УДК 004
DOI https://doi.org/10.32782/2663-5941/2026.1.2/03

Аскеров В.В.
https://orcid.org/0009-0009-1176-9812
Хмельницький національний університет

ЗАСОБИ КЕРУВАННЯ ЗАХИЩЕНИМИ ТРАНЗАКЦІЯМИ В БЛОКЧЕЙН-СИСТЕМАХ НА ОСНОВІ НЕЙРОМЕРЕЖЕВОЇ ОЦІНКИ РИЗИКУ ТРАНЗАКЦІЙ

У статті запропоновано архітектуру керування захищеними транзакціями в блокчейн-системах, що поєднує штатні ончейн-компоненти (формування транзакції, мемпул, консенсус, блоки та реєстр) із довіреним позаланцюговим контуром нейромережевого оцінювання ризику. Метою підходу є зниження прикладних ризиків (шахрайство, відмивання коштів, аномальні ланцюжки адрес) без модифікації базового алгоритму консенсусу та без порушення детермінізму мережі. Запропоновано метод багаторівневої маршрутизації й допуску транзакцій за трьома зонами ризику White, Gray і Black з урахуванням невизначеності прогнозу: для White застосовується стандартна передконсенсусна валідація, для Gray – посилена перевірка і відкладене включення, для Black – блокування або карантин. Для забезпечення довіри до позаланцюгових рішень розроблено механізм криптографічно верифікованої фіксації метаданих (хеші ознак, версій моделі та політик, хеш пояснення, часова мітка) з підписом довіреного оракула і прив'язкою до транзакції в ланцюгу. Нейромережева модель формує ризик-скоринг на основі структурних, часових і контекстних ознак; локальна інтерпретація (Integrated Gradients) виділяє ключові фактори впливу для аудиту. Експерименти на Elliptic Bitcoin Dataset із часовим поділом вибірок показали ROC-AUC 0.854 на тесті та AUPRC 0.815 на валідації; для зони Black (стабільні рішення) отримано Precision 0.5912 і Recall 0.4858. Результати підтверджують практичну придатність запропонованого контурного підходу для адаптивного керування транзакціями та подальшого розслідування інцидентів. Пороги зонування twhite, tblack та uтах визначаються на валідаційній вибірці й задають компроміс між швидкістю допуску та часткою хибних рішень. Підписаний журнал рішень робить позаланцюговий висновок відтворюваним і придатним для аудиту мережі.

Ключові слова: *керування транзакціями, блокчейн, класифікація ризику транзакцій, нейромережева модель, позаланцюговий контур, пояснюваний штучний інтелект, Elliptic Bitcoin Dataset.*

Постановка проблеми. Блокчейн-системи широко застосовуються як базова інфраструктура для обробки транзакцій у фінансових сервісах, міжорганізаційних реєстрах, ланцюгах постачання та цифрових платформах обміну даними [1, с. 94, 2, с. 213]. Незважаючи на криптографічну цілісність блоків і незмінність записів, безпечність виконання транзакцій у таких системах не є гарантованою, оскільки значна частина ризиків формується на прикладному рівні у вигляді шахрайських сценаріїв, маніпулятивних транзакційних ланцюжків, відмивання коштів та аномальних патернів взаємодії адрес [3, с. 83]. Базові механізми консенсусу забезпечують узгодження стану розподіленого реєстру, проте не виконують оцінювання ризику транзакції як події до її включення в блок.

Існуючі підходи до підвищення безпеки транзакцій у блокчейн-мережах здебільшого ґрунтуються на статичних правилах, евристиках, чорних списках адрес та порогових значеннях окремих показників. Такі методи є відносно простими для реалізації, однак вони не забезпечують достатньої гнучкості в умовах різноманітних транзакційних сценаріїв, нерівномірного розподілу класів і дрейфу даних [4, с. 1]. Крім того, застосування жорстких правил допуску призводить або до зростання кількості хибнопозитивних спрацювань і затримок обробки транзакцій, або до пропуску потенційно небезпечних операцій.

Використання методів машинного та глибокого навчання для класифікації транзакцій дозволяє враховувати складні взаємозв'язки між структурними, часовими та контекстними ознаками

[5, с. 2]. Проте більшість відомих рішень обмежується бінарною класифікацією транзакцій без урахування невизначеності прогнозу та без інтеграції результатів аналізу в механізми керування виконанням транзакцій. Окремою проблемою є забезпечення довіри до результатів нейромережевого аналізу: виконання моделей безпосередньо у блокчейн-середовищі є обмеженим, тоді як позаланцюгове оцінювання потребує механізмів фіксації, верифікації та відтворюваності прийнятих рішень [6, с. 3].

