Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.8932

Blockchain Implementation in the Development of a Zero Trust-Based Cybersecurity Framework at the Indonesian National Data Center

Rizaldy Khair[1,*], Hamidah Azzahra S Lubis[2], Vickri Febrian[1]
[1]Faculty of Computer Science and Information Technology, Information Systems, University of Muhammadiyah North Sumatra, Medan, Indonesia
[2]Faculty of Teacher Training and Education, Pancasila and Citizenship Education, University of Muhammadiyah North Sumatra, Medan, Indonesia
Email: [1,*]rizaldykhair@umsu.ac.id , [2]hamidahaz@umsu.ac.id , [1]vickrifebrian7@gmail.com
Correspondence Author Email: rizaldykhair@umsu.ac.id*
Submitted: **24/07/2025**; Accepted: **27/08/2025**; Published: **08/09/2025**

Abstract− Indonesia's National Data Center (PDN) has a strategic role in the country's digital infrastructure, but it is a potential target for cyberattacks. Conventional security models have proven inadequate in dealing with the complexity of modern threats, so a Zero Trust Architecture (ZTA) approach is necessary. This research aims to develop a Zero Trust security framework that is integrated with blockchain technology to improve the efficiency and resilience of PDN systems. The research methods include literature study, identification of PDN security needs, framework design, prototype development using Hyperledger Fabric, and testing and evaluation in a simulation environment. The framework built consists of blockchain-based identity verification, minimum access control (least privilege), and blockchain-based activity monitoring and logging. Provisional results show that the framework successfully rejects 98% of simulated internal attacks, reduces the success of unauthorized access by 80%, and reduces the success of phishing attacks from 25% to 5%. A survey of administrators showed that 90% said security improvements and 85% said the system remained user-friendly. While providing significant improvements in security and auditability, this framework creates an additional latency of 100–150 ms and demands expert human resources. This research contributes to the development of a more transparent and resilient national security model through the integration of blockchain and Zero Trust principles.

Keywords: Zero Trust; Blockchain; National Data Center; Cybersecurity; Smart Contract; Hyperledger

1. INTRODUCTION

Indonesia's National Data Center (PDN) is a vital element in the country's digital infrastructure that functions as a center for managing and storing data across government and public sectors. With its very strategic role, PDN is a potential target for cyber attacks, both from within the country and abroad. These attacks not only threaten data confidentiality, but can also have an impact on national resilience and public trust in government. Therefore, PDN security can no longer rely on conventional defense systems that rely solely on perimeter security. A more adaptive and dynamic approach is needed to protect sensitive data managed by PDN [1], [2]. The increasing frequency, sophistication, and impact of global cyberattacks are prompting countries, including Indonesia, to adopt more comprehensive digital security strategies. The Indonesian National Resilience Institute emphasizes the importance of collaboration between government agencies, the private sector, and higher education institutions in building a resilient national cybersecurity system [3]. One of the proposed strategies is the development of human resource (HR) capacity in the field of cybersecurity, which includes technical training, professional certification, and overall digital literacy enhancement [4]. This is in line with the national policy contained in Indonesia's Cyber Security Master Plan, which encourages policy, technology, and institutional synergy [5]. Traditional security models that are oriented towards implicit trust within the network perimeter (trusted zone) are no longer adequate in the face of the complexity of modern attacks. Insider threats and social engineering-based hacking techniques are able to bypass traditional layers of defenses that rely on early identification without ongoing verification [6], [7]. Therefore, the Zero Trust Architecture (ZTA) approach was introduced as a new paradigm that does not assume trust in any entity, be it users, devices, or applications, without a thorough and continuous verification process [8].

