КОМБИНИРОВАНИЕ МЕТОДОВ ТОПОЛОГИЧЕСКОГО АНАЛИЗА ДАННЫХ И ГРАФОВЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В БЛОКЧЕЙН-СИСТЕМАХ ЛОГИСТИКИ

Владимиркин А. А.[1]

DOI: 10.21681/2311-3456-2026-2-37-44

Цель исследования: *повышение качества обнаружения аномалий в блокчейн-системах логистики на основе методов топологического анализа данных и графовых нейронных сетей.*

Методы исследования: *комбинирование алгебраической топологии и графовых нейронных сетей в рамках гибридной модели классификации узлов. Верификация подхода выполнена посредством полусинтетического моделирования циклических и кластерных атак на транзакциях логистической сети.*

Результаты исследования: *в статье раскрыты вопросы, связанные с влиянием аномалий в блокчейн-системах логистики на цепочки поставок и эффективность грузопотоков. Отмечена необходимость применения прогрессивного подхода для своевременного обнаружения и управление аномалиями в режиме реального времени за счет интеграции таких технологий, как машинное обучение и анализ больших данных. Проведена сравнительная характеристика различных методов детектирования отклонений в распределенных реестрах, отмечены их достоинства и недостатки. Разработан гибридный подход к обнаружению аномалий в блокчейне, реализующий совместную обработку транзакционных данных методами графовых нейронных сетей и алгебраической топологии.*

Научная новизна: *в отличие от известных методов, основанных на локальной агрегации признаков, гибридный подход позволяет выявлять глобальные структурные аномалии, обеспечивая полноту обнаружения сложных схем фиктивного оборота.*

Ключевые слова: *распределенный реестр, граф транзакций, персистентная диаграмма, персистентная гомология, гибридный вектор признаков, циклическая фальсификация, кластерный сговор, темпоральные нарушения.*

Введение

В эпоху цифровой глобализации логистика превратилась в сложную экосистему, основанную на данных, в которой поток товаров, информации и решений должен управляться в режиме реального времени по взаимосвязанным сетям. Обеспечивать и удовлетворять данные требования на высоком уровне позволяет технология блокчейн, которая стала одной из самых революционных инноваций XXI века, предлагая беспрецедентные возможности в области распределенного хранения данных, одноранговой передачи, высокой конфиденциальности и удобной отслеживаемости [1]. Третье поколение блокчейна (Blockchain 3.0) позволило осуществлять программируемые транзакции, самоисполняющийся код, который запускается при выполнении определенных условий, известный как смарт-контракты.

Однако, увеличение масштабов и сложности международных цепочек поставок привело к тому, что блокчейн-системы логистики стали подвержены широкому спектру неожиданных аномалий, которые нарушают операционную эффективность, ставят под угрозу целостность данных или сигнализируют о киберфизических угрозах. Аномалии в сетях блокчейна могут принимать различные формы, включая вредоносные учетные записи, финансовые пирамиды, уязвимости PoW, криптоджекинг, спам-транзакции, атаки на кошельки, фишинговые атаки и многое другое [2]. В таблице 1 представлены данные, которые наглядно свидетельствуют о критическом уровне финансовых и операционных потерь, связанных с аномалиями блокчейна в глобальных цепочках поставок.

Таблица 1 убедительно доказывает тот факт, что обнаружение аномалий в блокчейн-системах логистики приобретает первостепенное значение. Это помогает выявлять и предотвращать потенциальные вредоносные действия, тем самым поддерживая целостность системы. Тем не менее, присущий дисбаланс между нормальными и аномальными данными в информационных массивах блокчейна, представляет собой существенную проблему для традиционных методов детектирования. Во многих случаях частота аномальных точек данных значительно меньше по сравнению с частотой нормальных точек, что приводит к несбалансированным наборам данных [3]. Такое искаженное распределение может негативно

1 **Владимиркин Андрей Андреевич**, аспирант кафедры «Прикладная математика и информатика» Ульяновского Государственного Технического Университета, Ульяновск, Россия. E-mail: vladimirkin2017@gmail.com

Таблица 1.

Оценка ущерба от аномалий в блокчейн-логистике[2]

Тип инцидента / аномалии	Средний ущерб на 1 инцидент	Доля скомпрометированных операций (%)	Характер последствий
Циклическая накрутка	$45,000 – $120,000	1,5 %–3,2 %	Искажение рыночных цен, неверное начисление бонусов поставщикам
Подмена данных	$200,000+	4,8 %	Приемка контрафакта, нарушение температурного режима
Фиктивный документооборот	$500,000 – $2M	0,9 %	Двойное финансирование одной поставки
Простои из-за сбоев	$15,000 / час	—	Штрафы за срыв сроков, порча скоропортящихся грузов

повлиять на эффективность алгоритмов обнаружения аномалий. Эти алгоритмы, часто смещенные в сторону мажоритарного класса, испытывают трудности с точным определением аномальных данных. Кроме того, выявление аномалий в блокчейн-сетях, используемых в логистических приложениях, существенно усложняется вследствие значительного объема и высокой динамики транзакционных потоков, отражающих перемещение товаров и сопроводительных документов, возрастающей сложности мошеннических схем, а также выраженной несбалансированности данных, обусловленной редкостью аномальных логистических операций и участников.

