ISSN 2311-4738 (print)
ISSN 2413-3000 (online)

УДК 004.75:004.056:658.7 DOI: 10.20998/2413-3000.2026.12.4

P. ZHERZHERUNOV, O. SHMATKO

DOCKERIZED BLOCKCHAIN ARCHITECTURE FOR SECURE SUPPLY CHAIN MANAGEMENT SYSTEMS

Modern supply chain management systems increasingly rely on distributed architectures to ensure transparency, integrity, and trust between participants. Blockchain technology provides a promising foundation for such systems; however, traditional consensus mechanisms introduce high computational overhead, energy inefficiency, and privacy risks. These limitations are particularly critical for small and medium-sized enterprises (SMEs) with constrained computational resources, that they are using to expand on their traditional informational systems and not to integrate distributed technologies into the work process, as setup process for blockchain tools is more complex than centralized approach. This paper proposes a private, dockerized blockchain architecture for supply chain management that combines the Proof of Friendship (PoF) consensus mechanism with Zero-Knowledge Proofs (ZKP). By integrating a private, dockerized framework with the Proof of Friendship consensus and Zero-Knowledge Proofs, this architecture enables resource-constrained enterprises to achieve a high-performance decentralized network that simultaneously ensures sub-second transaction validation through social trust metrics, robust protection of competitive business intelligence via cryptographic privacy, and seamless cross-platform deployment through containerization, ultimately overcoming the traditional trade-offs between system transparency, operational cost, and data confidentiality in global trade. PoF extends Proof of Stake by incorporating social trust indicators, including transaction success rate and geographic diversity of validators, enabling resource-efficient and decentralized consensus. ZKP mechanisms are integrated through an off-chain prover module, allowing transaction correctness to be verified without revealing sensitive business data. The proposed approach enhances cybersecurity, data confidentiality, and system scalability while reducing computational costs. Simulation results demonstrate improved resistance to Sybil attacks, reduced validator centralization, and acceptable transaction latency for corporate blockchain deployments.

Keywords: blockchain security, supply chain management, proof of friendship, zero-knowledge proofs, privacy-preserving systems, distributed information systems.

П. Ю. ЖЕРЖЕРУНОВ, О. В. ШМАТКО

ДОКЕРИЗОВАНА АРХІТЕКТУРА БЛОКЧЕЙНУ ДЛЯ БЕЗПЕЧНИХ СИСТЕМ УПРАВЛІННЯ ЛАНЦЮГАМИ ПОСТАЧАННЯ

Сучасні системи управління ланцюгами постачання дедалі частіше використовують розподілені архітектури для забезпечення прозорості, цілісності та довіри між учасниками. Технологія блокчейн створює перспективну основу для таких систем, однак традиційні механізми консенсусу характеризуються високими обчислювальними витратами, енергетичною неефективністю та ризиками для конфіденційності. Ці обмеження є особливо критичними для малих і середніх підприємств (МСП), які мають обмежені обчислювальні ресурси та використовують їх переважно для розширення своїх традиційних інформаційних систем, а не для інтеграції розподілених технологій у робочі процеси, оскільки налаштування інструментів блокчейну є складнішим порівняно з централізованим підходом. У роботі запропоновано приватну докеризовану архітектуру блокчейну для систем управління ланцюгами постачання, що поєднує механізм консенсусу Proof of Friendship (PoF) із використанням Zero-Knowledge Proofs (ZKP). Завдяки інтеграції приватного контейнеризованого середовища з механізмом консенсусу Proof of Friendship та криптографічними доказами з нульовим розголошенням запропонована архітектура дозволяє підприємствам з обмеженими ресурсами створювати високопродуктивну децентралізовану мережу. Така мережа забезпечує підтвердження транзакцій менш ніж за секунду на основі метрик соціальної довіри, надійний захист конфіденційної комерційної інформації за допомогою криптографічних методів, а також зручне розгортання на різних платформах завдяки контейнеризації. У результаті долаються традиційні компроміси між прозорістю системи, операційними витратами та конфіденційністю даних у глобальній торгівлі. Механізм PoF розширює підхід Proof of Stake, включаючи індикатори соціальної довіри, зокрема рівень успішності транзакцій та географічну різноманітність валідаторів, що забезпечує ресурсоефективний і децентралізований процес досягнення консенсусу. Механізми ZKP інтегруються через модуль доказу поза блокчейном (off-chain prover), що дозволяє перевіряти коректність транзакцій без розкриття конфіденційних бізнес-даних. Запропонований підхід підвищує рівень кібербезпеки, конфіденційності даних та масштабованості системи, одночасно зменшуючи обчислювальні витрати. Результати моделювання демонструють підвищену стійкість до атак типу Sybil, зменшення централізації валідаторів та прийнятну затримку транзакцій для корпоративних блокчейн-рішень.

