КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1141
УДК 004.415:004.9

Аронов Андрій Олексійович
к.т.н., доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій,
Київ, Україна
ORCID:0009-0000-7868-8341
a.aronov@duikt.edu.ua

МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМ ШЛЯХОМ АДАПТИВНОГО ВИЯВЛЕННЯ АНОМАЛІЙ У БЛОКЧЕЙН-МЕРЕЖАХ ІЗ ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Анотація. У статті розглянуто проблему забезпечення безпеки децентралізованих інформаційних систем, зокрема блокчейн-мереж, що набувають широкого застосування у сучасних інформаційних технологіях. Визначено, що характерними особливостями таких систем є відсутність централізованого управління, розподілений характер обробки даних та відкритість мережі, що, з одного боку, підвищує їх стійкість до відмов, а з іншого - створює нові вектори атак та ускладнює процес виявлення загроз. Проаналізовано основні типи атак, притаманні блокчейн-середовищам, зокрема атаки типу Sybil, подвійне витрачання та аномальну поведінку вузлів. Обґрунтовано необхідність розробки проактивних методів виявлення загроз, що базуються на аналізі поведінкових характеристик учасників мережі. Запропоновано метод підвищення безпеки блокчейн-мереж, який поєднує графове представлення транзакційної структури, витяг інформативних ознак та застосування алгоритмів машинного навчання. Блокчейн-мережу формалізовано у вигляді орієнтованого графа, що дозволяє враховувати топологічні та часові аспекти взаємодії вузлів. Сформовано простір ознак, який включає транзакційні, часові, структурні та поведінкові характеристики. Для виявлення аномалій використано алгоритм Isolation Forest, що забезпечує ефективне визначення вузлів із нетиповою поведінкою без необхідності використання розмічених даних. Додатково введено адаптивну метрику довіри вузлів, яка враховує як рівень аномальності, так і відхилення поведінкових характеристик від нормального стану, що дозволяє підвищити точність і стабільність оцінювання. Проведене моделювання підтвердило ефективність запропонованого підходу. Отримані результати демонструють підвищення точності виявлення аномалій на 7-13% у порівнянні з традиційними методами, а також зменшення кількості хибнопозитивних спрацювань. Запропонований метод характеризується адаптивністю, масштабованістю та можливістю інтеграції у реальні блокчейн-платформи. Практична цінність роботи полягає у можливості використання отриманих результатів для створення систем моніторингу безпеки у децентралізованих середовищах, а також підвищення надійності функціонування інформаційних систем у сфері фінансових технологій, кібербезпеки та розподілених обчислень.

Ключові слова: блокчейн; децентралізовані системи; кібербезпека; виявлення аномалій; машинне навчання; графовий аналіз; метрика довіри; Isolation Forest, інформаційна технологія.

ВСТУП

Постановка проблеми. У сучасних умовах стрімкого розвитку цифрових технологій та зростання обсягів даних особливої актуальності набувають децентралізовані інформаційні системи. Однією з ключових технологій, що забезпечує реалізацію таких систем, є блокчейн, який дозволяє організувати розподілене зберігання та обробку даних без використання централізованих довірених сторін [4].

Завдяки своїм властивостям – незмінності даних, прозорості та відмовостійкості – блокчейн знаходить застосування у фінансових системах, електронному урядуванні, кіберфізичних системах та Інтернеті речей [3, 7]. Проте відсутність централізованого контролю та відкритий характер мережі створюють нові виклики у сфері кібербезпеки [3, 8].

Серед основних загроз функціонуванню блокчейн-мереж можна виділити атаки типу Sybil [9], double spending [3], маніпуляції транзакційними потоками [8], а також аномальну поведінку вузлів, що може призводити до порушення консенсусних механізмів [2]. Існуючі підходи до забезпечення безпеки переважно орієнтовані на реактивне виявлення атак або використовують статичні правила, що обмежує їх ефективність у динамічних умовах [1, 8].

