УДК 004.056:004.75

Баришев Ю.В.
Зарезенко Д. П.

ПРИВАТНІ ТА КОНСОРЦІУМНІ РОЗПОДІЛЕНІ СИСТЕМИ: АНАЛІЗ ЗАХИСТУ ДАНИХ

Вінницький національний технічний університет

Анотація

У роботі виконано аналіз сучасних приватних і консорціумних систем розподіленого реєстру з позиції реалізованих у них методів зберігання та захисту даних. Досліджено архітектурні особливості платформ R3 Corda, Quorum, Hyperledger Besu, MultiChain, IBM Blockchain (Hyperledger Fabric), Energy Web Chain та B3i. Проведено порівняння механізмів забезпечення конфіденційності, цілісності, автентифікації, а також моделей зберігання даних (on-chain та off-chain). Визначено ключові обмеження сучасних рішень, пов'язані з масштабованістю, актуалізацією криптографічних алгоритмів і гнучкістю керування доступом.

Ключові слова: розподілений реєстр, блокчейн, конфіденційність даних, цілісність, консенсус, криптографічний захист, розподілені інформаційні системи, масштабованість.

Abstract

The paper presents an analysis of modern private and consortium distributed ledger systems from the perspective of implemented data storage and protection mechanisms. Architectural features of R3 Corda, Quorum, Hyperledger Besu, MultiChain, IBM Blockchain (Hyperledger Fabric), Energy Web Chain, and B3i platforms are investigated. A comparative assessment of confidentiality, integrity, authentication mechanisms, as well as on-chain and off-chain storage models, is performed. Key limitations of current solutions related to scalability, cryptographic algorithm modernization, and flexible access control are identified.

Keywords: distributed ledger, blockchain, data confidentiality, integrity, consensus, cryptographic protection, distributed information systems, scalability.

Вступ

Цифровізація державного управління та корпоративних інформаційних систем зумовлює необхідність використання розподілених технологій зберігання даних. Розподілені реєстри (DLT) забезпечують цілісність і доступність інформації завдяки реплікації даних на множині вузлів мережі [1, 2]. Водночас їх впровадження для розв'язання прикладних задач актуалізує питання забезпечення конфіденційності, масштабованості та ефективності консенсусу [3].

Метою роботи є покращення безпеки розподілених інформаційних систем шляхом аналізу сучасних приватних і консорціумних блокчейн-платформ та визначення меж застосування реалізованих у них механізмів захисту даних.

Порівняльний аналіз архітектур і механізмів захисту в приватних DLT-системах

У роботі розглянуто такі системи: R3 Corda, Quorum, Hyperledger Besu, MultiChain, IBM Blockchain (Hyperledger Fabric), Energy Web Chain та B3i. Встановлено, що архітектурно вони реалізують різні моделі зберігання: глобальний ланцюг блоків, частковий реєстр або канал-орієнтована структура. Внаслідок порівняльного аналізу визначено низку ключових особливостей цих платформ:

- Платформа R3 Corda використовує модель часткового реєстру та механізм нотаріального підтвердження унікальності транзакцій, що дозволяє забезпечити високий рівень конфіденційності завдяки прямому P2P-обміну між сторонами угоди [4].

- Quorum та Hyperledger Besu реалізують модель приватних транзакцій із використанням зовнішніх менеджерів конфіденційності (Tessera), де відкрито зберігаються лише геші зашифрованих даних, а самі дані передаються off-chain [5].
- Hyperledger Fabric застосовує механізми каналів та приватних колекцій даних, що дозволяє ізолювати транзакції між визначеними групами учасників [6].
- MultiChain орієнтований на permissioned-модель із гнучким керуванням правами доступу, однак за замовчуванням всі вузли бачать усі дані, якщо не використовується прикладне шифрування [7].
- Energy Web Chain реалізує гібридну модель: публічний реєстр із обмеженим колом валідаторів і підтримкою приватних транзакцій із використанням зовнішнього сервісу керування ключами [8].

Визначено, що загальним недоліком цих систем є недостатня гнучкість впроваджених інструментів щодо захисту інформації, які потребують впровадження додаткових надбудов механізмів розмежування прав доступу [9], що поступаються вбудованим. Крім того, механізми, які в цих системах забезпечують захист цілісності даних, водночас зменшують гнучкість систем до внесення змін, які критичні у випадках зміни навантаження або появі нових загроз безпеці даних в цих розподілених системах.