Ключові слова: безпека блокчейну, управління ланцюгами постачання, proof of friendship, zero-knowledge proofs, системи зі збереженням конфіденційності, розподілені інформаційні системи.

Introduction. The increasing adoption of blockchain technologies in distributed management systems, including logistics platforms and Industry 4.0 environments, has intensified the fundamental tension between transparency requirements and the need to preserve the confidentiality of sensitive data. Core blockchain properties such as immutability, traceability, and public verifiability enhance trust among stakeholders, yet simultaneously complicate compliance with data protection regulations and the safeguarding of commercial secrets [1] - [6]. To address this dilemma, contemporary research increasingly promotes the concept of “privacy by design,” whereby cryptographic primitives such as zero-knowledge proofs, secure multi-party computation, and homomorphic encryption are embedded directly into consensus protocols and smart contract execution layers [1]–[3].

Related Work. Comparative studies of cryptographic privacy-preserving techniques indicate that the integration of zero-knowledge proofs, multi-party computation, and homomorphic encryption with public verification mechanisms enables a new class of verifiable privacy-preserving computing architectures [1], [3]. These approaches either relocate computation to off-chain environments with on-chain verifiability through succinct

proofs, distribute sensitive data among multiple parties to prevent unilateral disclosure, or allow computations to be performed directly over encrypted data. Empirical evaluations of lightweight homomorphic encryption schemes, such as Paillier-based constructions, demonstrate acceptable computational overhead and robustness against replay and forgery attacks, rendering them suitable for industrial and logistics scenarios characterized by high event frequency and stringent reliability requirements [2], [3].

From a systems perspective, the literature emphasizes that privacy in distributed management systems is achieved through layered architectural patterns combining identity and consent management, data channel separation, privacy-preserving computation, and regulatory compliance mechanisms [1], [5]. Self-sovereign identity models and consent-aware access control frameworks enable fine-grained governance of participant rights, while channelized ledgers and context-specific sub-registries reduce unnecessary data exposure. To ensure compatibility with regulatory regimes such as the GDPR, redactable and editable distributed ledger technologies have been proposed, notably through initiatives such as the NIST Data Block Matrix for Hyperledger Fabric, which reconcile integrity guarantees with controlled data modification or removal—an essential requirement for industrial systems with evolving access policies [6], [5].

Evidence from high-load domains, particularly healthcare and Internet of Medical Things systems, further illustrates the feasibility of scalable, privacy-preserving blockchain architectures employing hybrid cryptographic schemes, lightweight authorization proofs, and energy-efficient consensus protocols [7]. These solutions achieve substantial reductions in latency and energy consumption without compromising confidentiality, offering transferable insights for distributed management systems. Specifically, the use of multi-channel ledgers, private smart contracts, and cryptographic access proofs enables the separation of production, supply, and project management data flows while preserving auditability without exposing primary data [1]-[7].

In the context of collective decision-making and knowledge management, blockchain-supported federated learning has emerged as a viable paradigm for reconciling local data privacy with global model consistency and incentive-compatible collaboration [4]. Such architectures are applicable to management systems tasked with demand forecasting, route optimization, and real-time quality control, while consent-centric and self-sovereign identity frameworks further strengthen governance over data subject rights in multi-stakeholder environments [5], [4].

Ukrainian research in logistics and project management provides domain-specific problem formulations that align closely with privacy-oriented blockchain architectures in distributed management systems. Studies on proactive logistics project management emphasize early risk detection and transparent communication, which are compatible with immutable event logs and zero-knowledge-based auditing mechanisms that avoid disclosure of commercially sensitive information [8]. Strategic supply chain modeling under information asymmetry highlights the need for controlled data sharing, where permissioned blockchains combined with consent policies and self-sovereign identity mechanisms can reduce information leakage while maintaining access to critical performance indicators [9]. Multi-level planning of production and concrete supply chains underscores the importance of vertical and horizontal integration, for which channelized ledgers and redactable distributed ledgers enable differentiated access across operational units, contractors, and executive management without undermining audit trails [10].

Despite significant progress, several challenges remain unresolved, including the operational costs of zero-knowledge proofs, multi-party computation, and fully homomorphic encryption in high-frequency transactional environments, the reconciliation of cryptographic immutability with the right to erasure, and the long-term post-quantum resilience of distributed management infrastructures [2], [6], [7]. Current research points toward hybrid architectures that combine trusted execution environments with cryptographic proofs or integrate homomorphic encryption with granular access-controlled channels, as well as incentive mechanisms that promote correct behavior of agents in project-oriented and logistics networks [1], [4].