У зв'язку з цим виникає необхідність розробки нових методів, які забезпечують проактивне виявлення загроз на основі аналізу поведінки учасників мережі та здатні адаптуватися до змін у структурі та інтенсивності транзакцій [2, 5].

Аналіз останніх досліджень і публікацій. Питання забезпечення безпеки децентралізованих систем та блокчейн-мереж активно досліджуються у сучасній науковій літературі [3, 4, 7, 12]. У наукових працях, присвячених цій тематиці, значна увага приділяється аналізу основних принципів функціонування блокчейн-технологій [4, 11], вивченню типових вразливостей, пов'язаних із реалізацією механізмів консенсусу [3, 8, 11], а також дослідженню впливу атак типу Sybil на стабільність мережі [9] та класифікації загроз для публічних блокчейн-систем [3, 7].

Окремий напрям досліджень пов'язаний із застосуванням методів машинного навчання для виявлення аномалій у мережевому трафіку та розподілених системах [1, 5, 6]. Такий підхід дозволяє підвищити ефективність виявлення нетипової поведінки вузлів і зменшити кількість хибних спрацьовувань за рахунок аналізу транзакційних, часових та структурних характеристик [2, 10].

Разом із тим аналіз сучасних підходів свідчить, що переважна частина робіт орієнтована або на використання графових моделей для аналізу транзакцій [3], або на застосування методів машинного навчання для класифікації вузлів [2, 5], тоді як питання адаптивної оцінки довіри до вузлів та інтеграції графового аналізу з методами машинного навчання в єдину систему виявлення загроз висвітлено недостатньо [2, 5]. Навіть у випадках, коли модель здатна виявити аномалію з високою точністю, не завжди враховуються структурні особливості блокчейн-мереж, зокрема їх графова природа та специфіка транзакційних взаємодій [2, 10], що обмежує можливості практичного застосування отриманих результатів.

Таким чином, існує потреба у створенні методу, який би поєднував графове представлення транзакційної структури, витяг інформативних ознак, адаптивну оцінку довіри вузлів та застосування алгоритмів машинного навчання в єдину систему виявлення аномалій [2, 5, 10]. Такий підхід є доцільним як з точки зору підвищення точності виявлення загроз у децентралізованих мережах, так і з точки зору забезпечення адаптивності та масштабованості систем моніторингу безпеки [1, 5].

Метою статті є розробка методу підвищення безпеки блокчейн-мереж на основі адаптивного виявлення аномалій шляхом поєднання графового аналізу транзакцій та алгоритмів машинного навчання.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для забезпечення ефективного аналізу поведінки учасників децентралізованої системи блокчейн-мережу доцільно формалізувати у вигляді математичної моделі. У даній роботі запропоновано представляти блокчейн як орієнтований зважений граф:

$$G = (V, E) \tag{1}$$

де $V = \{v_1, v_2, \dots, v_n\}$ } – множина вузлів мережі (адрес або користувачів), $E = \{e_{ij}\}$ – множина ребер, що відображають транзакції між вузлами.

Кожне ребро $e_{ij} \in E$ відповідає транзакції від вузла v_i до вузла v_j та характеризується набором атрибутів:

$$e_{ij} = (a_{ij}, t_{ij}, f_{ij}) \tag{2}$$

де a_{ij} – обсяг транзакції, t_{ij} – часовий штамп, f_{ij} – частота взаємодії між вузлами.

З урахуванням динамічного характеру блокчейн-мережі вводиться часове вікно аналізу ΔT, у межах якого формується підграф:

$$G_{\Delta T} = (V_{\Delta T}, E_{\Delta T}) \tag{3}$$

Це дозволяє враховувати зміну поведінки вузлів у часі та виявляти короткочасні аномалії.

Для кожного вузла визначаються основні топологічні характеристики:

- вхідний ступінь deg−(v);
- вихідний ступінь deg+(v);
- загальний ступінь зв'язності;
- коефіцієнт кластеризації;
- середня довжина шляху до інших вузлів.

Запропонована модель дозволяє формалізувати структуру транзакцій у блокчейн-мережі, враховувати часову динаміку взаємодій та підготувати дані для подальшого застосування методів машинного навчання.

