ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004 DOI https://doi.org/10.35546/kntu2078-4481.2026.2.24

В. В. АСКЕРОВ
аспірант кафедри комп'ютерної інженерії та інформаційних систем
Хмельницький національний університет
ORCID: 0009-0009-1176-9812

ПРОТОКОЛ КЕРУВАННЯ ЗАХИЩЕНИМИ ТРАНЗАКЦІЯМИ У БЛОКЧЕЙН-МЕРЕЖІ З РИЗИК-ОРІЄНТОВАНИМ ДОПУСКОМ

У роботі запропоновано протокол керування захищеними транзакціями у блокчейн-мережі з ризик-орієнтованим допуском, який забезпечує адаптивну передконсенсусну обробку без модифікації базового механізму консенсусу. Протокол спирається на позаланцюговий сервіс оцінювання ризику, що для кожної транзакції формує ознаковий профіль, обчислює ризик-оцінку нейромережевим модулем трансформерного типу для табличних ознак та оцінює невизначеність прогнозу. Ризик-оцінка та невизначеність перетворюються політикою зонування на зони White, Gray і Black з формуванням протокольної директиви, яка визначає режим обробки, пріоритет, правила допуску і аудит. Введено три режими: STD як стандартна перевірка, ENH як посилена перевірка з додатковими процедурами контролю, QUAR як карантинна обробка з обмеженням допуску та журналюванням.

Експериментальну перевірку виконано на розміченій частині графового набору транзакцій, у якому після вилучення нерозмічених прикладів використано 46 564 транзакції з профілем із 188 ознак та розбиттям на тренувальну, валідаційну і тестову підвибірки; дисбаланс класів враховано ваговою корекцією позитивного класу. На тесті досягнуто ROC-AUC 0.9207 та AUPRC 0.7588, що підтверджує придатність ризик-оцінки для протокольного керування. Налаштовані пороги зонування сформували розподіл потоку 0.6845 у White, 0.2929 у Gray і 0.0226 у Black, забезпечивши високу селективність карантину з Precision 0.9655 та ескалацію ризикових транзакцій на підвищений контроль із Recall 0.8596 для Gray та Black. Мікробенчмарк у пакетному виконанні B=256 показав середні затримки 0.0778 мс для STD, 0.5215 мс для ENH і 0.5815 мс для QUAR, що робить суцільну посилену перевірку ресурсоємною. За фактичних часток зон середня нормована вартість передконсенсусної обробки становить 2.816 на транзакцію, а економія порівняно з політикою суцільної ENH сягає 57.98%, зберігаючи контроль ризикового потоку без втручання у консенсус.

Ключові слова: *керування транзакціями, блокчейн, захищені транзакції, ризик-орієнтований допуск, протокол керування транзакціями*

V. V. ASKEROV
Postgraduate Student at the Department of Computer Engineering
and Information Systems
Khmelnytskyi National University
ORCID: 0009-0009-1176-9812

PROTOCOL FOR MANAGING SECURE TRANSACTIONS IN A BLOCKCHAIN NETWORK WITH RISK-BASED ADMISSION

The paper proposes a protocol for managing secure transactions in a blockchain network with risk-based admission, which provides adaptive pre-consensus processing without modifying the underlying consensus mechanism. The protocol relies on an off-chain risk assessment service that generates a feature profile for each transaction, calculates a risk score using a transformer-type neural network module for tabular features, and estimates the prediction uncertainty. The risk score and uncertainty are transformed by a zoning policy into White, Gray, and Black zones with the formation of a protocol directive that defines the processing mode, priority, admission rules, and audit. Three modes are introduced: STD as standard verification, ENH as enhanced verification with additional control procedures, QUAR as quarantine processing with access restrictions and logging.

Experimental verification was performed on the labeled part of the graph transaction set, in which, after removing unlabeled examples, 46,564 transactions with a profile of 188 features and a partition into training, validation and test subsamples were used; class imbalance was taken into account by weight correction of the positive class. The test achieved ROC-AUC 0.9207 and AUPRC 0.7588, which confirms the suitability of the risk assessment for protocol control.

ISSN 2078-4481

The configured zoning thresholds formed a flow distribution of 0.6845 in White, 0.2929 in Gray and 0.0226 in Black, ensuring high quarantine selectivity with Precision 0.9655 and escalation of risky transactions to increased control with Recall 0.8596 for Gray and Black. The microbenchmark in batch execution B=256 showed average latencies of 0.0778 ms for STD, 0.5215 ms for ENH and 0.5815 ms for QUAR, making continuous hard verification resource-intensive. With actual zone shares, the average normalized cost of pre-consensus processing is 2.816 per transaction, and the savings compared to the continuous ENH policy reach 57.98%, while maintaining control of the risk flow without interfering with the consensus.