This paper aims to develop and evaluate a private, dockerized blockchain architecture for supply chain management that integrates the Proof of Friendship consensus mechanism with zero-knowledge proofs in order to enhance cybersecurity, data confidentiality, and consensus efficiency while addressing the requirements of small and medium-sized enterprises.

Proposed model. The proposed model builds upon recent advances in distributed management systems and supply chain platforms, where blockchain technologies are increasingly adopted to ensure data integrity, transparency, and confidentiality. Prior studies emphasize the importance of integrating blockchain into supply chain management systems in order to enhance trust among participants and mitigate the risks of unauthorized data access [11] - [15]. At the architectural level, modularity and scalability are identified as key requirements that enable adaptation to diverse business scenarios and operational constraints, particularly in multi-stakeholder environments [11].

In the proposed model, these principles are realized through a private, dockerized blockchain architecture designed for supply chain management systems. The model adopts a modular structure in which blockchain functionality is decoupled from application logic, enabling flexible deployment and independent scaling of system components. This approach is consistent with existing research on secure data transmission systems, where consensus mechanisms play a central role in maintaining consistency and reliability of shared information across distributed participants [12]. Unlike traditional

architectures, the proposed model explicitly targets the requirements of small and medium-sized enterprises by minimizing infrastructure complexity and computational overhead.

A key element of the proposed model is the use of a containerized blockchain mediator, which acts as an intermediary between client applications and the underlying blockchain network. Prior work on dockerized blockchain mediators demonstrates that containerization significantly improves deployment speed, configurability, and maintainability of blockchain-based systems [13]. In the proposed architecture, containerization enables logical isolation of functional components and supports rapid integration into existing enterprise infrastructures, thereby reducing operational costs and lowering entry barriers for SMEs [15].

The model further incorporates blockchain-based mechanisms for ensuring traceability and integrity of supply chain processes, which are critical in geographically distributed and globally interconnected logistics networks [14]. By recording verification results and cryptographic commitments rather than raw transactional data, the architecture supports auditability while preserving confidentiality. This design choice aligns with the broader trend identified in the literature toward combining blockchain technologies with modern containerization and orchestration approaches to achieve scalable, flexible, and privacy-aware distributed management systems [1] - [5].

Overall, the proposed model synthesizes architectural concepts from prior studies into a unified dockerized blockchain framework that addresses security, scalability, and confidentiality requirements of contemporary supply chain management systems. By leveraging modular design principles, containerized deployment, and blockchain-based trust mechanisms, the model provides a practical foundation for secure and efficient integration of blockchain technologies in SME-oriented distributed management environments.

Mathematical Model and Proof of Friendship Consensus Mechanism. The distributed blockchain-based supply chain management system is modeled as a set of network nodes:

$$V = \{v_1, v_2, \dots, v_n\} \quad (1)$$

where each node v_i represents a potential validator capable of participating in transaction validation and block formation.

Interactions among validators are governed by trust relationships established through prior cooperation history, operational stability, and organizational links between supply chain participants. These relationships are represented by a trust graph:

$$G = (V, E), E \subseteq V \times V \quad (2)$$

where E denotes the set of verified trust connections between validators.

For each validator, a set of quantitative trust-related attributes is defined, forming a trust attribute vector:

$$A_i = (S_i, G_i, E_i), S_i \in [0,1] \quad (3)$$

This vector characterizes the reliability and contribution of the validator to the network. The transaction success coefficient $S_i$is defined as the ratio between the number of correctly validated transactions and the total number of validation attempts:

$$S_i = \frac{T_i^{valid}}{T_i^{total}} \quad (4)$$

where T_i^{valid} denotes the number of correctly validated transactions;

T_i^{total} is the total number of validation attempts performed by validator v_i during the considered simulation interval.

The geographic diversification coefficient G_i reflects the spatial distribution of validators and is introduced to mitigate regional concentration of validation power. In the experimental evaluation, G_i was modeled as a normalized coefficient derived from the validator's region membership, with values assigned in the range $[0, 1]$. Specifically, validators belonging to underrepresented regions were assigned higher G_i values, while validators from regions with higher representation were assigned lower G_i values. This formulation ensures that geographic diversity influences committee composition while preserving the simplicity of the SME-oriented simulation setup.

An optional energy efficiency coefficient $E_i \in [0,1]$ may be used to represent the utilization of renewable energy sources. However, for corporate and private dockerized deployments this component is typically difficult to measure reliably and does not directly affect the core security properties of a permissioned SME-oriented blockchain network. Therefore, in the experimental evaluation presented in this paper, a simplified Trust Factor model was applied in which E_i was omitted.