Таким чином, представлення блокчейн-мережі у вигляді графа створює основу для побудови ефективних алгоритмів виявлення аномальної поведінки вузлів.

Для забезпечення можливості автоматизованого виявлення аномалій у блокчейн-мережі необхідно сформувати інформативний простір ознак, який відображає поведінкові характеристики вузлів. На основі побудованої графової моделі $G_{\Delta T}$ для кожного вузла $v \in V$ формується вектор ознак:

$$X(v) = \{x_1, x_2, \dots, x_k\} \tag{4}$$

де x_i – окрема характеристика вузла.

У роботі запропоновано використовувати такі групи ознак:

Транзакційні ознаки відображають інтенсивність та характер фінансових операцій вузла:

$$x_1(v) = N_{tx}(v) = \sum_j I(e_{vj}) \tag{5}$$

де $N_{tx}(v)$ – кількість транзакцій вузла за період ΔT, I(·) – індикатор наявності транзакції.

Середній обсяг транзакцій:

$$x_2(v) = \frac{1}{N_{tx}(v)} \sum_j a_{vj} \tag{6}$$

Дисперсія обсягів транзакцій:

$$x_3(v) = \frac{1}{N_{tx}(v)} \sum_j \left(a_{vj} - x_2(v)\right)^2 \tag{7}$$

Часові ознаки дозволяють оцінити регулярність активності вузла:

Середній інтервал між транзакціями:

$$x_4(v) = \frac{1}{N_{tx}(v) - 1} \sum_k (t_{k+1} - t_k) \tag{8}$$

Коефіцієнт варіації інтервалів:

$$x_5(v) = \frac{\sigma_t}{\mu_t} \tag{9}$$

де μ_t – середній інтервал, σ_t – стандартне відхилення.

Структурні (графові) ознаки характеризують положення вузла у мережі.

Вхідний та вихідний ступені:

$$x_6(v) = deg^-(v), \quad x_7(v) = deg^+(v) \tag{10}$$

Коефіцієнт кластеризації:

$$x_8(v) = \frac{2E_v}{k_v(k_v - 1)} \tag{11}$$

де E_v – кількість зв'язків між сусідами вузла, k_v – кількість сусідів.

Поведінкові ознаки відображають стабільність або аномальність дій вузла:

Коефіцієнт активності:

$$x_9(v) = \frac{N_{tx}(v)}{\Delta T} \tag{12}$$

Коефіцієнт зміни активності:

$$x_{10}(v) = \left| \frac{N_{tx}^{(t)} - N_{tx}^{(t-1)}}{N_{tx}^{(t-1)}} \right| \tag{13}$$

Сформований вектор ознак $X(v)$ дозволяє розглядати кожен вузол як точку у багатовимірному просторі. Нормальна поведінка вузлів характеризується відносною стабільністю ознак та їх належністю до певних кластерів.

Аномальна поведінка проявляється у вигляді:

- різких змін транзакційної активності;
- нетипових обсягів операцій;
- відхилень у часових інтервалах;
- аномальної топологічної позиції у графі.

Таким чином, задача виявлення аномалій зводиться до ідентифікації вузлів, ознаки яких суттєво відхиляються від нормального розподілу.

Запропонований підхід до формування ознак забезпечує комплексне врахування як структурних, так і поведінкових характеристик вузлів, що є основою для подальшого застосування алгоритмів машинного навчання.

На основі сформованого простору ознак $X(v)$ задача виявлення аномалій у блокчейн-мережі формалізується як задача пошуку вузлів, поведінка яких суттєво відрізняється від більшості.

Нехай задано множину вузлів $V = \{v_1, v_2, \dots, v_n\}$ та відповідні вектори ознак $X(v_i) \in R^k$ Необхідно визначити функцію аномальності $A: V \to [0,1]$, де значення $A(v) \to 1$ відповідає високій ймовірності аномальної поведінки.

Для розв'язання задачі виявлення аномалій у роботі запропоновано використання алгоритму Isolation Forest, який належить до класу методів неконтрольованого навчання.

