https://doi.org/10.31891/2307-5732-2026-363-41
УДК 004.7

АСКЕРОВ В'ЯЧЕСЛАВ
Хмельницького національного університету
https://orcid.org/0009-0009-1176-9812
e-mail: v.askerov@khmnu.edu.ua

МЕТОД ПІДТРИМКИ ЦІЛІСНОСТІ ТА ДОВІРИ ДО РЕЗУЛЬТАТІВ ОБРОБКИ ТРАНЗАКЦІЙ У БЛОКЧЕЙН-СИСТЕМАХ З КРИПТОГРАФІЧНО ВЕРИФІКОВАНОЮ ФІКСАЦІЄЮ ПРИЙНЯТИХ РІШЕНЬ

У статті розроблено та обґрунтовано метод підтримки цілісності та довіри до результатів обробки транзакцій у блокчейн-системах з криптографічно верифікованою фіксацією прийнятих рішень, спрямований на забезпечення доказової цілісності, перевірюваності походження та відтворюваності результатів прийняття рішень без втручання у базові механізми консенсусу мережі. Запропонований підхід розглядає рішення сервісу як відтворюваний інженерний артефакт і передбачає формування структурованого запису з фіксацією ризик-класу, показника ризику, хеш-зобов'язань для вектора ознак, версій моделі та політики обробки, часової мітки, а також криптографічного зв'язування послідовності записів журналу. На основі канонічної серіалізації обчислюється хеш запису, який підписується довіреним сервісом, тоді як у транзакції блокчейну закріплюється мінімальний якір рішення, що дозволяє незалежну перевірку незмінності та автентичності. Запропоновано процедуру аудиту, яка включає повторне обчислення хешу, перевірку цифрового підпису та контроль цілісності історії журналювання. Експериментальну перевірку виконано на відкритому наборі даних Bitcoin Heist Ransomware Address із хронологічним розбиттям для запобігання витоку інформації. Оцінювання ризику реалізовано із застосуванням градієнтного бустингу над деревами рішень з оптимізацією порогового значення за F_1-мірою. Результати експерименту підтвердили, що всі сформовані рішення успішно проходять криптографічну верифікацію, а будь-які спроби модифікації змісту рішення або порушення зв'язування записів надійно виявляються під час аудиту. Отримані результати засвідчують придатність методу для використання у безпеково критичних блокчейн-архітектурах, де необхідне формально перевірюване поєднання позаланцюгового аналізу та внутрішньоланцюгової фіксації. Також метод забезпечує простежуваність рішень у часі завдяки фіксації версійності використаних даних, моделей і правил обробки, що підвищує керованість безпекових політик та обґрунтованість результатів під час незалежної перевірки.

Ключові слова: *блокчейн-система, транзакція, оцінювання ризику, позаланцюговий сервіс, криптографічна верифікація, цифровий підпис, хешування, аудит.*

ASKEROV VIACHESLAV
Khmelnytskyi National University

METHOD FOR MAINTAINING INTEGRITY AND TRUST IN TRANSACTION PROCESSING RESULTS IN BLOCKCHAIN SYSTEMS WITH CRYPTOGRAPHICALLY VERIFIED RECORDING OF DECISIONS MADE

The article develops and substantiates the method for maintaining integrity and trust in transaction processing results in blockchain systems with cryptographically verified recording of decisions made, aimed at ensuring evidentiary integrity, traceability of origin, and reproducibility of decision-making results without interfering with the basic consensus mechanisms of the network. The proposed approach considers the service decision as a reproducible engineering artifact and involves the formation of a structured record with fixation of the risk class, risk indicator, hash commitments for the feature vector, model versions and processing policy, timestamp, and cryptographical linking of the sequence of log records. Based on canonical serialization, a hash of the record is calculated, which is signed by a trusted service, while a minimal anchor of the decision is fixed in the blockchain transaction, which allows independent verification of immutability and authenticity. An audit procedure is proposed that includes recalculation of the hash, verification of the digital signature, and control of the integrity of the log history. Experimental verification was performed on the open Bitcoin Heist Ransomware Address dataset with chronological partitioning to prevent information leakage. Risk assessment was implemented using gradient boosting over decision trees with threshold optimization by F1-measure. The experimental results confirmed that all generated solutions successfully pass cryptographic verification, and any attempts to modify the solution content or violate the record binding are reliably detected during the audit. The obtained results demonstrate the suitability of the method for use in security-critical blockchain architectures, where a formally verifiable combination of off-chain analysis and on-chain commit is required. The method for maintaining integrity and trust in transaction processing results in blockchain systems with cryptographically verified recording of decisions made also ensures the traceability of solutions over time by fixing the versioning of the data used, models, and processing rules, which increases the manageability of security policies and the validity of the results during independent verification.

Keywords: *blockchain system, transaction, risk assessment, off-chain service, cryptographic verification, digital signature, hashing, audit.*

Стаття надійшла до редакції / Received 02.02.2026
Прийнята до друку / Accepted 19.02.2026
Опубліковано / Published 26.03.2026

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Сучасні блокчейн-системи забезпечують криптографічну цілісність транзакцій і незмінність розподіленого реєстру, однак ці властивості не гарантують довіру до результатів позаланцюгової обробки, яка дедалі частіше використовується для оцінювання ризиків, протидії шахрайству та підтримки політик допуску транзакцій [1]. У практичних сценаріях безпекового керування транзакціями рішення щодо їх дозволу,

відкладення або посиленої перевірки формується поза блокчейном на основі ознак, правил та моделей, що можуть змінюватися в часі, оновлюватися різними версіями, а також піддаватися компрометації або неконтрольованій модифікації [2]. За відсутності формально верифікованого механізму фіксації таких рішень та їхніх артефактів виникає розрив довіри між ончейн-подіями та позаланцюговими висновками [3]: неможливо однозначно підтвердити, які саме ознаки, яка версія моделі та які політики були використані при ухваленні рішення для конкретної транзакції, чи не було підміни результату після обчислення, а також чи може третя сторона відтворити та незалежно перевірити історію рішень у межах аудиту або розслідування інцидентів.

