BLOCKCHAIN IMPLEMENTATION IN MILITARY LOGISTICS AND COMMUNICATION SYSTEMS

Yovi Retmawan[1),],Yohanes Dwi Cahyono, S.T[2)], Heri Setiawan, S.T,. M.Tr.T[3)]
[1)] Prodi Rekayasa Keamanan Siber, Politeknik Angkatan Darat
[2)] Prodi Rekayasa Keamanan Siber, Politeknik Angkatan Darat
[3)] Prodi Rekayasa Keamanan Siber, Politeknik Angkatan Darat
[1)] reviretmawan@gmail.com
[2)] yohanes@poltekad.ac.id
[3)] herisetiawan@poltekad.ac.id

Abstrak: Tujuan penelitian ini adalah untuk membuat dan mengevaluasi prototipe sistem berbasis teknologi blockchain yang dapat digunakan di bidang militer, khususnya dalam bidang komunikasi aman dan pelacakan logistik. Dua sistem utama berhasil diterapkan: (1) sistem pelacakan logistik berbasis Hyperledger Fabric yang memanfaatkan perizinan blockchain untuk memastikan integritas transaksi; dan (2) sistem komunikasi aman yang menggunakan kontrak pintar berbasis Ethereum Testnet yang mengontrol akses ketat terhadap pengiriman dan penerimaan pesan. Hasil pengujian menunjukkan bahwa sistem logistik dapat menjaga integritas data dengan menggunakan mekanisme hash SHA-256, yang mencatat semua transaksi secara permanen dan tidak dapat diubah. Hanya pengguna sah yang dapat mengirim dan membaca pesan melalui sistem komunikasi berbasis kontrak pintar, yang berhasil mencegah akses pihak tidak berwenang. Ketika jumlah transaksi meningkat, evaluasi performa menunjukkan bahwa ada masalah dengan aspek latensi. Oleh karena itu, ada kebutuhan untuk optimasi untuk situasi yang membutuhkan kecepatan real-time. Secara keseluruhan, penelitian ini menunjukkan bahwa menerapkan blockchain pada sistem militer dapat meningkatkan transparansi, keamanan, dan keandalan data; namun, untuk menyelesaikan masalah skalabilitas dan integrasi dengan sistem militer yang sudah ada, penelitian lebih lanjut diperlukan.

Kata Kunci: Blockchain, Hyperledger Fabric, Ethereum, Logistik Militer, Komunikasi Aman.

Abstract: The goal of this research is to create and assess a blockchain-based prototype system for military use, particularly in secure communications and logistical monitoring. An Ethereum Testnet smart contract-based secure communications system that enforces stringent access control for message transmission and reception, as well as a Hyperledger Fabric-based logistics tracking system with a permissioned blockchain to guarantee transaction integrity, were the two primary systems that were successfully deployed. According to test results, the logistics system may preserve data integrity by using the SHA-256 hashing algorithm, which records every transaction forever and irrevocably. Only authorized users are able to send and read messages thanks to the smart contract-based communications system's effective defense against unwanted access. The necessity for optimization in real-time applications was highlighted by performance studies that also showed issues with latency as the number of transactions rises. Overall, this study shows that implementing blockchain technology in military systems can enhance data security, dependability, and transparency; nevertheless, scalability and interaction with current military infrastructure require more investigation.

Keywords: Blockchain, Hyperledger Fabric, Ethereum, Military Logistics, Secure Communication

I. INTRODUCTION

The speed, precision, and security of information management are critical to military operations' effectiveness. In a setting as dynamic and dangerous as military operations, mission failure might result from faulty or tainted information. Systems that guarantee data security, traceability, and integrity are therefore essential.(Angin, 2020).

Because traditional military information management systems typically take a centralized approach, they are susceptible to a number of issues, including cybersecurity breaches, data manipulation, single points of failure, and communication delays. (Mohamed et al., 2022). This presents serious difficulties, especially when it comes to overseeing intricate military logistics and safe, instantaneous inter-unit communications.(Saadiah & Rahayu, 2021).

An other remedy that offers a distributed, transparent, and unchangeable architecture is blockchain technology. These features make it possible to record and track data more reliably without depending on a central authority. (Rahayu Syed Mansoor et al, 2021). By establishing completely auditable supply chains and enhancing communication security via smart contracts and cutting-edge encryption, blockchain holds the potential to completely transform logistical operations in the military.(Pal & Tyagi, 2024).