Основною ідеєю алгоритму є те, що аномальні об'єкти мають меншу щільність у просторі ознак та швидше ізолюються при випадковому розбитті простору.

Для кожного вузла v визначається середня довжина шляху ізоляції h(v) у ансамблі дерев.

Нормалізований показник аномальності обчислюється як:

$$A(v) = 2^{-\frac{E(h(v))}{c(n)}} \tag{14}$$

де $E(h(v))$ – середня довжина шляху до ізоляції вузла, $c(n)$ – коефіцієнт нормалізації, що залежить від розміру вибірки n.

Чим менше значення $E(h(v))$, тим більша ймовірність того, що вузол є аномальним.

Рис. 1. Алгоритм виявлення аномалій

Для врахування динаміки мережі запропоновано адаптивний механізм оновлення моделі:

- використання ковзного часового вікна ΔT;
- періодичне перенавчання моделі;
- оновлення статистичних параметрів ознак.

Це дозволяє:

- враховувати зміну поведінки вузлів;
- зменшувати кількість хибних спрацювань;

– підвищувати точність у реальному часі.

4. Метрика довіри вузлів. Для підвищення ефективності виявлення загроз у блокчейн-мережі доцільно не лише визначати аномальні вузли, але й оцінювати рівень довіри до кожного учасника мережі. З цією метою у роботі запропоновано адаптивну метрику довіри, яка враховує як нормальну поведінку вузла, так і ступінь його аномальності.

$$Trust(v) = \alpha \cdot N(v) - \beta \cdot A(v) \tag{15}$$

де N(v) – узагальнений показник нормальної поведінки вузла; A(v) – рівень аномальності;
α,β – вагові коефіцієнти, що визначають внесок кожного компонента.

Показник нормальної поведінки N(v) визначається на основі відхилення ознак вузла від середніх значень у мережі:

$$N(v) = 1 - \frac{1}{k}\sum_{i=1}^{k}\left|\frac{x_i(v) - \mu_i}{\sigma_i}\right| \tag{16}$$

де $\mu_i \sigma_i$ – середнє значення та стандартне відхилення і-ї ознаки; k – кількість ознак.

Чим ближче значення ознак вузла до середніх, тим більшим є *N(v)*.

Для забезпечення інтерпретованості результатів значення довіри нормалізується до інтервалу:

$$Trust'(v) \in [0,1] \tag{17}$$

за допомогою лінійного перетворення:

$$Trust'(v) = \frac{Trust(v) - Trust_{min}}{Trust_{max} - Trust_{min}} \tag{18}$$

З урахуванням динамічного характеру блокчейн-мережі вводиться механізм оновлення довіри у часі:

$$Trust_t(v) = \gamma \cdot Trust_{t-1}(v) + (1 - \gamma) \cdot Trust_{new}(v) \tag{19}$$

де $\gamma \in [0,1]$ – коефіцієнт “забування”; $Trust_{new}(v)$ – значення, отримане на поточному кроці.

Такий підхід дозволяє враховувати історію поведінки вузла, згладжувати випадкові коливання та швидко реагувати на появу аномалій.

На основі значення Trust'(v) вузли можуть бути класифіковані:

– > 0.7 – надійні вузли;
– 0.4 < Trust′(v) ≤ 0.7 – нейтральні;
– ≤ 0.4 – потенційно небезпечні.

Це дозволяє використовувати метрику довіри для фільтрації транзакцій, модифікації консенсусних механізмів та обмеження активності підозрілих вузлів.

На рис.1 представлено блок-схему методу підвищення безпеки децентралізованих систем шляхом адаптивного виявлення аномалій у блокчейн-мережах із використанням машиного навчання.

Запропонована блок-схема відображає послідовність роботи методу підвищення безпеки блокчейн-мереж шляхом адаптивного виявлення аномалій із використанням алгоритмів машинного навчання. Основою методу є формування графового представлення транзакційної структури блокчейн-мережі, що дозволяє враховувати не лише характеристики окремих транзакцій, а й структурні взаємозв’язки між вузлами. У межах часового вікна здійснюється збір та попередня обробка даних, після чого формується простір ознак, який включає транзакційні, часові, структурні та поведінкові параметри вузлів мережі.