To quantitatively assess validator reliability, an integrated trust metric referred to as the Trust Factor is introduced in the general form:

$$\mathrm{TF_i} = \alpha \mathrm{S_i} + \beta \mathrm{G_i} + \gamma \mathrm{E_i}, \qquad \alpha, \beta, \gamma \geq 0 \quad (5)$$

where the weighting coefficients satisfy the constraint:

$$\alpha + \beta + \gamma = 1 \quad (6)$$

In the conducted experiments, the Trust Factor was computed using only the transaction success coefficient and the geographic diversification coefficient:

$$TF_i = \alpha S_i + \beta G_i, \alpha + \beta = 1 \quad (7)$$

The weighting coefficients were set to $\alpha = 0.7$and $\beta = 0.3$. This choice is justified by the fact that transaction correctness and validation reliability are primary security-critical factors in corporate blockchain deployments, while geographic diversification serves as an additional decentralization constraint aimed at reducing regional concentration and coordinated attack risks. The analysis of alternative weight configurations and sensitivity to parameter changes is considered a direction for future work.

The set of validators eligible for participation in a given consensus round is defined as:

$$V_\theta = \{v_i \in V \mid TF_i \geq \theta\} \quad (8)$$

From this set, a validator committee is formed to jointly validate a block. The probability of selecting a validator is proportional to its Trust Factor:

$$p_i = \frac{TF_i}{\sum_{v_j \in V_\theta} TF_j} \quad (9)$$

Committee formation follows a stochastic selection process without replacement, which reduces the risks of validator dominance and long-term centralization.

To further prevent regional monopolization, geographic diversification constraints are imposed. Each validator $v_i$is associated with a geographic region:

$$r(v_i) \in R \quad (10)$$

Let m denote the maximum allowed number of validators from the same region in a committee. Additionally, the number of distinct regions represented in the committee is defined as:

$$\rho(C_k) = \mid \{r(v_i) \mid v_i \in C_k\} \mid \quad (11)$$

and must satisfy the constraint:

$$\rho(C_k) \geq q \quad (13)$$

where q denotes the minimum required regional diversity.

The Proof of Friendship committee selection process can therefore be expressed as the following constrained optimization problem:

$$C_k = arg \max_{\substack{C \subseteq V_\theta \\ |C|=k}} \sum_{v_i \in C} TF_i \quad (14)$$

subject to the geographic concentration and diversity constraints defined above.

The proposed mathematical model formalizes Proof of Friendship as a multi-criteria, trust-aware, and geographically diversified consensus mechanism. By combining an integrated Trust Factor with committee-based validation and spatial constraints, the model improves resistance to Sybil and Eclipse attacks, reduces centralization risks, and ensures practical applicability for corporate blockchain-based supply chain management systems.

Results and Discussion. The experimental study aims to evaluate the effectiveness of the proposed Proof of Friendship (PoF) consensus mechanism with committee-based validation and geographic diversification of validators in the context of supply chain management systems. The experiments are designed to test three key hypotheses: (i) the use of the integrated Trust Factor reduces the risk of validator centralization; (ii) committee selection with geographic constraints increases resistance to coordinated attacks; (iii) stochastic validator selection does not cause a significant degradation in system performance.

A private blockchain network consisting of $n = 10$ validators was simulated, where each validator represents a typical small or medium enterprise node. All nodes were configured with a 3 GHz CPU, 16 GB RAM, and a 50 Mbps network connection. The committee size was fixed at $k = 5$. Geographic diversification constraints were defined as a maximum of $m = 2$ validators per region and a minimum of $q = 3$ distinct regions per committee (Table 1). The Trust Factor weights were set to $\alpha = 0.6$, $\beta = 0.4$, and $\gamma = 0$, in accordance with the proposed mathematical model. The optional energy efficiency coefficient E_i was excluded from the experimental evaluation, since it is not reliably measurable in private dockerized deployments and does not directly affect the considered security and decentralization properties in a permissioned network

Table 1 – Experimental Setup Parameters

Parameter	Value
Number of validators n	10
Committee size k	5
Max. validators per region m	2
Min. regions per committee q	3
CPU per node	3 GHz
RAM per node	16 GB
Network bandwidth	50 Mbps
Trust Factor model	$TF_i = \alpha S_i + \beta G_i$, E_i omitted

At the initial stage, Trust Factor values were computed for all validators based on their transaction success rate $S_i$and geographic diversification coefficient G_i. The results (Table 2) demonstrate a clear differentiation among validators, enabling effective ranking and selective participation in consensus. Validators with consistently high S_i values maintained priority positions during committee selection, while nodes with marginal Trust Factor values exhibited limited participation.

These results confirm that the Trust Factor model adaptively reflects validator behavior and supports dynamic prioritization based on reliability.