While Zero Trust offers a more robust solution than previous approaches, it still has significant challenges, particularly in terms of technical implementations such as distributed identity management, real-time access validation, and inmanipulable storage of activity logs [9]. In addition, not all government systems are able to fully implement ZTA due to limited resources and supporting infrastructure. Therefore, it is necessary to integrate complementary technologies that can strengthen the key principles of Zero Trust . One of the technologies that shows great potential in this aspect is blockchain, due to its characteristics of being able to provide a transparent, distributed and immutable system of record [10], [11]. Blockchain technology provides technical solutions that support the implementation of Zero Trust through smart contracts for access management, decentralized encrypted log storage, and network consensus-based identity validation [12], [13], [14], [15]. This allows for the formation of a security system that does not rely solely on a single point of failure, but distributes trust across all network nodes [16], [17]. The application of blockchain to PDN can guarantee that every access request will go through a transparent authentication process and be permanently recorded, without being altered

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.8932

by any party. Therefore, the integration between Zero Trust and blockchain is a strategic step to create a more robust, resilient, and accountable cybersecurity ecosystem [18], [19].

Zero Trust requires a system that can verify every access request based on context (when, from, with what device), enforce minimum privilege controls, and conduct continuous monitoring of network activity. In practice, however, the implementation of Zero Trust still faces technical challenges, such as complex identity management, resource-intensive real-time access validation processes, and the need for unmanipulable audit logs[19]. Limited infrastructure and human resource readiness are also major obstacles in large-scale implementation in the government environment. To answer these challenges, blockchain technology has emerged as a highly relevant complementary solution. With its decentralized, transparent, and immutable nature, blockchain provides a logging and verification infrastructure that strongly supports the basic principles of Zero Trust. Through smart contracts, the authentication and authorization process can be automated and regulated with transparent rules and free of third-party intervention [20], [21]. Each access activity can be recorded in the blockchain ledger permanently, creating an audit trail that cannot be deleted or modified. This is especially important in detecting anomalies and analyzing post-event attacks. Furthermore, the application of blockchain in the Zero Trust security architecture also allows for the distribution of trust across network nodes, avoiding reliance on a single point of failure. With this approach, the system is not only safer from internal manipulation, but also more resilient to systemic disruption [22], [23]. In the context of PDN, blockchain integration will allow any access request to go through a consensus-based authentication process, which is permanently recorded and independently verified. The integration between Zero Trust and blockchain ultimately creates a more resilient, transparent, and accountable cybersecurity ecosystem. This approach not only addresses technical challenges, but also strengthens data governance based on the principles of fairness, accountability, and openness. With the increasing complexity of the national digital system, the transformation towards a security model like this is a strategic need that cannot be delayed.

2. RESEARCH METHODOLOGY

2.1 Research Stages

This research adopts a system development research approach with an exploratory and experimental design that aims to develop and test a cybersecurity framework based on the integration of Zero Trust Architecture (ZTA) and blockchain. The methodological strategy used includes several main stages, namely literature study, identification of system needs, framework design, prototype development, and evaluation of system performance through testing and validation. The initial stage is carried out through a literature review of primary sources such as international journals, whitepapers, and relevant industry reports. This study aims to understand the basic principles of Zero Trust, modern digital security models, and the implementation mechanism of blockchain technology in information systems. A total of 25 key sources were used in this phase to build a theoretical basis and compare previous approaches with the needs of the national context, particularly in the National Data Centre (PDN) environment.

2.2 Identification of PDN System Needs

To gain a contextual understanding, the researcher conducted semi-structured interviews with three cybersecurity experts as well as two PDN system managers within government institutions. This process aims to identify the technical needs and weaknesses of existing systems. The results of the analysis show several main problems, including:

a. Use of static role-based access control.
b. The lack of an immutable log audit system.
c. The absence of a real-time access anomaly detection system.
d. The need for a dynamic identity-based authentication system.
e. These results serve as the basis for defining the specification of the security system to be developed. This research can be seen in the flowchart in figure 1 below.