Зазначена проблема має безпосередній зв'язок із ключовими завданнями комп'ютерної інженерії, що охоплюють проєктування надійних апаратно-програмних контурів, протоколів взаємодії між підсистемами та механізмів забезпечення цілісності даних у розподілених середовищах. Для блокчейн-мереж це проявляється як потреба у такому способі інтеграції результатів позаланцюгового ризик-аналізу, який не вимагає модифікації базового консенсусу, не переносить обчислювально важкі процедури в ончейн-середовище, але водночас забезпечує криптографічно перевірюваний зв'язок між транзакцією та відповідним рішенням безпекового сервісу [4]. Практична значущість проблеми зумовлена необхідністю підвищення керованості виконання транзакцій у системах на дозволах і в гібридних архітектурах, де рішення про маршрутизацію транзакції, застосування додаткової верифікації або обмеження виконання повинні бути не лише коректними на момент обчислення, а й відтворюваними, аудитованими та неспростовними впродовж життєвого циклу системи [5]. Саме тому актуальним є розроблення методу криптографічно верифікованої фіксації рішень позаланцюгового сервісу оцінювання ризику транзакцій із забезпеченням доказової цілісності, походження та версійності артефактів прийняття рішення при мінімальному ончейн-накладному навантаженні.

Аналіз досліджень та публікацій

Дослідження у сфері криптографічно захищених розподілених реєстрів свідчать про суттєві обмеження традиційних механізмів забезпечення довіри лише до внутрішньоланцюгових даних та операцій [6]. Існуючі підходи до гарантування цілісності транзакційних даних у блокчейн-системах здебільшого зосереджуються на криптографічних механізмах забезпечення незмінності полів транзакції і структури блоку, тоді як питання формальної верифікації рішень, що формуються у зовнішніх компонентах, належним чином не охоплюються [7]. Ця прогалина особливо помітна у випадках, коли для оцінювання ризику транзакцій застосовуються алгоритмічні модулі або моделі машинного навчання, які працюють поза межами базових механізмів обробки транзакцій і мають власні артефакти ухвалення рішення, включаючи версії ознак, моделей та правил політик обробки транзакцій [8].

У галузі систем розподіленого реєстру були запропоновані моделі взаємодії між внутрішньоланцюговими елементами та зовнішніми сервісами позаланцюгової обробки, які зосереджуються на формалізації інтерфейсів та гарантіях довіри до даних, що надходять із зовнішніх джерел даних або обчислень. У цих роботах підкреслюється необхідність забезпечення аудиторської перевірки та криптографічної несуперечності таких позаланцюгових рішень без модифікації базових протоколів консенсусу, що є ключовим для архітектур, де рішення про ризик транзакції має впливати на подальшу обробку без втручання в механізми узгодження стану мережі [9, 10].

Важливим напрямленням сучасних досліджень є застосування машинного навчання для класифікації транзакційних патернів з метою виявлення аномалій або шахрайських дій. У цих роботах доведено ефективність поєднання структурних, часових та контекстних ознак транзакції для формування ризик-метрик і їх подальшої інтерпретації. Проте у більшості таких досліджень відсутній формальний опис механізмів криптографічної фіксації артефактів ухвалення рішення і забезпечення їхнього зв'язку з конкретною транзакцією в розподіленому реєстрі, що є ключовою та недостатньо розробленою вимогою для систем класу «безпеково-критичних» [11, 12].

З позицій комп'ютерної інженерії, критично важливим є формування структур, що забезпечують журналювання з доказовою цілісністю та можливістю виявлення несанкціонованих змін. Класичні криптографічні структури для таких журналів, що включають підписані записи та послідовності хеш-зв'язків, створюють формальну основу для побудови механізму, подібного до запропонованого у цій статті, де репрезентація версій, хеш-зобов'язання та підписані записи інтегровані з транзакціями блокчейн-системи як доказові артефакти рішення [13].

Таким чином, існуючі дослідження вказують на високу значущість теми криптографічно верифікованої фіксації рішень, особливо в контексті інтеграції з ризик-аналізом на основі моделей машинного навчання та адаптивним коригуванням протоколів обробки транзакцій. Однак вони не охоплюють комплексного підходу до побудови механізму, що гарантує збереження версійності ознак, моделей і правил поряд із доказовою цілісністю та відтворюваністю результатів оцінювання у межах блокчейн-середовища.

Формулювання цілей статті

Метою роботи є: розроблення та обґрунтування методу підтримки цілісності та довіри до результатів обробки транзакцій у блокчейн-системах з криптографічно верифікованою фіксацією прийнятих рішень, який забезпечує доказову цілісність і відтворюваність результатів оцінювання шляхом фіксації версій ознак, моделей і політик обробки транзакцій, формування криптографічних зобов'язань на основі хешу, накладення цифрового підпису довіреного сервісу та інтеграції криптографічно зв'язаних метаданих у транзакцію з можливістю незалежної перевірки коректності й незмінності історії рішень без модифікації базових механізмів консенсусу мережі.

