https://doi.org/10.31891/2219-9365-2026-87-12
УДК 004

АСКЕРОВ В'ячеслав
Хмельницький національний університет
https://orcid.org/0009-0009-1176-9812
e-mail: v.askerov@khmnu.edu.ua

МЕТОД КЛАСИФІКАЦІЇ ТРАНЗАКЦІЙ І ОКРЕМИХ ТРАНЗАКЦІЙНИХ ПАТЕРНІВ НЕЙРОМЕРЕЖЕВИМИ ЗАСОБАМИ ЗА РІВНЕМ БЕЗПЕЧНОСТІ У СИСТЕМАХ БЛОКЧЕЙН

У роботі розроблено апаратно-програмний метод класифікації транзакцій і окремих транзакційних патернів нейромережевими засобами за рівнем безпечності у системах блокчейн, орієнтований на керування допуском і режимами передконсенсусної обробки без модифікації базових механізмів консенсусу. Метод функціонує у виділеному позаланцюговому довіреному контурі оцінювання ризику та формує транзакційний профіль як узгоджене подання структурних, часових і контекстних ознак, придатне до подальшої криптографічної фіксації. Нейромережевий модуль трансформерного типу обчислює ризик-оцінку транзакції, а стабільність прогнозу оцінюється методом Monte Carlo Dropout, що забезпечує кероване врахування невизначеності як параметра протокольної політики. На основі ризик-оцінки та невизначеності виконується інженерне зонування транзакцій на зони «White», «Gray» і «Black» з формуванням протокольної директиви стандартної обробки, посиленої верифікації або карантинного режиму з відкладеним включенням. Окремо підтримується аналіз транзакційних патернів як повторюваних топологічно-часових мотивів у графі переказів із агрегацією їх характеристик у часовому вікні та формуванням патерн-орієнтованих керувальних сигналів. Для забезпечення доказовості й відтворюваності результатів реалізовано журналювання рішень у вигляді підписаних записів із криптографічними зобов'язаннями на ознаки та криптографічним зв'язуванням записів у ланцюг. Експериментальну перевірку проведено на «Elliptic Data Set» (Bitcoin) з використанням розміченої підвибірки 46 564 транзакцій та розширеного профілю 188 ознак. Отримано тестові значення ROC-AUC 0.9207 та AUPRC 0.7588; політика зонування забезпечує ескалацію 0.8596 ризикових транзакцій на підвищені режими контролю при навантаженні 0.3155, а мікробенчмарк накладних витрат підтверджує зниження середньої вартості передконсенсусної обробки на 57.98% відносно суцільної посиленої верифікації. Практична цінність полягає у реалізації ризик-орієнтованого керування ресурсами верифікації та аудиту рішень у блокчейн-вузлі.

Ключові слова: блокчейн-система, транзакція, транзакційні патерни, нейромережеве оцінювання ризику, трансформерна модель, оцінювання невизначеності прогнозу, Monte Carlo Dropout, ризик-орієнтоване зонування.

ASKEROV Viacheslav
Khmelnytskyi National University

METHOD OF CLASSIFICATION OF TRANSACTIONS AND SEPARATE TRANSACTION PATTERNS BY NEURAL NETWORK MEANS ACCORDING TO SECURITY LEVEL IN BLOCKCHAIN SYSTEMS

The paper develops a hardware-software method for classifying transactions and separate transaction patterns by neural network means according to the level of security in blockchain systems, focused on managing admission and pre-consensus processing modes without modifying the basic consensus mechanisms. The method operates in a dedicated off-chain trusted risk assessment loop and forms a transaction profile as a consistent representation of structural, temporal, and contextual features suitable for subsequent cryptographic fixation. A transformer-type neural network module calculates the transaction risk assessment, and the stability of the forecast is assessed using the Monte Carlo Dropout method, which provides controlled consideration of uncertainty as a parameter of the protocol policy. Based on the risk assessment and uncertainty, engineering zoning of transactions into "White", "Gray," and "Black" zones is performed with the formation of a protocol directive for standard processing, enhanced verification, or quarantine mode with delayed inclusion. Separately, the analysis of transaction patterns as recurring topological-temporal motifs in the transfer graph with the aggregation of their characteristics in a time window and the formation of pattern-oriented control signals is supported. To ensure the provability and reproducibility of the results, logging of decisions in the form of signed records with cryptographic commitments to features and cryptographic linking of records into a chain is implemented. Experimental verification was carried out on the "Elliptic Data Set" (Bitcoin) using a labeled subsample of 46,564 transactions and an extended profile of 188 features. The test values of ROC-AUC 0.9207 and AUPRC 0.7588 were obtained; the zoning policy ensures the escalation of 0.8596 risky transactions to increased control modes at a load of 0.3155, and the overhead microbenchmark confirms a 57.98% reduction in the average cost of pre-consensus processing relative to solid enhanced verification. The practical value lies in implementing risk-based management of verification resources and audit decisions in a blockchain node.

Keywords: blockchain system, transaction, transaction patterns, neural network risk assessment, transform model, forecast uncertainty assessment, Monte Carlo Dropout, risk-based zoning.