Обозначенные проблемы сделали обнаружение аномалий ключевой областью исследований в системах блокчейна, что и предопределило выбор темы данной статьи.

1. Анализ публикаций по теме исследования

Подходы для прогнозирования аномалий в транзакциях с помощью концепции блокчейн-аналитики, т.е. внедрения инструментов искусственного интеллекта для обнаружения мошенничества в данных блокчейн-транзакций, рассматривают в своих трудах Владимиркин А. А. [4], Утакаева И. Х. [5], Shiyang Chen, Yang Liu, Qun Zhang, Zhouhang Shao, Zewei Wang [6].

Перспективы использования глубокого обучения и алгоритмов без учителя в задачах нахождения аномалий распределенного реестра с отдельным акцентом на потенциал этих методов для обнаружения сложных и новых типов отклонений без необходимости предварительной разметки данных, описывают Haoyang Tan, Qiang Zhang, Mingxian Li, Xinxing Liu, Lei Hu [7], Попова М. В. [8].

2 Данные агрегированы автором на основе анализа рисков цифровых платформ Supply Chain Finance.

2. Нерешенные части общей проблемы

Несмотря на активное развитие блокчейн-технологий в логистике, вопросы автоматического обнаружения аномалий остаются недостаточно изученными. Так, отдельного внимания заслуживает задача разработки методов, обеспечивающих интерпретируемость и объяснимость обнаруженных аномалий. Кроме того, проблема выявления отклонений в блокчейн-логистике усложняется отсутствием методов, способных эффективно работать с потоками данных в реальном времени и адаптироваться к изменяющейся структуре сети. Отдельный акцент следует сделать на том, что большинство существующих решений недостаточно масштабируемы для работы с большими и распределёнными блокчейн-сетями, что препятствует их практическому применению в сложных логистических системах.

3. Выбор подхода для обнаружения аномалий

Анализ существующих подходов к выявлению нелегитимной активности в распределенных реестрах выявил критический разрыв между возможностями современных алгоритмов и сложностью атак в логистике. Установлено, что классические алгоритмы и базовые нейронные сети не способны надежно детектировать глобальные структурные аномалии, такие как многоходовые циклические транзакции, из-за ограничений рецептивного поля и потери информации при агрегации [9, 10, 11]. В целях формализации данных ограничений автором было проведено сопоставление методов по ключевым для данной задачи критериям: способности учитывать реляционную структуру данных и глобальную топологию сети. Особое внимание в ходе анализа уделялось оценке устойчивости алгоритмов к специфическим для цепочек поставок паттернам мошенничества, включая кольцевые схемы и кластерный сговор. Итоговая

Таблица 2.

Сравнительный анализ различных подходов к обнаружению аномалий в блокчейн-логистике[3]

Методы	Математический базис	Уровень анализа данных	Преимущества	Ограничения и недостатки в задачах логистики
Статистические методы	Анализ плотности распределения, построение разделяющих гипер-плоскостей	Атрибутивный. Анализируются только признаки отдельной транзакции (сумма, время).	Высокая скорость работы, интерпретируемость результатов. Эффективны для поиска выбросов в числовых данных.	Игнорирование структуры. Не учитывают связи между контрагентами. Неспособны выявить схемы сговора или циклические накрутки, если суммы транзакций выглядят «нормально».
Методы случайных блужданий	Стохастические процессы, матричная факторизация.	Локально-структурный. Учитывают ближайшее окружение узла.	Способность обучаться на неразмеченных данных, учет локального контекста.	Потеря глобальной информации. Плохо масштабируются на динамических графах. Низкая эффективность при обнаружении сложносоставных атак (длинных цепочек).
Графовые нейронные сети	Спектральная свертка, механизм агрегации сообщений	Соседский (k-hop). Агрегация признаков от соседей на k шагов.	SOTA-решение для классификации узлов. Учитывают и атрибуты, и локальные связи.	Проблема пересглаживания. При увеличении глубины сети векторы узлов становятся неразличимыми. Сложность в детектировании замкнутых циклов, если они превышают радиус рецептивного поля.
Топологический анализ данных	Алгебраическая топология, персистентные гомологии (H_0, H_1,...).	Глобально-структурный. Анализ формы данных и инвариантов (пустот, компонент связности).	Устойчивость к шуму и деформациям. Безошибочное детектирование циклов (H_1) и полостей любой длины.	Отсутствие обучаемости. Сам по себе метод не адаптируется к данным. Высокая вычислительная сложность ($O(N^3)$) без оптимизации. Сложность интеграции с атрибутивными признаками.
Гибридные подходы	Синтез персистентных гомологий и обучаемых графовых сверток	Мультимасштабный. Сочетает локальные признаки и глобальные топологические инварианты.	Комплексный анализ. GNN обрабатывает атрибуты транзакций, а TDA-слой детектирует структурные аномалии (циклы, клики), невидимые для обычных сверток.	Повышенные требования к вычислительным ресурсам на этапе предобработки (расчет фильтрации), необходимость настройки параметров фильтрации.