Виклад основного матеріалу

Сутність запропонованого методу полягає в тому, що рішення позаланцюгового сервісу оцінювання ризику транзакції розглядається як відтворюваний інженерний артефакт, для якого фіксуються не лише результат у вигляді ризик-класу, а й контекст прийняття рішення через версії ознак, моделі та політик обробки; далі формується структурований запис рішення з криптографічними зобов'язаннями на основі хешу, накладається цифровий підпис довіреного сервісу та виконується внутрішньоланцюгове закріплення мінімального набору верифікованих метаданих у транзакції блокчейн-мережі, що забезпечує доказову цілісність, перевірюваність походження та аудитованість історії рішень без перенесення обчислювально складних процедур оцінювання ризику у внутрішньоланцюговий контур і без модифікації базових механізмів консенсусу.

На рис.1 подано узагальнену структурно-функціональну схему методу підтримки цілісності та довіри до результатів обробки транзакцій у блокчейн-системах з криптографічно верифікованою фіксацією прийнятих рішень. У лівому контурі, який відповідає довіреному позаланцюговому середовищу прийняття рішень, формується сукупність даних рішення: визначений ризик-клас транзакції («White», «Gray», «Black»), ознаки транзакції, ідентифікатори версій моделі оцінювання ризику та політики обробки, а також локальне пояснення або його стислий представник. У центральному контурі виконується формування структурованого запису рішення, у якому фіксуються ідентифікатор транзакції та криптографічно зв'язані метадані артефактів прийняття рішення (хеші ознак, версій моделі та політики, хеш пояснення, часова мітка, а також посилання на попередній запис журналу). Далі запис піддається криптографічному хешуванню, після чого на отримане хеш-значення накладається цифровий підпис довіреного сервісу, що забезпечує перевірюваність походження рішення та його незмінність.

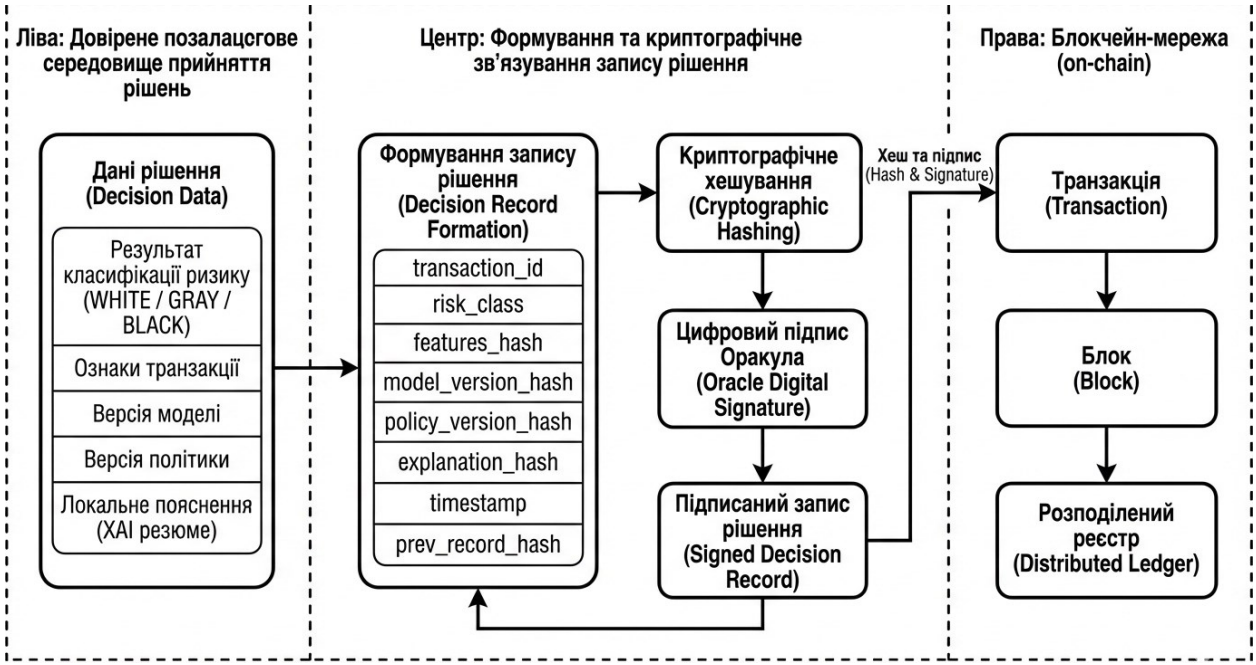

Рис. 1. Загальна схема криптографічно верифікованої фіксації рішень позаланцюгового сервісу оцінювання ризику транзакцій у блокчейн-системі

Правий контур відображає блокчейн-мережу, у межах якої до транзакції інтегрується лише мінімальний набір криптографічно верифікованих даних – хеш запису рішення та цифровий підпис, після чого транзакція включається до блоку і фіксується у розподіленому реєстрі. Таким чином, аналіз ризику та формування повного запису рішення виконуються поза блокчейном, тоді як у блокчейн-середовищі закріплюються лише криптографічні зобов'язання, що дозволяють незалежну верифікацію цілісності та автентичності рішення без перенесення обчислювально складних процедур оцінювання ризику у внутрішньоланцюговий контур.