Table 2 – Trust Attributes (S_i, G_i) and Trust Factor Values (TF) in the Simulated PoF Network

Validator	Region	Si	Gi	TFi
V1	R1	0.95	1.0	0.97
V2	R1	0.92	0.8	0.88
V3	R2	0.98	1.0	0.99
V4	R2	0.90	0.8	0.86
V5	R3	0.96	1.0	0.98
V6	R3	0.89	0.8	0.85
V7	R4	0.94	1.0	0.96
V8	R4	0.88	0.8	0.85
V9	R5	0.91	1.0	0.95
V10	R5	0.87	0.8	0.83

The experimental results (Table 3) show that stochastic committee selection without replacement, combined with geographic constraints, consistently produces committees of size $k = 5$that satisfy all diversification requirements. In all experimental rounds, the constraints $\mid C_k \cap r \mid \leq m$and $\rho(C_k) \geq q$were met.

Table 3 – Example Committee Composition Across Consensus Rounds

Round	Selected Validators	Regions Represented
1	V1, V3, V5, V7, V9	R1, R2, R3, R4, R5
2	V1, V3, V5, V7, V2	R1, R2, R3, R4
3	V3, V5, V7, V9, V4	R2, R3, R4, R5
4	V1, V5, V7, V9, V6	R1, R3, R4, R5
Round	Selected Validators	Regions Represented
1	V1, V3, V5, V7, V9	R1, R2, R3, R4, R5
2	V1, V3, V5, V7, V2	R1, R2, R3, R4

No committee exhibited regional concentration, and each consensus round involved validators from at least three distinct regions, confirming the effectiveness of the proposed geographic diversification constraints.

A comparative analysis of scenarios with and without geographic constraints shows that removing diversification requirements significantly increases the probability of committee dominance by validators from a single region (Table 4). In contrast, the PoF-based model effectively prevents such concentration. Moreover, the combination of Trust Factor thresholds and geographic limits complicates Sybil attacks, as the creation of multiple fictitious nodes does not automatically increase trust metrics.

Table 4 – Example Committee Composition Across Consensus Rounds

Scenario	Max. validators from one region	Centralization risk
PoF with geo-constraints	≤ 2	Low
PoF without geo-constraints	4–5	Medium
Random selection	5	High

Performance measurements (Table 5) indicate that committee-based validation does not lead to significant increases in transaction confirmation latency compared to full-validator participation. Limiting the number of active validators reduces synchronization overhead and message exchange costs. The stochastic selection mechanism introduces negligible computational overhead and is therefore suitable for SME-oriented deployments.

Table 5 – Performance Comparison

Validation mode	Avg. latency (ms)	Message overhead	CPU load
Full participation	1850	High	High
PoF committee-based	1420	Medium	Medium
Random committee	1380	Medium	Medium

The experimental results confirm that the proposed Proof of Friendship mechanism achieves an effective balance between security, decentralization, and performance in blockchain-based supply chain management systems. The integrated Trust Factor enables dynamic selection of reliable validators, while committee-based validation with geographic diversification reduces centralization risks and improves resistance to coordinated attacks. At the same time, performance remains stable and computational overhead is kept at a level acceptable for small and medium-sized enterprises. These findings support the practical applicability of Proof of Friendship in corporate and inter-organizational blockchain solutions.

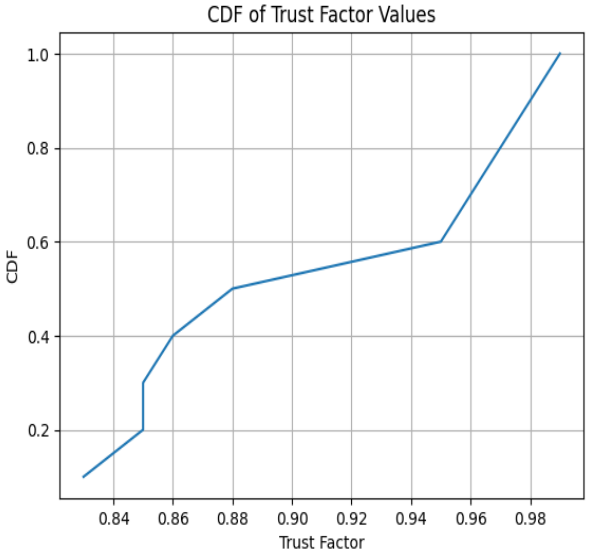

Fig. 1. Cumulative distribution function (CDF) of Trust Factor values for validators in the simulated Proof of Friendship network