Стаття надійшла до редакції / Received 04.04.2026
Прийнята до друку / Accepted 30.06.2026
Опубліковано / Published 10.09.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Блокчейн-системи забезпечують криптографічну цілісність даних і незмінність реєстру, однак ці властивості не усувають прикладних загроз безпеці транзакцій у мережевому середовищі [1]. На практиці ризиковість операцій визначається не лише формальною валідністю полів транзакції, а й її структурним положенням у графі переказів, часовою динамікою активності та контекстом взаємодій адрес. У таких умовах штатні механізми передконсенсусної перевірки гарантують коректність виконання, але не забезпечують керованого відбору транзакцій за рівнем ризику й не надають засобів адаптивного використання ресурсів верифікації [2]. Це формує потребу в апаратно-програмних рішеннях, які здатні до включення транзакції в блок формувати ризик-оцінку, керувати режимами допуску та підтримувати аудит прийнятих рішень без модифікації базового консенсусу.

Відомі підходи до оцінювання ризику транзакцій, що ґрунтуються на правилах або простих статистичних моделях, є обмеженими з погляду інженерної масштабованості та стійкості до еволюції атак. Їхня ефективність залежить від ручного супроводу правил і вони недостатньо враховують взаємодію різнорідних ознак, які одночасно описують структуру транзакції, її часовий режим і контекст у графі мережевих взаємодій [3]. Натомість нейромережеві моделі, зокрема трансформерні архітектури, дозволяють будувати узагальнені подання транзакційного профілю та отримувати ризик-оцінку на основі взаємозв'язків між ознаками. Для задач комп'ютерної інженерії принциповою є не лише точність прогнозу, а й придатність результату до протокольної інтеграції, керованість режимів обробки та вимірюваність накладних витрат у контурі передконсенсусної верифікації. Додатковим чинником є необхідність врахування невизначеності прогнозу, оскільки в системах керування безпекою критичними є надмірно впевнені помилки, які мають компенсуватися протокольним механізмом ескалації перевірок [4].

Тому є необхідною розробка методу нейромережевої класифікації транзакцій та окремих транзакційних патернів за рівнем безпечності у системах блокчейн, який функціонує у виділеному позаланцюговому контурі оцінювання ризику та взаємодіє з вузлом мережі на рівні керувальних директив передконсенсусної обробки. Метод має формувати транзакційний профіль як апаратно-програмний інженерний механізм, що поєднує структурні параметри транзакції, часові характеристики її появи та контекстні властивості локального оточення у графі транзакцій. На основі цього профілю нейромережевий модуль отримує ризик-оцінку та показник невизначеності прогнозу, після чого виконується ризик-орієнтоване зонування з подальшим вибором режиму протокольної обробки. У результаті для кожної транзакції формується директива керування допуском, яка визначає стандартну обробку, посилену верифікацію або карантинний режим з відкладеним включенням, що забезпечує адаптивне використання ресурсів вузла без зміни базових механізмів консенсусу.

Окремою складовою проблеми є виявлення транзакційних патернів як типових топологічно-часових мотивів у графі переказів, які відображають повторювані сценарії поведінки та можуть свідчити про організовані ризикові операції. Метод має підтримувати агреговане оцінювання таких патернів у часовому вікні та формувати патерн-орієнтовані сигнали керування, що доповнюють транзакційний рівень контролю [5, 6]. Оскільки обчислення ризику виконується поза блокчейном, необхідно забезпечити доказовість і відтворюваність результатів шляхом фіксації рішення у вигляді верифікованого підписаного запису журналу з криптографічними зобов'язаннями на ознаки та криптографічним зв'язуванням записів. Проблема зводиться до побудови й експериментального обґрунтування методу, який одночасно забезпечує коректне зонування ризику, протокольну маршрутизацію транзакцій, виявлення ризикових патернів і контроль накладних витрат передконсенсусної обробки у блокчейн-вузлі, зберігаючи можливість перевірки та аудиту прийнятих рішень.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У сучасних наукових публікаціях суттєво зросла увага до задачі ідентифікації шахрайських та ризикованих транзакцій у блокчейн-системах із використанням методів машинного та глибокого навчання [7, 8]. Переважна частина таких робіт орієнтується на побудову класифікаторів, що відокремлюють легітимні операції від небезпечних за умов вираженої незбалансованості даних, коли частка шахрайських транзакцій є істотно меншою за частку легітимних [9, 10].

Зокрема, у роботі [11] запропоновано підхід до класифікації криптовалютних транзакцій на основі глибокої нейромережевої архітектури трансформерного типу. Для компенсації дисбалансу класів автори застосовують штучне розширення навчальної вибірки, а інтерпретацію результатів моделі реалізують через SHAP-аналіз. Водночас постановка задачі в [11] залишається бінарною і не передбачає формування декількох рівнів ризику, а вихід моделі використовується як ознака належності до класу без інженерного механізму подальшої адаптації протоколу виконання транзакцій та без явного оцінювання невизначеності прогнозу.

Інший напрям представлено у дослідженні [12], де розглянуто багаторівневий глибокий фреймворк виявлення шахрайства в блокчейн-мережах, що поєднує згорткові та рекурентні нейронні мережі. Автори акцентують увагу на досягненні високих показників якості класифікації та зменшенні затримок обробки транзакцій. Разом із тим підхід у [12] не фокусується на інтерпретації рішень на рівні окремої транзакції, не

формує зон невизначеності та не розглядає інтеграцію результатів нейромережевого аналізу у вигляді адаптивних політик керування транзакціями [13].