Технічна реалізація методу підтримки цілісності та довіри до результатів обробки транзакцій у блокчейн-системах з криптографічно верифікованою фіксацією прийнятих рішень базується на однозначному формуванні криптографічно зв'язаного запису рішення та його подальшому внутрішньоланцюговому закріпленні. Структурований запис рішення подається у канонічному вигляді, що передбачає фіксований склад і порядок полів, однозначні типи даних та узгоджене кодування, завдяки чому однаковий зміст запису завжди породжує однакове представлення для обчислення хешу. На основі канонічно серіалізованого запису обчислюється криптографічне зобов'язання у вигляді значення record_hash = H(serialize(record)), де H є стійкою хеш-функцією, а serialize(record) є канонічним поданням запису. Цифровий підпис формується саме над значенням record_hash, що забезпечує перевірюваність походження рішення та виключає можливість

непомітної модифікації змісту запису після його підписання, а внутрішньоланцюговий якір рішення інтегрується до транзакції як сукупність щонайменше ідентифікатора транзакції, record_hash, цифрового підпису та ідентифікатора ключа, за яким однозначно визначається відкритий ключ для перевірки підпису. Для підтримки керованості криптографічної інфраструктури використовується реєстр відкритих ключів довіреного сервісу з можливістю ротації, при цьому значення key_id дозволяє коректно відтворити, який саме ключ був чинним для конкретного рішення в момент його формування. За потреби повні записи журналу можуть зберігатися у зашифрованому вигляді з метою забезпечення конфіденційності, при цьому хеш-зобов'язання для внутрішньоланцюгового закріплення формується від канонічного подання запису до застосування шифрування, а процедура аудиту передбачає доступ уповноваженого суб'єкта до відновлення структурованого запису для повторного обчислення хешу та перевірки підпису. Така побудова забезпечує відтворюваність ланцюга прийняття рішення, оскільки у записі фіксуються версійні ідентифікатори артефактів оцінювання, а зв'язування записів у послідовність через prev_record_hash забезпечує виявлення несанкціонованих змін у історії журналу.

На рис. 2 наведено схему верифікації та аудиту рішення позаланцюгового сервісу оцінювання ризику транзакції, яка забезпечує доказову перевірку походження та незмінності зафіксованого рішення після його внутрішньоланцюгового закріплення.

Рис. 2. Схема верифікації та аудиту рішення позаланцюгового сервісу оцінювання ризику транзакції за якорем у блокчейн-мережі та записом у журналі

Вхідними даними процедури є якір рішення, зчитаний із блокчейн-мережі для відповідної транзакції та представлений ідентифікатором транзакції, хешем запису рішення, цифровим підписом і ідентифікатором ключа; повний структурований запис рішення з позаланцюгового сховища журналу, що містить ризик-клас та криптографічно зв'язані метадані артефактів прийняття рішення, зокрема хеші ознак, версій моделі та політики, часову мітку і посилання на попередній запис; а також відкритий ключ сервісу, отриманий із реєстру ключів за значенням key_id. На основі повного запису рішення виконується канонічна серіалізація структурованих полів і повторне обчислення хешу, після чого отримане значення порівнюється з хешем, зафіксованим у якорі транзакції, що дозволяє встановити незмінність запису з моменту його закріплення в блокчейні. Далі здійснюється перевірка цифрового підпису сервісу на хеші запису з використанням відповідного відкритого ключа, що підтверджує походження рішення та виключає підміну підписанта. Завершальним етапом є перевірка цілісності історії журналу за ланцюжком prev_record_hash, яка дозволяє виявляти несанкціоновані вилучення або вставки записів у послідовності рішень. Вихідними даними процедури є статус верифікації та аудиту, що визначається коректністю підпису, збігом хешів і цілісністю ланцюжка журналу.

Експериментальну перевірку працездатності методу підтримки цілісності та довіри до результатів обробки транзакцій у блокчейн-системах з криптографічно верифікованою фіксацією прийнятих рішень виконано на відкритому часовому датасеті «Bitcoin Heist Ransomware Address» [14], який містить понад 2,9 млн записів поведінкових ознак, що описують транзакційні патерни у мережі Bitcoin у добовому інтервалі, та мітки приналежності до відомих сімейств програм-вимагачів або класу white. Для усунення витоку інформації застосовано хронологічне розбиття, за якого навчання моделі ризик-оцінки виконувалося на даних попередніх років, а тестування – на даних останнього року спостереження [15]. На основі тестових записів формувалися

структуровані записи журналу рішень позаланцюгового сервісу з фіксацією хеш-зобов'язань для вектора ознак, версій моделі та політики прийняття рішення, після чого обчислювався record_hash і накладався цифровий підпис сервісу; мінімальний якір рішення у вигляді пари record_hash та підпису інтегрувався у транзакційні метадані розподіленого реєстру. Подальший аудит здійснював повторне обчислення record_hash з канонічного подання запису, перевірку підпису за відкритим ключем та контроль цілісності ланцюжка журналу через prev_record_hash, що дозволило експериментально продемонструвати відтворюваність і незалежну перевірюваність рішень, а також виявлення будь-якої підміни змісту рішення або модифікації історії журналювання.

Таблиця 1

Параметри експериментальної перевірки та конфігурація методу підтримки цілісності та довіри до результатів обробки транзакцій у блокчейн-системах

Група	Параметр	Значення	Призначення
Дані	Джерело даних	Bitcoin Heist Ransomware Address (UCI), DOI: 10.24432/C5BG8V	Вхідні транзакційні патерни
Ознаки	Набір ознак	year, day, length, weight, count, looped, neighbors, income	Формування features_hash
Політика	Пороги ризику	t_white = 0.2; t_black = 0.8	Мапінг risk_score , клас
Хешування	Алгоритм	SHA-256	record_hash і хеш-зобов'язання
Серіалізація	Формат	Канонічний JSON	Однозначність представлення
Підпис	Схема	Ed25519	Перевірка походження рішення
Версійність	Ідентифікатор моделі	f362e160c837…	Відтворюваність рішення
Версійність	Ідентифікатор політики	b1f3a499ca2f…	Фіксація правил рішення
Якір	Склад	tx_id; record_hash; signature; key_id	Мінімум ончейн-метаданих
Журнал	Зв'язування	prev_record_hash	Контроль цілісності історії

У таблиці 1 наведено склад вхідних даних, параметри формування вектора ознак і політики віднесення до ризик-класів, а також ключові налаштування механізму фіксації та аудиту рішень: канонічну серіалізацію запису, хешування для побудови криптографічного зобов'язання record_hash, схему цифрового підпису, склад внутрішньоланцюгового якоря та правило зв'язування записів журналу через prev_record_hash. Наведені значення забезпечують однозначність обчислення хешу, перевірюваність походження рішення та контроль цілісності історії журналу під час незалежної верифікації.

