УДК 004.6

БАГАТОВУЗЛОВА МОДЕЛЬ У ФЕДЕРАТИВНІЙ БЛОКЧЕЙН-СОЦІАЛЬНІЙ МЕРЕЖІ

Цудзенко Ю. Є. [1]; Павлишенко Б. М.[2], д.т.н.
[1,2] Львівський національний університет імені Івана Франка
[1,2] Україна, Львів
[1] yura9989@gmail.com; [2] b.pavlyshenko@gmail.com

Анотація. *У роботі запропоновано гібридну модель інтелектуального аналізу транзакцій користувачів в децентралізованих соціальних мережах. Модель поєднує принципи федеративного навчання і блокчейн-технологій та дозволяє виявити аномалії та витоку інформації. Крім того, обґрунтовано механізми синхронізації у децентралізованих системах і підтверджено підвищену стійкість до атак і зменшення ризиків втрати даних.*

Ключові слова: *федеративне навчання; блокчейн; соціальні мережі; децентралізовані системи; машинне навчання.*

Вступ. Зі стрімким розвитком децентралізованих соціальних мереж особливої актуальності набувають питання збереження приватності користувачів, безпечного обміну інформацією та достовірності результатів інтелектуального аналізу даних. Традиційні централізовані моделі машинного навчання вимагають акумулювання великих обсягів даних на центральних серверах, що створює загрозу витоку, маніпуляцій та, про що свідчать сучасні дослідження у сфері безпеки штучного інтелекту [1]. Альтернативою цим підходам є федеративне навчання, яке дозволяє здійснювати локальну обробку даних користувачів і формувати глобальну модель без прямого доступу до приватної інформації [2]. Блокчейн-технології, що забезпечують децентралізовану верифікацію транзакцій та немодифікованість записів, відкривають нові можливості для зміцнення довіри у процесі спільного навчання моделей [3-5].

Метою роботи є інтеграція принципів федеративного навчання та блокчейн технологій дозволяє створити гібридну архітектуру, у якій навчання та перевірка оновлень відбуваються колективно в межах розподіленого середовища. Такий підхід усуває залежність від центрального сервера, підвищує рівень стійкості системи до атак і сприяє формуванню надійних моделей штучного інтелекту у розподілених середовищах.

Основна частина. Розроблена архітектура системи передбачає визначення кожного вузла децентралізованої соціальної мережі функціонує як автономний учасник процесу навчання, який оперує власними локальними даними, транзакціями при соціальній взаємодії [2]. На кожному вузлі розгортається локальна модель машинного навчання, яка оновлюється на основі даних конкретної спільноти без потреби передавання сирої інформації за межі пристрою [4]. Після завершення кожної епохи навчання вузол обчислює власні ваги параметрів моделі (*Wi*) та створює хеш оновлення, який фіксується у блокчейні [5]. Це забезпечує криптографічно підтверджувану історію змін і запобігає підробці результатів. Верифікацію оновлень здійснює смарт-контракт, який автоматично перевіряє цілісність ваг, репутацію вузла-учасника та відповідність консенсусним правилам оновлення, як можна побачити на Fig.1 Лише підтверджені дані надходять до рівня агрегації, де спеціальний сервер або обраний вузол блокчейну виконує secure aggregation — об’єднання ваг локальних моделей із збереженням приватності.

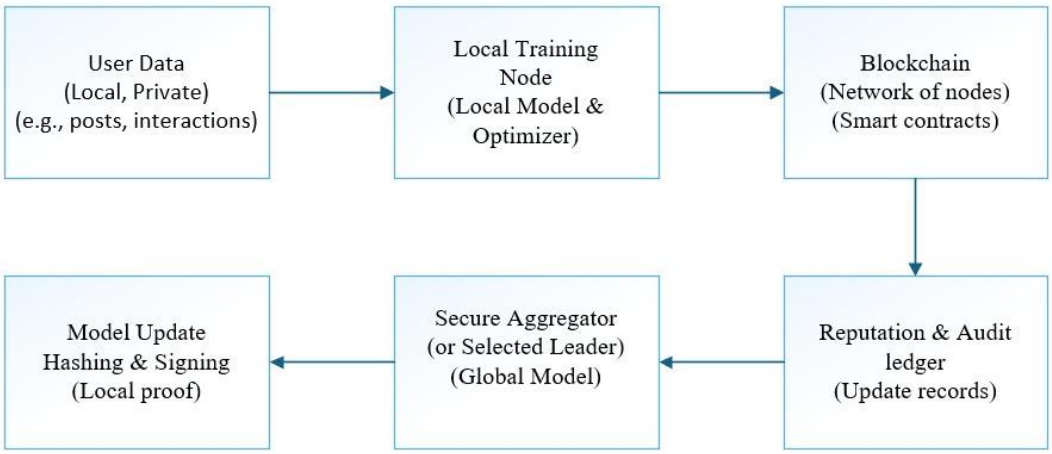


Рисунок 1. Архітектурна блок-схема відображення роботи системи

У результаті формується глобальна модель, що відображає узагальнені закономірності поведінки користувачів без розкриття їхніх індивідуальних даних. Така архітектура поєднує переваги федеративного навчання та блокчейн-консенсусу, забезпечуючи децентралізовану довіру, масштабованість і стійкість до зловмисних дій у середовищі розподіленого аналізу даних.