Key words: *transaction management, blockchain, secure transactions, risk-based admission, transaction management protocol.*

Постановка проблеми

Розглядається блокчейн-мережа з фіксованим механізмом консенсусу та передконсенсусною підсистемою приймання і обробки транзакцій. На вхід вузлів надходить потік транзакцій, для яких формується ознаковий профіль і часові характеристики. Позаланцюговий модуль оцінювання ризику для кожної транзакції обчислює ризик-оцінку та показник невизначеності прогнозу. Необхідно розробити протокол керування захищеними транзакціями, який на основі цих оцінок формує протокольну директиву та визначає порядок допуску транзакції до передконсенсусної черги, правила її маршрутизації та набір політик передконсенсусної перевірки і пріоритезації, не змінюючи процедури консенсусу та правила формування блоку.

Протокол має підтримувати три режими передконсенсусної обробки. Стандартний режим відповідає базовій перевірці транзакції. Режим посиленої перевірки передбачає застосування додаткових процедур контролю та уточнення оцінки. Карантинний режим забезпечує ізоляцію транзакції від стандартного потоку обробки з обмеженням допуску та розширеним аудитом. Вибір режиму задається політикою зонування, яка відносить транзакцію до зони низького ризику, до буферної зони для посиленої перевірки або до зони високого ризику для карантину.

Вимагається забезпечити зменшення імовірності включення транзакцій підвищеного ризику до блоку за рахунок ризик-орієнтованого допуску, обмежити помилкові блокування коректних транзакцій і не допустити неприйнятного зростання накладних витрат та затримок передконсенсусної обробки. Додатковою вимогою є відтворюваність прийнятих рішень для контролю та аудиту шляхом фіксації параметрів протокольної директиви та результатів застосованих політик.

Аналіз останніх досліджень і публікацій

Сучасні публікації зосереджуються на тому, що передконсенсусний контур у публічних блокчейн-мережах є вузьким місцем для керування навантаженням і ризиками, оскільки саме на рівні мемпулу формуються пріоритети включення, затримки підтвердження та фактичні витрати на валідацію. Емпіричні дослідження механізму комісій Ethereum після впровадження EIP-1559 показують вимірювані зміни у розподілі комісій і часі очікування транзакцій, але не знімають проблеми черг та стратегічної поведінки учасників, що підтримує актуальність інженерних рішень саме у передконсенсусному шарі протоколу [1, 2].

Паралельно з аналізом ефективності ринку комісій розвивається напрям протидії зловмисному навантаженню на мемпул. Роботи останніх років описують атаки, у яких вразливості механізмів ціноутворення та чергування можуть штучно змінювати базові параметри протоколу, впливаючи на включення транзакцій та економіку валідаторів, що підкреслює потребу у контрольованих політиках допуску й маршрутизації без втручання у базовий консенсус [3].

Окремий пласт робіт присвячено захисту мемпулу від виснаження ресурсів і спаму через механізми обробки транзакцій до консенсусу. Запропоновано схеми підвищення стійкості мемпулу до навмисного перевантаження та деградації сервісу, включно з оптимізацією обробки підозрілих транзакцій та спеціалізованими механізмами протидії безкоштовному спаму, які фактично вводять елементи керованого відбору транзакцій у передконсенсусному контурі [4].

У напрямі ідентифікації ризикових та незаконних транзакцій домінують методи машинного навчання на транзакційних графах, де модель формує оцінку ризику за структурою та атрибутами взаємодій і демонструє перспективність для протидії відмиванню коштів та пов'язаним загрозам [5, 6]. Водночас для практичного керування допуском важливо не лише отримати оцінку ризику, а й контролювати надійність прогнозу, тому у суміжних задачах активно застосовують підходи оцінювання невизначеності на основі стохастичних прогонів моделі під час інференсу, зокрема Monte Carlo dropout, як інженерно простий механізм підкріплення рішень у критичних режимах [7]. Сукупно це формує незакритий розрив між якісною детекцією ризику та протокольним керуванням режимами передконсенсусної валідації і маршрутизації, що й мотивує роботи з ризик-орієнтованим допуском у межах незмінного консенсусу.

Формулювання мети дослідження

Мета дослідження полягає у розробленні та експериментальному обґрунтуванні протоколу керування захищеними транзакціями у блокчейн-мережі з ризик-орієнтованим допуском, який на основі позаланцюгового оцінювання ризику та невизначеності прогнозу формує протокольну директиву режиму передконсенсусної обробки,

визначає правила допуску й пріоритезації транзакцій та забезпечує адаптивне застосування стандартного, посиленого і карантинного режимів без модифікації базового механізму консенсусу, з одночасним зменшенням імовірності включення ризикових транзакцій, контролем помилкових блокувань коректного потоку та оцінкою ресурсних накладних витрат.