У межах експерименту позаланцюгове оцінювання ризику виконувалося за допомогою градієнтного бустингу над деревами рішень (XGBClassifier) [16], який формує числовий показник ризику у вигляді ймовірнісної оцінки належності до класу підвищеного ризику [17]. Порогове значення для бінарного рішення визначалося на валідаційній вибірці шляхом максимізації F_1-міри та становило 0.4655. За результатами тестування отримано такі показники якості: Accuracy 0.8856, Macro-F_1 0.8855, Precision 0.9091 і Recall 0.8568 для класу 0, Precision 0.8646 і Recall 0.9143 для класу 1, де клас 0 відповідає транзакційним патернам, що належать до легітимної множини (мітка white у датасеті), тобто не пов'язані з відомими сімействами програм-вимагачів, тоді як клас 1 відповідає патернам, асоційованим із програмами-вимагачами (мітки конкретних сімейств), тобто таким, що розглядаються як підвищено ризикові Вказані метрики наведено для підтвердження придатності модуля оцінювання ризику як джерела рішень, які надалі підлягають криптографічній фіксації та аудиту запропонованим методом.

Для ілюстрації роботи запропонованого підходу до фіксації та аудиту рішень сформовано репрезентативну вибірку тестових записів, яка містить як транзакції класу white, так і записи, пов'язані з відомими сімействами програм-вимагачів [18]. Для кожного запису позаланцюговий сервіс обчислював числовий показник ризику та формував ризик-клас відповідно до політики порогів, після чого створювався структурований запис журналу рішення з криптографічними зобов'язаннями та цифровим підписом і виконувався аудит за якорем, зафіксованим у розподіленому реєстрі [19]. Результати для вибірки прикладів наведено у Таблиці 2.

У таблиці 2 наведено вибірку тестових транзакційних записів із реальними мітками та результатами оцінювання ризику. Колонка TP/TN/FP/FN відображає узгодженість бінарного рішення з еталонною міткою, тоді як «статус аудиту» характеризує результат криптографічної перевірки цілісності та походження рішення.

Таблиця 2

Приклади рішень позаланцюгового сервісу оцінювання ризику та результати аудиту

№	tx_id	label	is_ransomware	risk_score	risk_class	TP/TN/FP/FN	Статус аудиту
1	333ba1579d…	white	0	0.4233	gray	TN	VERIFIED
2	d7c1f7b419…	princetonCerber	1	0.6636	gray	TP	VERIFIED
3	f41fcbce36…	montrealCryptoLocker	1	0.7645	gray	TP	VERIFIED
4	6c3f6c4608…	montrealDMALockerv3	1	0.9290	black	TP	VERIFIED
5	34e6ce2b0a…	montrealCryptXXX	1	0.9747	black	TP	VERIFIED
6	f69c7ea031…	princetonCerber	1	0.9808	black	TP	VERIFIED
7	cd3b81158f…	white	0	0.3538	gray	TN	VERIFIED
8	9e86074785…	montrealCryptoLocker	1	0.8311	black	TP	VERIFIED
9	c978ca7af7…	white	0	0.0599	white	TN	VERIFIED
10	5ff7a194e8…	paduaCryptoWall	1	0.9486	black	TP	VERIFIED

Для узагальненого представлення результатів експериментальної перевірки сформовано інтегральну візуалізацію, яка відображає розподіл сформованих ризик-класів за політикою порогів та узгодженість бінарного рішення з еталонними мітками датасету [20]. Додатково на рис.3 наведено агрегований результат криптографічного аудиту сформованих записів рішень, що підтверджує їх цілісність і походження в умовах відсутності втручання.