систематизация преимуществ и недостатков рассматриваемых подходов, представлена в таблице 2.

На основе проведенного анализа предлагаем использовать гибридный подход, объединяющий топологический анализ данных (TDA) и графовые нейронные сети (GNN). По мнению автора, эти методы хорошо дополняют друг друга: нейросети эффективно анализируют характеристики транзакций и прямые связи между участниками, а топологический анализ, в свою очередь, позволяет увидеть глобальную структуру всей сети [12]. Такое сочетание устраняет недостатки отдельных методов и дает возможность с высокой точностью находить сложные замкнутые схемы (циклы), которые часто используются мошенниками в логистике.

4. Архитектура и математическая формализация гибридной модели TDA GNN

Итак, пусть блокчейн-сеть представлена графом $G = (V, E, X)$, где V – множество узлов, E – множество ребер, а X – матрица атрибутивных признаков.

3 Составлено автором

Задача обнаружения аномалий формализуется как поиск отображения $\Phi: V \longrightarrow \{0,1\}$, минимизирующего эмпирический риск. Архитектура TDA-GNN аппроксимирует эту функцию через композицию двух ортогональных каналов [13]:

1. Атрибутивный канал (GNN): реализует функцию локальной агрегации, чувствительную к статистическим характеристикам ближайшего окружения узла.
2. Топологический канал (TDA): реализует отображение пространства локальных подграфов в пространство векторных представлений, инвариантное к изометрическим деформациям, но чувствительное к гомологическим структурам (циклам, полостям).

Итоговое предсказание модели для произвольного узла v определяется следующим аналитическим выражением:

$$\hat{y}_v = \sigma\left(\mathcal{F}_{CLF}\left(\mathcal{F}_{Fusion}\left(h_{gnn}^{(v)}, z_{topo}^{(v)}\right)\right)\right), \quad (1)$$

где $\hat{y}_v$ — оценка вероятности принадлежности узла v к классу аномальных участников (выход модели); σ – нелинейная функция активации (Sigmoid), отображающая выходное значение в интервале [0, 1]; $\mathcal{F}_{CLF}$ – функция классификатора (реализуется как многослойный перцептрон, MLP), отображающая скрытое представление в скалярную оценку; $\mathcal{F}_{Fusion}$ — оператор адаптивного слияния признаковых пространств; $h_{gnn}^{(v)}$ – вектор латентного представления узла v, полученный на выходе атрибутивного канала (GNN); $z_{topo}^{(v)}$ – вектор топологических дескрипторов узла v, полученный на выходе канала TDA.

На рисунке 1 представлена общая схема предлагаемого гибридного подхода.

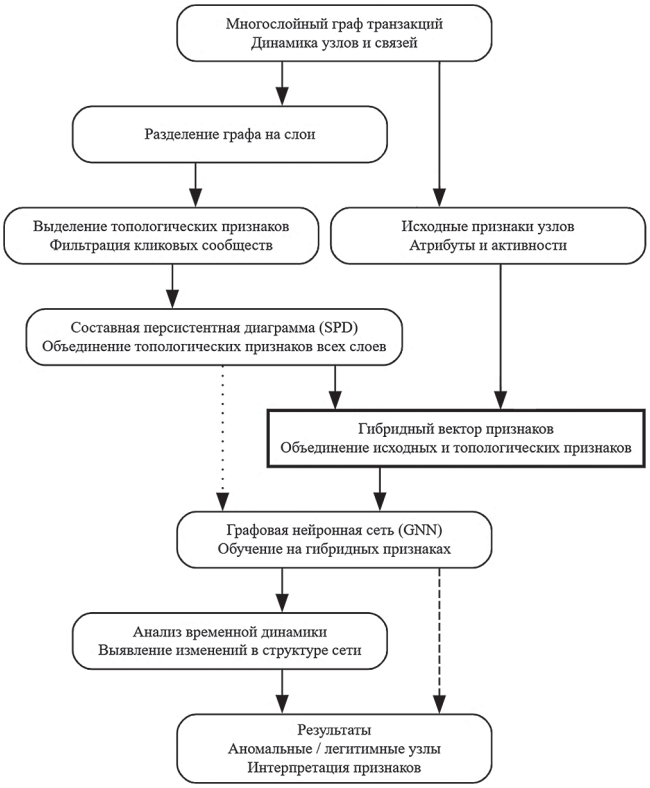

Рис. 1 Концептуальная схема гибридной архитектуры TDA-GNN

Модуль извлечения признаков базируется на теории персистентных гомологий. Для каждого узла v рассматривается локальное метрическое пространство $\mathcal{X}_v$, индуцированное его окрестностью [14]. На пространстве $\mathcal{X}_v$ строится фильтрация — последовательность вложенных симплициальных комплексов:

$$\emptyset = \mathcal{K}_o \subseteq \mathcal{K}_1 \subseteq \cdots \subseteq \mathcal{K}_m = \mathcal{K}. \quad (2)$$