Подальший етап передбачає застосування алгоритму Isolation Forest для визначення рівня аномальності кожного вузла. На основі отриманих результатів обчислюється адаптивна метрика довіри, що дозволяє класифікувати вузли за рівнем надійності та виявляти потенційно небезпечні об’єкти мережі. Використання механізму адаптації та періодичного перенавчання моделі забезпечує врахування змін у поведінці учасників блокчейн-мережі та підвищує стійкість системи до динамічних атак і короткочасних аномалій. Це дозволяє підвищити точність виявлення загроз, зменшити кількість

хибнопозитивних спрацювань та забезпечити більш ефективний моніторинг безпеки децентралізованих систем.

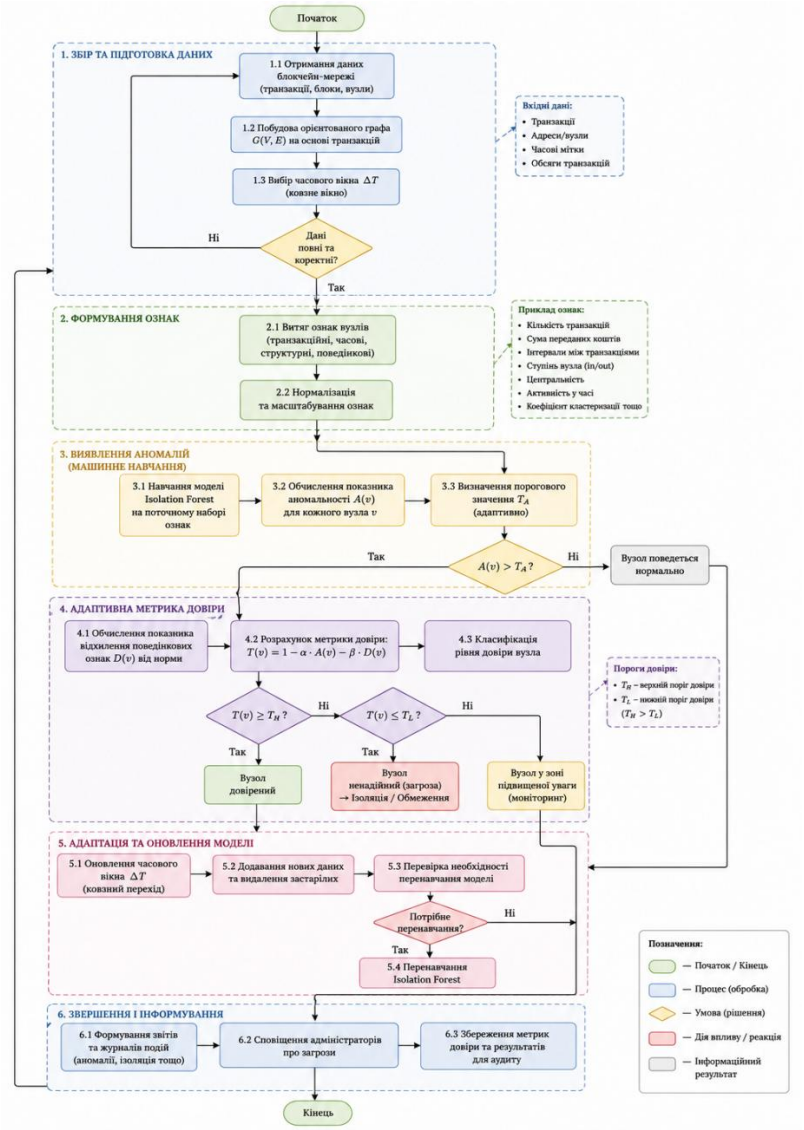

Рис. 2. Блок-схема методу підвищення безпеки децентралізованих систем шляхом адаптивного виявлення аномалій у блокчейн-мережах із використанням машиного навчання

5. Результати моделювання. Для оцінки ефективності запропонованого методу було проведено моделювання процесу виявлення аномалій у блокчейн-мережі на основі синтетичних та напівреальних даних транзакцій.