Окремо варто відзначити порівняльні роботи, зокрема [14], у яких аналізується застосування класичних методів машинного навчання для класифікації блокчейн-транзакцій і підтверджується можливість отримання високих узагальнених показників точності. Проте такі рішення часто залишаються чутливими до змін розподілу даних, не надають оцінки ступеня впевненості прогнозу та не підтримують ризик-орієнтованого розподілу транзакцій за рівнем безпечності з подальшим адаптивним керуванням їх протокольною обробкою.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є розроблення та експериментальне обґрунтування апаратно-програмного методу класифікації транзакцій і окремих транзакційних патернів нейромережевими засобами за рівнем безпечності у системах блокчейн, який забезпечує ризик-орієнтоване керування допуском і режимами передконсенсусної обробки транзакцій у виділеному позаланцюговому контурі, з урахуванням невизначеності прогнозу та з фіксацією результатів у вигляді верифікованого підписаного журналу для забезпечення перевірюваності й відтворюваності прийнятих рішень.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Архітектура розробленого методу

Запропонований метод (схема наведена на рисунку 1) призначений для апаратно-програмного керування безпечністю виконання транзакцій у системах блокчейн шляхом позаланцюгового нейромережевого оцінювання ризику. Метод забезпечує формування ризик-орієнтованої директиви передконсенсусної обробки транзакції, що дозволяє адаптивно розподіляти ресурси перевірки між стандартним режимом, посиленою верифікацією та карантинним режимом без модифікації базових механізмів консенсусу. Додатково метод підтримує аналіз транзакційних патернів як повторюваних структурно-часових мотивів у графі транзакцій і забезпечує доказовість прийнятих рішень шляхом криптографічно верифікованого журналювання результатів оцінювання.

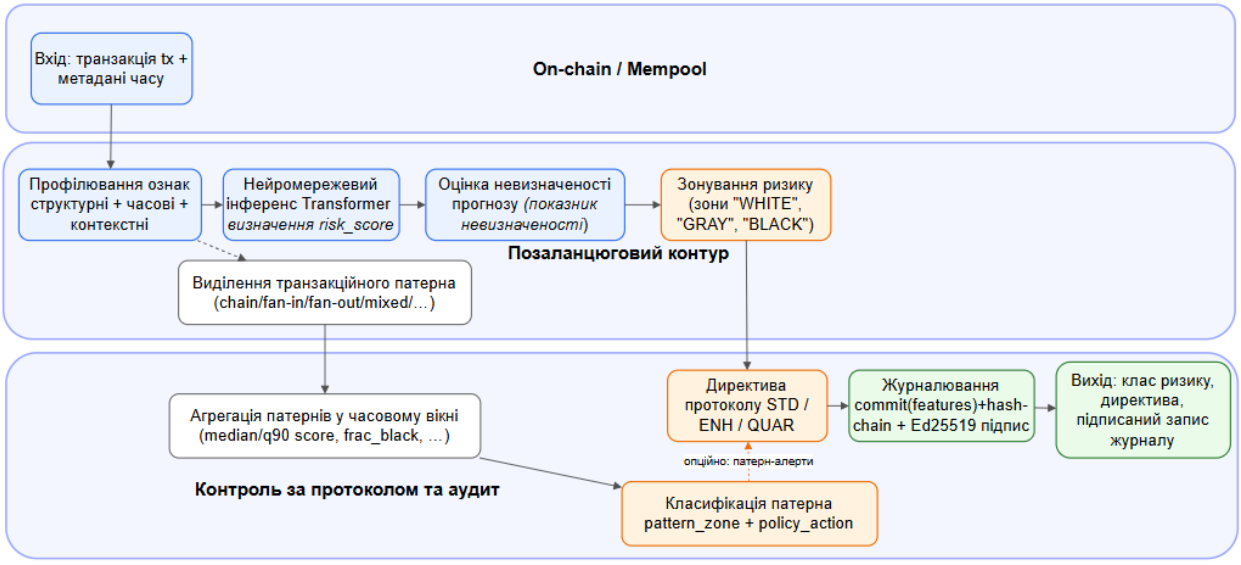

Рис. 1. Схема методу класифікації транзакцій і окремих транзакційних патернів нейромережевими засобами за рівнем безпечності

Вхідні дані методу формуються на рівні мемпулу та позаланцюгового контуру оцінювання ризику і включає транзакцію та її профіль ознак. Профіль транзакції є узгодженим поданням, що поєднує структурні характеристики транзакції, часові параметри її появи та контекстні властивості локального оточення у графі транзакцій. Окрім профілю, використовуються параметри політики зонування ризику, які визначають пороги віднесення транзакцій до зон безпечності та допустимий рівень невизначеності прогнозу.

Спочатку виконується формування вхідного профілю транзакції. На цьому етапі дані транзакції приводяться до канонічного подання, після чого обчислюються структурні ознаки, що відображають параметри потоків входів і виходів та локальні топологічні характеристики у графі транзакцій, часові ознаки, що описують режим активності у часовому вікні, а також контекстні ознаки, що характеризують оточення транзакції у графі та його агреговані властивості. Особливістю кроку є те, що ознаки формуються так, щоб вони були відтворюваними та придатними до подальшого криптографічного зобов'язання у журналі.