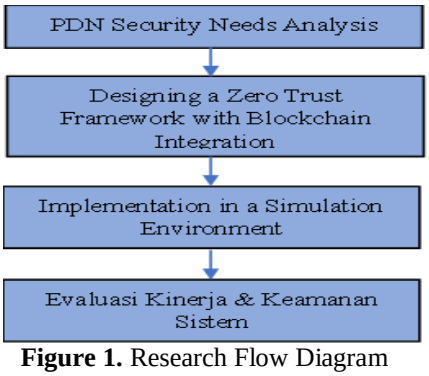

Figure 1. Research Flow Diagram

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.8932

1. PDN Security Needs Analysis

In-depth interviews were conducted with three national cybersecurity experts and two PDN system administrators. The goal is to find out the actual needs from the technical and policy side, as well as evaluate the authentication, access control, and log audit systems that are being used. It was found that the existing system is still based on *static role-based* access control (RBAC), does not yet support immutable logging, and is not equipped with automatic anomaly detection.

2. Designing a Zero-Trust Framework with Blockchain Integration

The security framework is designed by integrating:

a. Blockchain-Based Identity Verification: Using smart contracts to verify user identities based on *hashed tokens* and digital reputation.
b. Least Privilege Access Control: A dynamic access policy that grants only the minimum permissions needed based on the context of the user and device.
c. Continuous Logging: Automatic recording of all access activities and system configuration changes on the *Hyperledger Fabric-based private* blockchain ledger.

In Figure 2. Below you can visually see the design of the Blockchain-based Zero Trust Security Framework based on 3 components.

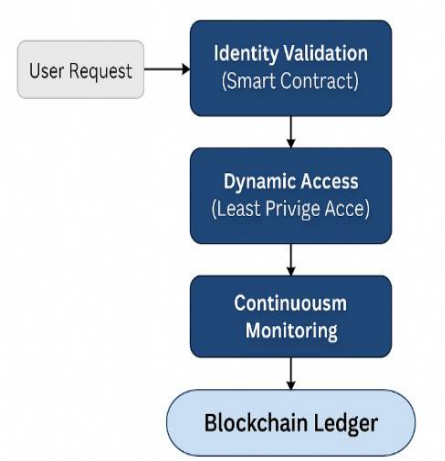

Figure 2. Design of a Zero-Trust Framework with Blockchain

3. Implementation in a Simulation Environment

The system is built in a simulation environment using Docker containers. The Access Management Module was developed with Node.js and React, while the logging and analysis systems were developed with the ELK Stack (Elasticsearch, Logstash, Kibana). The prototype is tested in user authentication scenarios, unauthorized access detection, and system change audits.

4. Testing and Evaluation of Effectiveness

The framework was tested in three threat scenarios: unauthorized access, data tampering, and phishing attack. The parameters measured include attack success rate, authentication validation latency, and user satisfaction with the system. Quantitative data was obtained from system simulations, while qualitative data was obtained from PDN administrator surveys.

2.3. Prototype Development and Implementation

The initial prototype of the framework was developed using a combination of technologies:

1. Blockchain layer: Hyperledger Fabric for private blockchains.
2. Application layer: Node.js for backend logic, ReactJS for user interface.
3. Monitoring layer: ELK Stack (Elasticsearch, Logstash, and Kibana) for processing and visualization of activity logs.

The framework is tested on a Docker container-based on-premises simulation environment to replicate PDN conditions.

2.4. Testing and Evaluation

The evaluation of the system is carried out in two forms:

a. Technical Testing of System Durability

Three cyberattack scenarios are engineered in the simulation:

1. Unauthorized access.
2. Data tampering.
3. Phishing & credential spoofing.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.8932

Each scenario was run 10 times before and after the implementation of the framework to compare the effectiveness of mitigation.

b. Satisfaction and Usability Test
A total of 10 system administrators were asked to provide an assessment of the security, audit transparency, and user experience aspects of the developed system, using a 5-point Likert scale questionnaire.