Таблиця 1

Параметри мережі

Кількість вузлів	1000
Кількість транзакцій	> 50 000
Часовий інтервал аналізу	24 години
Частка аномальних вузлів	5-10%

Аномальна поведінка моделювалася шляхом:

- різкого збільшення частоти транзакцій (імітація Sybil-атак);
- генерації нетипових обсягів транзакцій;
- створення штучних кластерів взаємодії.

Таблиця 2

Порівняння запропонованого методу

Метод	Accuracy	Recall	F1-score
Пороговий аналіз	0,78	0,71	0,74
K-means	0,81	0,75	0,78
Без графових ознак	0,84	0,79	0,81
Запропонований метод	0,91	0,88	0,89

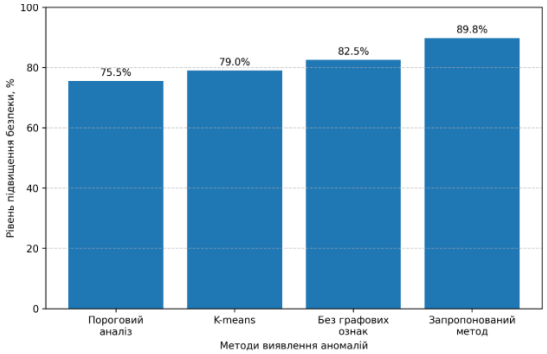

Рис. 3. Оцінка рівня підвищення безпеки децентралізованої системи за різними методами виявлення аномалій

Результати оцінювання рівня підвищення безпеки свідчать, що запропонований метод забезпечує найвищі показники ефективності серед розглянутих підходів. Підвищення інтегрального показника безпеки досягається завдяки поєднанню графового аналізу транзакцій, алгоритму Isolation Forest та адаптивної метрики довіри вузлів, що дозволяє більш точно виявляти аномальну поведінку у блокчейн-мережі.

Отримані результати підтверджують, що використання комплексного підходу до аналізу поведінкових, структурних та часових характеристик вузлів дозволяє зменшити кількість хибнопозитивних спрацювань і підвищити стійкість децентралізованої системи до атак типу Sybil, маніпуляцій транзакціями та інших аномальних впливів.

Аналіз отриманих результатів. Результати моделювання свідчать, що запропонований метод демонструє підвищення точності виявлення аномалій на 7-13% у порівнянні з базовими підходами, значне зростання повноти, що вказує на кращу здатність виявляти реальні атаки. Збалансованість показників, підтверджену високим значенням F1-міри.

Покращення результатів досягається за рахунок використання комплексного простору ознак, врахування графової структури транзакцій та застосування алгоритму Isolation Forest.

Використання метрики довіри дозволило зменшити кількість хибнопозитивних спрацювань на 10-15%, більш точно ідентифікувати вузли з нестабільною поведінкою та підвищити стійкість системи до короткочасних аномалій.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розроблено комплексний підхід до виявлення аномальної поведінки вузлів у блокчейн-мережах на основі графового представлення транзакцій, методів витягу ознак та алгоритмів машинного навчання. На відміну від традиційних підходів, запропонована модель поєднує транзакційні, часові, структурні та поведінкові характеристики вузлів у єдиній логіці аналізу, використовує алгоритм Isolation Forest для виявлення аномалій без розмічених даних і доповнює її адаптивною метрикою довіри, що враховує як нормальну поведінку, так і рівень аномальності.

Наукова новизна роботи полягає у введенні адаптивної метрики довіри вузлів до структури виявлення аномалій на основі Isolation Forest у блокчейн-мережах. Запропонований підхід визначено як інтегрований результат аналізу транзакційної активності, часової динаміки, структурних зв’язків та поведінкових патернів вузлів.

