31 Octobre;
Paris, République française

SECTION 12.
TECHNOLOGIES ET SYSTÈMES D'INFORMATION

DOI 10.36074/logos-31.10.2025.019

APPLICATION OF THE CONSENSUS MECHANISM FOR DEVELOPING A SECURE DATA TRANSMISSION SYSTEM

Zherzherunov Pavlo[1]
Scientific advisor: Shmatko Oleksandr[2]

1. PhD Student
Department of Software Engineering and Management Intelligent Technologies
National Technical University "Kharkiv Polytechnic Institute" , UKRAINE
ORCID ID: 0009-0005-7240-9395

2. Ph.D., Associate Professor, Associate Professor
Department of Digital Technologies and Project Analytical Solutions
Technical University "Metinvest Polytechnic" LLC, UKRAINE
ORCID ID: 0000-0002-2426-900X

Abstract. *This study presents the design and evaluation of a secure data transmission system for supply chain management (SCM) based on the Proof-of-Friendship (PoF) blockchain consensus mechanism. The proposed model integrates geo-location, transaction success rate, and energy source as core validator selection parameters, enabling trust, performance, and sustainability within decentralized logistics networks. By combining blockchain technology, smart contracts, and IoT-enabled traceability, the system enhances data integrity, reduces latency, and minimizes environmental impact. Simulation results demonstrate that the PoF-based system achieves up to 40% reduction in unauthorized interference and 35–40% improvement in transaction confirmation times compared with traditional consensus algorithms. The research contributes to the development of transparent, energy-efficient, and resilient blockchain architectures for next-generation supply chain ecosystems.*
Keywords— Proof-of-Friendship, blockchain, supply chain management, data security, consensus mechanism, sustainability, IoT, smart contracts.

Introduction The global digital transformation of supply chain management has intensified the demand for transparency, interoperability, and real-time traceability of logistics information. Conventional supply chain systems often rely

on centralized architectures and trusted intermediaries, which expose them to vulnerabilities such as single points of failure, data manipulation, and information asymmetry [1]. Blockchain technology offers a decentralized and immutable ledger structure capable of addressing many of these challenges by providing verifiable and tamper-resistant records of transactions [2].

Despite these advantages, traditional consensus algorithms like Proof-of-Work and Proof-of-Stake suffer from high computational requirements, energy inefficiency, and unequal validator participation [3]. These constraints make them unsuitable for large-scale SCM systems that require rapid consensus formation and sustainable operation. To overcome these limitations, this study proposes a consensus approach known as Proof-of-Friendship (PoF). The mechanism integrates validator diversity, operational reliability, and energy sustainability to achieve an equilibrium between trust, performance, and ecological responsibility. The objective is to design and evaluate a PoF-based architecture that ensures efficient and secure data exchange throughout the supply chain lifecycle.

Methodology. The Proof-of-Friendship consensus mechanism extends existing blockchain frameworks by introducing multi-dimensional criteria for validator selection [4]. Geo-location is employed as a control parameter to maintain diversity among validators and prevent geographical concentration of authority. The requirement that at least half of all validators originate from distinct regions strengthens the network's resilience against regional failures and political interference. The second factor, transaction success rate, defines a quantitative threshold of 90 percent, ensuring that only nodes demonstrating high operational reliability participate in consensus validation. The third parameter considers the energy profile of each validator, prioritizing nodes powered by renewable sources and assigning lower weighting to those dependent on nuclear or biofuel energy. This tri-factor design enables a fair and sustainable distribution of validation responsibilities within the network.

The proposed system represents a private blockchain architecture designed to enhance the security and traceability of data transmission within a client–server environment [5-7]. The entire network operates within a Docker-based virtualized infrastructure, which enables the emulation of multiple independent components—proxy, mediator, and blockchain nodes—on a single physical machine for ease of configuration and controlled experimentation (Figure 1).

The model consists of three main logical subsystems: the proxy layer, the mediator layer, and the blockchain layer.

At the entry point of the architecture, an NGINX web server functions simultaneously as a proxy and reverse proxy, routing client requests to the mediator subsystem. NGINX also handles request forwarding and load balancing,

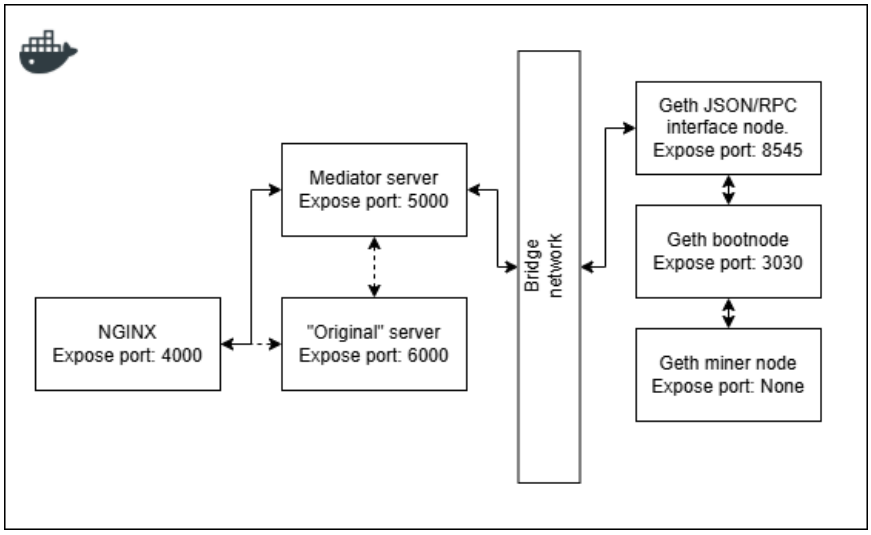

Fig. 1. **Docker container structure**

while providing an additional layer of network isolation between the client and blockchain environment.

