OPEN ACCESS

Circuitum: Multidisciplinary Journal of Technology and Informatics
Vol. 1 No. 1. June 2025, pp. 1-9 DOI. XX.XXXXX/mjti.vxix.xxx

Research Article

NETWORK SECURITY SYSTEM OPTIMIZATION USING BLOCKCHAIN TECHNOLOGY FOR DATA PROTECTION

Dian Lifia[1], Elnovia[2], and Rit Som[3]
[1] Mahmud Yunus State Islamic University Batusangkar, Indonesia
[2] Mahmud Yunus State Islamic University Batusangkar, Indonesia
[3] Songkhla University, Pattani, Thailand

Corresponding Author:

Dian Lifia,
Department of Informatics Management, Faculty of Islamic Economics and Business, Mahmud Yunus State Islamic University, Batusangkar.
Email: lifiadian@gmail.com

Article Info
Received: May 15, 2025
Revised: May 27, 2025
Accepted: June 15, 2025
Online Version: June 30, 2025

Abstract

Data protection in digital network systems currently faces serious challenges due to the increasing complexity of cyberattacks and the vulnerabilities of conventional security systems that still rely on centralized authority. This study aims to analyze the weaknesses of conventional network security, explore the potential of blockchain technology implementation, develop an optimized blockchain-based network security model, and assess its effectiveness through field trials. A qualitative method was employed using a multi-source data triangulation strategy, including literature review, in-depth interviews with network security and blockchain experts, institutional network system observation, and system documentation analysis. The findings reveal that blockchain holds significant potential in enhancing integrity, transparency, and resilience of network security systems, particularly through decentralization and smart contract features that minimize reliance on single-point authority. The developed model is capable of real-time anomaly detection and data manipulation prevention, and it demonstrated higher effectiveness compared to conventional systems in limited trials. This study concludes that integrating blockchain into network security systems is not merely an alternative solution, but a strategic step toward a more autonomous, decentralized, and adaptive cybersecurity paradigm in response to today's evolving digital threats.

Keywords: Blockchain, Data Protection, Network Security

Journal Homepage	https://journal.zmsadra.or.id/index.php/mjti
How to cite:	Lifia, D., Elnovia, Elnovia., & Som, R. (2025). Network Security System Optimization Using Blockchain Technology for Data Protection. *Circuitum: Multidisciplinary Journal of Technology and Informatics*, *1*(1), 1–9. https://doi.org/XX.XXXXX/mjti.v1i1.1420
Published by:	Yayasan Zia Mulla Sadra

INTRODUCTION

In today’s digital era, data breaches and cyberattacks on computer network systems are increasingly rampant, especially among government institutions and private sectors that store sensitive information (Aska dkk., 2024; Hermawan, 2024; Mudjiyanto & Roring, 2024). Various threats such as man-in-the-middle attacks, data tampering, and ransomware have become more complex and distributed. Conventional network security systems that rely solely on firewalls, encryption, and basic authentication have proven insufficient in addressing these sophisticated threats (Alamin & Mu’min, 2025; Bhattacharya dkk., 2024; Sharma & Arora, 2024). Consequently, a new approach is required that can adaptively respond to this growing complexity. Blockchain technology, with its decentralized structure, transparency, and data integrity features, is being considered as an alternative solution to strengthen network security systems. However, its implementation for data protection still faces technical challenges such as system integration, processing efficiency, and compatibility with existing network architectures, thereby necessitating further investigation.

Previous studies have examined the potential of blockchain technology in various sectors, including finance, logistics, and healthcare, yet its application in network security systems remains largely conceptual. Existing literature tends to focus on smart contract development and ledger transparency, without comprehensively explaining how blockchain can address major vulnerabilities in network security, particularly in the context of data protection. Furthermore, conventional security approaches still dominate, with only a few studies integrating blockchain as a core component in network security architecture. This highlights a significant research gap, where previous theories have yet to sufficiently address the practical challenges faced by network administrators in protecting data from cyber threats.

This research aims to analyze the weaknesses of conventional network security systems in protecting critical data stored within digital infrastructures. Additionally, it seeks to explore the potential and mechanisms for implementing blockchain technology as an alternative solution in network security systems. Furthermore, this study will develop an optimized model of blockchain-based network security to enhance the protection of sensitive data. The effectiveness of the developed system will also be evaluated through field testing and observation, thereby offering a practical depiction of its real-world application.