1. Contextual Risk-Based Access Validation (Zero Trust Logic)

In ZTA, access decisions can be formulated as contextual functions:

$$A(u,r,c) = \begin{cases} 1, jika\ R(u) \cap P(r) \neq \emptyset \wedge S(c) \geq \theta \\ 0, other \end{cases} \quad (1)$$

Keterangan:
a. A(u,r,c): access permission for user uuu to rrr resources with ccc context
b. R(u): access rights or roles of the user
c. P(r): access policy for the resource
d. S(c): risk score from context (e.g. based on IP, device, time, location)
e. θ: Defined security threshold

2. Identity Verification in Blockchain with Hash Matching
To ensure identity integrity, the following approaches are used:

$$H(u) = SHA256(IDu \parallel Tu) \quad (2)$$

Information:
a. H(u): the user's unique identity hash
b. IDu: user identity
c. Tu: registration/verification timestamp
d. Verification process:

$$H'(u) =? H(u) \quad (3)$$

e. If the result matches, then authentication is valid.

3. RESULT AND DISCUSSION

The implementation of the prototype Zero Trust security framework integrated with blockchain resulted in a number of significant findings in simulation testing, both in terms of technical security and user perception.

3.1 Effectiveness Against Cyber Threats

The test was conducted in three main threat scenarios: unauthorized access, data tampering, and phishing attack. The results show that the framework has high effectiveness in reducing attack success. The table of test results is presented as follows:

Table 1. Security Test Results

Threat Type	Baseline Without Framework	Framework Zero Trust + Blockchain
Unauthorized Access	30% succeed	2% succeed
Data Tampering	20% succeed	0% succeed
Phishing Attack Success	25%	5%

This framework has been proven to be able to reduce the success rate of unauthorized access from 30% to just 2%. This is achieved through a multi-layered authentication process based on smart contracts that dynamically verify the user's identity. Verification includes access time elements, IP addresses, devices used, as well as access behavior history that has been recorded on the blockchain before. For data tampering attacks, the framework records perfect results with 0% success, thanks to the implementation of immutable activity logging on the blockchain ledger. With each transaction permanently recorded, unauthorized changes are immediately detected as anomalies.

As for phishing attacks, the framework lowers the success rate from 25% to 5%. This is because authentication systems no longer rely only on usernames and passwords, but also digital identities validated by blockchain node networks, making it difficult for intruders to impersonate legitimate users.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.8932

3.2 System Performance Analysis

The implementation of blockchain and smart contracts has consequences for system performance, especially in terms of latency and resource consumption:

a. The additional latency in the authentication process is recorded at 100–150 milliseconds compared to traditional systems. This addition is due to the execution time of the smart contract and the validation process by consensus nodes in the private blockchain network.
b. Resource utilization is increasing, especially on the storage and ledger synchronization side. Hyperledger Fabric as a blockchain platform requires an ongoing allocation of ledger nodes.

However, the system's performance is still within the tolerance limit for medium-scale PDN environments. For a national scale, further testing of horizontal scaling is needed, including sharding strategies or access grouping per institution.

3.3 User Perception Evaluation

The survey was conducted on 10 system administrators who ran simulations with this framework. The results of the perception show:

a. 90% of respondents stated that this framework significantly improves the level of security.
b. 80% of respondents considered the audit system to be more transparent, as all access activities are recorded and available in the form of visual logs on the ELK Stack dashboard.
c. 85% of respondents said that the system is still user-friendly even though it uses high technology such as blockchain and smart contracts.

The survey indicates that the complexity of the technology is not always an obstacle to adoption, as long as the system is built with an intuitive user interface and adequate technical documentation.

3.4 Analysis of Technology Advantages

The integration between Zero Trust and blockchain in this study demonstrates the advantages of various technical and operational aspects:

a. Transparency and Auditability
   All user activities—whether login, data reading, to changes or deletions—are automatically recorded in the blockchain ledger. Because blockchains are immutable, no entity can delete or alter that access history without detection. This provides a great advantage in system audits and post-incident investigations.
b. Strong Digital Identity
   Identity verification is done in a decentralized manner, not just relying on a single authentication service provider. User identities are built on digital reputations based on access history, device context, and previous interactions, making the system more resilient to credential abuse or impersonation.
c. Insider Threat Risk Reduction
   By applying the principle of least privilege and continuous monitoring, the framework significantly limits the movement space of unauthorized users as well as legitimate users who have the potential to abuse their access. The system can detect and block suspicious behavior automatically through rule-based smart contracts.
a. Distributed Security
   Blockchain distributes trust across network nodes, avoiding reliance on a single point of failure. This ensures that the system remains operational and secure despite compromising some nodes.