На основі отриманих даних можна сформувати математичну модель з низкою параметрів для порівняння при федеративній, централізованій та децентралізованій системі. Множина вузлів позначається як N={n1, n2,…, nk}, де кожен вузол n_i має власний локальний набір даних за формулою D_i={$(x_j^{(i)}, y_j^{(i)})$}$j = 1^{mi}$. Кожен вузол виконує локальну оптимізацію параметрів моделі w_i шляхом мінімізації власної функції втрат $w_i^{(t+1)}$=$w_i^{(t)}$-$\eta\nabla_w L_i(w_i^{(t)}, D_i)$, де L_i— локальна функція втрат, η— швидкість навчання, t — номер ітерації. А результатом кожної епохи є набір ваг w_i, які відображають локальні закономірності поведінки користувачів на вузлі. Такі параметри дозволяють здійснювати оцінку хешування та верфікацію транзакцій користувачів для запису у смарт-контакти та виявлення цілісності даних.

Після верифікації вузли надсилають зміни до агрегатора у зашифрованому вигляді. Глобальна модель формується як зважене середнє за формулою $w_g = \sum_{i=1}^{k} \alpha_i w_i$, де $\alpha_i = \frac{|D_i|}{\sum_{i=1}^{k} |D_i|}$.

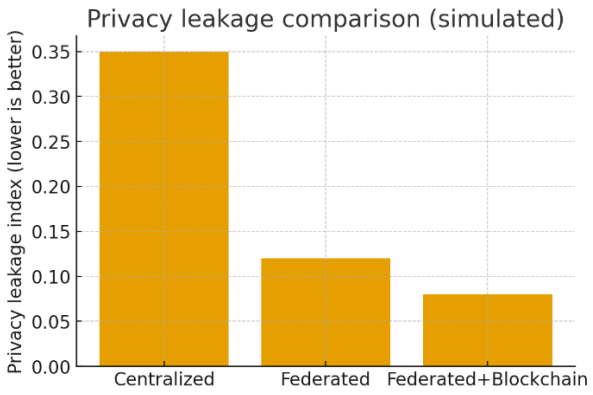
Для оцінювання ефективності запропонованої моделі федеративної моделі на базі блокчейн застосовано комплекс метрик, що враховують як якість навчання, так і характеристики безпеки та продуктивності системи. Основним показником є Accuracy, який визначає частку правильно класифікованих прикладів і відображає загальну точність моделі. Додатково використовується F1-score — гармонійне середнє між точністю (*precision*) та повнотою (*recall*), що дозволяє об'єктивно оцінити збалансованість моделі за умов нерівномірного розподілу класів. Показник Loss характеризує ступінь відхилення прогнозованих значень від реальних під час процесу навчання та слугує індикатором ефективності оптимізації. Окрему увагу приділено метриці Privacy leakage index (ΔP), яка відображає рівень потенційного витоку приватних даних під час обміну оновленнями між вузлами; чим менше значення ΔP, тим вищий рівень захисту конфіденційної інформації. Метрика Convergence time використовується для вимірювання кількості ітерацій або часу, необхідного для стабілізації глобальної моделі, що свідчить про швидкість збіжності системи. Крім того, оцінюється Blockchain latency — середній час затримки, спричинений виконанням

смарт-контрактів і верифікацією оновлень у блокчейні. Сукупне застосування цих показників дозволяє комплексно оцінити ефективність, надійність і практичну придатність запропонованої архітектури у децентралізованому середовищі.

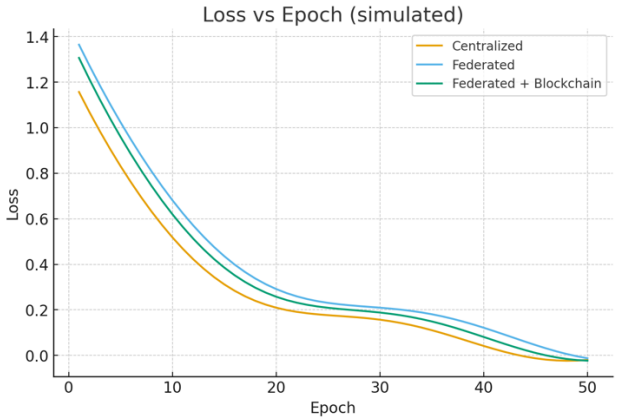
Табл.1. Порівняльна таблиця моделей

Модель	**Точність (%)**	**F1**	**Privacy ΔP ↓**	**Час навчання (сек)**	**Latency (мс)**
Централізована	91.2	0.88	0.35	35	—
Federated	89.7	0.86	0.12	48	—
Federated + Blockchain	90.5	0.87	0.08	52	120