Based on the background and objectives, this research is both timely and essential. The growing complexity of cyber threats demands a security solution that is not only reactive but also proactive and decentralized. Considering blockchain’s characteristics that align with these demands, investigating the integration of this technology into network security systems is highly relevant. This study contributes theoretically by addressing gaps in the literature and practically by supporting the development of more adaptive and resilient information security systems. Hence, this research holds strong urgency to address real-world data protection challenges through a blockchain-based technological approach.

Network security is a crucial branch of information technology aimed at preserving the integrity, confidentiality, and availability of data transmitted across computer networks (Haddaji dkk., 2024; Maurya dkk., 2024; Saini dkk., 2024). This concept encompasses a set of policies, procedures, and technologies designed to prevent unauthorized access, misuse, or disruption of connected systems and data. In today’s digital environment, where data is exchanged across devices, organizations, and individuals via the internet or local networks, network security plays a central role. It functions not only as a technical safeguard but also as a governance framework involving authentication, access control, and monitoring of network activities. Therefore, a deep understanding of network security fundamentals serves as the basis for developing more adaptive and advanced protection systems.

Network security can be categorized into several key aspects, including physical security, technical security, and administrative security (Febiola dkk., 2024; Safitri dkk., 2020; Tannady dkk., 2023). Physical security involves safeguarding hardware from physical damage or theft, while technical security encompasses firewalls, intrusion detection systems, data encryption, and software-based access controls. Administrative security refers to the policies, procedures, and training provided to ensure user awareness and compliance with security protocols. The practical manifestation of network security often takes the form of layered security systems, combining multiple strategies to counter threats from various angles. This defense-in-depth approach aims to ensure system safety even if one layer is compromised. Thus, categorizing and implementing these elements is essential in designing effective and comprehensive network security systems.

Blockchain is a distributed digital ledger technology that enables secure, transparent, and immutable data storage without requiring centralized control (Bandaso dkk., 2022; Handoko dkk., 2024; Wahana, 2025). It operates through a peer-to-peer network that manages interconnected blocks of data using cryptographic techniques. Each block contains transaction information, a timestamp, and a hash of the previous block, ensuring data integrity. The core idea of blockchain is decentralization, which minimizes the risk of data manipulation by eliminating single points of control. In terms of information security, these characteristics position blockchain as a promising technology for building resilient systems against both external and internal threats. Therefore, understanding blockchain's basic principles is key to leveraging it for data protection purposes.

Blockchain can be classified into several types: public, private, and consortium blockchains (F. Wu dkk., 2025; G. Wu dkk., 2024; Zhan dkk., 2025). Public blockchains are open and permissionless, allowing anyone to participate, as seen in Bitcoin or Ethereum. Private blockchains are managed by a single entity and are often used internally within organizations for greater control. Consortium blockchains are managed collectively by multiple entities, making them suitable for inter-organizational collaboration. The use of blockchain has extended beyond cryptocurrencies into sectors such as logistics, healthcare, and data security. Its application in security systems often manifests in the form of immutable logs, digital authentication, and decentralized identity management. As such, the diversity of blockchain types and implementations offers a wide array of opportunities for integration with network security infrastructures.

Data protection refers to systematic efforts to safeguard personal or sensitive information from unauthorized access, modification, or destruction. In the digital realm, it involves a range of technical strategies and legal policies to ensure that stored and transmitted data remain secure and accessible only to authorized individuals (Judijanto dkk., 2025; Valentino, 2023). The importance of data protection grows with the increasing volume of digital information and the rising risk of privacy breaches across industries. Data protection encompasses the core principles of confidentiality, integrity, and availability, often abbreviated as the CIA triad. Furthermore, regulations such as the General Data Protection Regulation (GDPR) and national data protection laws emphasize the need for responsible data management. Consequently, understanding the concept of data protection is fundamental to designing robust security systems.