Таким чином, актуальною є науково-прикладна проблема розроблення архітектури та методів керування захищеними транзакціями в блокчейн-системах, які на основі нейромережевої оцінки ризику транзакцій забезпечують багаторівневу класифікацію ризику, підтримують адаптивне коригування протоколу виконання транзакцій без модифікації базового консенсусу, а також гарантують цілісність, перевірюваність і аудит результатів позаланцюгового аналізу.

Аналіз останніх досліджень і публікацій. Упродовж останніх років інтенсивно розвиваються методи машинного та глибокого навчання для виявлення ризикованих і шахрайських транзакцій у блокчейн-мережах. Типовою постановкою задачі є класифікація транзакцій або адрес на «легітимні» та «нелегітимні» за сукупністю графових, часових і контекстних ознак, часто в умовах істотної нерівномірності класів і дрейфу даних. Водночас більшість підходів фокусується на досягненні метрик якості бінарного детектора, тоді як інженерні вимоги керування транзакціями (багаторівнева політика ризику, оцінювання невизначеності, відтворюваність і верифікованість позаланцюгових рішень) висвітлені неповно.

Окремий напрям сучасних робіт становлять графові нейромережі для задач детекції підозрілих рахунків і транзакцій у мережах криптовалют. Так, у роботі [7] запропоновано модель LineMVGNN, орієнтовану на виявлення підозрілих сутностей у спрямованих транзакційних графах та врахування «потоку коштів» через спеціальні механізми поширення інформації. Ці результати підтверджують доцільність глибоких моделей для виявлення складних схем, однак у таких постановках зазвичай переважає метрика якості детекції як кінцева ціль, тоді як інженерна складова контур керування транзакціями та криптографічно верифікована фіксація позаланцюгового висновку як артефакту аудиту не є центральним предметом дослідження.

У статті [8] розглядаються підходи до детекції фінансових шахрайських сценаріїв у блокчейн-мережах з опорою на ознаки транзакцій і навчання моделей для підвищення точності виявлення. Такі роботи корисні як підтвердження того, що комбінація структурних і поведінкових характеристик дійсно підсилює детектування, проте типово не ставлять за мету інженерну інтеграцію результату в протокол керування транзакціями через багаторівневу політику ризику та не формалізують криптографічно верифіковану фіксацію позаланцюгового рішення, що критично для аудиту та розслідувань.

У статті [9] запропоновано підхід Robust Recurrent Graph Convolutional Network для послідовного прогнозування нелегітимних транзакцій у криптовалютних графах. Робота використовує графові та часові ознаки і враховує динаміку сценаріїв, однак постановка зводиться до задачі «детектор» і не розгортається в інженерний контур керування транзакціями: відсутні формалізовані ризик-зони для маршрутизації («білий», «сірий», «чорний» / «White», «Gray», «Black»), немає явного оцінювання невизначеності як підстави для спрямування у зону перевірки.

Однак навіть у таких узагальненнях головний фокус зберігається на моделях детекції та їхніх метриках, тоді як питання багаторівневої політики допуску, оцінювання невизначеності прогнозу та криптографічно перевірюваного журналювання рішень позаланцюгового ризик-аналізу розглядаються фрагментарно або як перспективні напрями.

Таким чином, аналіз публікацій останніх років показує, що наявні рішення здебільшого: (1) обмежуються бінарною детекцією «ризик» або «не ризик» без політики «White», «Gray», «Black» для керування допуском; (2) не вводять явного критерію невизначеності для відсікання нестабільних прогнозів і маршрутизації на посилену перевірку; (3) рідко забезпечують криптографічно верифіковану фіксацію позаланцюгових рішень із прив'язкою до версій ознак і моделі; (4) не пов'язують результат ML-оцінки з інженерною схемою керування транзакціями без втручання в механізми консенсусу. Саме ці обмеження усуває запропонований у статті підхід, поєднуючи нейромережевий ризик-скоринг, оцінювання невизначеності, локальне пояснення та верифіковане журналювання результатів для подальшого аудиту і застосування політик.

Постановка завдання. Метою статті є розроблення та дослідження архітектури і методів керування захищеними транзакціями в блокчейн-системах на основі нейромережевої оцінки ризику

транзакцій, які забезпечують багаторівневу класифікацію ризику, адаптивне коригування протоколу виконання транзакцій без модифікації механізмів консенсусу, а також криптографічно верифіковану фіксацію результатів позаланцюгового аналізу для подальшого аудиту та узгодженого застосування політик безпеки.