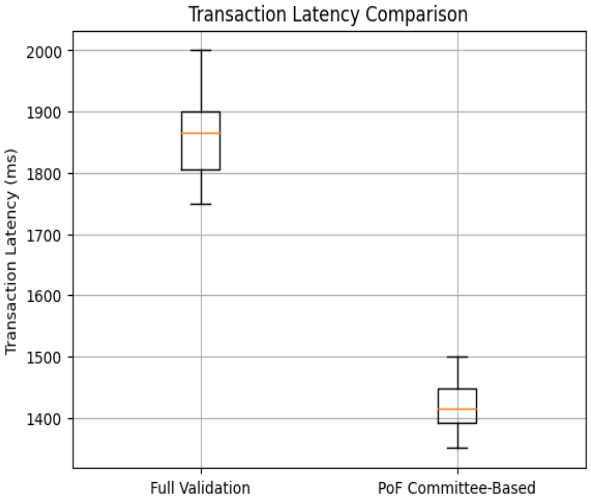

Fig. 2. Boxplot comparison of transaction latency for full validation and Proof of Friendship committee-based validation

The CDF of Trust Factor (Fig.1) values demonstrates a pronounced concentration of validators with high trust levels, indicating effective differentiation and prioritization within the proposed model. Furthermore, the latency boxplot (Fig.2) shows that committee-based validation under Proof of Friendship achieves lower median latency and reduced variability compared to full-validator participation, confirming that stochastic committee selection does not introduce significant performance degradation.

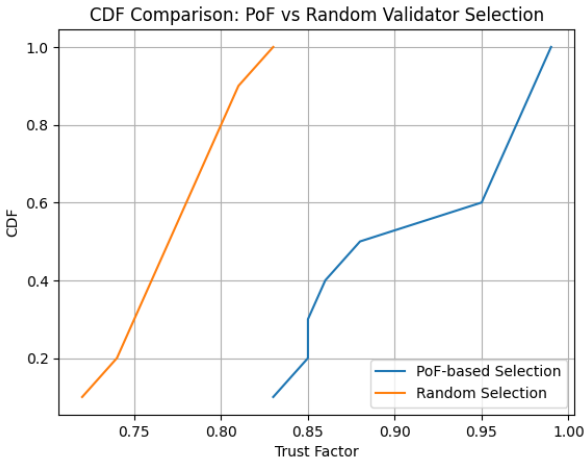

Fig. 3. Cumulative distribution function (CDF) comparison of Trust Factor values for Proof of Friendship–based and random validator selection

The CDF comparison between Proof of Friendship–based and random validator selection (Fig.3) highlights a pronounced shift toward higher Trust Factor values under PoF. While random selection results in a relatively uniform distribution concentrated at lower trust levels, PoF consistently prioritizes validators with higher reliability scores. This behavior confirms the effectiveness of the proposed trust-aware selection mechanism in reducing the participation of low-trust nodes and strengthening resistance to centralization and Sybil-style attacks.

Conclusion. This paper presented a privacy-preserving and resource-efficient blockchain architecture for supply chain management systems based on the integration of the Proof of Friendship consensus mechanism and zero-knowledge proof techniques. By extending traditional Proof of Stake with socially oriented trust metrics and geographic diversification constraints, the proposed approach addresses key limitations of existing blockchain solutions, including validator centralization, susceptibility to coordinated attacks, and excessive computational overhead.

A formal mathematical model was introduced to describe trust-aware validator selection as a constrained optimization problem, enabling transparent and reproducible committee formation. Experimental evaluation using simulation data demonstrated that the proposed mechanism effectively prioritizes high-trust validators, enforces geographic diversity, and significantly reduces centralization risks compared to random or unconstrained selection strategies. At the same time, committee-based validation under Proof of Friendship maintains stable transaction throughput and lower latency, confirming that stochastic trust-based selection does not degrade system performance.

The results indicate that the proposed dockerized blockchain architecture is well suited for small and medium-sized enterprises, offering a practical balance between security, decentralization, and efficiency. Future work will focus on large-scale deployment studies, formal security proofs against advanced adversarial models, and the integration of post-quantum cryptographic mechanisms to further enhance the long-term resilience of blockchain-based supply chain management system.