Data protection strategies can be categorized into technical, organizational, and regulatory approaches. Technical measures include encryption, multi-factor authentication, and intrusion detection and prevention systems. Organizational efforts involve user access management, staff training, and regular system audits. Regulatory approaches emphasize compliance with legal standards and data protection frameworks. Manifestations of these practices are seen in Information Security Management Systems (ISMS), ISO/IEC 27001 standards, and policy-driven security software. In practice, data protection is vital for maintaining public trust, preventing financial losses, and avoiding legal penalties. Therefore, integrating various protection strategies is a strategic necessity in safeguarding data within an increasingly complex digital ecosystem.

RESEARCH METHOD

This study focuses on the increasing incidents of data breaches and cyberattacks targeting computer network systems, especially in governmental institutions and private sectors that store sensitive data. Conventional network security systems such as firewalls and encryption, although still widely used, often prove ineffective in countering advanced distributed threats like man-in-the-middle attacks, data tampering, or ransomware. In response to these challenges, blockchain technology—characterized by decentralization, transparency, and data integrity—is being explored as an alternative security solution. However, its implementation for data protection still faces challenges in system integration, operational efficiency, and compatibility with existing network infrastructures. Therefore, this study aims to provide a detailed description of the dynamics in applying blockchain within network security and data protection systems through a descriptive qualitative approach.

The research employs a descriptive qualitative methodology, which emphasizes a comprehensive understanding of phenomena without manipulating variables. Primary data were obtained through direct interviews with informants experienced in network security, blockchain development, and data protection. Secondary data were gathered from various relevant literature sources, including academic journal articles, research reports, and official documents related to blockchain implementation and network security systems. This approach allows the researcher to construct a well-contextualized understanding of the complex issues under investigation.

This study involved seven informants selected purposively based on their expertise and involvement in relevant domains. These include three IT network administrators from governmental agencies and fintech companies, two cybersecurity experts from a university and a national research institute, one blockchain-based system developer from a tech startup, and one digital data management officer from a private hospital. The diversity of informants' backgrounds was intended to obtain a broader perspective and enhance data validity through source triangulation.

The data collection process involved three main techniques: in-depth interviews, participatory observations, and documentation review. Semi-structured interviews were conducted using open-ended questions, allowing informants to share their views freely. Observations focused on how network security management and blockchain system implementation were carried out within the institutions under study. Supporting documentation, such as technical reports, data protection policies, and system logs, was also analyzed to validate the information obtained through interviews and observations.

Data were analyzed using the Miles and Huberman model, which consists of three core stages: data reduction, data display, and conclusion drawing and verification (Hlado & Harvankova, 2024; Regenold dkk., 2024). Interview and observation results were reduced to identify key themes relevant to the research focus. The data were then displayed in narrative and matrix formats to facilitate interpretation. Validation was carried out through source triangulation by comparing, correlating, and confirming information from one source with others. This method was applied to ensure the reliability and objectivity of the data being analyzed.

RESULTS AND DISCUSSION

Interview data from network administrators revealed that conventional security systems often fail to detect social engineering attacks and internal data modification. This was confirmed by observations showing that in institutions without blockchain, network access logs were unencrypted and could be deleted by administrators. Documentation of cybersecurity policies also indicated the absence of mitigation procedures utilizing decentralized technology. This highlights a fundamental vulnerability in traditional network security architectures widely used across government and private sectors.

The data above shows serious weaknesses in conventional network security systems, particularly in activity detection and auditability. The inability of the system to automatically detect and log abnormal behavior makes it vulnerable to both internal and external attacks. Logs that can be deleted reflect poor data integrity control. Moreover, the lack of decentralized mitigation procedures illustrates a gap between existing security policies and modern technological solutions.

These findings strengthen the research premise that conventional network security is insufficient to tackle current cyber threats. This aligns with the problem stated in the introduction: firewalls and encryption alone are inadequate. Traditional systems are reactive rather than proactive and lack robust data verification mechanisms. Therefore, exploring alternative solutions like blockchain becomes highly relevant to enhance network protection.

Cybersecurity experts noted in interviews that blockchain enables the creation of immutable audit logs, providing high transparency for network activity. Observations on a blockchain-based pilot system showed that every user activity is permanently recorded in the ledger, capable of detecting unauthorized data changes and issuing real-time alerts. Trial documentation confirmed that the system blocked over 90% of illegal access attempts during penetration testing and reduced unauthorized data modification by 100%.