Для досягнення поставленої мети необхідно: сформувати модель архітектури апаратно-програмної блокчейн-системи із позаланцюговим довіреним контуром нейромережевого оцінювання ризику та механізмом адаптивного коригування протоколу виконання транзакцій; удосконалити протокол керування транзакціями шляхом введення порядку допуску і маршрутизації за ризик-класами та режимів передконсенсусної обробки і валідації на рівні політик виконання; удосконалити метод підтримки цілісності та довіри до результатів позаланцюгового аналізу шляхом фіксації версій ознак, моделі та правил із криптографічним зв'язуванням метаданих у блоці; розробити метод нейромережевої класифікації транзакцій і транзакційних патернів за рівнем безпечності на основі структурних, часових і контекстних ознак із фіксацією результату у вигляді верифікованого підписаного запису журналу.

Виклад основного матеріалу. Для реалізації запропонованих методів керування захищеними транзакціями розроблено архітектуру блокчейн-системи, яка поєднує базові механізми ончейн-обробки транзакцій із довіреним позаланцюговим контуром нейромережевого оцінювання ризику. Такий підхід дозволяє виконувати складний аналіз транзакцій без втручання у механізми консенсусу блокчейн-мережі та без порушення її детермінізму, зберігаючи при цьому можливість адаптивного керування процесом виконання транзакцій. Запропонована архітектура системи керування захищеними транзакціями наведена на рисунку 1.

Архітектура складається з двох логічно відокремлених, але функціонально взаємопов'язаних частин: ончейн-компонентів блокчейн-мережі та позаланцюгового довіреного контуру оцінювання ризику. Ончейн-частина включає стандартні елементи блокчейн-системи – формування транзакції, мемпул, механізми консенсусу, формування блоків та розподілений реєстр. При цьому базові механізми консенсусу не модифікуються і використовуються у штатному режимі.

Позаланцюговий контур оцінювання ризику реалізує попередній аналіз транзакції до її включення в блок. На цьому етапі формується вектор транзакційних ознак, після чого нейромережева модель визначає ризик-клас транзакції та оцінює стабільність отриманого прогнозу [10, с. 438]. На основі результатів нейромережевого аналізу застосовуються політики керування транзакціями, які визначають режим їх подальшої обробки: стандартну валідацію для транзакцій низького ризику, посилену перевірку для транзакцій із невизначеним або проміжним рівнем

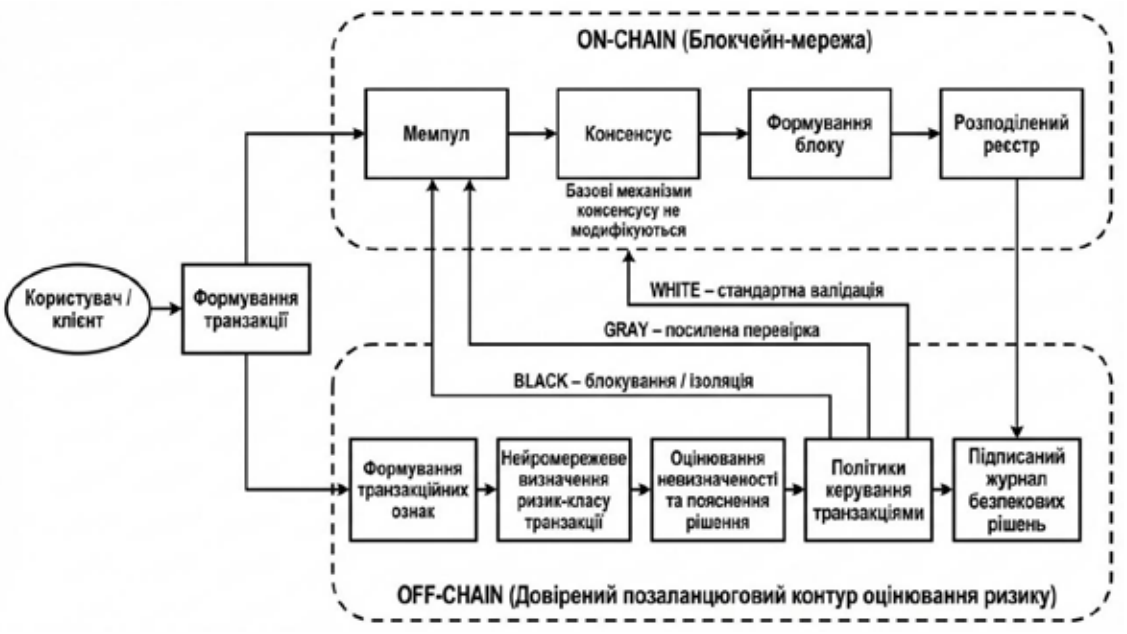

Рис. 1. Архітектура керування захищеними транзакціями в блокчейн-системі з позаланцюговим контуром нейромережевого оцінювання ризику