Список літератури

1. Valadares D. C. G., Perkusich A., Martins A. F., Alshawki M. B., Seline C. Privacy Preserving Blockchain Technologies. *Sensors*. 2023. Vol. 23, no. 16. 7172. doi: 10.3390/s23167172
2. Wang G., Li C., Dai B., Zhang S. Privacy Protection Method for Blockchain Transactions Based on Lightweight Homomorphic Encryption. *Information.* 2024. Vol. 15, no. 8. 438. doi: 10.3390/info15080438
3. Bontekoe T. H., Karastoyanova D., Turkmen F. Verifiable Privacy Preserving Computing. *arXiv.* 2023. URL: https://arxiv.org/pdf/2309.08248
4. Liu J., Chen C., Li Y., Sun L., Song Y., Zhou J., Jing B., Dou D. Enhancing trust and privacy in distributed networks: A comprehensive survey on blockchain based federated learning. *Knowledge and Information Systems.* 2024. Vol. 66. P. 4377–4403. doi: 10.1007/s10115-024-02117-3
5. Garcia R. D., Ramachandran G., Dunnett K., Jurdak R., Ranieri C. M., Krishnamachari B., Ueyama J. A Survey of Blockchain Based Privacy Applications: An Analysis of Consent Management and Self Sovereign Identity Approaches. *arXiv.* 2024. URL: https://arxiv.org/abs/2411.16404
6. Roberts J. D., DeFranco J. F., Kuhn D. R. Data Block Matrix and Hyperledger Implementation: Extending Distributed Ledger Technology for Privacy Requirements. *NIST preprint.* 2023. URL: https://csrc.nist.gov/projects/redactable-distributed-ledger
7. Hao L., Wang R., Wang X., Yue X., Tariq N., Sajid A. Post-quantum inspired scalable blockchain architecture for internet hospital systems with lightweight privacy preserving access control. *PLOS ONE.* 2025. Vol. 20, no. 12. e0332887. doi: 10.1371/journal.pone.0332887
8. Шадура Д., Меленчук В. Проактивне управління проєктами логістичних підприємств. *Вісник НТУ «ХПІ». Сер.: Стратегічне управління, портфель, програма та проєктний менеджмент.* 2023. № 1 (7). С. 93–99. doi: 10.20998/2413-3000.2023.7.12
9. Семенчук К. Моделювання стратегій ланцюгів постачань у проєктній діяльності. *Вісник НТУ «ХПІ». Сер.: Стратегічне управління, портфель, програма та проєктний менеджмент.* 2024. № 1 (8). С. 58–65. doi: 10.20998/2413-3000.2024.8.8
10. Бугаєвський М., Петренко Я. Багаторівневе планування й управління у розвитку виробництва та ланцюжках поставок бетону. *Вісник НТУ «ХПІ». Сер.: Стратегічне управління, портфель, програма та проєктний менеджмент.* 2025. № 1 (10). С. 10–17. doi: 10.20998/2413-3000.2025.10.2
11. Zherzherunov P., Shmatko O. Architectural approach to data protection in distributed supply chain management system using blockchain nodes. *Bulletin of National Technical University «KhPI». Ser.: System Analysis, Control and Information Technologies.* 2025. № 2 (14). P. 26–33.
12. Zherzherunov P., Shmatko O. Application of the consensus mechanism for developing a secure data transmission system. *Collection of Scientific Papers «ЛОГОС»*. Paris, France, 2025. P. 109–113. doi: 10.36074/logos-31.10.2025.019
13. Zherzherunov P., Shmatko O. Designing the architecture and software components of the dockerised blockchain mediator. *Bulletin of National Technical University «KhPI». Ser.: System Analysis, Control and Information Technologies.* 2025. № 1 (13). P. 101–105.
14. Zherzherunov P., Shmatko O. Advancing supply chain integrity and traceability through blockchain integration. *Collection of Scientific Papers «ЛОГОС».* Cambridge, UK, 2025. P. 306–310. doi: 10.36074/logos-09.05.2025.063
15. Zherzherunov P., Shmatko O. Enhancing supply chain integrity in SMEs through dockerized blockchain architecture. *Матеріали конференцій МЦНД.* Черкаси, Україна, 2025. С. 171–174. doi: 10.62731/mcnd-11.04.2025.006

References (transliterated)

