https://doi.org/10.51885/3107-2755_JISC_2026_1_4
МРНТИ 20.53.19; 20.53.21

КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ ТРАНЗАКЦИЙ В ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ БЛОКЧЕЙНАХ: СОВРЕМЕННОЕ СОСТОЯНИЕ ИССЛЕДОВАНИЙ И ТРЕБОВАНИЯ К FORENSIC-ENGINE ДЛЯ SOLANA

ЖОҒАРЫ ӨНІМДІ БЛОКЧЕЙНДЕРДЕГІ ТРАНЗАКЦИЯЛАРДЫ КРИМИНАЛИСТИКАЛЫҚ ТАЛДАУ: ЗЕРТТЕУЛЕРДІҢ ҚАЗІРГІ ЖАҒДАЙЫ ЖӘНЕ SOLANA ҮШІН FORENSIC ENGINE ҚОЙЫЛАТЫН ТАЛАПТАР

FORENSIC ANALYSIS OF TRANSACTIONS IN HIGH-PERFORMANCE BLOCKCHAINS: CURRENT STATE OF RESEARCH AND REQUIREMENTS FOR THE FORENSIC ENGINE FOR SOLANA

Н.П. Рохас-Криулько [1], В.А. Еремеев [1], Д.А. Попов [1], К.Н. Киричёк [1], Т.Р. Черных [1]*

[1] Восточно-Казахстанский технический университет имени Д. Серикбаева,
г. Усть-Каменогорск, Казахстан
*Автор-корреспондент: Черных Тимур Равильевич, e-mail: rewvtrew@gmail.com

Ключевые слова:
Solana, blockchain forensics, кибербезопасность, Rust, графовый анализ, обнаружение мошенничества, SPL-токены, MEV

АННОТАЦИЯ

Высокопроизводительные блокчейны усложняют цифровую криминалистику: транзакции исполняются с высокой частотой, активы представлены различными токенами, а пользовательская идентичность остается псевдонимной. Цель статьи - систематизировать современные научные подходы к blockchain forensics и показать, какие из них применимы к анализу подозрительных операций в сети Solana. Обзор выполнен как нарративно-систематизированный: рассмотрены публикации из международных издательских платформ и наукометрически индексируемых баз за 2013-2026 гг., включая работы IEEE, ACM, Springer Nature, Elsevier и MDPI по графовому анализу транзакций, AML/CFT-аналитике, выявлению Ponzi-схем, wash trading, pump-and-dump и MEV-атак, а также исследования безопасности Solana и языка Rust. Показано, что прямой перенос методов, разработанных для Bitcoin и Ethereum, недостаточен: в Solana необходимо учитывать account model, SPL-токены, instruction traces, параллельную модель исполнения Sealevel, высокий уровень неуспешных транзакций и различие между кошельком и токеновым счетом. На основе обзора сформулированы требования к self-hosted forensics-движку на Rust: read-only сбор данных, нормализация атомарных единиц, построение мультиграфа переводов, объяснимые эвристики, воспроизводимость сигналов и безопасность by design. Практическая значимость работы состоит в переводе технической идеи forensic-движка в научную рамку, пригодную для дальнейшей экспериментальной проверки и

публикационной дискуссии.

Түйінді сөздер:
Solana, blockchain forensics, киберқауіпсіздік, Rust, графтық талдау, алаяқтықты анықтау, SPL токендер, MEV