Практичне значення полягає у підвищенні точності виявлення аномалій, зменшенні кількості хибних спрацювань, покращенні моніторингу безпеки децентралізованих інформаційних систем, а також у можливості подальшої інтеграції запропонованої метрики довіри у механізми прийняття рішень та консенсусні алгоритми.

Перспективами подальших досліджень є застосування глибинних нейронних мереж для покращення якості виявлення складних аномалій; дослідження масштабованості методу для великих блокчейн-мереж; адаптація підходу до приватних та консорціумних блокчейн-систем; інтеграція метрики довіри у консенсусні алгоритми; а також використання потокової обробки даних для реалізації виявлення аномалій у режимі реального часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ahmed, M., Naser Mahmood, A., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19-31. https://doi.org/10.1016/j.jnca.2015.11.016
2. Cholevas, C., et al. (2024). Anomaly detection in blockchain networks using unsupervised learning: A survey. *Algorithms, 17*(5), 201. https://doi.org/10.3390/a17050201
3. Conti, M., et al. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416-3452. https://doi.org/10.1109/COMST.2018.2842460
4. Zheng, Z., et al. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352. https://doi.org/10.1504/IJWGS.2018.095647
5. Luo, Y., et al. (2021). Deep learning-based anomaly detection in cyber-physical systems. *ACM Computing Surveys, 54*(5), 1-36. https://doi.org/10.1145/3453155
6. Hodge, V., & Austin, J. (2004). A survey of outlier detection methodologies. *Artificial Intelligence Review, 22*(2), 85-126. https://doi.org/10.1023/B:AIRE.0000045502.10941.A9
7. Lee, M. S., & Jang, D. J. (2020). A survey of blockchain security issues. *JP Journal of Heat and Mass Transfer*, Special Issue, 29-35. https://doi.org/10.17654/HMSI120029
8. Mostafa, M. (2020). Bitcoin's blockchain peer-to-peer network security attacks and countermeasures. *Indian Journal of Science and Technology, 13*(7), 767-786. https://doi.org/10.17485/ijst/2020/v13i07/149691
9. Ramchandani, H. K. (2012). Sybil attack. *Engineering & Technology Reference, 1*(1). https://doi.org/10.1049/etr.2016.0101
10. Sakurada, M., & Yairi, T. (2014). Anomaly detection using autoencoders with nonlinear dimensionality reduction. In *Proceedings of the 2nd Workshop on Machine Learning for Sensory Data Analysis (MLSDA 2014)*. ACM. https://doi.org/10.1145/2689746.2689747
11. Malinov, V., Zhebka, V., Kokhan, I., Storchak, K., & Dovzhenko, T. (2024). Cryptocurrency as a tool for attracting investment and ensuring the strategic development of the bioenergy potential of processing enterprises in Ukraine. *Lecture Notes on Data Engineering and Communications Technologies, 195*, 387-405. https://doi.org/10.1007/978-3-031-54012-7_17
12. Zhebka, V., Zhebka, S., Bazhan, T., Skladannyi, P., & Sokolov, V. (2024). Methodology for choosing a consensus algorithm for blockchain technology. *CEUR Workshop Proceedings*. https://ceur-ws.org/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Andrii Aronov
Candidate of Technical Sciences, Associate Professor at the Department of Digital Development Technologies State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID:0009-0000-7868-8341
a.aronov@duikt.edu.ua

METHOD FOR ENHANCING THE SECURITY OF DECENTRALIZED SYSTEMS THROUGH ADAPTIVE ANOMALY DETECTION IN BLOCKCHAIN NETWORKS USING MACHINE LEARNING