Далі виконується нейромережевий інференс у позаланцюговому довіреному контурі, де

трансформерна модель обчислює ризик-оцінку транзакції. Вибір трансформерної архітектури обґрунтовується здатністю моделювати взаємодії між різнорідними ознаками транзакції та формувати узагальнене представлення, стійке до варіативності поведінкових сценаріїв.

Після чого здійснюється оцінювання невизначеності прогнозу. Для цього застосовується Monte Carlo Dropout (MC Dropout), що дозволяє отримати показник невизначеності як характеристику стабільності прогнозу моделі. Особливістю цього кроку є те, що невизначеність використовується не як довідкова метрика, а як керувальний параметр, який впливає на зонування транзакції та вибір режиму перевірки у протоколі.

Наступним виконується зонування ризику та віднесення транзакції до зон «White», «Gray» або «Black» на основі ризик-оцінки та показника невизначеності з урахуванням порогів політики. Особливістю зонування є його інженерний характер: зони трактуються як протокольні режими керування допуском, а не як класи навчальної вибірки. Зона «White» відповідає стандартній обробці, зона «Gray» активує посилену перевірку стандартними засобами, зона «Black» ініціює карантинний режим або відкладене включення із застосуванням додаткових перевірок.

Далі формується протокольна директива передконсенсусної обробки, яка передається у контур керування протоколом і визначає набір операцій валідації, пріоритет та правила допуску транзакції до включення в блок. Особливістю цього кроку є відсутність втручання у механізми консенсусу: метод впливає на обробку транзакції на рівні політик передконсенсусної верифікації та маршрутизації.

Після чого забезпечується аудит шляхом журналювання результатів оцінювання. Формується запис журналу, що містить криптографічне зобов'язання на вхідні ознаки та ідентифікатори артефактів оцінювання, а також криптографічне зв'язування записів у ланцюг та накладання цифрового підпису. Особливістю журналювання є доказовість: запис може бути незалежно верифікований, що знижує ризик підміни рішення позаланцюгового модуля.

Паралельно, починаючи з етапу формування ознак, виконується виділення транзакційних патернів як типових мотивів у графі транзакцій. Далі здійснюється агрегація характеристик патернів у часовому вікні, формуються інтегральні показники ризику патерна та визначається керувальна дія. Особливістю патерн-рівня є можливість виявляти повторювані ризикові сценарії та використовувати патерн-орієнтовані алерти для підсилення протокольного контролю.

Результатом роботи методу є ризик-оцінка транзакції, показник невизначеності прогнозу та віднесення транзакції до однієї із зон безпечності. На основі зони ризику формується протокольна директива передконсенсусної обробки, яка задає режим виконання перевірок і допуску транзакції до включення в блок. Додатково формується підписаний запис журналу з криптографічними зобов'язаннями на ознаки та артефакти оцінювання, що забезпечує перевірюваність і відтворюваність прийнятого рішення. Для транзакційних патернів результатом є агрегована оцінка ризику патерна та керувальна дія, яка може використовуватися для формування патерн-орієнтованих алертів і уточнення протокольної політики.

Набір експериментальних даних

У дослідженні використано «Elliptic Data Set» [15] – часовий граф транзакцій мережі Bitcoin, що є одним із найбільш уживаних відкритих еталонів для задач виявлення ризикових та нелегітимних транзакцій у блокчейн-мережах. Датасет представлено як орієнтований граф, у якому вузли відповідають транзакціям, а ребра потокам платежів між транзакціями. Набір даних містить 203 769 транзакцій (вузлів) та 234 355 зв'язків (ребер), а кожна транзакція описується 166 ознаками.

Ключовою властивістю датасету є часова розгортка: транзакції віднесені до дискретних часових кроків (time steps), що дозволяє моделювати передконсенсусну обробку як потік і будувати коректні схеми навчання та валідації з урахуванням часу (щоб уникати витоку інформації між періодами). У вихідній розмітці використано три стани міток: «illicit», «licit» і «unknown», тобто значна частка транзакцій є нерозміченою щодо легітимності. За описом датасету, близько 2% транзакцій мають мітку нелегітимних, близько 21% - легітимних, решта «unknown».

У базовому наборі «Elliptic Data Set» кожна транзакція описується 166 ознаками, однак у роботі використано розширений транзакційний профіль розмірності 188, який включає базові ознаки датасету та додаткові інженерні структурно-часові й контекстні характеристики, обчислені з графа транзакцій і часових міток для підтримки протокольного зонування ризику.

Експеримент, результати та дискусія

Експериментальна перевірка методу виконувалась у постановці позаланцюгового ризик-двигуна, який для транзакції формує ризик-оцінку нейромережевим модулем трансформерного типу [16], оцінює невизначеність прогнозу та виконує інженерне зонування ризику з формуванням протокольної директиви режиму передконсенсусної обробки. Для забезпечення відтворюваності рішення результати фіксувалися у вигляді підписаного запису журналу з криптографічним зобов'язанням на профіль ознак і зв'язуванням записів у ланцюг. Додатково оцінювалась протокольна ефективність зонування через навантаження на контури перевірки та через накладні витрати за результатами мікробенчмарку виконання сценаріїв STD, ENH і QUAR.