ТҮЙІНДЕМЕ

Жоғары өнімді блокчейндер цифрлық криминалистиканы қиындатады: транзакциялар жоғары жиілікте орындалады, активтер әртүрлі белгілермен ұсынылған және пайдаланушы сәйкестігі бүркеншік ат болып қалады. Мақаланың мақсаты - blockchain forensics-ке заманауи ғылыми тәсілдерді жүйелеу және олардың қайсысы Solana желісіндегі күдікті операцияларды талдауға қолданылатынын көрсету. Шолу баяндау және жүйелеу ретінде орындалды: IEEE, ACM, Springer Nature, Elsevier және MDPI операцияларын қоса алғанда, 2013-2026 жылдардағы халықаралық баспа платформалары мен ғылыми индекстелген базалардың басылымдары қарастырылды. транзакцияларды графикалық талдау, AML/CFT аналитикасы, Ponzi схемаларын анықтау, жуу саудасы, сорғы және-dump және MEV-шабуылдар, сондай-ақ Solana және Rust тілінің қауіпсіздігін зерттеу. Bitcoin және Ethereum үшін әзірленген әдістерді тікелей тасымалдау жеткіліксіз екендігі көрсетілген: Solana есептік жазба моделін, SPL таңбалауыштарын, Нұсқаулық тректерін, Sealevel параллель орындау моделін, сәтсіз транзакциялардың жоғары деңгейін және әмиян мен токен шоты арасындағы айырмашылықты ескеруі керек. Шолу негізінде Rust-тегі self-hosted forensics-қозғалтқышқа қойылатын талаптар тұжырымдалған: тек қана деректерді жинау, атомдық бірліктерді қалыпқа келтіру, аударма мультиграфын құру, түсіндірілетін эвристика, сигналдардың қайталануы және дизайн қауіпсіздігі. Жұмыстың практикалық маңыздылығы forensic-қозғалтқыштың техникалық идеясын одан әрі эксперименттік тексеруге және жариялау талқылауына жарамды ғылыми шеңберге аударудан тұрады.

keywords:
Solana, blockchain forensics, cybersecurity, Rust, graph analysis, fraud detection, SPL tokens, MEV

ABSTRACT

T High-throughput blockchains complicate digital forensics because transactions are processed at high frequency, assets are represented by heterogeneous tokens, and user identity remains pseudonymous. This review systematizes blockchain forensics methods and discusses their applicability to suspicious-transaction analysis in Solana. The review focuses on international peer-reviewed literature and scholarly publisher platforms from 2013 to 2026, including IEEE, ACM, Springer Nature, Elsevier and MDPI sources on transaction-graph analysis, AML/CFT analytics, Ponzi schemes, wash trading, pump-and-dump manipulation, MEV attacks, Solana security and Rust. The paper argues that techniques designed for Bitcoin and Ethereum cannot be transferred to Solana mechanically: account model, SPL token accounts, instruction traces, Sealevel parallel execution, failed transactions and token-account ownership must be considered. The review derives requirements for a self-hosted Rust-based forensic engine: read-only data collection, normalization of atomic units, multigraph construction, explainable heuristics, reproducible alerts and security by design.

ВВЕДЕНИЕ

Публичные блокчейны создают для расследователя редкое сочетание открытости и неопределенности. С одной стороны, транзакции доступны для независимой проверки, а история операций не зависит от единого администратора. С другой стороны, адреса не

равны установленным личностям, движение средств часто проходит через промежуточные кошельки, а экономические атаки маскируются под обычную торговую активность. Поэтому современный blockchain forensics не сводится к просмотру эксплорера: он требует нормализации данных, построения графов связей, интерпретации смарт-контрактных вызовов и проверки гипотез на больших потоках транзакций.

Классическая литература по Bitcoin показала, что псевдонимность не означает полной анонимности. Адресные эвристики, кластеризация и сопоставление on-chain и off-chain индикаторов позволяют восстановить существенную часть экономических связей (Meiklejohn et al., 2016; Conti et al., 2018). Позднее исследовательский фокус сместился к Ethereum и DeFi: появились методы обнаружения Ponzi-схем, анализа децентрализованных бирж, MEV и манипуляций объемом торгов (Bartoletti et al., 2020; Chen et al., 2018; Daian et al., 2020; Victor & Weintraud, 2021). Эти подходы сформировали базовый инструментарий цифровой криминалистики, но они не полностью описывают сети с иной архитектурой исполнения.

Solana является показательной средой для такого перехода. Ее учетная модель, SPL-токены, параллельное исполнение и отсутствие EVM-совместимой структуры журналов событий требуют иной модели извлечения признаков. Для исследователя это означает, что источник доказательств находится не только в факте перевода, но и в составе instruction traces, списке затронутых аккаунтов, типе токенового счета, статусе транзакции и временном контексте слота. Вследствие этого forensic-движок для Solana должен быть не просто быстрым парсером RPC-ответов, а системой, в которой скорость, безопасность и объяснимость связаны между собой.