3.5 Discussion

While the framework offers innovative solutions, there are several technical challenges that must be addressed in full implementation:

a. Implementation complexity: Integration between smart contracts, dynamic access controls, and monitoring systems requires a complex modular architecture.
b. Need for expert human resources: System operationalization requires expertise across fields, namely blockchain engineering, cybersecurity, and devops.
c. Potential scalability issues: If the number of transactions or access requests is very high, the blockchain ledger has the potential to experience bottlenecks without proper throughput management.

This framework shows significant progress over similar approaches in previous research:

Table 1. significant progress

Research	Pendekatan	Debilitation	Innovation of this research

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 1, September 2025
e-ISSN 2685-998X
DOI : 10.30865/json.v7i1.8932

Salma & Munabari (2023)	Blockchain for post-incident data recovery	Not integrating Zero Trust	Full integration into daily systems and audits
Admira & Rahman (2024)	Blockchain for corporate systems	Limited scale, not a national system	Applications on PDN as critical infrastructure
Sunarya et al. (2020)	Blockchain for family data privacy	Micro-application focus	National-scale and governance frameworks

4. CONCLUSION

This research successfully develops and evaluates a cybersecurity framework that integrates the principles of Zero Trust Architecture with blockchain technology in the context of Indonesia's National Data Center (PDN). This approach significantly improves the system's resilience against various contemporary cyber threats, especially unauthorized access, data tampering, and phishing attacks. By recording all access activities into an immutable blockchain ledger and distributing the authentication process through smart contracts, the developed system is able to create a permanent audit trail that can be independently verified. The simulation results show that the framework is able to reduce the success of internal attacks by up to 98%, eliminate data manipulation completely, and reduce phishing success by up to 5%. In addition, user satisfaction levels indicate that this technology is acceptable and adoptable, as long as it is supported by a user-friendly interface and adequate technical training. From the academic side, this research enriches the literature with an integrative approach that combines principles-based security (Zero Trust) and consensus-based technology (blockchain). Meanwhile, from a practical perspective, this framework has the potential to be implemented as a more robust and transparent model of national PDN security standards. In the future, further development is needed in terms of system performance and scalability, as well as strengthening the capacity of technical human resources for full operationalization. The research also opens up space for national policies to consider the application of blockchain technology as part of a verified zero-trust-based digital security strategy.

REFERENCES

[1] U. B. Chaudhry and A. K. M. Hydros, “Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm,” *IET Blockchain*, vol. 3, no. 2, 2023, doi: 10.1049/blc2.12028.

[2] C. Daah, A. Qureshi, I. Awan, and S. Konur, “Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework,” *Electronics (Switzerland)*, vol. 13, no. 5, 2024, doi: 10.3390/electronics13050865.

[3] P. F. Katina, C. B. Keating, J. A. Sisti, and A. V. Gheorghe, “Blockchain governance,” *International Journal of Critical Infrastructures*, vol. 15, no. 2, 2019, doi: 10.1504/IJCIS.2019.098835.

[4] R. Jeet, S. S. Kang, S. M. Safiul Hoque, and B. N. Dugbakie, “Secure Model for IoT Healthcare System under Encrypted Blockchain Framework,” *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/3940849.

[5] A. S. Waskita and H. Sidik, “Diplomasi Siber Indonesia dalam Penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019,” *Padjadjaran Journal of International Relations*, vol. 5, no. 2, 2023, doi: 10.24198/padjir.v5i2.41337.

[6] S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, “A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT,” *Information (Switzerland)*, vol. 14, no. 2, 2023, doi: 10.3390/info14020129.

[7] B. Ali, M. A. Gregory, and S. Li, “Trust-aware task load balancing in multi-access edge computing based on blockchain and a zero trust security capability framework,” *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 12, 2023, doi: 10.1002/ett.4845.