Ключевым инструментом анализа является граничный оператор ∂_k отображающий k-мерные цепи в $(k-1)$-мерные. Ядро оператора $ker\partial_k$ состоит из всех k-мерных циклов, то есть цепей, не имеющих границы. Однако не каждый цикл несет самостоятельную топологическую информацию, поскольку часть циклов может являться границей $(k+1)$-мерных объектов. Такие тривиальные циклы образуют образ оператора $im\partial_{k+1}$). Детектирование структурных аномалий сводится к вычислению k-й группы гомологий H_k, определяемой как фактор группа ядра оператора по его образу:

$$H_k = \frac{ker\partial_k}{im\partial_{k+1}}. \quad (3)$$

Элементы группы H_1 соответствуют нетривиальным циклам, которые не являются границами более высоких размерностей [15]. В контексте задачи это интерпретируется как устойчивые замкнутые схемы транзакций.

Результатом работы топологического слоя является множество персистентных диаграмм $\mathcal{D}$. Для интеграции с нейронной сетью применяется отображение векторизации Ψ, трансформирующее пространство диаграмм в евклидово пространство признаков $\mathbb{R}_d$:

$$z_{topo} = \Psi(\mathcal{D}). \quad (4)$$

Отображение Ψ конструируется таким образом, чтобы удовлетворять свойству устойчивости относительно метрики Вассерштейна [16], что обеспечивает робастность модели к шуму во входных данных.

Для синтеза локальных (атрибутивных) и глобальных (топологических) признаков применяется дифференцируемый механизм внимания Gated Fusion. Данный подход позволяет модели адаптивно определять вклад каждого канала в итоговое решение, избегая потери информации при простой конкатенации [17].

Пусть h_{gnn} – вектор скрытого состояния узла, полученный после сверточных слоев, а z_{topo} — вектор топологических признаков. Введем оператор проекции W_{proj} для отображения топологического вектора в латентное пространство размерности GNN:

$$\tilde{z} = \phi(W_{proj} \cdot z_{topo} + b). \quad (5)$$

Коэффициент слияния $\alpha \in [0,1]$ вычисляется через механизм самовнимания [18]:

$$\alpha = \sigma(w_g^T \cdot [h_{gnn} \oplus \tilde{z}] + b_g), \quad (6)$$

где $\oplus$ — операция объединения векторов.

Итоговый гибридный вектор Z_{final} формируется как выпуклая комбинация представлений:

$$Z_{final} = (1 - \alpha) \odot h\_gnn + \alpha \odot \tilde{z}. \quad (7)$$

Такая формулировка позволяет градиентам ошибки распространяться на оба канала обучения. В случае обнаружения сильного структурного сигнала (цикла), механизм внимания увеличивает вес α, усиливая влияние топологической компоненты [19].

Обучение параметров модели Θ осуществляется методом градиентного спуска. Целевой функционал

$\mathcal{L}\Theta$ конструируется как суперпозиция функции потерь классификации и члена регуляризации [20]. В качестве основного компонента используется взвешенная функция перекрестной энтропии, учитывающая априорное распределение классов:

$$\mathcal{L}_{cls} = -\mathbb{E}_{(x,y)\sim\mathcal{D}_{train}}[w(y) \cdot logp(y|x;\Theta)], \quad (8)$$

где $w(y)$ — весовая функция, компенсирующая дисбаланс выборки.

Для повышения обобщающей способности модели вводится L_2 – регуляризация на весовые матрицы нейронной сети:

$$\mathcal{L}_{reg} = \lambda\|\Theta\|_F^2. \quad (9)$$

Итоговая задача оптимизации формулируется следующим образом:

$$\Theta^* = arg\min_{\Theta}(\mathcal{L}_{cls}(\Theta) + \mathcal{L}_{reg}(\Theta)). \quad (10)$$

Минимизация данного функционала обеспечивает сходимость модели к состоянию, в котором она способна различать как явные нарушения в атрибутах транзакций (через $\mathcal{L}_{cls}$ и GNN-ветку), так и скрытые структурные паттерны, передаваемые через механизм слоя слияния.

5. Экспериментальная апробация методики и анализ результатов

Для верификации разработанной методики и оценки эффективности гибридного подхода (TDA-GNN) была сформирована экспериментальная выборка. Ввиду сложности получения верифицированной разметки мошеннических операций из открытых источников, в работе применена методология полусинтетического моделирования.