Исходный прикладной проект, на основе которого подготовлена данная обзорная статья, описывает self-hosted forensics-движок на Rust для мониторинга Solana-транзакций, выявления wash trading, dusting, sandwich/MEV и pump-and-dump-сценариев. В настоящей редакции акцент перенесен с декларации возможностей прототипа на научный обзор: какие методы подтверждены литературой, какие ограничения существуют при переносе на Solana и какие требования следует предъявлять к открытой системе анализа транзакций.

Цель статьи - сформировать научно обоснованную рамку для разработки и оценки безопасного Rust-движка blockchain forensics в среде Solana. Для достижения цели решаются четыре задачи: во-первых, обобщить основные направления исследований в области криптовалютной криминалистики; во-вторых, выделить классы мошеннических паттернов, значимых для высокопроизводительных блокчейнов; в-третьих, сопоставить Bitcoin, Ethereum и Solana с точки зрения извлечения forensic-признаков; в-четвертых, предложить набор требований к архитектуре, безопасности и верифицируемости результатов анализа.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

Статья выполнена в формате обзорного исследования с элементами систематизации. Она не претендует на полноценный метаанализ, поскольку рассматриваемая область сочетает разные типы данных: транзакционные графы Bitcoin, смарт-контрактные журналы Ethereum, DeFi-операции, Solana-специфические account traces и исследования языковой безопасности Rust. Вместо количественного объединения результатов применена тематическая классификация публикаций по исследовательским задачам.

Поисковая рамка включала международные издательские платформы и базы, традиционно представленные в Scopus/WoS-ориентированной библиографии: IEEE

Xplore, ACM Digital Library, SpringerLink, ScienceDirect, MDPI, Wiley Online Library, а также вспомогательные библиографические индексы DBLP и Crossref для уточнения DOI и метаданных. Временной интервал выбран с 2013 по 2026 гг.: 2013 г. отражает появление работ, системно показавших аналитическую ценность транзакционного графа Bitcoin, а 2025-2026 гг. учитывают новые публикации по Solana и современным MEV-сценариям.

Критериями включения были: наличие связи с blockchain forensics, AML/CFT-аналитикой или обнаружением аномалий; использование on-chain данных, графов, машинного обучения или объяснимых правил; применимость к мошенничеству в криптовалютных экосистемах; публикация в рецензируемом журнале, конференции или официальной технической документации платформы. Критериями исключения были маркетинговые обзоры, новостные материалы без методики, непроверяемые заявления о производительности и публикации, где блокчейн упоминался только как общий контекст.

Особое внимание уделялось воспроизводимости. Поэтому в текст включены не только выводы отдельных исследований, но и типы данных, на которых эти выводы основаны: транзакционные графы, смарт-контрактные события, DEX-ордера, токеновые балансы, слоты, аккаунты и признаки взаимодействия с централизованными сервисами. Такой подход важен для Solana: один и тот же экономический факт может быть представлен через разные уровни данных, а неправильное сопоставление кошелька и токенового счета приводит к ложным выводам.

Таблица 1. Поисковая стратегия и критерии отбора литературы

Элемент	Содержание	Назначение для статьи
Ключевые запросы	blockchain forensics; cryptocurrency anomaly detection; transaction graph analysis; Ethereum Ponzi schemes; DeFi attacks; wash trading; MEV; Solana transaction network; Solana smart contract vulnerabilities; Rust safety	Сформировать корпус работ по криминалистике, мошенничеству и техническим особенностям Solana/Rust.
Базы и платформы	IEEE Xplore, ACM DL, SpringerLink, ScienceDirect, MDPI, Wiley, DBLP, Crossref	Сместить библиографию от блогов и whitepaper к публикациям с DOI и устойчивыми метаданными.
Период	2013-2026 гг.	Охватить развитие от адресной кластеризации Bitcoin до современных исследований Solana и DeFi.
Включение	Рецензируемые статьи и конференции; официальная документация протокола; работы с описанной методикой анализа данных	Поддержать научную проверяемость выводов.
Исключение	Рекламные отчеты, новости, непроверяемые бенчмарки, материалы без методики	Снизить риск неподтвержденных claims и повысить пригодность статьи для рецензирования.