1. Valadares D. C. G., Perkusich A., Martins A. F., Alshawki M. B., Seline C. Privacy Preserving Blockchain Technologies. *Sensors***.** 2023, vol. 23, no. 16, article 7172. doi: 10.3390/s23167172
2. Wang G., Li C., Dai B., Zhang S. Privacy Protection Method for Blockchain Transactions Based on Lightweight Homomorphic Encryption. *Information***.** 2024, vol. 15, no. 8, article 438. doi: 10.3390/info15080438
3. Bontekoe T. H., Karastoyanova D., Turkmen F. Verifiable Privacy Preserving Computing. *arXiv***.** 2023. Available at: https://arxiv.org/pdf/2309.08248 (accessed 03.05.2026).
4. Liu J., Chen C., Li Y., Sun L., Song Y., Zhou J., Jing B., Dou D. Enhancing trust and privacy in distributed networks: A comprehensive survey on blockchain based federated learning. *Knowledge and Information Systems***.** 2024, vol. 66, pp. 4377–4403. doi: 10.1007/s10115-024-02117-3
5. Garcia R. D., Ramachandran G., Dunnett K., Jurdak R., Ranieri C. M., Krishnamachari B., Ueyama J. A Survey of Blockchain Based Privacy Applications: An Analysis of Consent Management and Self Sovereign Identity Approaches. *arXiv***.** 2024. Available at: https://arxiv.org/abs/2411.16404 (accessed 03.05.2026).
6. Roberts J. D., DeFranco J. F., Kuhn D. R. Data Block Matrix and Hyperledger Implementation: Extending Distributed Ledger Technology for Privacy Requirements. *NIST preprint***.** 2023. Available at: https://csrc.nist.gov/projects/redactable-distributed-ledger (accessed 03.05.2026).
7. Hao L., Wang R., Wang X., Yue X., Tariq N., Sajid A. Post-quantum inspired scalable blockchain architecture for internet hospital systems with lightweight privacy preserving access control. *PLOS ONE***.** 2025, vol. 20, no. 12, article e0332887. doi: 10.1371/journal.pone.0332887
8. Shadura D., Melenchuk V. Proaktyvne upravlinnya proyektamy lohistychnykh pidpryyemstv [Proactive project management of logistics enterprises]. *Visnyk NTU "KhPI". Seriya: Stratehichne upravlinnya, portfel', prohrama ta proektnyy menedzhment* [Bulletin of NTU "KhPI". Series: Strategic Management, Portfolio, Program and Project Management]. 2023, no. 1 (7), pp. 93–99. doi: 10.20998/2413-3000.2023.7.12
9. Semenchuk K. Modelyuvannya stratehiy lantsyuhiv postachan' u proyektniy diyal'nosti [Modeling supply chain strategies in project activity]. *Visnyk NTU "KhPI". Seriya: Stratehichne upravlinnya, portfel', prohrama ta proektnyy menedzhment* [Bulletin of NTU "KhPI". Series: Strategic Management, Portfolio, Program and Project Management]. 2024, no. 1 (8), pp. 58–65. doi: 10.20998/2413-3000.2024.8.8
10. Buhayevs'kyy M., Petrenko Ya. Bahatorivne planuvannya y upravlinnya u rozvytku vyrobnytstva ta lantsyuzhkakh postavok betonu [Multilevel planning and management in the development of production and concrete supply chains]. *Visnyk NTU "KhPI". Seriya: Stratehichne upravlinnya, portfel', prohrama ta proektnyy menedzhment* [Bulletin of NTU "KhPI". Series: Strategic Management, Portfolio, Program and Project Management]. 2025, no. 1 (10), pp. 10–17. doi: 10.20998/2413-3000.2025.10.2
11. Zherzherunov P., Shmatko O. Architectural approach to data protection in distributed supply chain management system using blockchain nodes. *Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies*. 2025, no. 2 (14), pp. 26–33.
12,. Zherzherunov P., Shmatko O. Application of the consensus mechanism for developing a secure data transmission system. *Collection of Scientific Papers "ΛΟΓΟΣ"*. Paris, France, 2025, pp. 109–113. doi: 10.36074/logos-31.10.2025.019
13. Zherzherunov P., Shmatko O. Designing the architecture and software components of the dockerised blockchain mediator. *Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies*. 2025, no. 1 (13), pp. 101–105.
14. Zherzherunov P., Shmatko O. Advancing supply chain integrity and traceability through blockchain integration. *Collection of Scientific Papers "ΛΟΓΟΣ"*. Cambridge, UK, 2025, pp. 306–310. doi: 10.36074/logos-09.05.2025.063
15. Zherzherunov P., Shmatko O. Enhancing supply chain integrity in SMEs through dockerized blockchain architecture. *Materialy konferentsiy MTsND* [Proceedings of MCND Conferences]. Cherkasy, Ukraine, 2025, pp. 171–174. doi: 10.62731/mcnd-11.04.2025.006

Надійшла (received) 05.02.2026

Відомості про авторів / Сведения об авторах / About the Authors

Жержерунов Павло Юрійович (Zherzherunov Pavlo Yuriyovych) – аспірант, Національний технічний університет «Харківський політехнічний інститут», м. Харків, Україна, e-mail: Pavlo.Zherzherunov@cs.khpi.edu.ua; ORCID: https://orcid.org/0009-0005-7240-9395

Шматко Олександр Віталійович (Shmatko Oleksandr Vitaliyovych) – к.т.н., доцент, доцент кафедри програмної інженерії та інтелектуальних технологій управління, Національний технічний університет «Харківський політехнічний інститут», м. Харків, Україна, e-mail: oleksandr.shmatko@khpi.edu.ua, ORCID: https://orcid.org/0000-0002-2426-900X.