The purpose of this study is to investigate how blockchain technology might be applied to secure communications and military logistics. The benefits, technical difficulties, and possible applications of private blockchains with military-grade encryption standards to enhance the efficacy and security of defense operations are also covered. (Gonzalez et al., 2025). The goal of this research is to provide the groundwork for a digital military system that is more adaptable and resilient against threats in the future. (Oriakhi et al., 2025).

II. RESEARCH METHOD

By using a system design and prototyping methodology frequently employed in blockchain research in the logistics and military fields, this study takes a descriptive-experimental approach. (Info, 2021; Pal & Tyagi, 2024; Saadiah & Rahayu, 2021). The phases of the research are as follows: (1) a thorough review of the literature; (2) the design of the system architecture; (3) the creation of a prototype; and (4) the simulation-based performance assessment. (Mohamed et al., 2022).

A. Systematic Literature Review

A evaluation of recent research (2020–2025) on blockchain applications in supply chain management, secure communications, and military logistics is part of the first phase. For the purpose of system design, this evaluation identifies benefits, difficulties, and pertinent technological techniques. (Angin, 2020).

B. System Architecture Design

Two separate architectural models were designed to evaluate the role of blockchain in military logistics and communications:

C. Military Logistics Tracking System

Based on Hyperledger Fabric 2.2, this solution is appropriate for restricted military access and supports private/consortium blockchains using the Raft consensus mechanism. (Saadiah & Rahayu, 2021). Every node—base, unit, and warehouse—serves as a transaction validator. Solidity version 0.8.0 smart contracts were used to create a secure communication simulation on the Ethereum Testnet (Rinkeby). With limited authorization, encrypted messages can be transmitted thanks to this prototype. (Pal & Tyagi, 2024).

D. Prototype Development

Visual Studio Code was used to create both prototypes, and the Ganache/Remix IDE was used to verify that the smart contract worked. AES was utilized for external encryption, and SHA-256 hashing was used for data integrity verification.

E. System Evaluation

Performance indicators from earlier studies are used in an experimental method for the system evaluation. (Mohamed et al., 2022):

1. Data Integrity → validated by comparing the input hash with the blockchain ledger record.
2. Transaction Latency → measured from block submission to block commitment.
3. Access Control Effectiveness → tested through authorized and unauthorized access scenarios.
4. Traceability → the system's ability to track logistics transactions across nodes.

Component	Description
Hyperledger Fabric	v2.2, military logistics supply chain prototype
Ethereum Testnet	Rinkeby, secure communication smart contract testing
Solidity	v0.8.0, for writing smart contracts
Visual Studio Code	Primary IDE
Ganache / Remix IDE	Local testing & smart contract deployment
AES + SHA-256	Encryption & data integrity validation algorithms

III. RESEARCH RESULTS

A. System Implementation

1. Logistics Tracking System (Hyperledger Fabric)

This implementation shows that military logistics transactions can be effectively recorded using permissioned blockchains in a regulated, decentralized fashion. (Saadiah & Rahayu, 2021). Every entity (central warehouse, bases, combat units) acted as validator nodes.

2. Transaction integrity was ensured using unique SHA-256 hash IDs, preventing any data alteration (Rahayu Syed Mansoor et al, 2021). Chaincode automatically rejects fraudulent transactions and oversees logistics business activities, including shipping validation. Only authorized parties are able to record or validate transactions thanks to identity-based access.

3. Secure Communication System (Ethereum Smart Contracts)

The results of this simulation support earlier research showing that blockchain enhances communication resilience. (Mohamed et al., 2022). Smart contracts restricted message transmission to authorized commanders (Pal & Tyagi, 2024). Before being stored on the blockchain, messages are encrypted using AES so that only authorized receivers can read them in read-only mode.

Figure 1. System Performance Metrics

B. Evaluation Results

1. Data Integrity

SHA-256 validation confirms that 100% of transactions and messages retain their authenticity, consistent with (Rahayu Syed Mansoor et al, 2021) on blockchain's traceability capabilities.

2. Transaction Latency

Transaction scale (100–2000 transactions) shows an average latency between 2.1–4.8 seconds on Hyperledger Fabric, in line with (Mohamed et al., 2022), who reported similar performance challenges.