Викладення основного матеріалу дослідження

Запропонований протокол керування захищеними транзакціями у блокчейн-мережі ґрунтується на тому, що кожна транзакція до етапу консенсусу отримує не лише базову передконсенсусну перевірку, а керовану протокольну директиву, сформовану за результатами позаланцюгового оцінювання ризику та невизначеності прогнозу. Директива відносить транзакцію до однієї з інженерних зон ризику та визначає режим передконсенсусної обробки, правила допуску до включення в блок і пріоритет виконання, забезпечуючи адаптивний перерозподіл ресурсів перевірки між стандартною, посиленою та карантинною обробкою. Такий підхід зменшує імовірність проходження транзакцій підвищеного ризику, обмежує помилкові блокування коректного потоку і досягає цього без втручання у базовий механізм консенсусу вузлів, оскільки змінює лише передконсенсусні політики допуску, пріоритезації та контролю.

Для уточнення логіки запропонованого протоколу та взаємодії його передконсенсусних компонентів використано структурну схему, що відображає повний шлях транзакції від надходження у мережу до рішення про включення в блок. Схема (рисунок 1) акцентує увагу на тому, що керування виконується на етапі передконсенсусної обробки через формування протокольної директиви, тоді як механізм консенсусу залишається незмінним.

Вхідний потік транзакцій після приймання вузлом і буферизації проходить етап профілювання, на якому формується набір структурних, часових та контекстних ознак, що характеризують транзакцію в термінах поведінки та взаємодій. На основі цього профілю позаланцюговий модуль оцінювання обчислює ризик-оцінку транзакції, а також показник невизначеності прогнозу, який використовується для підвищення надійності подальших протокольних рішень у прикордонних випадках.

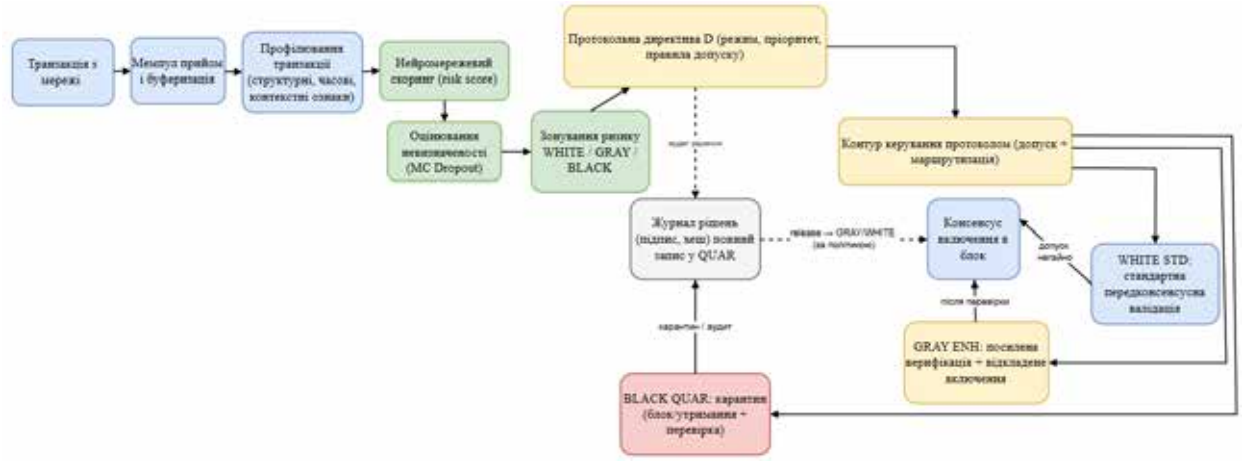

Рис. 1. Структурна схема протоколу керування захищеними транзакціями з ризик-орієнтованим допуском у блокчейн-мережі

Далі ризик-оцінка та невизначеність перетворюються інженерною політикою зонування на одну з трьох зон ризику. Низькоризикова зона відповідає стандартному режиму передконсенсусної валідації, у якому транзакція допускається до обробки без додаткових процедур. Проміжна зона активує посилену перевірку та може передбачати відкладене включення, що дозволяє застосувати додаткові правила контролю, не блокуючи весь потік. Високоризикова зона ініціює карантинну обробку, у межах якої транзакція ізолюється від стандартного процесу та підлягає максимально строгій перевірці відповідно до встановлених політик.

Ключовим елементом схеми є протокольна директива, яка фіксує обраний режим обробки, пріоритет і правила допуску, а також керує маршрутизацією транзакції між передконсенсусними контурами. Для підвищення відтворюваності та контрольованості рішень передбачено журналювання, яке у карантинному режимі доповнюється криптографічними механізмами фіксації параметрів обробки. Результатом роботи протоколу є допуск транзакції до включення в блок або відкладення чи блокування, при цьому консенсусна процедура включення залишається незмінною і отримує на вхід уже керований за ризиком потік транзакцій.

Після загальної структурної схеми доцільно деталізувати, яким саме чином політика зонування перетворює результати оцінювання ризику на конкретні протокольні дії. Для цього введено поняття протокольної директиви, яка є інженерним представленням рішення про режим передконсенсусної обробки та містить параметри, необхідні для реалізації допуску, пріоритезації, маршрутизації й аудиту у вузлі мережі (рисунок 2).