Для навчання та тестування використано розмічену частину графового набору транзакцій, у якому для кожної транзакції сформовано ознаковий профіль та часовий індекс. Після фільтрації нерозмічених прикладів отримано 46 564 транзакції з відомими мітками, що було розділено на тренувальну, валідаційну та тестову підвибірки (таблиця 1). Для врахування дисбалансу застосовано вагову корекцію позитивного класу при оптимізації.

Таблиця 1

Характеристики вибірки та розбиття даних

Параметр	Значення
Кількість розмічених транзакцій	46 564
Тренувальна підвибірка	26 905
Валідаційна підвибірка	2 989
Тестова підвибірка	16 670
Кількість ознак у профілі	188
Ваговий коефіцієнт для дисбалансу (pos_weight)	8.224

Нейромережевий модуль побудовано на трансформерній архітектурі для табличного профілю ознак [17]. Якість оцінювалась за ROC-AUC та AUPRC [18] як більш інформативними метриками в умовах суттєвого дисбалансу, а також за Precision, Recall і F_1 [19] при фіксованому порозі 0.5 для базового двійкового рішення (таблиця 2). Валідаційна динаміка протягом 20 епох демонструвала стабільне зростання ROC-AUC і AUPRC із максимумом на 17-й епосі, що свідчить про здатність моделі виділяти ризикові транзакції на основі поєднання структурних, часових і контекстних ознак [20].

Таблиця 2

Якість нейромережевого ризик-двигуна

Показник	Валідація (краще значення)	Тест
ROC-AUC	0.9849 (еп. 17)	0.9207
AUPRC	0.9514 (еп. 17)	0.7588
Precision при порозі 0.5	–	0.2914
Recall при порозі 0.5	–	0.8024
F1 при порозі 0.5	–	0.4276

У дискусійному аспекті важливо, що низька точність при порозі 0.5 не є аномалією для дисбалансних безпекових даних: базовий поріг не оптимізований під вартісні обмеження протоколу та не враховує вимогу мінімізувати помилкові блокування. Тому подальший рівень методу виконує не жорстку бінаризацію, а інженерне зонування, яке поєднує ризик-оцінку з оцінкою невизначеності прогнозу та переводить результат у протокольні режими керування.

Зонування реалізовано як політика віднесення транзакції до зон «White», «GRAY» і «Black» на основі ризик-оцінки та показника невизначеності прогнозу. Зона «White» відповідає стандартній обробці, зона «Gray» активує посилену перевірку, зона «Black» ініціює карантинний режим або відкладене включення. Порогові значення підбирались так, щоб зона «Black» мала високу точність і не створювала надлишкових помилкових блокувань, а зона «Gray» забезпечувала ескалацію більшості ризикових транзакцій на контур посиленого контролю. Отримані значення зонування та розподіл потоків за режимами наведено у таблиці 3.

Таблиця 3

Параметри зонування, розподіл потоків та якість ескалації

Показник	Значення
Поріг «BLACK» (t_black)	0.9791
Поріг «WHITE» (t_White)	0.7724
Межа невизначеності (u_max)	0.5399
«White», кількість транзакцій	11 411
«Gray», кількість транзакцій	4 882
«Black», кількість транзакцій	377
Частка навантаження на ENH+QUAR («Gray»+«Black»)	0.3155
Частка навантаження на QUAR («Black»)	0.0226
Precision для «Black»	0.9655
Recall для «Black»	0.3361
Recall для ескалації («Gray» ∪ «Black»)	0.8596
Precision для ескалації («Gray» ∪ «Black»)	0.1770
Частка ризикових, пропущених у «White»	0.1404

Висока точність зони «Black» означає, що автоматичний карантин використовується обмежено і майже не створює помилкових блокувань, що є критичним для керування транзакціями у реальній системі. Натомість зона «Gray» виконує роль буферної області для ескалації, в якій ризикові випадки відправляються

на посилену перевірку стандартними засобами, що пояснює нижчу точність ескалації загалом. Частка ризикових транзакцій, що потрапили у «White», становить 14.04%; це є прямим відображенням вибраної політики, зорієнтованої на обмеження навантаження на посилену верифікацію. З інженерної точки зору цей показник не є “помилкою метрики”, а параметром компромісу між безпекою та ресурсами, який підлягає керованому налаштуванню через «t_White», «t_black» та «u_max» залежно від вимог до допустимого ризику.

Для обґрунтування доцільності зонування в термінах комп’ютерної інженерії оцінено накладні витрати трьох сценаріїв обробки. Сценарій STD відповідав одиничному інференсу. Сценарій ENH реалізовував посилену перевірку через багаторазовий інференс із MC Dropout для оцінювання невизначеності. Сценарій QUAR доповнював ENH операціями журналювання з криптографічними зобов’язаннями та підписанням записів. Вимірювання виконано мікробенчмарком з синхронізацією GPU-викликів; ключовим для практики є режим пакетної обробки (таблиця 4).