Висновки

Порівняльний аналіз показав, що більшість платформ використовує криптографічні алгоритми ECDSA та геш-функції SHA-256 або Keccak-256. З урахуванням перспектив розвитку квантових обчислень ці алгоритми можуть втратити криптостійкість, що створює потребу у механізмах криптографічної агностичності та можливості гнучкого оновлення примітивів без зупинки мережі.

Також виявлено обмежену гнучкість у розмежуванні прав доступу та реконфігурації моделей зберігання даних. Більшість систем побудована на жорстко фіксованих архітектурних рішеннях (глобальному або частковому реєстрі), що ускладнює адаптацію до зростання навантаження та змін вимог безпеки.

Отримані результати дозволяють зробити висновок, що сучасні приватні та консорціумні розподілені системи забезпечують достатній рівень базового захисту даних для промислових застосувань, проте потребують подальшого розвитку в напрямках підвищення масштабованості, модернізації криптографічних механізмів і гнучкого керування доступом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Sun J., Yao X., Wand S., Wu Y. Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS. IEEE Access. 2020. Vol. 8. pp. 59389–59401. URL: https://doi.org/10.1109/access.2020.2982964 (accessed: 03.03.2026).
2. Semenzin, S., Rozas, D., & Hassan, S. Blockchain-based application at a governmental level: Disruption or illusion? The case of Estonia. Policy and Society, 41(3), 2022, P. 386–401. https://doi.org/10.1093/polsoc/puac014 (accessed: 03.03.2026)
3. Баришев Ю. В., Ланова В. С. Метод захищеного зберігання медичних даних на основі реляційної бази даних та блокчейну. Наукові праці ВНТУ. №3. 2023. 9 с. URL: https://praci.vntu.edu.ua/index.php/praci/article/view/701/662 (дата звернення: 06.02.2026)
4. Louvieris P., Ioannou G., White G. Making Tax Smart: Feasibility of Distributed Ledger Technology for Building Tax Compliance Functionality to Central Bank Digital Currency // Applied System Innovation. 2024. Vol. 7, No. 6. P. 1–37. URL: https://doi.org/10.3390/asi7060106 (дата звернення: 06.02.2026).
5. Wu Y., Wang H., Wang Y., et al. Blockchain for finance: A survey // IET Blockchain. – 2024. – Vol. 3, Iss. 1. – P. 1–28. – DOI: 10.1049/bkc2.12037. – URL: https://doi.org/10.1049/blc2.12067 (дата звернення: 06.02.2026).

6. Thakkar P., Nathan S., Viswanathan B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS). Milwaukee, WI, USA, 2018. P. 264–276. URL: https://doi.org/10.1109/MASCOTS.2018.00034 (дата звернення: 10.02.2026).
7. Mollah M. B., Zhao J., Niyato D., Lam K.-Y., Zhang X., Ghias A. M. Y. M., Koh L. H., Yang L. Blockchain for Future Smart Grid: A Comprehensive Survey. IEEE Internet of Things Journal. 2021. Vol. 8, no. 1. P. 18–43. URL: https://doi.org/10.1109/JIOT.2020.2993601 (дата звернення: 10.02.2026).
8. Gupta M., Giri S., Shanmugam P. K., Bhaskar M. S., Holm-Nielsen J. B., Padmanaban S. Adoption of Blockchain Platform for Security Enhancement in Energy Transaction. arXiv preprint arXiv:2305.19490. 2023. URL: https://www.alphaxiv.org/abs/2305.19490 (дата звернення: 10.02.2026).
9. Baryshev Y., Zarezenko D. Mandatory access control method application for smart contracts. International Scientific Technical Journal "Problems of Control and Informatics", 71(1), pp. 82–95. doi: 10.34229/1028-0979-2026-1-7 (дата звернення: 03.03.2026).

Баришев Юрій Володимирович — канд. техн. наук, доцент кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yuriy.baryshev@vntu.edu.ua

Зарезенко Дмитро Павлович — аспірант кафедри обчислювальної техніки, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: dmytro.zarezenko@gmail.com

Yurii Baryshev — PhD. (Eng), Associate Professor of Information Protection Department, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua

Dmytro Zarezenko — Postgraduate Student of Computer Engineering Department, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dmytro.zarezenko@gmail.com