ризику, а також блокування чи ізоляцію транзакцій із високим рівнем ризику.

Важливою особливістю архітектури є фіксація результатів позаланцюгового аналізу у вигляді підписаного журналу безпекових рішень [11, с. 4]. Такий журнал містить метадані щодо використаних ознак, версії нейромережевої моделі, визначеного ризик-класу та застосованих політик, що забезпечує криптографічну перевірюваність, відтворюваність і можливість подальшого аудиту прийнятих рішень. Включення цього механізму дозволяє інтегрувати результати інтелектуального аналізу в процес керування транзакціями без порушення цілісності та незмінності блокчейн-реєстру.

Запропонований метод керування захищеними транзакціями ґрунтується на використанні результатів нейромережевого оцінювання ризику для адаптивного коригування порядку допуску та маршрутизації транзакцій у блокчейн-мережі. На відміну від традиційних підходів, у яких усі транзакції обробляються за єдиним сценарієм передконсенсусної валідації, запропонований метод вводить диференційовані режими обробки залежно від визначеного ризик-класу транзакції без модифікації базового алгоритму консенсусу. Схема реалізації методу адаптивного керування транзакціями наведена на рисунку 2.

Після формування транзакції користувачем та побудови вектора транзакційних ознак у довіреному позаланцюговому контурі нейромережева модель визначає ризик-клас транзакції. Залежно від отриманого результату транзакція відноситься до одного з трьох класів: низького ризику (White), зони перевірки (Gray) або високого ризику (Black). Для кожного класу застосовується окрема політика керування виконанням транзакції.

Для транзакцій класу «White» використовується стандартний режим обробки: транзакція отримує типовий пріоритет, проходить звичайну передконсенсусну валідацію та безпосередньо включається до мемпулу для подальшої обробки механізмом консенсусу. Такий режим забезпечує мінімальні затримки обробки та не впливає на пропускну здатність мережі.

Транзакції, віднесені до класу «Gray», характеризуються підвищеною невизначеністю нейромережевого прогнозу або проміжним рівнем ризику. Для них застосовується режим посиленої перевірки, що може включати знижений пріоритет обробки, додаткові перевірки політик допуску або відкладене включення до мемпулу. Такий підхід дозволяє зменшити ймовірність хибних автоматичних рішень і спрямувати потенційно проблемні транзакції на додатковий контроль без їх негайного блокування.

Для транзакцій класу «Black» застосовується обмежувальний режим керування: транзакція блокується або ізолюється на етапі допуску, забороняється її включення до мемпулу, а також може ініціюватися процедура карантину або аудиту. Це

Рис. 2. Метод адаптивної маршрутизації та допуску транзакцій за ризик-класами без зміни механізму консенсусу

дозволяє запобігти включенню явно небезпечних транзакцій до блокчейн-реєстру ще до запуску механізмів консенсусу.

Ключовою особливістю запропонованого методу є те, що всі зміни у виконанні транзакцій реалізуються на рівні політик допуску та маршрутизації, тоді як алгоритм консенсусу вузлів блокчейн-мережі залишається незмінним. Це забезпечує сумісність методу з існуючими блокчейн-платформами та дозволяє інтегрувати його без порушення детермінізму і властивостей розподіленого реєстру.

Однією з ключових інженерних проблем інтеграції нейромережевого аналізу в блокчейн-системи є забезпечення довіри до результатів позаланцюгового прийняття рішень [12, с. 15]. Хоча блокчейн гарантує криптографічну цілісність транзакцій і блоків, результати аналізу ризику, виконаного поза ланцюгом, за відсутності формалізованого механізму фіксації не мають властивостей відтворюваності, перевірюваності та аудиту [13, с. 78].

Для усунення цього обмеження запропоновано метод підтримки цілісності та довіри до результатів обробки транзакцій, який доповнює ланцюг прийняття рішення щодо виконання транзакції етапом криптографічно верифікованої фіксації результатів позаланцюгового аналізу. Схема методу наведена на рисунку 3.