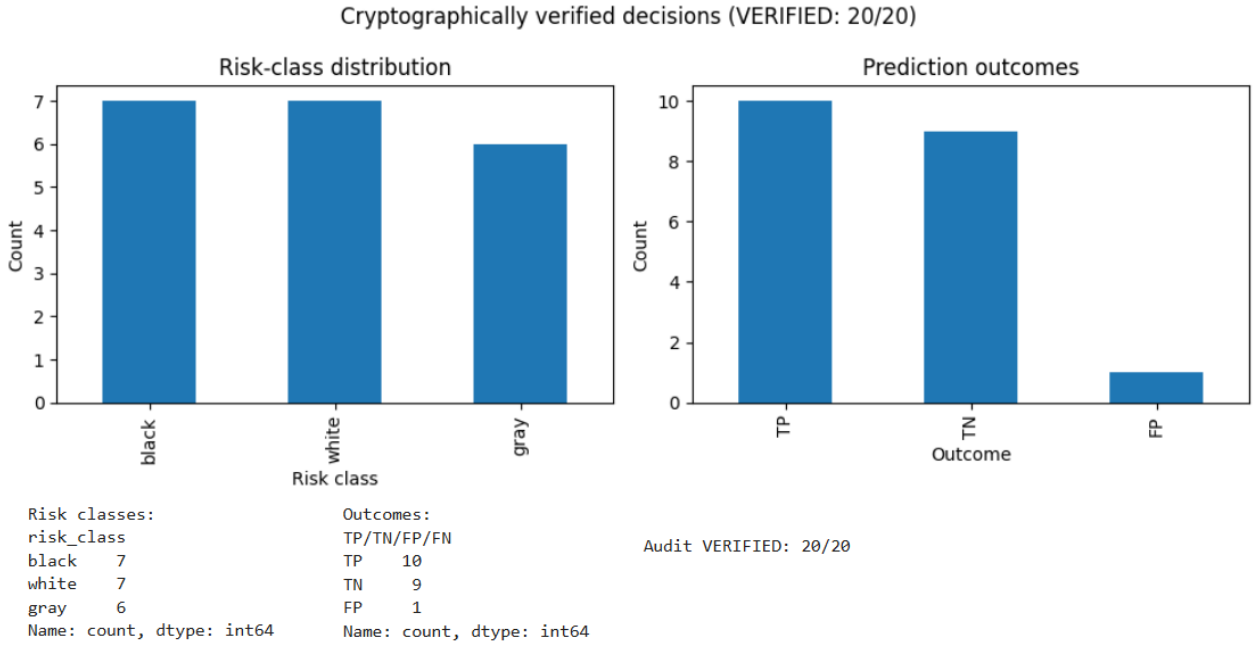

Рис. 3. Розподіл ризик-класів, узгодженість бінарних рішень з еталонними мітками та підсумок криптографічного аудиту записів рішень

З рис. 3 видно, що сформовані рішення сервісу покривають усі три класи ризику (white, gray, black), що підтверджує працездатність політики порогів та її здатність формувати проміжний клас для неоднозначних випадків. Розподіл результатів TP/TN/FP/FN демонструє узгодженість бінарної класифікації з еталонними мітками на вибірці прикладів, при цьому наявність поодиноких хибнопозитивних рішень відповідає очікуваній поведінці ризик-орієнтованого фільтра, чутливого до підозрілих патернів. Значення VERIFIED 20/20 підтверджує, що для кожного рішення забезпечено збіг хеш-зобов'язань і коректність цифрового підпису, а отже досягається криптографічно перевірюваний зв'язок між рішенням позаланцюгового сервісу та його внутрішньоланцюговим якорем без перенесення процедур оцінювання ризику у контур консенсусу.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У результаті дослідження розроблено та обґрунтовано метод підтримки цілісності та довіри до результатів обробки транзакцій у блокчейн-системах з криптографічно верифікованою фіксацією прийнятих рішень, спрямований на забезпечення доказової цілісності, перевірюваності походження та відтворюваності рішень упродовж життєвого циклу системи без втручання у базові механізми узгодження стану мережі. Метод передбачає формування однозначно структурованого запису рішення із фіксацією ключових параметрів контексту прийняття рішення, побудову криптографічного зобов'язання на основі стійкого хешування, накладення цифрового підпису довіреного сервісу та внутрішньоланцюгове закріплення мінімального набору перевірюваних метаданих у складі транзакції. Запропоновано процедуру верифікації та аудиту, яка забезпечує

повторне обчислення хеш-значення з канонічного подання запису, перевірку цифрового підпису та контроль цілісності послідовності журналювання, що унеможливлює непомітну підміну результату або модифікацію історії рішень. Експериментальна перевірка на відкритому транзакційному наборі даних підтвердила працездатність підходу: у штатному режимі рішення проходять криптографічну перевірку, а будь-які зміни у змісті рішення або порушення зв'язування записів виявляються під час аудиту.

Перспективи подальших досліджень пов'язані з розширенням умов застосування запропонованого методу у прикладних блокчейн-мережах на дозволах і в гібридних архітектурах, де рішення позаланцюгового оцінювання ризику впливають на політики допуску та виконання транзакцій. Також доцільним є детальне дослідження організації інфраструктури відкритих ключів, зокрема процедур ротації та відкликання ключів, із забезпеченням однозначної відтворюваності перевірки для історичних рішень. Окремої уваги потребує оцінювання накладних витрат методу за показниками затримки, пропускної здатності та обсягу додаткових даних у транзакціях, а також визначення меж застосовності для різних класів мережевих навантажень. Подальші роботи будуть спрямовані на формалізацію вимог до подання записів для забезпечення міжплатформної сумісності обчислення хеш-значень, а також на опрацювання підходів до збереження конфіденційності повних записів журналу транзакцій за збереження можливості незалежної перевірки коректності та незмінності рішень.

Література

1. Zara M., Wang S., ul Moin H. Blockchain-Based Verifiable Computation: A Review / M. Zara, S. Wang, H. ul Moin // Proceedings of the Pakistan Academy of Sciences: A. Physical and Computational Sciences. – 2024. – Vol. 61, No. 2. – P. 113–128.

2. Monteiro T. D., Sanchez O. P., Moraes G. H. S. M. D. Exploring off-chain voting and blockchain in decentralized autonomous organizations / T. D. Monteiro, O. P. Sanchez, G. H. S. M. D. Moraes // RAUSP Management Journal. – 2024. – Vol. 59, No. 4. – P. 335–349.

3. Heiss J., Grünewald E., Tai S., Haimerl N., Schulte S. Advancing blockchain-based federated learning through verifiable off-chain computations / J. Heiss, E. Grünewald, S. Tai, N. Haimerl, S. Schulte // Proceedings of IEEE International Conference on Blockchain (Blockchain 2022). – 2022. – P. 194–201.