Первый устойчивый исследовательский слой blockchain forensics возник вокруг Bitcoin. Работы этого направления показали, что публичный реестр создает основу для адресной кластеризации: если несколько адресов используются как входы одной транзакции, вероятно, они контролируются одним субъектом; если изменение возвращается на новый адрес, он может быть связан с отправителем. Эти эвристики не являются доказательством личности, но они превращают отдельные адреса в графовые

кластеры, которые можно сопоставлять с биржами, сервисами, миксерами и известными криминальными инфраструктурами.

Важный вывод ранней литературы состоит в том, что криминалистический анализ должен отличать наблюдаемый факт от интерпретации. Наблюдаемый факт - это транзакция, сумма, время, адреса и технические параметры. Интерпретация - предположение о владении, мошеннической цели или связи с конкретным сервисом. Для научной статьи и для судебно значимого расследования это различие принципиально: граф не должен выдавать гипотезу за установленный факт.

В Ethereum исследовательская задача стала сложнее. Помимо переводов нативной валюты, появились смарт-контрактные события, токены ERC-20, децентрализованные биржи и протоколы кредитования. Это расширило признаки: анализируются не только адреса и суммы, но и вызовы функций, логи событий, балансы до и после транзакции, пути свопов, ликвидации и последовательности операций в пределах блока. Такая многослойность создала фундамент для анализа DeFi-атак и экономических манипуляций.

Второй исследовательский слой связан с применением машинного обучения. Наиболее распространенная постановка - классификация транзакций или адресов как нормальных, подозрительных либо известных незаконных. В работах по AML/CFT используются направленные графы платежей, временные признаки, объемы, центральность узлов, повторяемость паттернов и расстояние до известных подозрительных кластеров. Графовые нейронные сети, GCN и GAT, рассматриваются как перспективные модели, поскольку они учитывают не только признаки отдельной операции, но и ее положение в сети переводов (Pocher et al., 2023).

Однако для практического forensic-движка точность модели не является единственным критерием. Рецензируемая литература подчеркивает важность объяснимости: аналитик должен понимать, почему событие получило высокий риск-скор, какие признаки сработали и можно ли воспроизвести результат на тех же данных. Для расследований это особенно важно, потому что черный ящик с высокой метрикой F1 не заменяет проверяемого доказательного следа. Поэтому в Solana-контексте целесообразно сочетать ML-подходы с прозрачными правилами: порогами сумм, циклическими структурами, временными окнами и проверяемыми графовыми мотивами.

Сама редкость мошеннических транзакций создает дисбаланс классов. Если модель обучается на большом потоке обычных платежей и малом числе подтвержденных атак, она может демонстрировать высокую общую точность при слабом выявлении реальных злоупотреблений. Отсюда следует требование к будущему движку: хранить не только итоговый флаг, но и версию правил, параметры окна, источник данных, хэш входного набора и объяснение признаков. Такая журналируемость делает возможной независимую повторную проверку.

DeFi-среда изменила природу криптовалютного мошенничества. Ранее основное внимание уделялось перемещению средств между адресами, а в DeFi значимыми становятся экономические паттерны: искусственное создание ликвидности, эксплуатация порядка исполнения, манипуляции оракулами, флеш-займы, wash trading и pump-and-dump. Эти сценарии часто выглядят как легитимные сделки, пока не учитываются последовательность, контекст и связь участников.

Работы по Ponzi-схемам на Ethereum показали, что мошеннический смарт-контракт может формально исполнять заданные правила, но экономическая модель остается обманной. Поэтому детектору недостаточно проверять только техническую корректность программы: нужно анализировать распределение входящих и исходящих платежей,

зависимость выплат от новых участников, а также структуру реинвестирования (Chen et al., 2018; Bartoletti et al., 2020).

Wash trading представляет иной класс риска. В децентрализованных биржах сделки записываются on-chain, но это не исключает манипуляции: один субъект может контролировать несколько аккаунтов и создавать видимость спроса. Для выявления таких схем используются самосделки, двухадресные циклы, повторяемые пары контрагентов, короткие временные окна и аномальное соотношение объема торгов к числу независимых участников (Victor & Weintraud, 2021).