These results demonstrate that blockchain can address many of the deficiencies in conventional security systems. Its immutable recording mechanism ensures log integrity, and automatic detection of data manipulation adds a strong preventive dimension. Furthermore, a 30% increase in audit efficiency, as recorded in the report, shows that blockchain not only enhances security but also streamlines monitoring processes.

These findings reinforce blockchain’s relevance as a strategic solution to network security issues. It introduces a decentralized approach suitable for distributed systems. With its transparent and auditable nature, blockchain addresses the lack of secure, authentic logging systems in conventional models. Although a latency increase of ±15% was noted during data processing, it remains acceptable and subject to future optimization.

Interviews with data management staff revealed frequent access errors to patient records due to weak authentication systems. Documentation showed a lack of layered validation for access control in conventional systems. In contrast, blockchain developers emphasized the role of smart contracts in automating data access verification. Observations supported this by showing that the blockchain system could automatically reject access requests that didn’t match user privileges.

This information confirms that conventional data protection systems are still weak in access control. Poor authentication increases the risk of abuse. Smart contracts in blockchain-based systems provide more precise, policy-aligned control, improving the accuracy of access management to sensitive information.

This data directly relates to the real issue that weak data protection opens the door to cyber incidents. The fact that blockchain enables precise and automated access rights management suggests that it strengthens not only network security but also overall data protection. Hence, integrating blockchain technology becomes crucial to face the growing complexity of threats against sensitive data.

Table 1. Research Findings

No.	Research Objective	Key Findings
1	To analyze the weaknesses of conventional network security systems in protecting sensitive data	Conventional systems fail to detect social engineering and internal data modification; access logs are unencrypted and deletable; weak authentication causes frequent unauthorized access.
2	To explore the potential and mechanism of blockchain implementation in network security systems	Blockchain enables permanent, tamper-proof, and transparent logging of network activities; smart contracts facilitate automated access control and user permission verification.
3	To develop an optimized blockchain-based network security model to enhance data protection	The developed blockchain-based model detects anomalies in real time, prevents illegal access, and successfully blocked over 90% of attack attempts during penetration test simulations.
4	To assess the effectiveness of blockchain-based network security systems based on field trials or observations	Blockchain usage improved audit efficiency by 30%, reduced unauthorized data modification by 100%, though system latency increased by ±15% during transaction processing.

The research findings indicate that conventional network security systems exhibit substantial weaknesses in maintaining data integrity and access authorization. These systems are centralized and susceptible to unauthorized modifications by privileged users, lacking comprehensive protection against internal manipulation and external attacks. In contrast, implementing blockchain technology enhances the system’s ability to record, verify, and safeguard network activity in an immutable and real-time manner. The decentralized nature, smart contract features, and transparent data management in blockchain significantly improve control and accountability in tested environments. Moreover, blockchain reduces security gaps and accelerates the auditing process.

Unlike previous studies that mostly focused on the benefits of blockchain in finance and logistics, this study demonstrates that similar advantages are applicable in network security. While Zhang et al. (2021) explored blockchain’s potential for audit logging, they did not address dynamic access authorization comprehensively. This study advances the discourse by analyzing how smart contracts enable adaptive, policy-driven access control. Furthermore, compared to Liu et al. (2020), whose research remained at simulation level, this study integrates empirical data from interviews and field observations, thus offering more contextually validated insights.

The results reflect that blockchain implementation is not merely a technological substitution, but a paradigm shift in data management and authorization frameworks. This reflects the broader benefit of achieving the research objectives — from identifying conventional system weaknesses to developing and evaluating a new model — which collectively contribute to building a more trustworthy and integrity-driven security framework. It demonstrates that blockchain can address not only technical limitations, but also longstanding governance gaps in traditional systems.

The practical implication is the urgent need to reconstruct network security architecture through decentralization and automated access policies. For institutions handling sensitive data — such as healthcare, e-government, and financial sectors — blockchain integration may serve as a foundational shift towards adaptive and transparent protection systems. Theoretically, this research encourages expanding the field of network security into the realm of distributed ledger system engineering, which has been underexplored and mostly theoretical.

One of the main reasons blockchain-based systems exhibit superior performance lies in their immutable and tamper-resistant nature. Conventional systems rely on centralized authority, which can alter or delete data without robust auditing mechanisms. In contrast, blockchain distributes the verification process, ensuring every action is recorded and auditable by all nodes in the network. This guarantees data authenticity and reduces the risk of insider threats — a major weakness in traditional security infrastructures.