Запропонований метод передбачає логічне розділення процесу на три взаємопов'язані компоненти: довірене позаланцюгове середовище прийняття рішення, модуль формування та криптографічного зв'язування запису рішення, а також блокчейн-мережу як незмінний реєстр.

На першому етапі у довіреному позаланцюговому середовищі формується повний набір даних рішення, який включає результат нейромережевої класифікації транзакції за рівнем ризику («White», «Gray» або «Black»), використані транзакційні ознаки, ідентифікатори версій моделі та політики, а також локальне пояснення рішення у вигляді скороченого резюме (наприклад, ключові ознаки впливу). Цей набір даних відображає контекст, у межах якого було прийняте рішення, і є необхідним для подальшого відтворення або аудиту.

На другому етапі виконується формування структурованого запису рішення, який містить ідентифікатор транзакції, визначений ризик-клас, криптографічні зобов'язання на основі хешів для набору ознак, версій моделі та політик, хеш пояснення рішення, часову мітку та посилання на попередній запис. Таким чином утворюється логічний ланцюг рішень, який відображає історію прийняття рішень щодо транзакцій.

Далі сформований запис проходить етап криптографічного хешування, після чого підписується цифровим підписом довіреного оракула. Резуль-

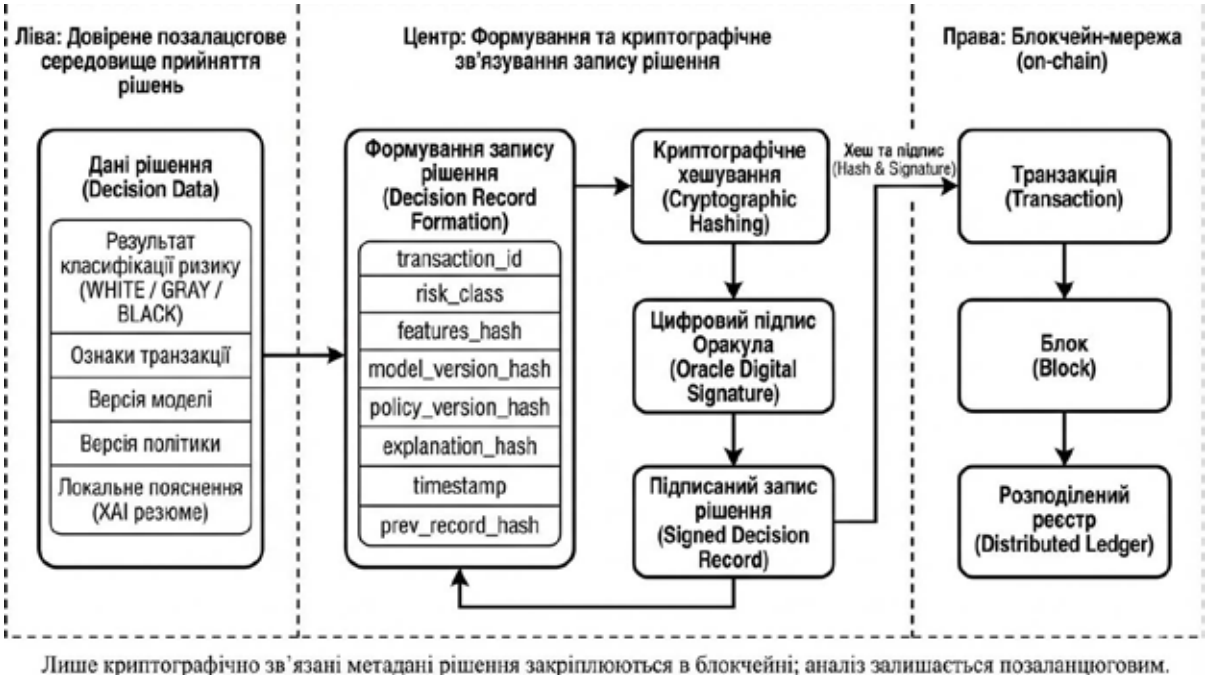

Рис. 3. Метод формування та криптографічного зв'язування запису позаланцюгового рішення з блокчейн-транзакцією

татом є підписаний запис рішення, який гарантує автентичність джерела, цілісність даних та неможливість непомітної модифікації результатів аналізу.