Таблиця 4

Мікробенчмарк накладних витрат (B=256) і нормовані ваги вартості

Режим	Mean, ms/tx	p95, ms/tx	Нормована вартість (mean)
STD	0.0778	0.0795	1.000
ENH	0.5215	0.5322	6.702
QUAR	0.5815	0.6462	7.472

Вагові коефіцієнти вартості режимів посиленої перевірки та карантинного режиму визначалися експериментально шляхом мікробенчмарку виконання відповідних сценаріїв у позаланцюговому контурі. На рисунку 2 наведено виміряні значення середньої затримки та 95-го перцентиля, а також нормовані ваги «C_enh» і «C_quar», отримані відносно базового режиму STD у пакетному виконанні (світлина з розробленого програмного забезпечення).

	B	std_mean_s	std_p95_s	enh_mean_s	enh_p95_s	quar_mean_s	quar_p95_s	std_mean_per_tx_ms	enh_mean_per_tx_ms	quar_mean_per_tx_ms	C_enh_mean	C_quar_mean	C_enh_p95	C_quar_p95
0	1	0.001028	0.001144	0.007081	0.007522	0.008366	0.012494	1.028284	7.080997	8.365959	6.886229	8.135847	6.575261	10.922258
1	16	0.002037	0.002513	0.010325	0.013867	0.009772	0.010225	0.127330	0.645312	0.610748	5.068017	4.796567	5.518188	4.068828
2	256	0.019921	0.020360	0.133504	0.136252	0.148853	0.165420	0.077816	0.521501	0.581456	6.701757	7.472236	6.692186	8.124794

Рис. 2. Результати мікробенчмарку накладних витрат режимів передконсенсусної обробки STD, ENH і QUAR у пакетному виконанні

На основі фактичного розподілу потоків за зонами та нормованих ваг вартості обчислено середню вартість передконсенсусної обробки у ризик-орієнтованому режимі. Для тестового розподілу частки «White», «Gray» і «Black» становили 0.6845, 0.2929 і 0.0226 відповідно, що дало середню нормовану вартість 2.816 на транзакцію. Відносно політики суцільної посиленої верифікації це відповідає економії 57.98% і зменшенню витрат у 2.38 раза, при цьому зберігається ескалація 85.96% ризикових транзакцій на контури підвищеного контролю. Такий результат підтверджує інженерну доцільність зонування як механізму адаптивного перерозподілу ресурсів перевірки, а не як допоміжної метрики класифікації.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У роботі розроблено та експериментально обґрунтовано апаратно-програмний метод класифікації транзакцій і окремих транзакційних патернів нейромережевими засобами за рівнем безпечності у системах блокчейн, що реалізується у виділеному позаланцюговому контурі та інтегрується з вузлом мережі на рівні керувальних директив передконсенсусної обробки без модифікації базового консенсусу. Метод формує транзакційний профіль як поєднання структурних, часових і контекстних ознак, виконує нейромережеве оцінювання ризику трансформерною архітектурою та доповнює прогноз оцінкою невизначеності методом Monte Carlo Dropout, що забезпечує керованість ризик-орієнтованого зонування та протокольної маршрутизації.

Експериментальну перевірку здійснено на часовому графі транзакцій «Elliptic Data Set» для мережі Bitcoin із використанням розміченої підвибірки 46 564 транзакцій та профілю ознак розмірності 188. Показано, що нейромережевий ризик-двигун забезпечує високу роздільну здатність у дисбалансній постановці задачі, що підтверджується значеннями ROC-AUC 0.9207 та AUPRC 0.7588 на тестовій вибірці, а також демонструє придатність до протокольного використання результатів за рахунок подальшого інженерного зонування замість жорсткої бінаризації.

Запропоновано та перевірено політику зонування ризику на три зони «White», «Gray» і «Black», у якій зона «Black» орієнтована на максимізацію точності автоматичного карантинного рішення, а зона «Gray» виконує роль керованої ескалації на посилену перевірку стандартними засобами. За підбраними порогами зонування підтверджено високу точність зони «Black» на рівні 0.9655 при обмеженому навантаженні на карантинний режим 0.0226, тоді як сумарна ескалація «Gray» в об’єднанні «Black» забезпечує виявлення

0.8596 ризикових транзакцій із контролем загального навантаження на підвищені режими перевірки 0.3155. Отримані результати інтерпретуються як інженерний компроміс між рівнем ризику, пропускною здатністю та ресурсами передконсенсусної верифікації, що може бути керовано налаштований через параметри «t_white», «t_black» та «u_max» відповідно до політики безпеки вузла.

Для обґрунтування протокольної доцільності методу в термінах комп'ютерної інженерії виконано мікробенчмарк накладних витрат режимів STD, ENH і QUAR у пакетному виконанні, на основі якого визначено нормовані ваги вартості C_enh = 6.702 та C_quar = 7.472 відносно STD. Показано, що за фактичним розподілом зон середня нормована вартість ризик-орієнтованої передконсенсусної обробки становить 2.816 на транзакцію та забезпечує економію 57.98% відносно політики суцільної посиленої верифікації, що підтверджує ефективність адаптивного перерозподілу ресурсів перевірки без ускладнення базового протокольного ядра.

Забезпечено доказовість і відтворюваність рішень позаланцюгового контуру шляхом журналювання результатів оцінювання у вигляді криптографічно зв'язаних записів із зобов'язанням на ознаки та артефакти оцінювання і цифровим підписом із незалежною перевіркою коректності. Така фіксація дозволяє відокремити функції обчислення ризику від базових механізмів блокчейну, зберігаючи можливість аудиту, перевірки та трасування рішень у критичних сценаріях керування транзакціями.