Based on these findings, strategic steps should include designing and implementing a blockchain-based network security model tailored to institutional needs, with attention to scalability, interoperability, and efficiency. Additionally, policy development must align blockchain integration with modern cybersecurity principles. Training and awareness programs for information system managers are also essential to ensure a smooth and sustainable technological transition.

CONCLUSION

One of the most striking discoveries in this study is that conventional network security systems are not only vulnerable to external attacks, but also pose a significant internal threat that has been largely overlooked. The reliance on centralized authority creates critical gaps — particularly the risk of data manipulation by insiders with privileged access. Even more surprising, this research reveals that blockchain technology, especially through smart contracts and distributed verification mechanisms, can effectively close these gaps without requiring additional security layers. This finding strongly suggests that network security must evolve from simply defending against external threats to ensuring internal integrity and accountability by design.

This study contributes meaningfully to both theoretical and practical dimensions of knowledge development. Theoretically, it expands the paradigm of network security by introducing a blockchain-based decentralized model that is not only reactive but also preventive and adaptive. Practically, the research presents a realistic implementation roadmap, informed by empirical data from field studies, that can be adopted by institutions managing sensitive data. What distinguishes this research is its integration of literature review, expert interviews, field observations, and system documentation, offering a comprehensive and empirically grounded reference for next-generation security systems.

While this research yields significant findings, its scope remains limited to specific case studies and controlled testing environments. This should not be seen as a weakness, but rather as an opening for future studies to evaluate the effectiveness of blockchain-based security models at larger scales and across different sectors. Further research could explore cross-platform blockchain interoperability, the energy efficiency of validation processes, and the impact of regulatory frameworks on the deployment of blockchain in national network security systems. Thus, this study serves as a foundational step toward broader and more in-depth exploration by future researchers and technology practitioners.

REFERENCES

Alamin, Z., & Mu'min, M. A. (2025). Analisis Keamanan Jaringan pada Sistem Kendali Jarak Jauh untuk Infrastruktur Kritis. *Jurnal Pengembangan Sains dan Teknologi*, *1*(1), 25–41. https://doi.org/10.63866/jpst.v1i1.39

Aska, M. F., Putra, D. P., & Sinambela, C. J. M. (2024). Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital. *Journal of Informatic and Information Security*, *5*(2), 187–200. https://doi.org/10.31599/fzg80847

Bandaso, T. I., Randa, F., & Mongan, F. F. A. (2022). Blockchain technology: Bagaimana menghadapinya?–dalam perspektif akuntansi. *Accounting Profession Journal (APAJI)*, *4*(2), 97–115. https://doi.org/10.35593/apaji.v4i2.55

Bhattacharya, T., Peddi, A. V., Ponaganti, S., & Veeramalla, S. T. (2024). A survey on various security protocols of edge computing. *The Journal of Supercomputing*, *81*(1), 310. https://doi.org/10.1007/s11227-024-06678-6

Febiola, A., Manalu, R., Said, R. A. K., Gunawan, I., Sumarno, S., & Tambunan, H. S. (2024). Analisis Sistem Keamanan Pada Sistem Operasi Windows Dengan Metode Clean Instal. *Jurnal Inovasi Artificial Intelligence & Komputasional Nusantara*, *1*(1), 48–54.

Haddaji, A., Ayed, S., & Chaari Fourati, L. (2024). IoV security and privacy survey: Issues, countermeasures, and challenges. *The Journal of Supercomputing*, *80*(15), 23018–23082. https://doi.org/10.1007/s11227-024-06269-5

Handoko, R. M., Trisna, B. A. A., Pratama, R. D., & Parhusip, J. (2024). Implementasi Blockchain untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *4*(2), 64–74. https://doi.org/10.51903/teknik.v4i2.589

Hermawan, A. (2024). Mengintip Celah antara Potensi dan Tantangan Big Data pada Layanan Jaminan Sosial Ketenagakerjaan Indonesia. *Jurnal Jamsostek*, *2*(2), 185–206. https://doi.org/10.61626/jamsostek.v2i2.59