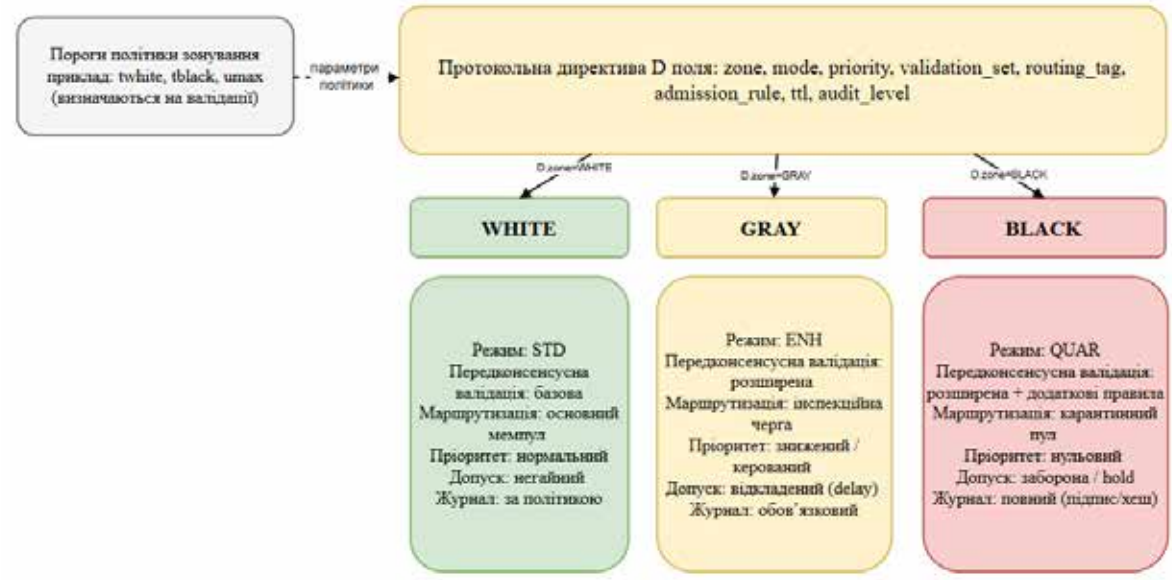

Рис. 2. Політика передконсенсусної обробки транзакцій за зонами ризику та структура протокольної директиви

У верхній частині схеми показано, що вибір дій визначається параметрами політики зонування, зокрема порогами для виділення високоризикової та низькоризикової областей і межею невизначеності, які підбираються за валідаційними даними. На виході політики формується протокольна директива, яка фіксує обрану зону ризику, режим обробки, пріоритет виконання, набір процедур валідації, правила допуску та службові атрибути, необхідні для керованого обігу транзакцій у передконсенсусному контурі.

Зона White відповідає стандартному режиму STD, у якому застосовується базова передконсенсусна валідація, транзакція спрямовується до основного мемпулу та отримує нормальний пріоритет. Такий режим орієнтований на мінімальні накладні витрати й підтримання пропускної здатності для потоку транзакцій, що не демонструють ознак підвищеного ризику, а журналювання виконується лише за необхідності відповідно до обраної політики.

Зона Gray задає проміжний режим ENH, який використовується для транзакцій із прикордонними значеннями ризику або підвищеною невизначеністю прогнозу. Для цього режиму передбачено розширену передконсенсусну валідацію та маршрутизацію в інспекційну чергу, а також керовану зміну пріоритету та можливість відкладеного включення, що дає змогу виконати додаткові перевірки без застосування жорстких блокувань. Журналювання у цій зоні є обов'язковим як елемент відтворюваності рішень у спірних випадках.

Зона Black відповідає карантинному режиму QUAR, у якому транзакція ізолюється від стандартного потоку обробки, підлягає максимальному набору перевірок і не допускається до включення в блок до завершення передбачених процедур контролю. Маршрутизація здійснюється до карантинного пулу, пріоритет виконання встановлюється нульовим, а журналювання виконується у повному обсязі з фіксацією параметрів обробки для подальшого аудиту та відтворення протокольного рішення.

Для формалізації поведінки протоколу у часі та уточнення переходів між режимами передконсенсусної обробки доцільно подати процес у вигляді станової моделі (рисунок 3). Така форма опису дозволяє однозначно зафіксувати, на якому етапі формується протокольна директива, за яких умов транзакція переходить у стандартний, інспекційний або карантинний контур, а також як саме забезпечується включення транзакції в блок без зміни консенсусної процедури.

Для зони White транзакція переводиться в режим STD і допускається до основного мемпулу, де очікує включення до блоку відповідно до незмінної консенсусної процедури. Для зони Gray транзакція спрямовується на інспекційний контур ENH, у межах якого виконуються розширені перевірки; у разі успішного проходження цього контуру транзакція повертається до мемпулу та може бути включена до блоку. Така логіка забезпечує посилену перевірку прикордонних випадків без жорсткого блокування і без загального перевантаження передконсенсусної обробки.