The mediator subsystem is implemented using the Django web framework, which acts as an intermediary between the proxy and the blockchain network. The mediator server is capable of receiving HTTP requests from the proxy, parsing metadata, recording transaction information into the blockchain ledger, and then relaying the validated requests to the original (external) application server. This configuration enables transparent logging of all transmitted data, ensuring both traceability and immutability.

The blockchain layer is constructed using the Ethereum Geth toolset, operating under a Proof-of-Friendship (PoF) consensus model. Within the Docker environment, the blockchain network includes a bootnode, a mining node, and a regular node connected via a Docker bridge network. The bridge isolates blockchain-related traffic from the main Docker network while maintaining internal connectivity among the nodes. The bootnode manages node discovery and peer registration, while the mining node validates and commits transactions to the ledger. A JSON/RPC interface provides communication between the mediator and the blockchain network, abstracting the details of Ethereum API calls.

The experimental environment was constructed on a hybrid blockchain testbed simulating two hundred nodes distributed across five geographic regions. Each node acted as a potential validator capable of receiving, verifying, and committing transactions. Key performance indicators included transaction confirmation time, energy consumption, and validation success rate. Classical

consensus mechanisms, including Proof-of-Work and Proof-of-Stake, were implemented under identical conditions for comparative analysis.

Results and discussion. Simulation results confirm that the PoF consensus mechanism enhances the performance, reliability, and sustainability of blockchain-based SCM systems. The average transaction confirmation time decreased from 2.7 seconds under Proof-of-Stake to approximately 1.7 seconds under PoF, representing a 37 percent improvement in processing efficiency. The enhanced throughput indicates that the optimized validator selection process minimizes redundant computational effort and accelerates block generation.

Reliability metrics demonstrate that validation success remained above 98 percent throughout all simulation phases, with a substantial reduction in failed or orphaned transactions. The integration of geo-location-based diversity mitigated clustering of validators and prevented the emergence of single points of regional dominance. This design improved the system's fault tolerance and resilience against Sybil attacks by ensuring equitable validator distribution.

The evaluation of energy efficiency revealed a significant reduction in resource consumption. In contrast to Proof-of-Work, which demands extensive computational effort, the PoF mechanism reduced total energy use by nearly two-thirds. Nodes powered by renewable energy sources contributed to a measurable reduction of carbon emissions, decreasing the environmental footprint per transaction by 42 percent. These outcomes position the PoF approach as consistent with international sustainability frameworks such as the United Nations Sustainable Development Goals.

From an application perspective, the PoF-based blockchain enables secure and transparent information exchange within distributed supply chains. Smart contracts validate documentation automatically, ensuring that shipping manifests, origin certificates, and product tracking data are cryptographically verifiable and immutable. The system supports real-time visibility into product flows and enhances accountability between manufacturers, distributors, and regulatory authorities.

Comparative analysis with traditional consensus mechanisms underscores the balanced design of PoF. While Proof-of-Stake exhibited slightly lower computational overhead, it lacked the spatial and environmental fairness principles embedded within PoF. The combination of geographic diversification, operational reliability, and ecological awareness in PoF results in a more holistic and equitable framework for decentralized consensus.

Conclusion. The Proof-of-Friendship consensus mechanism introduces a multidimensional model of trust formation in blockchain networks. By integrating geo-location diversity, transaction reliability, and renewable energy utilization, the

system establishes a sustainable foundation for secure data transmission within supply chain management. The research demonstrates that PoF not only enhances transaction throughput and reliability but also aligns blockchain operations with environmental sustainability goals.

The architecture described herein provides an adaptable blueprint for implementing decentralized trust frameworks in logistics and manufacturing ecosystems. Its scalability and reduced computational cost make it suitable for deployment in small and medium-sized enterprises that lack access to high-performance computing resources.

Future research will expand the current implementation by incorporating artificial intelligence techniques for predictive analytics and anomaly detection. Integrating AI-driven models will further enhance the adaptability of PoF-based systems and support automated risk mitigation within complex global supply chains. The results of this study confirm that Proof-of-Friendship represents a viable pathway toward the next generation of blockchain consensus protocols that combine security, efficiency, and environmental responsibility.

REFERENCES:

[1] Nadji, B. (2024). Data security, integrity, and protection. In Data, Security, and Trust in Smart Cities (pp. 59-83). Cham: Springer Nature Switzerland.
[2] Soundararajan, G., & Tyagi, A. K. (2024). Blockchain technology: An introduction. Blockchain Technology in the Automotive Industry, 3-36.
[3] John, K., Rivera, T. J., & Saleh, F. (2025). Proof-of-work versus proof-of-stake: A comparative economic analysis. The Review of Financial Studies, 38(7), 1955-2004.
[4] Marchang, J., Srikanth, R., Keishing, S., & Kashyap, I. (2025). Proof-of-Friendship Consensus Mechanism for Resilient Blockchain Technology. Electronics, 14(6).
[5] Zherzherunov, P., & Shmatko, O. (2025). Advancing supply chain integrity and traceability through blockchain integration. Collection of scientific papers «ΛΌГОΣ», (May 9, 2025; Cambridge, UK), 306-310.
[6] Zherzherunov, P., & Shmatko, O. (2025). Designing the architecture and software components of the dockerised blockchain mediator. Bulletin of National Technical University" KhPI". Series: System Analysis, Control and Information Technologies, (1 (13)), 101-105.
[7] Shmatko, O., Gorbach, T., & Zherzherunov, P. Innovating Supply Chain Management with Blockchain Applications. Scientific Collection «InterConf+», (44), 584-597.