4. Hartnell J. Verifiable Off-Chain Governance / J. Hartnell // arXiv preprint. – 2025. – arXiv:2512.23618. – DOI: 10.48550/arXiv.2512.23618.

5. Coppolino L., Cristiano G. M., D'Antonio S., Giglio J., Mazzeo G., Romano L. A Blockchain Solution for Decentralized Content Verification and its Application to Deepfake Detection and Fintech Credit Scoring / L. Coppolino, G. M. Cristiano, S. D'Antonio, J. Giglio, G. Mazzeo, L. Romano // Blockchain: Research and Applications. – 2025. – Article 100406.

6. South T., Camuto A., Jain S., Nguyen S., Mahari R., Paquin C., Pentland A. S. Verifiable evaluations of machine learning models using zkSNARKs / T. South, A. Camuto, S. Jain, S. Nguyen, R. Mahari, C. Paquin, A. S. Pentland // arXiv preprint. – 2024. – arXiv:2402.02675. – DOI: 10.48550/arXiv.2402.02675.

7. Keršič V., Karakatič S., Turkanović M. On-chain zero-knowledge machine learning: An overview and comparison / V. Keršič, S. Karakatič, M. Turkanović // Journal of King Saud University-Computer and Information Sciences. – 2024. – Vol. 36, No. 9. – Article 102207.

8. Zeng X., Xian Y., Li C., Hu Z., Zhou A., Liu P. DecTest: A Decentralised Testing Architecture for Improving Data Accuracy of Blockchain Oracle / X. Zeng, Y. Xian, C. Li, Z. Hu, A. Zhou, P. Liu // Proceedings of IEEE International Conference on Systems, Man, and Cybernetics (SMC 2024). – 2024. – P. 5105–5111.

9. Pasdar A., Lee Y. C., Dong Z. Connect API with blockchain: A survey on blockchain oracle implementation / A. Pasdar, Y. C. Lee, Z. Dong // ACM Computing Surveys. – 2023. – Vol. 55, No. 10. – P. 1–39.

10. Eberhardt J., Heiss J. Off-chaining models and approaches to off-chain computations / J. Eberhardt, J. Heiss // Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. – 2018. – P. 7–12.

11. Hasan M., Rahman M. S., Janicke H., Sarker I. H. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis / M. Hasan, M. S. Rahman, H. Janicke, I. H. Sarker // Blockchain: Research and Applications. – 2024. – Vol. 5, No. 3. – Article 100207.

12. Ashfaq T., Khalid R., Yahaya A. S., Aslam S., Azar A. T., Alsafari S., Hameed I. A. A machine learning and blockchain based efficient fraud detection mechanism / T. Ashfaq, R. Khalid, A. S. Yahaya, S. Aslam, A. T. Azar, S. Alsafari, I. A. Hameed // Sensors. – 2022. – Vol. 22, No. 19. – Article 7162.

13. Henry T., Assekour L., Rapetti A., Del Pozzo A., Tucci-Piergiovanni S. Secrets on the Chain: Cryptographic Blockchain Patterns for Verifiable and Confidential Data Handling / T. Henry, L. Assekour, A. Rapetti, A. Del Pozzo, S. Tucci-Piergiovanni // Blockchain: Research and Applications. – 2025. – Article 100422.

14. Bitcoin Heist Ransomware Address / Archive. – URL: https://archive.ics.uci.edu/dataset/526/bitcoinheistransomwareaddressdataset

15. Sobko O., Mazurets O., Molchanova M., Krak I., Barmak 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. – P. 84–98.

16. Niharika G., Sivasankar C. A Comparative Evaluation for False Data Injection Attacks using Bagging Classifier and XGB Classifier in enhancing the Control System Security / G. Niharika, C. Sivasankar // Proceedings of 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES). – 2024. – P. 1–5.

17. Zalutska O. O., Hladun O. V., Mazurets O. V. Method of Preventing Failures of Rotating Machines by Vibration Analysis Using Machine Learning Techniques / O. O. Zalutska, O. V. Hladun, O. V. Mazurets // Radio Electronics, Computer Science, Control. – 2025. – Vol. 1. – P. 142–152. – DOI: 10.15588/1607-3274-2025-1-13.

18. Cevallos-Salas D., Estrada-Jiménez J., Guamán D. S., Urquiza-Aguiar L. Ransomware dynamics: Mitigating personal data exfiltration through the SCIRAS lens / D. Cevallos-Salas, J. Estrada-Jiménez, D. S. Guamán, L. Urquiza-Aguiar // Computers & Security. – 2025. – Article 104583.

19. Molchanova M. O., Didur V. O., Mazurets O. V. Approach to Data Dimensionality Reduction and Defect Classification Based on Vibration Analysis for Maintenance of Rotating Machinery / M. O. Molchanova, V. O. Didur, O. V. Mazurets // Radio Electronics, Computer Science, Control. – 2025. – Vol. 1. – P. 84–95. – DOI: 10.15588/1607-3274-2025-1-8.

20. Li J. Area under the ROC Curve has the most consistent evaluation for binary classification / J. Li // PloS One. – 2024. – Vol. 19, No. 12. – Article e0316019.

References

1. Zara M., Wang S., ul Moin H. Blockchain-Based Verifiable Computation: A Review / M. Zara, S. Wang, H. ul Moin // Proceedings of the Pakistan Academy of Sciences: A. Physical and Computational Sciences. – 2024. – Vol. 61, No. 2. – P. 113–128.

2. Monteiro T. D., Sanchez O. P., Moraes G. H. S. M. D. Exploring off-chain voting and blockchain in decentralized autonomous organizations / T. D. Monteiro, O. P. Sanchez, G. H. S. M. D. Moraes // RAUSP Management Journal. – 2024. – Vol. 59, No. 4. – P. 335–349.