MEV и sandwich-атаки демонстрируют зависимость результата от порядка исполнения. На Ethereum это долго связывалось с mempool и приоритетными комиссиями, а на Solana ситуация имеет собственную специфику: отсутствует классический публичный mempool в том же виде, но возникают bundle-механизмы, взаимодействие с валидаторами и высокочастотная конкуренция за положение операции. Поэтому Solana-детектор должен анализировать не только одиночную транзакцию, но и соседние операции в слоте, путь обмена и изменение балансов до и после исполнения.

Таблица 2. Основные направления литературы и их значение для Solana-forensics

Направление	Типовые данные	Что дает для Solana	Ограничение переноса
Bitcoin forensics	UTXO-граф, адресные кластеры, суммы, временные метки	Базовые идеи графа потоков, кластеризации и псевдонимности	UTXO-модель отличается от account model Solana; нет SPL-токенов и instruction traces.
Ethereum/DeFi forensics	Смарт-контрактные события, ERC-20, DEX-логи, блоковый порядок	Методы анализа Ponzi, wash trading, MEV, pump-and-dump	Solana не является EVM-сетью; журнал событий и параллельное исполнение устроены иначе.
AML/CFT ML	Размеченные графы, признаки транзакций, GCN/GAT, ансамбли	Подходы к скорингу и приоритезации алертов	Размеченные наборы Solana-атак ограничены; нужна объяснимость и проверяемость.
Solana security	Аккаунты, программы, SPL-токены, eBPF/SBPF, транзакционные слоты	Понимание специфических уязвимостей и forensic-признаков	Академическая база пока меньше, чем для Ethereum.
Rust safety	Ownership, borrow checking, unsafe-блоки, формальные гарантии	Основание для безопасного парсинга и параллельной обработки данных	Безопасность Rust не отменяет ошибок бизнес-логики и supply-chain рисков.

Solana отличается от Bitcoin и Ethereum не только скоростью, но и моделью данных. В Bitcoin ключевым объектом является UTXO, в Ethereum - аккаунт и лог событий смарт-контракта, а в Solana - взаимодействие программ и аккаунтов, где транзакция заранее указывает набор читаемых и изменяемых состояний. Благодаря этому Sealevel может исполнять независимые операции параллельно, но для аналитика это означает дополнительный уровень реконструкции: нужно корректно интерпретировать список аккаунтов, инструкции, внутренние вызовы и изменения балансов.

SPL-токены усиливают эту сложность. Один кошелек может иметь отдельные token accounts для разных mint-аккаунтов, а токеновый счет имеет собственный адрес и владельца. Следовательно, наблюдаемый перевод между двумя token accounts не всегда

прямо равен переводу между двумя пользовательскими кошельками. Forensics-движок должен восстанавливать связь mint-owner-account, учитывать decimals и хранить суммы в атомарных единицах. Округление до display-формата допустимо для интерфейса, но не для сопоставления платежей и доказательной логики.

Недавнее графовое исследование Solana показывает, что сеть остается менее изученной, чем Ethereum, и обладает собственными структурными особенностями: высокой концентрацией операций вокруг центральных узлов, большой долей однонаправленных взаимодействий и заметной долей неуспешных или нулевых транзакций (Alizadeh & Khabbazian, 2025). Для forensic-практики это важно: нулевая или неуспешная операция может быть шумом, артефактом бота, попыткой атаки, частью тестирования или сигналом координации.

Поэтому Solana-forensics должен быть многослойным. Первый слой - сырой сбор данных через RPC или потоковую инфраструктуру. Второй - нормализация транзакций, балансов, token accounts и инструкций. Третий - построение графа переводов с временными атрибутами. Четвертый - правила и модели аномалий. Пятый - отчетность, где каждый вывод сопровождается объяснением и ссылкой на исходные транзакции.

