, W. (2020). Data Security of SaaS Platform based on Blockchain and Decentralized Technology. *2020 International Conference on Inventive Computation Technologies (ICICT)*, *Query date: 2024-08-16 10:55:49.* https://doi.org/10.1109/icict48043.2020.9112421

Wen, W., Ma, J., & Liu, S. (2021). Data security management of logistics network based on blockchain technology. *2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE)*, *Query date: 2024-08-16 10:55:49.* https://doi.org/10.1109/iciscae52414.2021.9590784

Xie, S., Hong, Y., Wang, X., & Shen, J. (2021). Research on Data Security Technology Based on Blockchain Technology. *2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, *Query date: 2024-08-16 10:55:49.* https://doi.org/10.1109/bigdatasecurityhpscids52275.2021.00016

Yan, G. (2023). BlockChain Based Data Security Mechanism for Vehicular Networks. *2023 6th International Conference on Electronics Technology (ICET)*, *Query date: 2024-08-16 10:55:49.* https://doi.org/10.1109/icet58434.2023.10211276

Yu, H. (2022). Application of blockchain technology in the data processing security system of financial enterprises. *SECURITY AND PRIVACY*, 6(2). https://doi.org/10.1002/spy2.230

Zhang, Z., Wang, F., Zhong, C., & Ma, H. (2020). Grid Terminal Data Security Management Mechanism Based On Master-Slave Blockchain. *2020 5th International Conference on Computer and Communication Systems (ICCCS)*, *Query date: 2024-08-16 10:55:49.* https://doi.org/10.1109/icccs49078.2020.9118554