3. Heiss J., Grünewald E., Tai S., Haimerl N., Schulte S. Advancing blockchain-based federated learning through verifiable off-chain computations / J. Heiss, E. Grünewald, S. Tai, N. Haimerl, S. Schulte // Proceedings of IEEE International Conference on Blockchain (Blockchain 2022). – 2022. – P. 194–201.

4. Hartnell J. Verifiable Off-Chain Governance / J. Hartnell // arXiv preprint. – 2025. – arXiv:2512.23618. – DOI: 10.48550/arXiv.2512.23618.

5. Coppolino L., Cristiano G. M., DAntonio S., Giglio J., Mazzeo G., Romano L. A Blockchain Solution for Decentralized Content Verification and its Application to Deepfake Detection and Fintech Credit Scoring / L. Coppolino, G. M. Cristiano, S. DAntonio, J. Giglio, G. Mazzeo, L. Romano // Blockchain: Research and Applications. – 2025. – Article 100406.

6. South T., Camuto A., Jain S., Nguyen S., Mahari R., Paquin C., Pentland A. S. Verifiable evaluations of machine learning models using zkSNARKs / T. South, A. Camuto, S. Jain, S. Nguyen, R. Mahari, C. Paquin, A. S. Pentland // arXiv preprint. – 2024. – arXiv:2402.02675. – DOI: 10.48550/arXiv.2402.02675.

7. Keršič V., Karakatič S., Turkanović M. On-chain zero-knowledge machine learning: An overview and comparison / V. Keršič, S. Karakatič, M. Turkanović // Journal of King Saud University-Computer and Information Sciences. – 2024. – Vol. 36, No. 9. – Article 102207.

8. Zeng X., Xian Y., Li C., Hu Z., Zhou A., Liu P. DecTest: A Decentralised Testing Architecture for Improving Data Accuracy of Blockchain Oracle / X. Zeng, Y. Xian, C. Li, Z. Hu, A. Zhou, P. Liu // Proceedings of IEEE International Conference on Systems, Man, and Cybernetics (SMC 2024). – 2024. – P. 5105–5111.

9. Pasdar A., Lee Y. C., Dong Z. Connect API with blockchain: A survey on blockchain oracle implementation / A. Pasdar, Y. C. Lee, Z. Dong // ACM Computing Surveys. – 2023. – Vol. 55, No. 10. – P. 1–39.

10. Eberhardt J., Heiss J. Off-chaining models and approaches to off-chain computations / J. Eberhardt, J. Heiss // Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. – 2018. – P. 7–12.

11. Hasan M., Rahman M. S., Janicke H., Sarker I. H. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis / M. Hasan, M. S. Rahman, H. Janicke, I. H. Sarker // Blockchain: Research and Applications. – 2024. – Vol. 5, No. 3. – Article 100207.

12. Ashfaq T., Khalid R., Yahaya A. S., Aslam S., Azar A. T., Alsafari S., Hameed I. A. A machine learning and blockchain based efficient fraud detection mechanism / T. Ashfaq, R. Khalid, A. S. Yahaya, S. Aslam, A. T. Azar, S. Alsafari, I. A. Hameed // Sensors. – 2022. – Vol. 22, No. 19. – Article 7162.

13. Henry T., Assekour L., Rapetti A., Del Pozzo A., Tucci-Piergiovanni S. Secrets on the Chain: Cryptographic Blockchain Patterns for Verifiable and Confidential Data Handling / T. Henry, L. Assekour, A. Rapetti, A. Del Pozzo, S. Tucci-Piergiovanni // Blockchain: Research and Applications. – 2025. – Article 100422.

14. Bitcoin Heist Ransomware Address / Archive. – URL: https://archive.ics.uci.edu/dataset/526/bitcoinheistransomwareaddressdataset

15. Sobko O., Mazurets O., Molchanova M., Krak I., Barmak 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. – P. 84–98.

16. Niharika G., Sivasankar C. A Comparative Evaluation for False Data Injection Attacks using Bagging Classifier and XGB Classifier in enhancing the Control System Security / G. Niharika, C. Sivasankar // Proceedings of 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES). – 2024. – P. 1–5.

17. Zalutska O. O., Hladun O. V., Mazurets O. V. Method of Preventing Failures of Rotating Machines by Vibration Analysis Using Machine Learning Techniques / O. O. Zalutska, O. V. Hladun, O. V. Mazurets // Radio Electronics, Computer Science, Control. – 2025. – Vol. 1. – P. 142–152. – DOI: 10.15588/1607-3274-2025-1-13.

18. Cevallos-Salas D., Estrada-Jiménez J., Guamán D. S., Urquiza-Aguiar L. Ransomware dynamics: Mitigating personal data exfiltration through the SCIRAS lens / D. Cevallos-Salas, J. Estrada-Jiménez, D. S. Guamán, L. Urquiza-Aguiar // Computers & Security. – 2025. – Article 104583.

19. Molchanova M. O., Didur V. O., Mazurets O. V. Approach to Data Dimensionality Reduction and Defect Classification Based on Vibration Analysis for Maintenance of Rotating Machinery / M. O. Molchanova, V. O. Didur, O. V. Mazurets // Radio Electronics, Computer Science, Control. – 2025. – Vol. 1. – P. 84–95. – DOI: 10.15588/1607-3274-2025-1-8.

20. Li J. Area under the ROC Curve has the most consistent evaluation for binary classification / J. Li // PloS One. – 2024. – Vol. 19, No. 12. – Article e0316019.