Топология сети (G): в основе экспериментальной модели лежит подграф транзакций реальной логистической сети (на базе архитектуры, аналогичной Hyperledger Fabric), включающий:

- узлы (V): N = 15,400 сущностей (адреса поставщиков, логистических хабов, таможенных брокеров, ритейлеров);
- ребра (E): M = 142,000 транзакций;
- признаки (X): векторы размерности d = 16 (статистика активности, временные метки, объемы поставок).

Разметка аномалий (Y): вектор целевых меток формировался путем контролируемого внедрения (инъекции) трех типов атак, специфичных для цепочек поставок. Доля аномальных узлов в выборке составила 5,5 %.

1. Тип I: циклическая фальсификация. Замкнутые цепочки транзакций вида $v_1 \rightarrow v_2 \ldots \rightarrow v_k \rightarrow v_1$ (где $k \geq 3$) для искусственного завышения оборотов. Топологически данные структуры представляют собой генераторы группы гомологий H_1 (устойчивые циклы).
2. Тип II: кластерный сговор: формирование плотных клик (полносвязных подграфов), имитирующих активность группы фиктивных контрагентов.
3. Тип III: темпоральные нарушения. Аномалии временных меток, нарушающие причинно-следственную логику поставки.

Задача обнаружения инцидентов решалась как бинарная классификация узлов на классы C_0 (легитимный) и C_1 (аномальный). Формирование признакового пространства осуществлялось согласно описанному ранее алгоритму. Для сравнительного анализа были выбраны четыре подхода классификации:

1. Isolation Forest (изолирующий лес): базовый статистический метод обнаружения аномалий, не использующий топологию графа (Baseline).
2. GCN (Graph Convolutional Network): классическая сверточная нейронная сеть на графах.
3. GraphSAGE: индуктивная нейросетевая архитектура, агрегирующая признаки соседей.
4. TDA-GNN: разработанная гибридная модель.

Процедура обучения реализовывалась с применением стратегии кросс-валидации по 5 блокам. Результаты эксперимента представлены в таблице 3.

Как свидетельствуют данные таблицы 3, разработанный гибридный подход демонстрирует прирост F-меры на 6–8 % относительно нейросетевых аналогов (GCN, GraphSAGE). Наиболее значимый результат достигнут в метрике «Полноты» (0,91), что критически важно для минимизации рисков пропуска мошеннических схем.

Таблица 3.

Сравнительная эффективность методов обнаружения аномалий

Метод	Точность	Полнота	F-мера	Коэффициент Мэтьюса
Isolation Forest	0,62 ± 0,04	0,55 ± 0,05	0,58 ± 0,04	0,52
GCN (Базовая)	0,88 ± 0,02	0,81 ± 0,03	0,84 ± 0,02	0,80
GraphSAGE	0,89 ± 0,02	0,84 ± 0,02	0,86 ± 0,02	0,83
TDA-GNN	0,93 ± 0,01	0,91 ± 0,01	0,92 ± 0,01	0,89

Таблица 4.

Полнота обнаружения (Recall) в разрезе типов аномалий

Тип аномалии	Isolation Forest	GCN	GraphSAGE	TDA-GNN	Прирост к аналогам[4]
Тип I (Циклы)	0,45	0,72	0,75	0,98	+30,6 %
Тип II (Кластеры)	0,58	0,85	0,88	0,91	+3,4 %
Тип III (Временные)	0,62	0,88	0,89	0,89	0 %

С целью выявления границ применимости методов была проведена декомпозиция метрики «Полноты» в зависимости от типа внедренной аномалии. В таблице 4 представлено сравнение способности каждой модели детектировать конкретные виды угроз.

Полученные результаты позволяют сделать следующие выводы.

1. Isolation Forest демонстрирует низкую эффективность на всех типах атак, подтверждая непригодность методов, игнорирующих топологию связей, для глубокого аудита блокчейна.
2. GCN и GraphSAGE показывают умеренные результаты (0,72–0,75) в обнаружении циклов (Тип I). Это обусловлено механизмом агрегации сообщений, который усредняет признаки узлов, «размывая» информацию о глобальной циклической структуре.
3. TDA-GNN демонстрирует существенное улучшение (+30 %) именно на структурно сложных атаках Типа I. Топологический слой безошибочно выявляет циклы как устойчивые гомологические «дыры» (H_1), которые невозможно скрыть путем манипуляции суммами транзакций.

Анализ значимости признаков показал, что использование только 0-мерных гомологий (H_0, компоненты связности) дает прирост качества не более 1,5 %. Основной вклад в эффективность модели вносит учет 1-мерных гомологий (H_1), отвечающих за детектирование циклов. Расчетное время обработки одной транзакции составило $t \approx 26$ мс, что удовлетворяет требованиям к производительности промышленных систем мониторинга логистики.

Заключение

В ходе проведенного исследования была разработана и экспериментально апробирована гибридная архитектура, объединяющая методы топологического анализа данных и графовые нейронные сети для задачи обнаружения аномалий в блокчейн-системах логистики. Отличительной особенностью предложенной архитектуры является двухканальная обработка графа транзакций, объединяющая локальную агрегацию атрибутов через GNN с глобальным анализом структуры на основе персистентных гомологий.