На третьому етапі до блокчейн-мережі інтегруються лише криптографічно зв'язані метадані рішення – хеш та цифровий підпис. Повний зміст аналізу залишається поза ланцюгом, що дозволяє зберегти обчислювальну ефективність та конфіденційність, водночас забезпечуючи можливість перевірки коректності рішення будь-яким учасником мережі.

Принциповою особливістю запропонованого методу є те, що блокчейн використовується не для виконання нейромережевого аналізу, а як незмінний реєстр криптографічних зобов'язань щодо результатів цього аналізу. Це дозволяє поєднати переваги позаланцюгових обчислень із властивостями довіри та відтворюваності, притаманними блокчейн-системам.

Таким чином, удосконалений метод підтримки цілісності та довіри забезпечує можливість перевірки того, що рішення щодо виконання транзакції було прийняте з використанням конкретної версії моделі, визначеного набору ознак і політик, без необхідності повторного виконання нейромережевого аналізу у блокчейн-середовищі. Це створює технічні передумови для прозорого аудиту, розслідування інцидентів та узгодженого застосування політик керування транзакціями у розподілених блокчейн-системах.

Запропонований метод нейромережевої класифікації транзакцій за рівнем безпечності базується на опрацюванні структурних, часових і контекстних ознак транзакції у довіреному позаланцюговому контурі аналізу. Схема методу наведена на рисунку 4.

На вхід методу подається вектор ознак, сформований на основі графової структури мережі транзакцій, статистики попередніх операцій, часових характеристик та контекстних метаданих. У межах позаланцюгового модуля нейромережева модель виконує скоринг ризику транзакції, формуючи узагальнену оцінку її небезпечності.

Для підвищення надійності прийняття рішення додатково здійснюється оцінювання невизначеності прогнозу, що дозволяє відокремити стабільні рішення від прикордонних випадків [14, с. 498]. Паралельно застосовується механізм локального пояснення рішення, який визначає ключові ознаки та напрям їх впливу на результат класифікації, забезпечуючи інтерпретованість моделі на рівні окремої транзакції.

Результатом роботи методу є віднесення транзакції до одного з трьох рівнів ризику: низького ризику, зони перевірки або високого ризику. Відповідно до визначеного ризик-класу формується керуюча дія для процесу обробки транзакції, яка реалізується через політики маршрутизації: стандартну валідацію, посилену перевірку або блокування чи карантин транзакції. Таким чином, метод забезпечує адаптивне керування виконанням транзакцій без модифікації механізмів консенсусу блокчейн-мережі.

Дослідження ефективності методу нейромережевої класифікації транзакцій виконано на «Elliptic Bitcoin Dataset» [15] із часовим поділом на навчальну, валідаційну та тестову вибірки,

Рис. 4. Метод нейромережевої класифікації транзакцій за рівнем безпечності

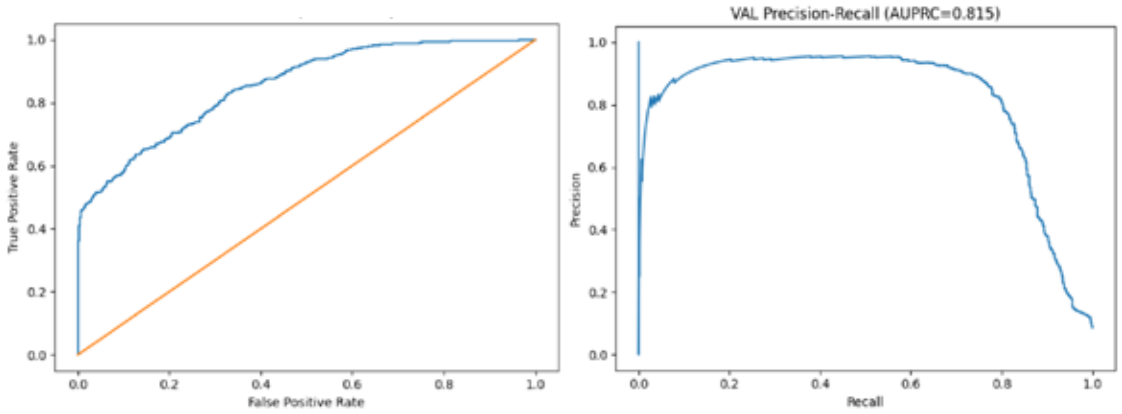

Рис. 5. ROC- та Precision-Recall криві нейромережевої моделі

що дозволяє врахувати дрейф даних і наблизити перевірку до умов реальної експлуатації [16]. Якість моделі оцінювали за ROC-AUC та AUPRC як найбільш інформативними метриками для задач із дисбалансом класів. На тестовій вибірці отримано ROC-AUC = 0.854, а на валідаційній вибірці AUPRC = 0.815 (рисунок 5), яке використовувалося для налаштування порогів зонування. Це підтверджує здатність моделі відокремлювати ризиковані транзакції за прийнятного рівня хибнопозитивних спрацювань.