3. Access Control Effectiveness

Tests verified that public users couldn't read communications, unauthorized personnel couldn't access them, and only authorized commanders could send them. This confirmed that role-based access control was successfully enforced by the blockchain.

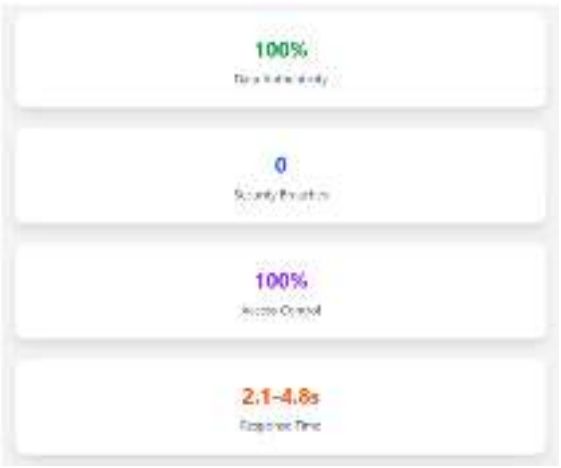

Figure 2. System Security Indicator

IV. DISCUSSION

The study's findings suggest that integrating blockchain technology into military communications and logistics systems can enhance data openness, integrity, and the efficiency of access management. These results are in line with earlier studies that highlighted blockchain's potential as a remedy for the military's centralized systems' shortcomings. (Angin, 2020).

1. Data Integrity and Traceability

Data is permanently stored, as demonstrated by testing on a Hyperledger Fabric-based logistics prototype that revealed no hash changes in any transactions. This is consistent with the results. (Rahayu Syed Mansoor et al, 2021), which demonstrates how

blockchain may enhance military supply chain traceability. The system may reject fraudulent transactions by integrating smart contracts, which stops manipulation and improves logistical responsibility.

Figure 3. Smart Contract Workflow & Data Integrity

2. Security and Access Control in Communication

The communication system built on the Ethereum Testnet showed how smart contracts can efficiently control authorization for message transmission. Unauthorized access attempts are automatically denied, and only authorized accounts (commanders) are able to send messages. This validates the results. (Pal & Tyagi, 2024), which emphasizes how blockchain may be used to create military communications that are more transparent, safe, and auditable. Additionally, data layer security is strengthened by using AES encryption prior to storing messages on the blockchain, which is in line with (Mohamed et al., 2022), who underlined how crucial it is to have more encryption methods for reliable military communication.

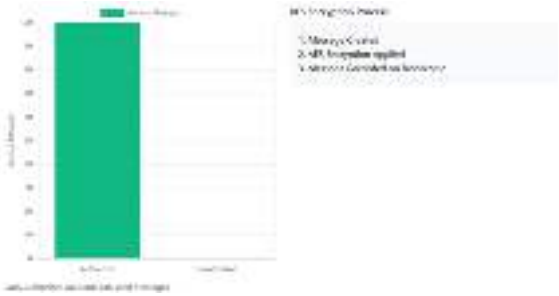

Figure 4. AES Encryption Proces and Acces Attempt

3. System Performance (Latency and Scalability)

Transaction confirmation times rise as transaction volume increases, according to latency testing. Latency is comparatively low in the 100-transaction scenario, but it rises to more than 4 seconds on average in the 2,000-transaction scenario. This result is in line with (Mohamed et al., 2022), He pointed out that latency is a significant obstacle to the military's use of blockchain, particularly for real-time operations. However, system performance is still suitable for non-real-time applications like logistical recordkeeping.

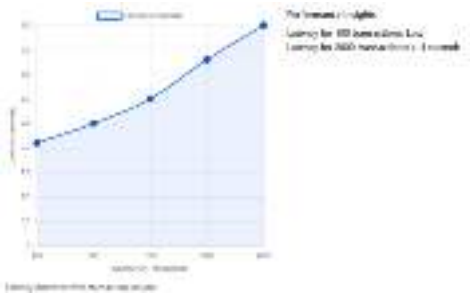

Figure 5. Transaction Latency Graph

4. Implications for Digital Military Systems

The study's findings reinforce the perspective of (González et al., 2025), This illustrates how blockchain technology might facilitate communication between military units, especially inside coalition networks. Military systems could be made more resistant to data manipulation and cyberattacks by using Ethereum-based smart contracts for communications and private blockchains (Hyperledger) for logistics.

