ISSN 1998-7927(print) ISSN 2664-6498 (online)

DOI: https://doi.org/10.33216/1998-7927-2026-301-3-45-49

УДК 004:62

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ІНТЕГРАЦІЇ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ТА ML-МОДЕЛЕЙ У СИСТЕМАХ УПРАВЛІННЯ ФІНАНСОВИМИ РИЗИКАМИ

Філоненко О. Ю.

STUDY OF THE POSSIBILITY OF INTEGRATING BLOCKCHAIN TECHNOLOGIES AND ML MODELS INTO FINANCIAL RISK MANAGEMENT SYSTEMS

Filonenko O. Yu.

У статті досліджено можливість розробки моделі інформаційної технології з використанням інтеграції блокчейн-технології Hyperledger Fabric та ML-моделей для управління фінансовими ризиками. Актуальність дослідження зумовлена зростанням обсягів транзакцій в сучасних фінансових установах, ускладненням фінансових інструментів, впровадженням більш суворих регуляторних вимог, що загострює необхідність забезпечення незмінності та автентичності даних. Досліджено особливість традиційних централізованих систем управління ризиками, а саме обмеження щодо забезпечення незмінності історичних даних, що створює потенційні ризики маніпуляцій та спотворення аналітичних результатів. Оскільки ML-моделі, які активно застосовуються для кредитного скорингу та виявлення шахрайства, критично залежать від якості вхідних даних, виникає необхідність вирішення науково-прикладної задачі, а саме створення інтегрованої архітектури, яка поєднує гарантії незмінності даних блокчейн-систем із прогностичною потужністю ML-моделей. При підготовці статті проведено аналіз закордонних і вітчизняних публікацій щодо застосування алгоритмів машинного навчання (логістична регресія, Random Forest, XGBoost, Isolation Forest) у фінансовому скорингу та ефективності permissioned-архітектур блокчейн, зокрема Hyperledger Fabric. Обґрунтовано, що інтеграція блокчейн-рівня як інфраструктури довіри для ML-процесів (provenance, audit trail, integrity of updates, governance) залишається недостатньо формалізованою. Запропоновано трирівневу архітектуру (Data Layer, Analytics Layer, Governance Layer) та формальні визначення простору транзакцій, ML-моделі ризику та формули інтегрованого ризику. В ході дослідження було використано синтетичний датасет та виконано порівняння ефективності моделейLogistic Regression, Random Forest та XGBoost.

За результатами моделювання виявлено, що модель XGBoost показала найвищі показники, а інтеграція з блокчейн не вплинула на прогностичну ефективність, і в той же час забезпечила повну трасованість рішень та підвищила аудиторську прозорість. Результати мають прогностичний характер і потребують подальшої емпіричної верифікації в умовах реального впровадження у фінансовій установі.

***Ключові слова**: блокчейн, Hyperledger Fabric, машинне навчання, управління фінансовими ризиками, кредитний скоринг, фінансовий моніторинг, permissioned blockchain.*

Вступ. Сучасні фінансові установи функціонують в умовах зростання обсягів транзакцій, ускладнення фінансових інструментів та підвищення регуляторних вимог. В Україні ці вимоги формуються з урахуванням положень Національного банку України [11] щодо управління ризиками та організації систем фінансового моніторингу, проте вимоги до програмного продукту не обмежуються ними – технічний аспект реалізації подібних рішень та вимоги інструментів можуть не отримувати достатньо належної уваги.

Традиційні централізовані системи управління ризиками мають обмеження щодо забезпечення

незмінності історичних даних, що створює потенційні ризики маніпуляцій та спотворення аналітичних результатів. Одночасно ML-моделі, які активно застосовуються для кредитного скорингу та виявлення шахрайства, критично залежать від якості вхідних даних. Таким чином, виникає науково-прикладна проблема створення інтегрованої архітектури, яка поєднує гарантії незмінності даних блокчейн-систем із прогностичною потужністю ML-моделей.

Аналіз закордонних і вітчизняних публікацій. Аналіз публікацій показує, що популярними алгоритмами машинного навчання, які часто застосовуються у фінансовому скорингу, управлінні ризиками та AML-аналізі [9] є: логістична регресія, Random Forest [3], Gradient Boosting (XGBoost) [2], нейронні мережі [4], Isolation Forest для виявлення аномалій [8], а дослідження у сфері застосування блокчейн-технологій [5, 7] у фінансовому секторі демонструють ефективність permissioned-архітектур для корпоративних середовищ. Зокрема, платформа Hyperledger Fabric [6] забезпечує модульність, розмежування доступу через MSP (Membership Service Provider) та реалізацію смарт-контрактів (chaincode).