Результаты численного моделирования авторского подхода позволяют сделать следующие выводы.

Интеграция топологических признаков (персистентных диаграмм и энтропии) в векторное представление узлов позволила преодолеть ограничения классических графовых сетей. В результате было достигнуто увеличение интегральной метрики F-меры на 8 % (до 0,92) по сравнению с базовой моделью GCN. Ключевым научным результатом является подтвержденная способность модели идентифицировать сложные схемы циклической фальсификации. В то время как стандартные методы (GCN, GraphSAGE) пропускают до 25–30 % таких атак из-за эффекта сглаживания, предложенный метод обеспечивает полноту обнаружения на уровне 0,98.

Несмотря на теоретическую сложность расчета гомологий, применение оптимизированных алгоритмов фильтрации позволило достичь времени обработки транзакции в 26 мс. Данный показатель подтверждает возможность внедрения разработанного метода в системы промышленного мониторинга. Помимо этого, он показал высокую эффективность в условиях сильного дисбаланса классов (5,5 % аномалий).

Таким образом, полученные данные позволяют рекомендовать гибридный подход для автоматизированного аудита смарт-контрактов в цепочках поставок.

Литература

1. Погребинская М.Н. Квантово-фрактальный метод анализа блокчейн-транзакций для обнаружения скрытой противозаконной активности // Право и государство: теория и практика. 2025. № 4. С. 472–474. DOI: 10.47643/1815-1337_2025_4_472.
2. Jinglin Li, Yihang Zhang, Chun Yang BlockDetective: A GCN-based student–teacher framework for blockchain anomaly detection // IET Blockchain. 2023. Volume 3, Issue 4. DOI: 10.1049/blc2.12044.
3. Vasavi Chithanuru, Mangayarkarasi Ramaiah An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions – A review // Concurrency and Computation: Practice and Experience. 2023. Volume 35, Issue 22. DOI: 10.1002/cpe.7724.

4 Прирост рассчитывается относительно лучшей базовой модели (GraphSAGE)

4. Владимиркин А. А. Аномалии в криптовалютных транзакциях и методы машинного обучения для их выявления // Вестник Ульяновского государственного технического университета. 2025. № 1(109). С. 40–43. DOI: 10.61527/1684-7016-2025-1-40-43.
5. Утакаева И. Х. Систем за счет комбинации графовых баз данных и неизменяемых журналов блокчейна // Кузнечно-штамповочное производство. Обработка материалов давлением. 2025. № 4. С. 199–208. EDN: UOWQIX.
6. Shiyang Chen, Yang Liu, Qun Zhang, Zhouhang Shao, Zewei Wang Multi-Distance Spatial-Temporal Graph Neural Network for Anomaly Detection in Blockchain Transactions // Advanced Intelligent Systems. 2025. Volume 7, Issue 8. DOI: 10.1002/aisy.202400898.
7. Haoyang Tan, Qiang Zhang, Mingxian Li, Xinxing Liu, Lei Hu Design and Optimization of a Blockchain-Enabled Decentralized Security Framework for Anomaly Detection in VANETs // Transactions on Emerging Telecommunications Technologies. 2025. Volume 36, Issue 10. DOI: /10.1002/ett.70275.
8. Попова М. В. Применение искусственного интеллекта для оптимизации смарт-контрактов в блокчейн-системах с использованием теории графов // Академический исследовательский журнал. 2023. Т. 1. № 1. С. 46–59. DOI: 10.25726/z8249-0282-8436-n.
9. Shipra Ravi Kumar, Mukta Goyal Design of an Iterative Method for Blockchain Optimization Incorporating DeepMiner and AnoBlock // Security and Privacy. 2024. Volume 8, Issue 1. DOI: 10.1002/spy2.492.
10. Kouros Zanbouri, Mehdi Darbandi, Mohammad Nassr, Arash Heidari, Nima Jafari Navimipour, Senay Yalcın A GSO-based multi-objective technique for performance optimization of blockchain-based industrial Internet of things // International Journal of Communication Systems. 2024. Volume 37, Issue 15. DOI: 10.1002/dac.5886.
11. Бушмелев А. С., Калинин М. О., Крундышев В. М. Верификация транзакций в блокчейн-системах, основанная на применении консорциум-ориентированных правил // Методы и технические средства обеспечения безопасности информации. 2025. № 34. С. 189–190. EDN: DDQKYI.
12. Горшков Е. А. Применение роллапов с нулевыми знаниями в блокчейн-технологии для оптимизации обработки транзакций с цифровыми активами // Актуальные проблемы современности: наука и общество. 2025. № 2(42). С. 3–7. EDN: VOAJKT.
13. Zejia Jing, Ali Parizad, Saifur Rahman Blockchain-Based Energy Trading Employing Hyperledger and Anomaly Detection Algorithms // Smart Cyber-Physical Power Systems: Fundamental Concepts, Challenges, and Solutions. 2025. Volume 1. DOI: 10.1002/9781394191529.ch27.
14. Kevin Martin, Mohamed Rahouti, Moussa Ayyash, Izzat Alsmadi Anomaly detection in blockchain using network representation and machine learning // Security and Privacy. 2021. Volume 5, Issue 2. DOI: 10.1002/spy2.192.
15. Yusuf Muhammad Tukur, Dhavalkumar Thakker, Irfan-Ullah Awan Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of Things // Transactions on Emerging Telecommunications Technologies. 2020. Volume 32, Issue 6. DOI: /10.1002/ett.4158.
16. Макаренко Е. Н., Клейменкин Д. В. Исследование механизмов шифрования, аутентификации и приватности в контексте блокчейн-технологий // Дневник науки. 2023. № 10(82). EDN: YPHWRA.
17. Горячкин Б. С., Солохов И. Р. Подбор алгоритма консенсуса для логистического блокчейна // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2023. № 4-2. С. 65-70. DOI: 10.37882/2223-2966.2023.04-2.07.
18. Gheyath Mustafa Zebari, Nasser Al Musalhi A Comprehensive Review of Integrating AI and Blockchain Security: Innovations, Challenges, and Future Directions // Security and Privacy. 2025. Volume 8, Issue 5. DOI: 10.1002/spy2.70094.
19. Jianhuan Mao, Mengxiao Zhu, Yi Sun, Lei Li, Haogang Zhu Transaction Spatio-Temporal Distribution for Permissioned Blockchain Performance Profiling // Concurrency and Computation: Practice and Experience. 2025. Volume 37, Issue 27-28. DOI: 10.1002/cpe.70316.
20. Помогалова А. В., Донсков Е. А., Елагин В. С. Модель интеграции адаптивного алгоритма выбора и смены консенсуса блокчейна при граничных значениях показателей сети // Электросвязь. 2024. № 12-2. С. 16–24. DOI: 10.34832/ELSV.2024.61.12.003.