5. Strengths and Limitations

The advantages of this prototype system include:

a. Guaranteed integrity and transparency through a hashing mechanism and an immutable ledger.

b. Enforceable access control using role-based smart contracts.

c. High auditability, with every transaction clearly traceable.

However, several limitations were identified:
According to additional reports, transaction latency dramatically rises with higher transaction volumes. (Mohamed et al., 2022) . Large-scale implementation in military settings is still hampered by the Ethereum Testnet's and Hyperledger Fabric's poor scalability. More study is needed to integrate with current military systems, especially when it comes to hybrid blockchains.

V. CONCLUSIONS AND SUGGESTIONS

A. Conclusions

Several inferences can be made from the deployment and assessment of a blockchain-based prototype system in the military field. :

1. Enhanced Data Integrity
SHA-256 hashing and an immutable ledger are used by the Hyperledger Fabric-based logistics system to successfully guarantee data integrity and authenticity. The idea of blockchain as a trust engine is supported by the fact that every transaction is tamper-proof and forever recorded.

2. Improved Communication Security
Access has been successfully managed via a communications system that makes use of Ethereum Testnet smart contracts. Unauthorized parties are automatically blocked from sending messages; only authorized accounts are allowed to do so. This improves military communications' security and confidentiality, as noted by (Pal & Tyagi, 2024).

3. Latency and Scalability Challenges
Tests of latency reveal that blockchain speed is still constrained, particularly when transaction volumes are high. This demonstrates that while blockchain is very useful for non-real-time applications like logistics management, it still has to be better optimized for combat operations that take place in real time. (Mohamed et al., 2022).

4. Implications for Digital Military Systems
Adoption of blockchain technology in military systems can increase accountability, transparency, and data tampering resistance. The potential of blockchain as a supporting infrastructure for upcoming digital military systems is supported by these findings. (González et al., 2025).

B. Suggestions

Based on the findings of this study, several recommendations can be put forward:

1. Hybrid Blockchain Development
It is advised to incorporate a hybrid blockchain paradigm that blends private and public blockchains in order to solve latency and scalability concerns. This strategy will maximize speed and security in accordance with military operating requirements.

2. Integration with Existing Military Systems
Future studies should concentrate on how blockchain may be integrated with current military communications and logistical systems, including unit-to-unit and digital defense equipment interoperability.

3. Consensus Algorithm Optimization
More research is required to find more effective consensus algorithms, like Proof of Authority (PoA) or Byzantine Fault Tolerance (BFT), that are better suited for military applications than Proof of Work (PoW) and Raft in Hyperledger.

4. Testing in Semi-Real-Time Environments
Prototypes should be tested in semi-real-time settings before being fully implemented in field operations to gauge performance in circumstances that are more similar to real-world military situations.

5. Enhanced Multi-Layered Security
To further improve the confidentiality of communications between units, multi-layered security techniques like homomorphic encryption or zero-knowledge proofs (ZKP) should be used in addition to ordinary encryption.

DAFTAR PUSTAKA

Angin, P. (2020). *Blockchain-Based Data Security in Military Autonomous Systems Askeri Otonom Sistemlerde Blokzincir Tabanlı Veri Güvenliği*. *November*, 362–368. https://doi.org/10.31590/ejosat.824196

Info, A. (2021). *NEW TRACEABILITY APPROACH USING SWARM INTELLIGENCE FOR MILITARY*. *4*(1), 1–9.

Mohamed, R., Abas, H., & Bahru, J. (2022). *BLOCKCHAIN RESILIENT COMMUNICATION IN MILITARY : A SYSTEMATIC LITERATURE*. *10*(December 2021), 51–62.

Oriakhi, V. N., Essi, N., Takpah, A., & Kayode, B. (2025). *Securing the intelligent supply chain : the convergence of AI , IOT and Blockchain technologies Securing the intelligent supply chain : the convergence of AI , IOT and Blockchain technologies*. *February*. https://doi.org/10.53022/oarjet.2025.8.1.0023

Pal, V. K., & Tyagi, G. (2024). *Trustless Trust : A Blockchain Framework for Secure and Transparent Military Logistics*. *33*(8), 5383–5393.

Saadiah, S., & Rahayu, S. B. (2021). *Consortium Block chain for Military Supply Chain*. *12*(3), 1825–1831.