Для зони Black транзакція переводиться у карантинний контур QUAR, де вона ізолюється від стандартного потоку обробки та підлягає додатковій перевірці, що може включати застосування правил контролю та аудиторські процедури. За результатом перевірки можливі два наслідки: відхилення транзакції або її повернення до інспекційного контуру з подальшим допуском до мемпулу за політикою. Таким чином, модель відображає керований ризик-орієнтований допуск і показує, що рішення про включення в блок приймається в межах існуючого консенсусу, тоді як протокол регламентує лише передконсенсусні переходи та політики обробки.

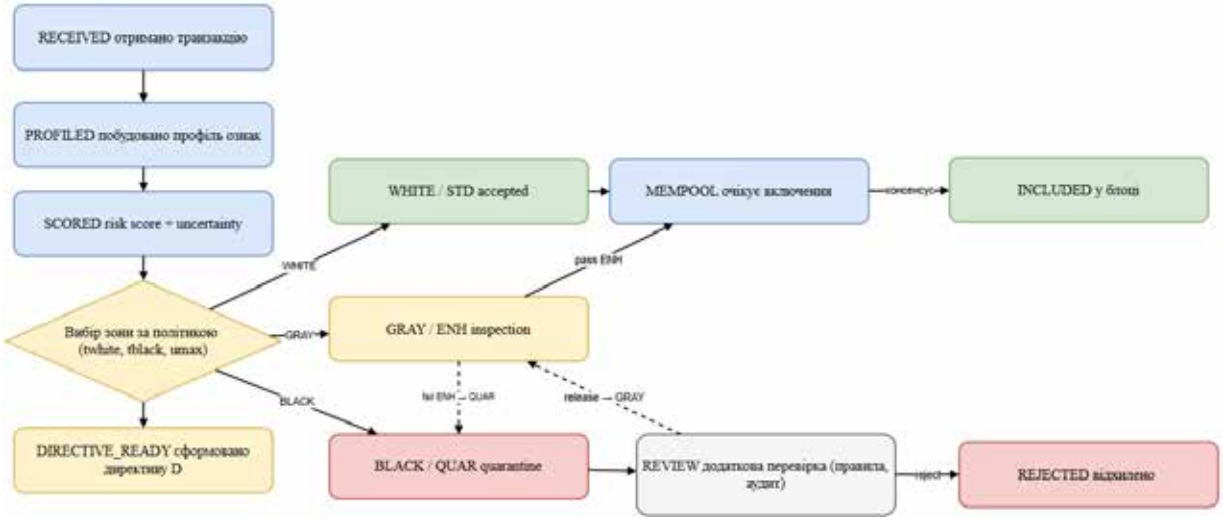

Рис. 3. Модель станів передконсенсусної обробки транзакції та переходів між режимами STD, ENH і QUAR

Експериментальну перевірку протоколу керування захищеними транзакціями виконано у постановці позаланцюгового сервісу оцінювання ризику транзакцій [8]. Для кожної транзакції формується ознаковий профіль, обчислюється ризик-оцінка нейромережевим модулем трансформерного типу для табличних ознак, оцінюється невизначеність прогнозу та застосовується інженерна політика зонування ризику з віднесенням транзакції до зон White, Gray або Black із формуванням протокольної директиви режиму передконсенсусної обробки STD, ENH або QUAR. У режимі QUAR передбачено фіксацію результату у журналі з метою аудиту та відтворюваності [9]. Дані для навчання і тестування отримано з розміченої частини графового набору транзакцій «Elliptic Bitcoin Dataset» [10]; після вилучення нерозмічених прикладів використано 46 564 транзакції з профілем із 188 ознак та розбиттям на тренувальну, валідаційну і тестову підвибірки. Суттєвий дисбаланс класів враховано за рахунок вагової корекції позитивного класу під час оптимізації [11].

Експериментальна перевірка працездатності протоколу обґрунтовується узгодженістю трьох груп результатів (Таблиця 1). Якість ризик-оцінки є достатньою для керування політиками передконсенсусної обробки, що підтверджується значеннями ROC-AUC і AUPRC [12] на тестовій підвибірці. Налаштовані пороги зонування разом із межею невизначеності формують керований розподіл транзакцій між стандартним, посиленим та карантинним режимами, забезпечуючи високу точність автоматичного карантину і направлення більшості ризикових транзакцій на контури підвищеного контролю. Практична доцільність зонування підтверджується вимірюванням накладних витрат трьох режимів у пакетному виконанні та розрахунком середньої відносної вартості передконсенсусної обробки з урахуванням фактичних часток транзакцій у кожній зоні. Така оцінка показує, що запропонований протокол дозволяє суттєво зменшити ресурсоємність порівняно з політикою, у якій посилена перевірка застосовується до всього потоку, зберігаючи при цьому високий рівень ескалації ризикових транзакцій на посилений контроль.