Проте інтеграція блокчейн-рівня як інфраструктури довіри для ML-процесів (provenance, audit trail, integrity of updates, governance) залишається недостатньо формалізованою – немає загальноприйнятих єдиних моделей, стандартних схем/метаданих, еталонних протоколів і метрик оцінювання.

Оглядові статті прямо фіксують «незрілість» і фрагментацію підходів. Зокрема, огляд arXiv з конвергенції ML і blockchain має окремий розділ «Limitations and Future Research Directions» і описує, що наявні рішення мають суттєві обмеження (інсентиви, приватність, вартість/дизайн протоколів/маркетплейсів, складність моделей тощо), а також потребують подальших досліджень. Це типовий індикатор відсутності усталеної формалізації (коли область вже «закрита» стандартами/референс-архітектурами, такі розділи значно коротші й менш фундаментальні). Додатково, у більш сучасних роботах часто підкреслюється, що значна частина підходів – концептуальні рамки або прототипи, а не стандартизована практика. Наприклад, у статті з експериментами на Hyperledger Fabric прямо сказано, що робота є лише мотивацією для майбутнього створення «comprehensive framework». Це фактично визнання, що «повної» узгодженої формалізації ще немає.

Дисбаланс напрямів досліджень: «ML для blockchain» переважає над «blockchain як довіра для ML». Огляд у ScienceDirect (2025) фіксує, що більшість робіт зосереджена на застосуванні ML для задач blockchain (безпека, оптимізація, вразливості), тоді як менше досліджень розглядає blockchain як механізм, що підсилює ML (тобто як «trust infrastructure»). Такий дисбаланс означає: напрям «blockchain → довіра в ML» ще не став настільки зрілим, щоб сформувати стандартні патерни/формальні моделі.

У прикладних роботах з provenance/audit звучить «framework/proposal», а не «standard». Нові праці про верифіковану provenance моделей/даних через блокчейн (AI supply chain, model provenance, audit trails) зазвичай описують «conceptual implementation framework / proposed integrated framework» – тобто авторські архітектури, які не є загальноприйнятою специфікацією. Це знову ж свідчення недостатньої формалізації рівня «як саме робити правильно».

Стандарти/фрейми з AI-управління ризиками вимагають provenance та accountability, але не дають формальної «blockchain-специфікації». Наприклад, NIST AI Risk Management Framework задає рамку управління ризиками й довірою в AI (governance, вимірювання/моніторинг, прозорість, документація тощо), але не стандартизує блокчейн як «референс-рівень довіри» для ML і не визначає формальний протокол/модель даних «blockchain-for-ML-provenance». Це означає: потреба в довірі формалізується на рівні вимог, але спосіб реалізації через блокчейн – ні.

Повторюваний набір «невирішених» технічних суперечностей є ознакою відсутності єдиної формальної моделі. У працях про blockchain-аудит FL та суміжні підходи типово підкреслюються компроміси масштабованість/вартість ↔ повнота логування, приватність ↔ прозорість, on-chain ↔ off-chain, управління ключами, політики доступу тощо. Коли ці компроміси не «закриті» стандартом, виникає багато несумісних реалізацій (а це і є недостатня формалізація).

Як підсумок, можна стверджувати, що інші публікації на дану тематику системно перелічують обмеження й future work, прикладні статті говорять мовою «proposed framework» і «motivation for future comprehensive framework»

(зокрема на Hyperledger Fabric), досліджень «blockchain як trust для ML» менше, а стандарти AI-ризиків формалізують вимоги до довіри, але не дають формальної блокчейн-специфікації для ML-процесів.

Мета роботи та обґрунтування необхідності її виконання.

Метою роботи є дослідження можливості розробки моделі інформаційної технології для інтеграції блокчейн-технології Hyperledger Fabric та ML-моделей для управління фінансовими ризиками з урахуванням вимог українського регуляторного середовища.

Необхідність розробки моделі інформаційної технології інтеграції Hyperledger Fabric та ML-моделей обумовлена зростанням регуляторних вимог до управління ризиками, потребою забезпечення незмінності та автентичності даних, необхідністю аудиторської простежуваності алгоритмічних рішень, відсутністю стандартизованих архітектур у вітчизняній науковій практиці.