Параметри політики багаторівневої маршрутизації визначалися на валідаційній вибірці для стабільних прогнозів: t_white=0.025479, t_black=0.419934, u_max=0.101192. Отримані розподіли за зонами ризику узгоджуються з інженерною логікою керування: зона «White» характеризується мінімальною часткою нелегітимних транзакцій, зона «Gray» концентрує прикордонні випадки, а зона «Black» має підвищену частку нелегітимних транзакцій; на тесті для «Black» (стабільні рішення) отримано Precision = 0.5912 та Recall = 0.4858. Відмінність значень Precision на тесті порівняно з валідаційною вибіркою зумовлена часовим дрейфом даних і складнішими умовами узагальнення [17]. Додатково локальне пояснення (Integrated Gradients) показало домінування структурно-контекстних ознак у формуванні рішення, що узгоджується з природою шахрайських транзакційних патернів [18].

Висновки. У роботі запропоновано архітектуру керування захищеними транзакціями в блокчейн-системі з довіреним позаланцюговим контуром нейромережевого оцінювання ризику, що не потребує модифікації механізмів консенсусу. Розроблено метод багаторівневої класифікації ризику з виділенням зон «White», «Gray» та «Black» і відповідними політиками допуску та маршрутизації транзакцій, які зменшують ризик хибних автоматичних рішень за рахунок урахування невизначеності прогнозу. Удосконалено підхід до забезпечення цілісності та довіри до позаланцюгових рішень шляхом криптографічно верифікованої фіксації метаданих аналізу (версії ознак, моделі, політик і результату) з прив'язкою до транзакції. Експериментальна перевірка на «Elliptic Bitcoin Dataset» підтвердила практичну придатність підходу: на тестовій вибірці досягнуто ROC-AUC 0.854, а механізм зонування формує інженерно коректну основу для адаптивного керування обробкою транзакцій і подальшого аудиту прийнятих рішень.

Список літератури:

1. Шаповалова С., Гулак О. Блокчейн технології в банківській сфері. *Системи управління, навігації та зв'язку. Збірник наукових праць*. 2022. № 1 (67). С. 94–97. DOI: https://doi.org/10.26906/SUNZ.2022.1.094

2. Шевчук О., Муравський В. Блокчейн та електронні трансакції в обліку. *Вісник економіки*. 2023. № 3. С. 212–237. DOI: https://doi.org/10.35774/visnyk2023.03.212

3. Іванюк О.О., Денисенко Н.С. Аналіз особливостей безпечної обробки даних в технології блокчейну на основі криптографічних хеш-функцій. *Вісник Національного університету «Львівська політехніка».* 2024. № 84. С. 83–94. DOI: https://doi.org/10.23939/csn2024.02.082

4. Hasan M., Rahman M.S., Janicke H., Sarker I.H. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis. *Blockchain: Research and Applications*. 2024. Vol. 5, № 3. Article 100207. DOI: https://doi.org/10.1016/j.bcra.2024.100207

5. Panigrahi A., Pati A., Sahu B., Paul R., Nayak A.K., Chowdhury S., Shreyas J. Enhancing blockchain transaction classification with ensemble learning approaches. *Scientific Reports*. 2025. Vol. 15, № 1. Article 22068. DOI: https://doi.org/10.1038/s41598-025-04072-7

6. Osterrieder J., Chan S., Chu J., Zhang Y., Misheva B.H., Mare C. Enhancing security in blockchain networks: Anomalies, frauds, and advanced detection techniques. *arXiv preprint*. 2024. arXiv:2402.11231. DOI: https://doi.org/10.48550/arXiv.2402.11231

7. Chen S., Liu Y., Zhang Q., Shao Z., Wang Z. Multi-Distance Spatial-Temporal Graph Neural Network for Anomaly Detection in Blockchain Transactions. *Advanced Intelligent Systems.* 2025. Article 2400898. DOI: https://doi.org/10.1002/aisy.202400898

8. Elmougy Y., Liu L. Demystifying fraudulent transactions and illicit nodes in the bitcoin network for financial forensics. *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. 2023. P. 3979–3990. DOI: https://doi.org/10.1145/3580305.3599803