Значення ROC-AUC 0.9207 та AUPRC 0.7588 підтверджують, що оцінка ризику містить достатньо інформації для керування передконсенсусними політиками в умовах дисбалансу, тобто протокол отримує керувальний сигнал, який розділяє низькоризикові та ризикові випадки краще за випадкове рішення.

Параметри зонування t_black, t_white та u_max визначають, яка частина потоку буде оброблятися стандартно, а яка буде ескалована на підвищений контроль. Отриманий розподіл зон показує, що протокол зберігає пропускну здатність для основного потоку, оскільки 0.6845 транзакцій залишаються у White, тоді як 0.3155 потоку спрямовується на контури ENH та QUAR. Карантинний режим застосовується лише до 0.0226 транзакцій, що означає обмежене використання найжорсткіших процедур і зменшує ризик надлишкових блокувань.

Показники ескалації відображають властивості протоколу з точки зору безпеки та керованості. Високе значення Precision для Black 0.9655 означає, що транзакції, переведені у карантин, у переважній більшості є справді ризиковими, отже автоматичний карантин працює селективно. Порівняно невисокий Recall для Black 0.3361 вказує, що карантин навмисно не використовується як основний фільтр, а роль масової ескалації виконує Gray. Це підтверджується Recall ескалації для Gray і Black 0.8596, тобто більшість ризикових транзакцій потрапляє на посилений контроль. Частка ризикових транзакцій у White 0.1404 є наслідком обраної політики компромісу між безпекою та ресурсами і задає рівень залишкового ризику, який допускається заради обмеження навантаження на ENH.

Таблиця 1

Узагальнення експериментальної перевірки протоколу зонування та режимів STD, ENH, QUAR

Компонент перевірки	Показник	Значення
Дані	Кількість розмічених транзакцій	46 564
Дані	Тестова підвибірка	16 670
Дані	Кількість ознак у профілі	188
Дані	Вагова корекція дисбалансу pos_weight	8.224
Інформативність ризик-оцінки	ROC-AUC на тесті	0.9207
Інформативність ризик-оцінки	AUPRC на тесті	0.7588
Політика зонування	Поріг t_black	0.9791
Політика зонування	Поріг t_white	0.7724
Політика зонування	Межа невизначеності u_max	0.5399
Потоки протоколу	Частка зони White на тесті	0.6845
Потоки протоколу	Частка зони Gray на тесті	0.2929
Потоки протоколу	Частка зони Black на тесті	0.0226
Потоки протоколу	Навантаження на ENH та QUAR	0.3155
Потоки протоколу	Навантаження на QUAR	0.0226
Ескалація ризику	Precision для Black	0.9655
Ескалація ризику	Recall для Black	0.3361
Ескалація ризику	Recall ескалації для Gray і Black	0.8596
Ескалація ризику	Частка ризикових транзакцій у White	0.1404
Мікробенчмарк у пакетному виконанні (B=256)	Середня затримка STD, мс на транзакцію	0.0778
Мікробенчмарк у пакетному виконанні	Середня затримка ENH, мс на транзакцію	0.5215
Мікробенчмарк у пакетному виконанні	Середня затримка QUAR, мс на транзакцію	0.5815
Мікробенчмарк у пакетному виконанні	p95 для STD, мс на транзакцію	0.0795
Мікробенчмарк у пакетному виконанні	p95 для ENH, мс на транзакцію	0.5322
Мікробенчмарк у пакетному виконанні	p95 для QUAR, мс на транзакцію	0.6462
Мікробенчмарк у пакетному виконанні	Нормована вартість STD	1.000
Мікробенчмарк у пакетному виконанні	Нормована вартість ENH	6.702
Мікробенчмарк у пакетному виконанні	Нормована вартість QUAR	7.472
Ефект протоколу	Середня нормована вартість на транзакцію	2.816
Ефект протоколу	Економія порівняно з політикою суцільної ENH	57.98%

Дані мікробенчмарку показують інженерну “ціну” кожного режиму. ENH у середньому потребує у 6.702 раза більше часу порівняно зі STD, а QUAR у 7.472 раза, що робить неприйнятною політику суцільної посиленої перевірки. За фактичних часток зон середня нормована вартість становить 2.816 на транзакцію, а економія відносно політики, де весь потік проходить ENH, дорівнює 57.98%. Це інтерпретується як практична доцільність протоколу зонування, оскільки він перерозподіляє ресурси перевірки на підвищений контроль лише для обмеженої частини потоку, зберігаючи високу селективність карантину та суттєву ескалацію ризикових транзакцій.