COMBINING METHODS OF TOPOLOGICAL DATA ANALYSIS AND GRAPH NEURAL NETWORKS TO DETECT ANOMALIES IN BLOCKCHAIN LOGISTICS SYSTEMS

Vladimirkin A. A.[5]

Keywords: *distributed ledger, transaction graph, persistent diagram, persistent homology, hybrid feature vector, cyclic falsification, cluster collusion, temporal violations.*

The purpose of the study: *to improve the quality of anomaly detection in blockchain logistics systems based on methods of topological data analysis and graph neural networks.*

Research methods: *combination of algebraic topology and graph neural networks within the framework of a hybrid node classification model. The approach was verified by semi-synthetic modeling of cyclic and cluster attacks on logistics network transactions.*

Research results: *The article reveals the issues related to the impact of anomalies in blockchain logistics systems on supply chains and the efficiency of cargo flows. The need for a progressive approach for timely detection and management of anomalies in real time through the integration of such technologies as machine learning and big data analysis is noted.*

5 **Andrey A. Vladimirkin**, Postgraduate Student, Department of Applied Mathematics and Informatics, Ulyanovsk State Technical University. Ulyanovsk, Russia. E-mail: vladimirkin2017@gmail.com

registers, their advantages and disadvantages are noted. A hybrid approach to detecting anomalies in the blockchain has been developed, which implements joint processing of transactional data using graph neural networks and algebraic topology methods.

Scientific novelty: *in contrast to the well-known methods based on local aggregation of features, the hybrid approach makes it possible to identify global structural anomalies, ensuring the completeness of detection of complex schemes of fictitious turnover.*