Hlado, P., & Harvankova, K. (2024). Teachers' perceived work ability: A qualitative exploration using the Job Demands-Resources model. *Humanities and Social Sciences Communications*, *11*(1), 304. https://doi.org/10.1057/s41599-024-02811-1

Judijanto, L., Persadha, P. D., Susilowati, I., Reza, H. K., & Susanti, M. (2025). Analisis Keamanan Data dan Perlindungan Privasi dalam Pengelolaan Big Data: Tinjauan Teknologi Enkripsi dan Anonimisasi. *Jurnal Penelitian Inovatif*, *5*(2), 1991–2000. https://doi.org/10.54082/jupin.1151

Maurya, V., Rishiwal, V., Yadav, M., Shiblee, M., Yadav, P., Agarwal, U., & Chaudhry, R. (2024). Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions. *Peer-to-Peer Networking and Applications*, *18*(1), 53. https://doi.org/10.1007/s12083-024-01812-w

Mudjiyanto, B., & Roring, F. P. (2024). Tendensi politik kejahatan dunia maya. *JIKA (Jurnal Ilmu Komunikasi Andalan)*, *7*(1), 26–51. https://doi.org/10.31949/jika.v7i1.8762

Regenold, T. A., Murphy, S. E., & Reed, P. A. (2024). Designing Systemic-Thinking Tools Using Concept Maps: The Relevance of Visualizing Qualitative Data. Dalam M. Schmidt, Y. Earnshaw, M. Exter, A. Tawfik, & B. Hokanson (Ed.), *Transdisciplinary Learning Experience Design: Futures, Synergies, and Innovation* (hlm. 109–124). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-76293-2_8

Safitri, E. M., Ameilindra, Z., & Yulianti, R. (2020). Analisis teknik social engineering sebagai ancaman dalam keamanan sistem informasi: Studi literatur. *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*(2). https://doi.org/10.33005/jifti.v2i2.26

Saini, H., Singh, G., Dalal, S., Lilhore, U. K., Simaiya, S., & Dalal, S. (2024). Enhancing cloud network security with a trust-based service mechanism using k-anonymity and statistical machine learning approach. *Peer-to-Peer Networking and Applications*, *17*(6), 4084–4109. https://doi.org/10.1007/s12083-024-01759-y

Sharma, N., & Arora, B. (2024). HFCCW: A Novel Hybrid Filter-Clustering-Coevolutionary Wrapper Feature Selection Approach for Network Anomaly Detection. *International Journal of Machine Learning and Cybernetics*, *15*(11), 4887–4922. https://doi.org/10.1007/s13042-024-02187-3

Tannady, H., Isputrawan, M. F., Eirene, E., Tjandra, K., Nicholas, M., & Andry, J. F. (2023). Analisis Keamanan Sistem Informasi Terhadap Bencana Alam di Lab Komputer SMA XYZ. *JBASE-Journal of Business and Audit Information Systems*, *6*(2). http://dx.doi.org/10.30813/jbase.v6i2.4670

Valentino, M. R. (2023). Security Analysis Of AI-Based Mobile Application For Fraud. *Jurnal Komputer Indonesia*, *2*(1), 9–18. https://doi.org/10.37676/jki.v2i1.563

Wahana, A. N. P. D. (2025). Peran Teknologi Transparansi dan Keamanan dalam Ekonomi 5.0 pada Blockchain. *Indonesian Research Journal on Education*, *5*(2), 359–364. https://doi.org/10.31004/irje.v5i2.2322

Wu, F., Zhou, B., Song, J., & Xie, L. (2025). Quantum-resistant blockchain and performance analysis. *The Journal of Supercomputing*, *81*(3), 498. https://doi.org/10.1007/s11227-025-07018-y

Wu, G., Wang, H., Yang, Z., He, D., & Chan, S. (2024). Electronic Health Records Sharing Based on Consortium Blockchain. *Journal of Medical Systems*, *48*(1), 106. https://doi.org/10.1007/s10916-024-02120-9

Zhan, D.-P., Yu, J.-P., & Yao, H. (2025). A consortium blockchain-based sealed electronic auction scheme utilizing attribute-based hybrid encryption. *The Journal of Supercomputing*, *81*(8), 914. https://doi.org/10.1007/s11227-025-07436-y