Висновки

У роботі досягнуто поставленої мети, що полягала у розробленні та експериментальному обґрунтуванні протоколу керування захищеними транзакціями у блокчейн-мережі з ризик-орієнтованим допуском без модифікації базового механізму консенсусу. Запропоновано механізм формування протокольної директиви, який переводить результати позаланцюгового оцінювання ризику та невизначеності прогнозу у режими передконсенсусної обробки та правила допуску, пріоритезації і маршрутизації.

За отриманими результатами протокол забезпечує вимірюваний інженерний ефект за рахунок перерозподілу витратних процедур перевірки лише на частину потоку. За налаштованої політики зонування 68.45% транзакцій обробляються у стандартному режимі, тоді як 31.55% спрямовуються на посилений або карантинний контур, причому карантин застосовується лише до 2.26% транзакцій і характеризується високою селективністю з точністю 0.9655. За таких часток зон середня нормована вартість передконсенсусної обробки становить 2.816 на транзакцію, що відповідає економії 57.98% порівняно з політикою суцільної посиленої перевірки, при цьому ескалація ризикових транзакцій на підвищений контроль зберігається на рівні 0.8596. Це демонструє практичну доцільність ризик-орієнтованого допуску як механізму керування компромісом між ресурсами перевірки та рівнем контролю ризикового потоку без втручання у консенсус.

До обмежень роботи належить те, що перевірка виконувалась у постановці позаланцюгового сервісу з мікробенчмарком режимів передконсенсусної обробки, тому часові характеристики відображають накладні витрати обчислювального контуру, але не включають мережеві затримки та ефекти розподіленого виконання у реальній мережі з багатьма вузлами. Результати також залежать від обраного набору ознак, розподілу даних і параметрів політики зонування, а рівень залишкового ризику у зоні White визначається прийнятим компромісом, який може

потребувати переналаштування для інших вимог до безпеки або інших доменів транзакцій. Окремим чинником є невизначеність прогнозу, яка у цій роботі оцінювалась через стохастичні прогони моделі, тоді як альтернативні методи калібрування та оцінювання невизначеності можуть змінювати розподіл зон і навантаження на контури перевірки.

Перспективи подальших досліджень пов'язані з розширенням експериментальної перевірки на сценарії змінного навантаження та імітацією мережевих умов, включно з аналізом впливу маршрутизації на поширення ризикових транзакцій і час включення коректного потоку. Практично важливим є адаптивне налаштування параметрів зонування з урахуванням цільових обмежень на ресурси та допустимий рівень ризику, а також розроблення методів моніторингу доменного зсуву і автоматичного перегляду політик.

Список використаної літератури

1. Yu Y. Empirical analysis of EIP-1559: Transaction fees, waiting times, and consensus security / Y. Yu, Y. Lu, K. Nayak, F. Zhang, L. Zhang, Y. Zhao // In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. November 2022. Pp. 2099–2113. https://doi.org/10.1145/3548606.3559341.

2. Leonardos S. Dynamics of Ethereum's EIP-1559 Transaction Fee Mechanism / S. Leonardos, D. Reijsbergen, B. Monnot, G. Piliouras // Distributed Ledger Technologies: Research and Practice. 2025. https://doi.org/10.1145/377329.

3. Azouvi S. Base fee manipulation in Ethereum's EIP-1559 transaction fee mechanism / S. Azouvi, G. Goren, L. Heimbach, A. Hicks // arXiv preprint arXiv:2304.11478. 2023. https://doi.org/10.4230/LIPIcs.DISC.2023.6.

4. Chotkan R. STARVESPAM: Mitigating Spam with Local Reputation in Permissionless Blockchains / R. Chotkan, B. Nasrulin, J. Decouchant, J. Pouwelse // In 2025 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). November 2025. Pp. 1–9. IEEE. https://doi.org/10.1109/BRAINS67003.2025.11302925.

5. Karim M. R. Scalable semi-supervised graph learning techniques for anti money laundering / M. R. Karim, F. Hermsen, S. A. Chala, P. De Perthuis, A. Mandal // IEEE Access. 2024. Vol. 12. Pp. 50012–50029. https://doi.org/10.1109/ACCESS.2024.3383784.

6. Poon C. H. LineMVGNN: Anti-money laundering with line-graph-assisted multi-view graph neural networks / C. H. Poon, J. Kwok, C. Chow, J. H. Choi // AI. 2025. Vol. 6, No. 4. P. 69. https://doi.org/10.3390/ai6040069.

7. Milanés-Hermosilla D. Monte Carlo dropout for uncertainty estimation and motor imagery classification / D. Milanés-Hermosilla, R. Trujillo Codorniú, R. López-Baracaldo, R. Sagaró-Zamora, D. Delisle-Rodriguez, J. J. Villarejo-Mayor, J. R. Nunez-Alvarez // Sensors. 2021. Vol. 21, No. 21. P. 7241. https://doi.org/10.3390/s21217241.