Література

1. Haider M. Z., Noreen T., Salman M. Blockchain Fraud Detection Using Ensemble Graph Neural Networks. *Journal of Artificial Intelligence Research*. 2025. Т. 2, № 2. С. 24–41. URL: https://doi.org/10.70891/jair.2025.080018
2. Anomalous Node Detection in Blockchain Networks Based on Graph Neural Networks / Z. Chang et al. *Sensors*. 2024. Vol. 25, no. 1. P. 1. URL: https://doi.org/10.3390/s25010001
3. Zhao Z., Wang J., Wei J. Graph-Neural-Network-Based Transaction Link Prediction Method for Public Blockchain in Heterogeneous Information Networks. *Blockchain: Research and Applications*. 2025. P. 100265. URL: https://doi.org/10.1016/j.bcra.2024.100265
4. Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions / H. F. Atlam et al. *Electronics*. 2024. Vol. 13, no. 17. P. 3568. URL: https://doi.org/10.3390/electronics13173568
5. A secure and efficient log storage and query framework based on blockchain / W. Li et al. *Computer Networks*. 2024. P. 110683. URL: https://doi.org/10.1016/j.comnet.2024.110683
6. Liu Z., Wu H. A framework for dynamic blockchain-based data auditing. *International Journal of Accounting Information Systems*. 2025. Vol. 56. P. 100737. URL: https://doi.org/10.1016/j.accinf.2025.100737
7. Abbas Jasim Al-Hchaimi A., Khalifa M. A., El-Shafai W. Explainable AI With Imbalanced Learning Strategies for Blockchain Transaction Fraud Detection. *Engineering Reports*. 2026. Vol. 8, no. 1. URL: https://doi.org/10.1002/eng2.70545
8. Wang C., Nie C., Liu Y. Evaluating Supervised Learning Models for Fraud Detection: A Comparative Study of Classical and Deep Architectures on Imbalanced Transaction Data. *Advances in Economics, Business and Management Research*. Dordrecht, 2025. P. 613–624. URL: https://doi.org/10.2991/978-94-6463-835-6_65
9. Sheng Z., Song L., Wang Y. Dynamic Feature Fusion: Combining Global Graph Structures and Local Semantics for Blockchain Phishing Detection. *IEEE Transactions on Network and Service Management*. 2025. P. 1. URL: https://doi.org/10.1109/tnsm.2025.3576130
10. Extending On-chain Trust to Off-chain - Trustworthy Blockchain Data Collection using Trusted Execution Environment (TEE) / C. Liu et al. *IEEE Transactions on Computers*. 2022. P. 1. URL: https://doi.org/10.1109/tc.2022.3148379
11. Cryptocurrency Transaction Fraud Detection Based on Imbalanced Classification With Interpretable Analysis / P. Yin et al. *International Journal of Intelligent Information Technologies*. 2024. Vol. 20, no. 1. P. 1–21. URL: https://doi.org/10.4018/ijiit.357696
12. Deep learning-based blockchain framework for fraud detection using multilevel supervision in hierarchical generative hashing / I. K. A. Hamdan et al. *International Journal of Machine Learning and Cybernetics*. 2026. Vol. 17, no. 1. URL: https://doi.org/10.1007/s13042-025-02916-2
13. Structural-temporal mining for motif-level anomaly detection in dynamic graphs / C. Huang et al. *Knowledge-Based Systems*. 2025. Vol. 325. P. 113962. URL: https://doi.org/10.1016/j.knosys.2025.113962
14. Taher S. S., Ameen S. Y., Ahmed J. A. Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach. *Engineering, Technology & Applied Science Research*. 2024. Vol. 14, no. 1. P. 12822–12830. URL: https://doi.org/10.48084/etasr.6641
15. Elliptic Data Set. *Kaggle*. URL: https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
16. Молчанова М., Мазурець О., Шурипа М. Об'єктно-орієнтований підхід до нейромережевого виявлення та відстеження БПЛА з використанням хмарних технологій. *Наука і техніка сьогодні*. 2025. № 9(50). URL: https://doi.org/10.52058/2786-6025-2025-9(50)-1346-1360

17. Похитун А.В., Мазурець О.В., Дидо Р.А., Молчанова М.О. Програмна архітектура для нейромережевого виявлення модифікованих фотографій облич людей. *Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки.* 2025. №3. Т.2. С. 493-500. https://doi.org/10.31891/2307-5732-2025-353-68

18. A Closer Look at AUROC and AUPRC under Class Imbalance / G. Angelotti et al. *Advances in Neural Information Processing Systems 37*, Vancouver, BC, Canada, 10–15 December 2024. San Diego, California, USA, 2024. P. 44102–44163. URL: https://doi.org/10.52202/079017-1400

19. Молчанова М.О., Дідур В.О., Мазурець О.В., Тищенко О.О., Залуцька О.О. Інформаційна технологія використання хмарних обчислень для класифікації залишків зруйнованих будівель засобами нейронних мереж за візуальними даними з безпілотних літальних апаратів. *Науковий журнал «Наука і техніка сьогодні».* 2025. №4 (45). С. 1259-1272. https://doi.org/10.52058/2786-6025-2025-4(45)-1259-1272