Таблица 3. Сравнение Bitcoin, Ethereum и Solana с точки зрения forensic-анализа

Критерий	Bitcoin	Ethereum	Solana
Базовая модель	UTXO: входы и выходы транзакций.	Account model, смарт-контракты, журналы событий.	Account model с программами, account keys и инструкциями.
Токены	Не являются базовой функцией протокола.	ERC-20/721 через события Transfer и вызовы контрактов.	SPL/Token-2022 через mint и token accounts; нужно различать владельца и счет.
Основные признаки	UTXO-граф, change address, co-spending.	Logs, calldata, internal calls, DEX events.	Instruction traces, pre/post balances, token account ownership, slot context.
Порядок исполнения	Блоковая последовательность транзакций.	Последовательность в блоке, mempool влияет на MEV.	Параллельное исполнение независимых состояний; анализ по слотам и затронутым аккаунтам.
Типичные риски	Миксеры, ransomware, адресная обфускация.	Ponzi, rug pull, flash-loan, MEV, фишинг.	SPL-фишинг, боты, failed/zero-value noise, Solana-specific MEV, account confusion.
Главное ограничение анализа	Эвристики владения вероятностны.	Сложность смарт-контрактных композиций.	Недостаток открытых размеченных наборов и необходимость точной интерпретации аккаунтов.

Предлагаемая архитектурная рамка исходит из принципа минимального доверия. Forensics-движок не должен подписывать транзакции, хранить приватные ключи или иметь возможность перемещать активы. Его базовая функция - читать публичные данные, нормализовать их и выдавать проверяемые аналитические сигналы. Даже если сервер с движком будет скомпрометирован, атакующий не должен получить возможность распоряжаться средствами пользователей.

Логически система состоит из пяти модулей. RPC-reader или streaming-reader получает транзакции и балансы. Parser разрешает account keys, инструкции, pre/post balances и SPL-структуры. Normalizer переводит суммы в атомарные единицы и связывает

token accounts с владельцами и mint. Graph builder строит направленный мультиграф, где ребра имеют сумму, токен, слот, подпись и статус. Detector применяет объяснимые правила и, при наличии размеченных данных, ML-модели. Reporting layer формирует алерт с перечнем транзакций, признаков и уровнем уверенности.

Rust является рациональным выбором для такой системы не потому, что автоматически делает программу безопасной, а потому, что снижает класс ошибок, связанных с памятью и гонками данных. Модель владения, borrow checker, строгая типизация и зрелая экосистема асинхронного ввода-вывода позволяют строить высоконагруженный парсер с меньшим риском неопределенного поведения. Вместе с тем unsafe-зависимости, ошибки нормализации и неверные бизнес-правила остаются ответственностью разработчика; их необходимо контролировать аудитом зависимостей, тестами и инвариантами.

Таблица 4. Архитектурные компоненты self-hosted forensics-движка

Компонент	Функция	Критические требования
Сбор данных	Чтение транзакций, балансов и token accounts через read-only RPC или streaming API.	Никаких приватных ключей; журналирование endpoint, времени запроса и статуса ответа.
Парсер	Разрешение account keys, инструкций, pre/post balances, ошибок исполнения.	Строгая обработка отсутствующих полей; сохранение сырого JSON/хэша для повторной проверки.
Нормализатор	Перевод amount в атомарные единицы, учет decimals, mint и owner.	Сопоставление проводится в raw-единицах; display-округление не используется в логике.
Графовый слой	Построение направленного мультиграфа кошельков, token accounts и переводов.	Временные атрибуты: slot, block time, статус, токен, подпись, источник данных.
Детектор	Правила wash trading, dusting, pump-and-dump, MEV/sandwich, аномальных потоков.	Объяснимость: список сработавших признаков и воспроизводимые параметры окна.
Отчетность	Формирование алерта для аналитика и сохранение evidence bundle.	Версионирование правил, неизменяемые логи, возможность ручной валидации.

В исходном техническом проекте присутствует идея сопоставления платежей по точной сумме в атомарных единицах. В научной редакции ее следует описывать как частный практический механизм, применимый для мониторинга платежей в системе, где пользователь заранее получает уникальную сумму и адрес получателя. Такой подход может быть полезен в self-hosted платежном мониторинге, но он не должен смешиваться с общим forensic-анализом подозрительных транзакций.

Сильная сторона детерминированного сопоставления - воспроизводимость. Если ожидаемая сумма хранится в raw-формате, а транзакция содержит тот же amount с допустимым отклонением, результат можно проверить независимо. Слабая сторона - риск коллизий, ошибки округления, влияние пользовательского поведения и невозможность использовать сумму как единственный признак в расследовании. Поэтому в движке сумма должна быть лишь одним из признаков наряду с токеном, временем, отправителем, статусом, получателем и историей адреса.