9. Alarab I., Prakoonwit S. Robust recurrent graph convolutional network approach based sequential prediction of illicit transactions in cryptocurrencies. *Multimedia Tools and Applications*. 2024. Vol. 83, № 20. P. 58449–58464. DOI: https://doi.org/10.1007/s11042-023-17323-4

10. Собко О.В., Молчанова М.О., Мазурець О.В., Гнатюк П.В. Алгоритмізація процесів керування та інтеракцій в ігрових об'єктно-орієнтованих застосунках. *Вісник Херсонського національного технічного університету.* 2025. № 3 (94), Т. 2. С. 435–442. DOI: https://doi.org/10.35546/kntu2078-4481.2025.3.2.55

11. Garcia R.D., Ramachandran G., Dunnett K., Jurdak R., Ranieri C., Krishnamachari B., Ueyama J. A survey of blockchain-based privacy applications: An analysis of consent management and self-sovereign identity approaches. *arXiv preprint*. 2024. DOI: https://doi.org/10.48550/arXiv.2411.16404

12. Zhang R., Xue R., Liu L. Security and privacy on blockchain. *ACM Computing Surveys*. 2019. Vol. 52, № 3. Article 51. P. 1–34. DOI: https://doi.org/10.1145/3316481

13. Xu X., Weber I., Staples M. Architecture for blockchain applications. *Springer Briefs in Computer Science*. Cham, 2019. P. 1–150. DOI: https://doi.org/10.1007/978-3-030-03035-3

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

15. Elliptic Data Set. Kaggle. URL: https://www.kaggle.com/datasets/ellipticco/elliptic-data-set.

16. Sobko O., Mazurets O., Molchanova M., Krak I., Barmak O. Method for analysis and formation of representative text datasets. *CEUR Workshop Proceedings.* 2025. Vol. 3899. P. 84–98. URL: https://ceur-ws.org/Vol-3899/paper9.pdf

17. Xiang Q., Zi L., Cong X., Wang Y. Concept Drift Adaptation Methods under the Deep Learning Framework: A Literature Review. *Applied Sciences*. 2023. Vol. 13, № 11. Article 6515. DOI: https://doi.org/10.3390/app13116515.

18. Wang Y., Zhang T., Guo X., Shen Z. Gradient based feature attribution in explainable AI: A technical review. *arXiv preprint*. 2024. DOI: arXiv:2403.10415.

Askerov V.V. TOOLS FOR MANAGING SECURE TRANSACTIONS IN BLOCKCHAIN SYSTEMS BASED ON NEURAL NETWORK TRANSACTION RISK ASSESSMENT

The article proposes the architecture for managing secure transactions in blockchain systems that combines standard on-chain components (transaction formation, mempool, consensus, blocks, and registry) with a trusted off-chain neural network risk assessment circuit. The goal of the approach is to reduce application risks (fraud, money laundering, anomalous address chains) without modifying the basic consensus algorithm and without violating the determinism of the network. A method for multi-level routing and transaction admission for three risk zones White, Gray, and Black is proposed, taking into account the uncertainty of the forecast: for White, standard pre-consensus validation is used, for Gray, enhanced verification and deferred inclusion, for Black, blocking or quarantine. To ensure trust in off-chain solutions, a mechanism for cryptographically verified metadata fixation (feature hashes, model and policy versions, explanation hash, timestamp) with a trusted oracle signature and binding to the transaction in the chain has been developed. The neural network model generates risk scoring based on structural, temporal and contextual features; local interpretation (Integrated Gradients) highlights key impact factors for audit. Experiments on the Elliptic Bitcoin Dataset with time-splitting of samples showed ROC-AUC 0.854 on test and AUPRC 0.815 on validation; for the Black zone (stable solutions) Precision 0.5912 and Recall 0.4858 were obtained. The results confirm the practical applicability of the proposed contour approach for adaptive transaction management and further incident investigation. The zoning thresholds twhite, tblack and umax are determined on the validation sample and set

a trade-off between the acceptance rate and the fraction of false decisions. The signed decision log makes the off-chain inference reproducible and suitable for network auditing.

Keywords: *transaction management, blockchain, transaction risk classification, neural network model, off-chain circuit, explainable artificial intelligence, Elliptic Bitcoin Dataset.*

Дата першого надходження статті до видання: 26.01.2026
Дата прийняття статті до друку після рецензування: 19.02.2026
Дата публікації (оприлюднення) статті: 08.04.2026