Виклад основного матеріалу дослідження. У дослідженні використано: нормативні документи НБУ [11] щодо управління ризиками та фінансового моніторингу; архітектурні специфікації Hyperledger Fabric [6] (версія 2.x); створено та застосовано синтетичний транзакційний датасет обсягом 100 000 записів; ML-бібліотеки Python (XGBoost [2], Scikit-learn). Датасет містив: ідентифікатор клієнта; суму транзакції; частоту операцій; історію дефолтів; мітку класу (0 – нормальна операція, 1 – ризикова).

Простір даних і позначення:

- $\mathcal{X} \subset \mathbb{R}^m$ — простір ознак транзакцій;
- $\mathcal{Y} = \{0,1\}$ — простір міток ризику (0 — нормальна операція, 1 — ризикова);
- $D = \{(x_i, y_i)\}_{i=1}^n$ — навчальна вибірка, де $x_i \in \mathcal{X}, y_i \in \mathcal{Y}$;
- $x \in \mathcal{X}$ — довільна нова транзакція;
- $t \in \mathbb{R}_+$ — час (timestamp);
- $\theta \in \Theta$ — вектор параметрів ML-моделі.

Транзакція визначається як кортеж: $\tau = (x, t, "id")$, де "id" – унікальний ідентифікатор транзакції. ML-модель оцінювання ризику визначається як вимірна функція: $f\_\theta: X \to [0,1]$, яка повертає умовну ймовірність ризикової події:

$$R(x) = f\_\theta(x) = P(Y = 1 | X = x). \quad (1)$$

Архітектура інтегрованої системи складається з трьох рівнів: Data Layer – транзакції зберігаються в Hyperledger Fabric [6], яка має канальну архітектуру, endorsement policy, приватні колекції даних для AML; Analytics Layer – ML-моделі виконують скоринг; Governance Layer – фіксація рішень у блокчейні [5] через chaincode.

Оцінювання ефективності запропонованої інтегрованої архітектури проводилось у форматі експериментального моделювання на основі анонімізованої вибірки історичних показників реалізації банківських IT-проєктів та згенерованих сценаріїв ризикових подій.

Дослідження не передбачало впровадження у конкретній фінансовій установі, а базувалося на порівнянні двох моделей функціонування системи управління ризиками: базова модель (традиційна централізована архітектура без ML та без блокчейн) та інтегрована модель (ML-прогнозування + фіксація критичних подій у Hyperledger Fabric).

Метод оцінювання. Для оцінки ефекту застосовано такі підходи: порівняння часу реакції на ризикові події; моделювання впливу раннього виявлення ризиків на бюджет; розрахунок коефіцієнта зниження інформаційної асиметрії; аналіз аудиторської відтворюваності даних [1].

Інтегрований ризик визначався за формулою:

$$R\_final = \sum\_\{i = 1\}\^n w\_i \cdot P\_i \cdot C\_i \cdot T\_bc \quad (2)$$

де T_bc – коефіцієнт довіри до даних блокчейн-рівня.

В межах підготовки даних було виконано нормалізацію та балансування класів методом SMOTE [9]. Порівнювались моделі Logistic Regression, Random Forest [3], XGBoost [2]. Інтеграція з блокчейн відбувалась наступним чином: через REST API результати скорингу передавалися до chaincode, який формував транзакцію та записував її у блок.

Таблиця 1

Порівняння метрик ML-моделей

Модель	ROC-AUC	Precision	Recall	F1-score
Logistic Regression	0,82	0,76	0,71	0,73
Random Forest	0,89	0,83	0,80	0,81
XGBoost	0,93	0,88	0,85	0,86

Результати моделювання. Інтеграція блокчейн-рівня не вплинула на ROC-AUC, але забезпечила повну трасованість рішень, зменшила ризик маніпуляції історичними даними, підвищила аудиторську прозорість, що в свою чергу має ряд переваг: раннє виявлення ризикових сценаріїв [10] потенційно дозволяє зменшити затримки реалізації ІТ-проєктів; інтеграція блокчейн-рівня підвищує аудитованість та знижує ймовірність ретроспективного редагування даних; використання ансамблевих ML-моделей [2, 3] забезпечує більш стабільну класифікацію ризикових подій порівняно з rule-based підходами.

Отримані кількісні оцінки слід розглядати як результати модельного експерименту, а не як статистику конкретного банку. Результати мають прогностичний характер та потребують подальшої емпіричної верифікації в умовах реального впровадження у фінансовій установі.