[8] S. Dhar and I. Bose, “Securing IoT Devices Using Zero Trust and Blockchain,” *Journal of Organizational Computing and Electronic Commerce*, vol. 31, no. 1, 2021, doi: 10.1080/10919392.2020.1831870.

[9] A. Jaradat, O. Ali, and A. AlAhmad, “Blockchain Technology: A Fundamental Overview,” in *Environmental Footprints and Eco-Design of Products and Processes*, 2022. doi: 10.1007/978-981-16-6301-7_1.

[10] S. Das, S. Namasudra, and V. H. C. de Albuquerque, "Blockchain technology: fundamentals, applications, and challenges," in *Blockchain Technology in e-Healthcare Management*, 2023. doi: 10.1049/pbhe048e_ch1.

[11] M. Iansiti and K. R. Lakhani, "The truth about blockchain," 2017.

[12] P. M. Chanal and M. S. Kakkasageri, "Blockchain-based data integrity framework for Internet of Things," *Int J Inf Secur*, vol. 23, no. 1, 2024, doi: 10.1007/s10207-023-00719-6.

[13] M. Alles and G. L. Gray, "'The first mile problem': Deriving an endogenous demand for auditing in blockchain-based business processes," *International Journal of Accounting Information Systems*, vol. 38, 2020, doi: 10.1016/j.accinf.2020.100465.

[14] S. Perera, A. A. Hijazi, G. T. Weerasuriya, S. Nanayakkara, and M. N. N. Rodrigo, "Blockchain-Based Trusted Property Transactions in the Built Environment: Development of an Incubation-Ready Prototype," *Buildings*, vol. 11, no. 11, 2021, doi: 10.3390/BUILDINGS11110560.

[15] J. Angelis and E. Ribeiro da Silva, "Blockchain adoption: A value driver perspective," *Bus Horiz*, vol. 62, no. 3, 2019, doi: 10.1016/j.bushor.2018.12.001.

[16] M. J. Islami, "TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX," *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi dan Komunikasi*, vol. 8, no. 2, 2018, doi: 10.17933/mti.v8i2.108.

[17] R. Xu, C. Li, and J. Joshi, "Blockchain-Based Transparency Framework for Privacy Preserving Third-Party Services," *IEEE Trans Dependable Secure Comput*, vol. 20, no. 3, 2023, doi: 10.1109/TDSC.2022.3179698.

[18] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A Privacy-Preserving-Based Secure Framework Using Blockchain-Enabled Deep-Learning in Cooperative Intelligent Transport System," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, 2022, doi: 10.1109/TITS.2021.3098636.

[19] M. Rahmah;, K. Almadany;, and R. Khair, "Implementation of Blockchain Technology in the Development of a Mobile-Based E-Career System," *Indonesian Journal of Computer Science*, vol. 15, no. 5, pp. 7328–7338, 2024, [Online]. Available: http://ijcs.stmikindonesia.ac.id/ijcs/index.php/ijcs/article/view/3135

[20] D. Appelbaum and R. A. Nehmer, "Auditing cloud-based blockchain accounting systems," *Journal of Information Systems*, vol. 34, no. 2, 2020, doi: 10.2308/isys-52660.

[21] E. Guustaaf, U. Rahardja, Q. Aini, N. A. Santoso, and N. P. L. Santoso, "Desain Kerangka Blockchain terhadap pendidikan: A Survey," *CESS (Journal of Computer Engineering, System and Science)*, vol. 6, no. 2, p. 236, 2021, doi: 10.24114/cess.v6i2.25099.

[22] J. M. Kapadia, "Blockchain Technology: Application in the Financial Industry," *Scholedge International Journal of Management & Development ISSN 2394-3378*, vol. 7, no. 8, 2021, doi: 10.19085/sijmd070801.

[23] M.Fahmideh, B. Abedin, and J.Shen, "Towards an integrated framework for developing blockchain systems," *Polym Test*, p. 106972, 2023, doi: 10.1016/j.dss.2024.114181.