Abstract. The article addresses the problem of ensuring the security of decentralized information systems, particularly blockchain networks, which are becoming widely adopted in modern information technologies. It is determined that the characteristic features of such systems include the absence of centralized control, the distributed nature of data processing, and network openness. On the one hand, these features increase fault tolerance, but on the other hand, they create new attack vectors and complicate the threat detection process. The main types of attacks inherent to blockchain environments are analyzed, including Sybil attacks, double-spending attacks, and anomalous node behavior. The necessity of developing proactive threat detection methods based on analyzing the behavioral characteristics of network participants is substantiated. A method for enhancing the security of blockchain networks is proposed, which combines a graph-based representation of the transactional structure, extraction of informative features, and the application of machine learning algorithms. The blockchain network is formalized as a directed graph, allowing for the consideration of topological and temporal aspects of node interactions. A feature space is formed, including transactional, temporal, structural, and behavioral characteristics.To detect anomalies, the Isolation Forest algorithm is used, which effectively identifies nodes with atypical behavior without the need for labeled data. Additionally, an adaptive node trust metric is introduced, which takes into account both the anomaly level and the deviation of behavioral characteristics from the normal state, thereby improving the accuracy and stability of the assessment. Conducted simulations confirm the effectiveness of the proposed approach. The obtained results demonstrate an increase in anomaly detection accuracy by 7-13% compared to traditional methods, as well as a reduction in the number of false positives. The proposed method is characterized by adaptability, scalability, and the ability to be integrated into real blockchain platforms. The practical value of the work lies in the possibility of using the obtained results to create security monitoring systems for decentralized environments, as well as to enhance the reliability of information systems in the fields of financial technology, cybersecurity, and distributed computing.

Keywords: blockchain; decentralized systems; cybersecurity; anomaly detection; machine learning; graph analysis; trust metric; Isolation Forest, information technology.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ahmed, M., Naser Mahmood, A., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19-31. https://doi.org/10.1016/j.jnca.2015.11.016
2. Cholevas, C., et al. (2024). Anomaly detection in blockchain networks using unsupervised learning: A survey. *Algorithms, 17*(5), 201. https://doi.org/10.3390/a17050201
3. Conti, M., et al. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416-3452. https://doi.org/10.1109/COMST.2018.2842460
4. Zheng, Z., et al. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352. https://doi.org/10.1504/IJWGS.2018.095647
5. Luo, Y., et al. (2021). Deep learning-based anomaly detection in cyber-physical systems. *ACM Computing Surveys, 54*(5), 1-36. https://doi.org/10.1145/3453155
6. Hodge, V., & Austin, J. (2004). A survey of outlier detection methodologies. *Artificial Intelligence Review, 22*(2), 85-126. https://doi.org/10.1023/B:AIRE.0000045502.10941.A9

7. Lee, M. S., & Jang, D. J. (2020). A survey of blockchain security issues. *JP Journal of Heat and Mass Transfer*, Special Issue, 29-35. https://doi.org/10.17654/HMSI120029
8. Mostafa, M. (2020). Bitcoin's blockchain peer-to-peer network security attacks and countermeasures. *Indian Journal of Science and Technology*, *13*(7), 767-786. https://doi.org/10.17485/ijst/2020/v13i07/149691
9. Ramchandani, H. K. (2012). Sybil attack. *Engineering & Technology Reference*, *1*(1). https://doi.org/10.1049/etr.2016.0101
10. Sakurada, M., & Yairi, T. (2014). Anomaly detection using autoencoders with nonlinear dimensionality reduction. In *Proceedings of the 2nd Workshop on Machine Learning for Sensory Data Analysis (MLSDA 2014)*. ACM. https://doi.org/10.1145/2689746.2689747
11. Malinov, V., Zhebka, V., Kokhan, I., Storchak, K., & Dovzhenko, T. (2024). Cryptocurrency as a tool for attracting investment and ensuring the strategic development of the bioenergy potential of processing enterprises in Ukraine. *Lecture Notes on Data Engineering and Communications Technologies*, *195*, 387-405. https://doi.org/10.1007/978-3-031-54012-7_17
12. Zhebka, V., Zhebka, S., Bazhan, T., Skladannyi, P., & Sokolov, V. (2024). Methodology for choosing a consensus algorithm for blockchain technology. *CEUR Workshop Proceedings*. https://ceur-ws.org/

Отримано редакцією журналу / Received: 26.02.26
Прорецензовано / Revised: 10.03.26
Схвалено до друку / Accepted: 25.06.26