Висновки. Інтеграція Hyperledger Fabric [6] із ML-моделями створює інфраструктуру довіри для управління фінансовими ризиками. Експеримент підтвердив: високу прогностичну точність XGBoost [2]; збереження ефективності при інтеграції з блокчейн; підвищення рівня прозорості та аудиту, що в свою чергу позитивно впливає на відповідність вимогам НБУ [11]. Подальші дослідження доцільно спрямувати на впровадження Explainable AI [12] та оптимізацію продуктивності permissioned-мереж.

Література

1. Basel Committee on Banking Supervision. Principles for effective risk data aggregation and risk reporting. Basel: Bank for International Settlements, 2013.
2. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2016. P. 785–794. DOI: https://doi.org/10.1145/2939672.2939785
3. Breiman L. Random Forests. Machine Learning. 2001. Vol. 45. P. 5–32. DOI: https://doi.org/10.1023/A:1010933404324
4. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge: MIT Press, 2016.
5. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. DOI: https://doi.org/10.2139/ssrn.3440802
6. Androulaki E. et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In: Proceedings of the Thirteenth EuroSys Conference. 2018. DOI: https://doi.org/10.1145/3190508.3190538
7. Dorri A., Steger M., Kanhere S., Jurdak R. Blockchain: A Distributed Solution to Automotive Security and Privacy. IEEE Communications Magazine. 2017. Vol. 55(12). P. 119–125. DOI: https://doi.org/10.1109/MCOM.2017.1700879
8. Aggarwal C. C. Outlier Analysis. 2nd ed. Cham: Springer, 2017. DOI: https://doi.org/10.1007/978-3-319-47578-3
9. Carcillo F., Dal Pozzolo A., Bontempi G., Snoeck M. Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection. Information Sciences. 2021. Vol. 557. P. 317–331. DOI: https://doi.org/10.1016/j.ins.2019.05.042
10. European Banking Authority. Guidelines on loan origination and monitoring. 2020.
11. National Bank of Ukraine. Regulation on Risk Management System in Banks of Ukraine. Resolution of the NBU Board No. 64, 11.06.2018.
12. Molnar C. Interpretable Machine Learning. 2022. DOI: https://doi.org/10.5281/zenodo.3718599

Filonenko O. Yu. Integration of Blockchain Technologies and ML Models in Financial Risk Management Systems.

The article examines the feasibility of developing a model of an information technology based on the integration of the Hyperledger Fabric blockchain technology and ML models for financial risk management. The relevance of the study is driven by the growing volume of transactions in modern financial institutions, the increasing complexity of financial instruments, and the introduction of stricter regulatory requirements, which intensify the need to ensure data immutability and authenticity.

The study analyzes the characteristics of traditional centralized risk management systems, particularly their limitations in ensuring the immutability of historical data, which creates potential risks of manipulation and distortion of analytical results. Since ML models, widely used for credit scoring and fraud detection, critically depend on the quality of input data, there arises a need to address a scientific and applied problem—namely, the creation of an integrated architecture that combines blockchain-based guarantees of data immutability with the predictive power of ML models. In preparing the article, an analysis of international and domestic publications was conducted regarding the application of machine learning algorithms (logistic regression, Random Forest, XGBoost, Isolation Forest) in financial scoring, as well as the effectiveness of permissioned blockchain architectures, particularly Hyperledger Fabric.

It is substantiated that the integration of a blockchain layer as a trust infrastructure for ML processes (provenance, audit trail, integrity of updates, governance) remains insufficiently formalized. A three-layer architecture (Data Layer, Analytics Layer, Governance Layer) is proposed, along with formal

definitions of the transaction space, ML-based risk model, and the integrated risk formula.

During the study, a synthetic dataset was used, and a comparison of the performance of Logistic Regression, Random Forest, and XGBoost models was conducted. The modeling results show that the XGBoost model achieved the highest performance, while integration with blockchain did not affect predictive efficiency but ensured full traceability of decisions and improved audit transparency. The results are of a predictive nature and require further empirical validation under real-world implementation conditions in financial institutions.

Keywords: *blockchain, Hyperledger Fabric, machine learning, financial risk management, credit scoring, financial monitoring, permissioned blockchain.*

Філоненко Орест Юрійович – аспірант кафедри інформаційних технологій та програмування Східноукраїнського національного університету імені Володимира Даля,
https://orcid.org/0009-0000-1480-4673
orest.filonenko@gmail.com

Дата першого надходження статті 15.01.2026.
Дата прийняття статті до друку після рецензування 25.02.2026.
Дата публікації 11.05.2026.