З Табл.1. видно, що запропонована модель із використанням блокчейну зберігає високий рівень точності (90.5%) і F1-метрики (0.87), наближених до централізованої системи, при цьому суттєво зменшує показник витоку приватності ΔP (до 0.08). Незначне збільшення часу навчання та затримки, зумовлене верифікацією транзакцій у блокчейні, компенсується підвищеною безпекою, прозорістю та надійністю процесу навчання. Таким чином, інтеграція блокчейн-рівня у федеративну архітектуру забезпечує оптимальний баланс між продуктивністю, конфіденційністю та точністю аналітичних моделей у децентралізованих середовищах.



a)



b)

Рисунок 2а Порівняльний графік потенційного витоку даних. Рисунок.2b Відображення зменшення значення функції втрат

З рисунку 2а можна побачити поступове зменшення значення функції втрат із кожною епохою, причому швидкість збіжності порівнянна з централізованими підходами, що підтверджує відсутність деградації якості навчання при збереженні приватності. А порівняльне відображення рисунку.2b показує значне зниження потенційного витоку даних у запропонованій моделі на більш ніж утричі відносно централізованих систем. Таким чином, розроблена аріхтектура підтверджує ефективність механізмів шифрування, локальної обробки та верифікації оновлень у блокчейні. Крім того, забезпечує оптимальний баланс між конфіденційністю та точністю, характеризується доброю масштабованістю при збільшенні кількості вузлів і демонструє помірне зростання затримки, яке компенсується підвищенням рівня надійності, прозорості та достовірності результатів моделювання.

Висновки. Практичні результати дослідження підтверджують ефективність запропонованої моделі Federated Blockchain Intelligence як гібридного підходу до безпечного аналізу користувацьких даних у децентралізованих соціальних мережах. Проведене експериментальне оцінювання показало, що інтеграція механізмів блокчейну у процес федеративного навчання забезпечує збереження високої точності класифікації (до 90,5%) при суттєвому зниженні ризику витоку приватної інформації (ΔP = 0.08), що є критично важливим для систем із розподіленим управлінням даними у соціальних мережах. Незначне збільшення

часу навчання та затримки, спричинене верифікацією оновлень у блокчейні, не впливає істотно на загальну продуктивність і компенсується підвищенням довіри до результатів моделювання. Запропонована архітектура продемонструвала стабільну збіжність моделей і стійкість до атак, а також здатність до ефективного масштабування при зростанні кількості вузлів. Отже, розроблена система може бути практично застосована для побудови приватних аналітичних платформ, систем рекомендацій, децентралізованих сервісів цифрової ідентичності та соціальних аналітик нового покоління, де необхідно поєднати високий рівень безпеки з якісним машинним аналізом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Liu, J., Chen, C., Li, Y., Sun, L., Song, Y., Zhou, J.,& Dou, D. (2024). Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning. *Knowledge and Information Systems*, *66*(8), 4377-4403. https://doi.org/10.1007/s10115-024-02117-3

[2] Abuzied, Y., Ghanem, M., Dawoud, F., Gamal, H., Soliman, E., Sharara, H., & Elbatt, T. (2024). A privacy-preserving federated learning framework for blockchain networks. *Cluster Computing*, *27*(4), 3997-4014. https://doi.org/10.1007/s10586-024-04273-1

[3] Bhardwaj, T., & Sumangali, K. (2025). An explainable federated blockchain framework with privacy-preserving AI optimization for securing healthcare data. *Scientific Reports*, *15*(1), 21799. https://doi.org/10.1038/s41598-025-04083-4

[4] Li, Y., Xia, C., Lin, W., & Wang, T. (2024). PPBFL: A privacy protected blockchain-based federated learning model. *arXiv preprint arXiv:2401.01204*. https://doi.org/10.48550/arXiv.2401.01204

[5] Salim, S., Moustafa, N., & Turnbull, B. (2025). BFL-SC: A blockchain-enabled federated learning framework, with smart contracts, for securing social media-integrated internet of things systems. *Ad Hoc Networks*, *169*, 103760. https://doi.org/10.1016/j.adhoc.2025.103760

Tsudzenko Y. Y., Pavlyshenko B. M.

Multi-node model in federated blockchain social networks

Abstract. *The paper proposes a hybrid model of intelligent analysis of user transactions in decentralized social networks. The model combines the principles of federated learning and blockchain technologies and allows you to identify anomalies and information leaks. In addition, the mechanisms of synchronization in decentralized systems are substantiated and increased resistance to attacks and reduced risks of data loss are confirmed.*

Keywords: *federated learning; blockchains; social networks; decentralized systems; machine learning.*