References

1. Pogrebinskaya M. N. Kvantovo-fraktal'ny'j metod analiza blokchejn-tranzakcij dlya obnaruzheniya skry'toj protivozakonnoj aktivnosti // Pravo i gosudarstvo: teoriya i praktika. 2025. № 4. S. 472–474. DOI: 10.47643/1815-1337_2025_4_472.
2. Jinglin Li, Yihang Zhang, Chun Yang BlockDetective: A GCN-based student–teacher framework for blockchain anomaly detection // IET Blockchain. 2023. Volume 3, Issue 4. DOI: 10.1049/blc2.12044.
3. Vasavi Chithanuru, Mangayarkarasi Ramaiah An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions – A review // Concurrency and Computation: Practice and Experience. 2023. Volume 35, Issue 22. DOI: 10.1002/cpe.7724.
4. Vladimirkin A. A. Anomalii v kriptovalyutny'x tranzakciyax i metody' mashinnogo obucheniya dlya ix vy'yavleniya // Vestnik Ul'yanovskogo gosudarstvennogo texnicheskogo universiteta. 2025. № 1(109). S. 40–43. DOI: 10.61527/1684-7016-2025-1-40-43.
5. Utakaeva I. X. Sistem za schet kombinacii grafovy'x baz danny'x i neizmenyaemy'x zhurnalov blokchejna // Kuznechno-shtampovochnoe proizvodstvo. Obrabotka materialov davleniem. 2025. № 4. S. 199–208. EDN: UOWQIX.
6. Shiyang Chen, Yang Liu, Qun Zhang, Zhouhang Shao, Zewei Wang Multi-Distance Spatial-Temporal Graph Neural Network for Anomaly Detection in Blockchain Transactions // Advanced Intelligent Systems. 2025. Volume 7, Issue 8. DOI: 10.1002/aisy.202400898.
7. Haoyang Tan, Qiang Zhang, Mingxian Li, Xinxing Liu, Lei Hu Design and Optimization of a Blockchain-Enabled Decentralized Security Framework for Anomaly Detection in VANETs // Transactions on Emerging Telecommunications Technologies. 2025. Volume 36, Issue 10. DOI: /10.1002/ett.70275.
8. Popova M. V. Primenenie iskusstvennogo intellekta dlya optimizacii smart-kontraktov v blokchejn-sistemax s ispol'zovaniem teorii grafov // Akademicheskij issledovatel'skij zhurnal. 2023. T. 1. № 1. S. 46–59. DOI: 10.25726/z8249-0282-8436-n.
9. Shipra Ravi Kumar, Mukta Goyal Design of an Iterative Method for Blockchain Optimization Incorporating DeepMiner and AnoBlock // Security and Privacy. 2024. Volume 8, Issue 1. DOI: 10.1002/spy2.492.
10. Kouros Zanbouri, Mehdi Darbandi, Mohammad Nassr, Arash Heidari, Nima Jafari Navimipour, Senay Yalcın A GSO-based multi-objective technique for performance optimization of blockchain-based industrial Internet of things // International Journal of Communication Systems. 2024. Volume 37, Issue 15. DOI: 10.1002/dac.5886.
11. Bushmelev A. S., Kalinin M. O., Krundy'shev V. M. Verifikaciya tranzakcij v blokchejn-sistemax, osnovannaya na primenenii konsorcium-orientirovanny'x pravil // Metody' i texnicheskie sredstva obespecheniya bezopasnosti informacii. 2025. № 34. S. 189–190. EDN: DDQKYI.
12. Gorshkov E. A. Primenenie rollapov s nulevy'mi znaniyami v blokchejn-texnologii dlya optimizacii obrabotki tranzakcij s cifrovy'mi aktivami // Aktual'ny'e problemy' sovremennosti: nauka i obshhestvo. 2025. № 2(42). S. 3–7. EDN: VOAJKT.
13. Zejia Jing, Ali Parizad, Saifur Rahman Blockchain-Based Energy Trading Employing Hyperledger and Anomaly Detection Algorithms // Smart Cyber-Physical Power Systems: Fundamental Concepts, Challenges, and Solutions. 2025. Volume 1. DOI: 10.1002/9781394191529.ch27.
14. Kevin Martin, Mohamed Rahouti, Moussa Ayyash, Izzat Alsmadi Anomaly detection in blockchain using network representation and machine learning // Security and Privacy. 2021. Volume 5, Issue 2. DOI: 10.1002/spy2.192.
15. Yusuf Muhammad Tukur, Dhavalkumar Thakker, Irfan-Ullah Awan Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of Things // Transactions on Emerging Telecommunications Technologies. 2020. Volume 32, Issue 6. DOI: /10.1002/ett.4158.
16. Makarenko E. N., Klejmenkin D. V. Issledovanie mexanizmov shifrovaniya, autentifikacii i privatnosti v kontekste blokchejn-texnologij // Dnevnik nauki. 2023. № 10(82). EDN: YPHWRA.
17. Goryachkin B. S., Soloxov I. R. Podbor algoritma konsensusa dlya logisticheskogo blokchejna // Sovremennaya nauka: aktual'ny'e problemy' teorii i praktiki. Seriya: Estestvenny'e i texnicheskie nauki. 2023. № 4-2. S. 65–70. DOI: 10.37882/2223-2966.2023.04-2.07.
18. Gheyath Mustafa Zebari, Nasser Al Musalhi A Comprehensive Review of Integrating AI and Blockchain Security: Innovations, Challenges, and Future Directions // Security and Privacy. 2025. Volume 8, Issue 5. DOI: 10.1002/spy2.70094.
19. Jianhuan Mao, Mengxiao Zhu, Yi Sun, Lei Li, Haogang Zhu Transaction Spatio-Temporal Distribution for Permissioned Blockchain Performance Profiling // Concurrency and Computation: Practice and Experience. 2025. Volume 37, Issue 27-28. DOI: 10.1002/cpe.70316.
20. Pomogalova A. V., Donskov E. A., Elagin V. S. Model' integracii adaptivnogo algoritma vy'bora i smeny' konsensusa blokchejna pri granichny'x znacheniyax pokazatelej seti // E'lektrosvyaz'. 2024. № 12-2. S. 16–24. DOI: 10.34832/ELSV.2024.61.12.003.