20. Ethereum Phishing Scam Detection Based on Data Augmentation Method and Hybrid Graph Neural Network Model / Z. Chen et al. *Sensors*. 2024. Vol. 24, no. 12. P. 4022. URL: https://doi.org/10.3390/s24124022

References

1. Haider, M. Z., Noreen, T., & Salman, M. (2025). Blockchain fraud detection using ensemble graph neural networks. Journal of Artificial Intelligence Research, 2(2), 24–41. https://doi.org/10.70891/jair.2025.080018

2. Chang, Z., et al. (2024). Anomalous node detection in blockchain networks based on graph neural networks. Sensors, 25(1), 1. https://doi.org/10.3390/s25010001

3. Zhao, Z., Wang, J., & Wei, J. (2025). Graph-neural-network-based transaction link prediction method for public blockchain in heterogeneous information networks. Blockchain: Research and Applications, 100265. https://doi.org/10.1016/j.bcra.2024.100265

4. Atlam, H. F., et al. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. Electronics, 13(17), 3568. https://doi.org/10.3390/electronics13173568

5. Li, W., et al. (2024). A secure and efficient log storage and query framework based on blockchain. Computer Networks, 110683. https://doi.org/10.1016/j.comnet.2024.110683

6. Liu, Z., & Wu, H. (2025). A framework for dynamic blockchain-based data auditing. International Journal of Accounting Information Systems, 56, 100737. https://doi.org/10.1016/j.accinf.2025.100737

7. Abbas Jasim Al-Hchaimi, A., Khalifa, M. A., & El-Shafai, W. (2026). Explainable AI with imbalanced learning strategies for blockchain transaction fraud detection. Engineering Reports, 8(1). https://doi.org/10.1002/eng2.70545

8. Wang, C., Nie, C., & Liu, Y. (2025). Evaluating supervised learning models for fraud detection: A comparative study of classical and deep architectures on imbalanced transaction data. Advances in Economics, Business and Management Research, 613–624. https://doi.org/10.2991/978-94-6463-835-6_65

9. Sheng, Z., Song, L., & Wang, Y. (2025). Dynamic feature fusion: Combining global graph structures and local semantics for blockchain phishing detection. IEEE Transactions on Network and Service Management, 1. https://doi.org/10.1109/TNSM.2025.3576130

10. Liu, C., et al. (2022). Extending on-chain trust to off-chain—Trustworthy blockchain data collection using trusted execution environment (TEE). IEEE Transactions on Computers, 1. https://doi.org/10.1109/TC.2022.3148379

11. Yin, P., et al. (2024). Cryptocurrency transaction fraud detection based on imbalanced classification with interpretable analysis. International Journal of Intelligent Information Technologies, 20(1), 1–21. https://doi.org/10.4018/ijiit.357696

12. Hamdan, I. K. A., et al. (2026). Deep learning-based blockchain framework for fraud detection using multilevel supervision in hierarchical generative hashing. International Journal of Machine Learning and Cybernetics, 17(1). https://doi.org/10.1007/s13042-025-02916-2

13. Huang, C., et al. (2025). Structural-temporal mining for motif-level anomaly detection in dynamic graphs. Knowledge-Based Systems, 325, 113962. https://doi.org/10.1016/j.knosys.2025.113962

14. Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced fraud detection in blockchain transactions: An ensemble learning and explainable AI approach. Engineering, Technology & Applied Science Research, 14(1), 12822–12830. https://doi.org/10.48084/etasr.6641

15. Elliptic. (n.d.). Elliptic data set. Kaggle. Retrieved February 19, 2026, from https://www.kaggle.com/datasets/ellipticco/elliptic-data-set

16. Молчанова, М., Мазурець, О., & Шурипа, М. (2025). Об'єктно-орієнтований підхід до нейромережевого виявлення та відстеження БПЛА з використанням хмарних технологій. Наука і техніка сьогодні, 9(50). https://doi.org/10.52058/2786-6025-2025-9(50)-1346-1360

17. Похитун, А. В., Мазурець, О. В., Дидо, Р. А., & Молчанова, М. О. (2025). Програмна архітектура для нейромережевого виявлення модифікованих фотографій облич людей. Вісник Хмельницького національного університету. Серія: Технічні науки, 3(2), 493–500. https://doi.org/10.31891/2307-5732-2025-353-68

18. Angelotti, G., et al. (2024). A closer look at AUROC and AUPRC under class imbalance. In Advances in Neural Information Processing Systems 37 (pp. 44102–44163). https://doi.org/10.52202/079017-1400

19. Молчанова, М. О., Дідур, В. О., Мазурець, О. В., Тищенко, О. О., & Залуцька, О. О. (2025). Інформаційна технологія використання хмарних обчислень для класифікації залишків зруйнованих будівель засобами нейронних мереж за візуальними даними з безпілотних літальних апаратів. Наука і техніка сьогодні, 4(45), 1259–1272. https://doi.org/10.52058/2786-6025-2025-4(45)-1259-1272

20. Chen, Z., Liu, S.-Z., Huang, J., Xiu, Y.-H., Zhang, H., & Long, H.-X. (2024). Ethereum phishing scam detection based on data augmentation method and hybrid graph neural network model. Sensors, 24(12), 4022. https://doi.org/10.3390/s24124022