8. Молчанова М. О. Інформаційна хмарна технологія нейромережевого аналізу зруйнованих споруд за візуальними даними з БПЛА / М. О. Молчанова, О. В. Мазурець, О. О. Залуцька, В. Д. Кадинська, В. В. Масловська // Науковий журнал «Вісник Херсонського національного технічного університету». 2025. № 3 (94), Т. 2. С. 345–351. https://doi.org/10.35546/kntu2078-4481.2025.3.2.44.

9. Wang, X., Li, H., Yi, L., Ning, Z., Tao, X., Guo, S., & Zhang, Y. A survey on off-chain networks: Frameworks, technologies, solutions and challenges. ACM Computing Surveys, 2025. 57(12), 1-35.

10. Elliptic Data Set. 2026. Kaggle. https://www.kaggle.com/datasets/ellipticco/elliptic-data-set.

11. Sobko O. Method for analysis and formation of representative text datasets / O. Sobko, O. Mazurets, M. Molchanova, I. Krak, O. Barmak // CEUR Workshop Proceedings. 2025. Vol. 3899. Pp. 84–98.

12. McDermott M. A closer look at AUROC and AUPRC under class imbalance / M. McDermott, H. Zhang, L. Hansen, G. Angelotti, J. Gallifant // Advances in Neural Information Processing Systems. 2024. Vol. 37. Pp. 44102–44163. https://doi.org/10.52202/079017-1400.

References

1. Liu, Y., Lu, Y., Nayak, K., Zhang, F., Zhang, L., & Zhao, Y. (2022, November). Empirical analysis of eip-1559: Transaction fees, waiting times, and consensus security. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 2099-2113). https://doi.org/10.1145/3548606.3559341.

2. Leonardos, S., Reijsbergen, D., Monnot, B., & Piliouras, G. (2025). Dynamics of Ethereum's EIP-1559 Transaction Fee Mechanism. Distributed Ledger Technologies: Research and Practice. https://doi.org/10.1145/377329.

3. Azouvi, S., Goren, G., Heimbach, L., & Hicks, A. (2023). Base fee manipulation in ethereum's EIP-1559 transaction fee mechanism. arXiv preprint arXiv:2304.11478. https://doi.org/10.4230/LIPIcs.DISC.2023.6.

4. Chotkan, R., Nasrulin, B., Decouchant, J., & Pouwelse, J. (2025, November). STARVESPAM: Mitigating Spam with Local Reputation in Permissionless Blockchains. In 2025 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (pp. 1-9). IEEE. https://doi.org/10.1109/BRAINS67003.2025.11302925.

5. Karim, M. R., Hermsen, F., Chala, S. A., De Perthuis, P., & Mandal, A. (2024). Scalable semi-supervised graph learning techniques for anti money laundering. IEEE Access, 12, 50012-50029. https://doi.org/10.1109/ACCESS.2024.3383784.

6. Poon, C. H., Kwok, J., Chow, C., & Choi, J. H. (2025). LineMVGNN: Anti-money laundering with line-graph-assisted multi-view graph neural networks. AI, 6(4), 69. https://doi.org/10.3390/ai6040069.

7. Milanés-Hermosilla, D., Trujillo Codorniú, R., López-Baracaldo, R., Sagaró-Zamora, R., Delisle-Rodriguez, D., Villarejo-Mayor, J. J., & Nunez-Alvarez, J. R. (2021). Monte carlo dropout for uncertainty estimation and motor imagery classification. Sensors, 21(21), 7241. https://doi.org/10.3390/s21217241.

8. Molchanova, M. O., Mazurets, O. V., Zalutska, O. O., Kadinska, V. D., & Maslovska, V. V. (2025). Informatsiina khmarna tekhnolohiia neiromerezhevoho analizu zruinovanykh sporud za vizualnymy danymy z BPLA [Cloud-based neural network technology for analysis of destroyed structures using UAV visual data]. Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu, 3(94), T. 2, 345–351. https://doi.org/10.35546/kntu2078-4481.2025.3.2.44 [in Ukrainian].

9. Wang, X., Li, H., Yi, L., Ning, Z., Tao, X., Guo, S., & Zhang, Y. (2025). A survey on off-chain networks: Frameworks, technologies, solutions and challenges. ACM Computing Surveys, 57(12), 1-35.

10. Elliptic Data Set (2026). *Kaggle dataset*. Retrieved from https://www.kaggle.com/datasets/ellipticco/elliptic-data-set.

11. Sobko, O., Mazurets, O., Molchanova, M., Krak, I., & Barmak, O. (2025). Method for analysis and formation of representative text datasets. CEUR Workshop Proceedings, 3899, 84–98.

12. McDermott, M., Zhang, H., Hansen, L., Angelotti, G., & Gallifant, J. (2024). A closer look at AUROC and AUPRC under class imbalance. Advances in Neural Information Processing Systems, 37, 44102-44163. https://doi.org/10.52202/079017-1400.

Дата першого надходження статті до видання: 11.02.2026
Дата прийняття статті до друку після рецензування: 17.03.2026
Дата публікації (оприлюднення) статті: 07.05.2026