Для научной корректности важно отказаться от формулировок вроде «нулевые ложные срабатывания» или «гарантированная идентификация», если они не подтверждены воспроизводимым экспериментом на опубликованном наборе данных.

Более корректная формулировка: «детерминированное сопоставление снижает неопределенность при известных платежных параметрах, но требует оценки коллизий, качества RPC-данных и пользовательских ошибок».

Безопасность forensic-движка должна рассматриваться отдельно от точности аналитики. Система, которая правильно выявляет подозрительные операции, но хранит приватные ключи или принимает неподписанные внешние команды, создает новый риск. Поэтому базовый дизайн должен исходить из read-only модели, минимальной сетевой поверхности, отказоустойчивого хранения состояния и прозрачного логирования действий.

Основные угрозы можно разделить на пять групп. Первая - подмена или неполнота RPC-данных. Вторая - ошибки нормализации токенов, особенно при decimals и token accounts. Третья - race conditions при параллельной обработке и записи результатов. Четвертая - supply-chain риск зависимостей Rust. Пятая - злоупотребление аналитическими результатами, когда вероятностный сигнал выдается за окончательное обвинение. Последняя угроза является не технической, но критической для научной и этической корректности.

Контрмеры должны быть встроены в архитектуру: кворум нескольких RPC-источников для критичных запросов, хранение хэшей исходных ответов, атомарная запись evidence bundle, Cargo.lock и аудит зависимостей, запрет write-RPC, версионирование правил, а также разделение уровней уверенности. Алерт должен означать «требует проверки», а не «доказано мошенничество».

Таблица 5. Угрозы для forensic-движка и рекомендуемые контрмеры

Угроза	Проявление	Контрмера
Подмена RPC-ответа	Движок получает неполные или искаженные данные о транзакции.	TLS, несколько источников, сохранение raw-response, повторная проверка критичных алертов.
Ошибки token-account интерпретации	Token account ошибочно принимается за пользовательский кошелек.	Явное хранение mint, owner, token account и decimals; тесты на известных транзакциях.
Race condition	Несколько потоков одновременно обновляют состояние алерта.	Атомарные операции записи, транзакционное хранилище, идемпотентность по signature.
Supply-chain риск	Компрометированная зависимость или небезопасный unsafe-код.	Cargo.lock, cargo-audit, минимизация зависимостей, review unsafe-блоков.
Ложная интерпретация алерта	Риск-скор воспринимается как доказательство вины.	Разделение факта и гипотезы; текстовое объяснение признаков; ручная валидация.
Утечка чувствительных данных	Логи содержат внутренние user ID или платежные инструкции.	Минимизация персональных данных, псевдонимизация, контроль доступа к evidence bundle.

Практический детектор должен начинаться не с универсальной модели, а с таксономии паттернов. В противном случае разные явления смешиваются в один класс «подозрительности», что ухудшает и точность, и интерпретируемость. Для Solana целесообразно выделить минимум пять классов: dusting и фишинговые микропереводы; wash trading; pump-and-dump; MEV/sandwich; многошаговое рассеивание средств после взлома или rug pull.

Dusting в Solana-контексте может включать микропереводы токенов, NFT или SOL,

которые используются не для экономической передачи стоимости, а для привлечения внимания пользователя, связывания адресов или доставки вредоносной ссылки через сопутствующие метаданные. В отличие от классической модели Bitcoin, здесь важна не только сумма, но и тип токена, metadata, частота рассылки и повторяемость отправителя.

Wash trading обнаруживается через циклы и повторяемые структуры. Для Solana такие циклы могут включать не только прямые переводы, но и операции на DEX/AMM, где субъект создает искусственный объем вокруг токена. На графовом уровне признаком служат короткие циклы с близкими суммами, повторяющиеся пары аккаунтов, отсутствие независимых контрагентов и синхронность операций в узком временном окне.

Pump-and-dump требует сочетания on-chain и рыночных признаков. On-chain данные показывают концентрацию закупок, распределение токенов, быстрый рост числа держателей и последующий сброс. Рыночные данные показывают всплеск цены, объема и волатильности. Для обзорной статьи важно подчеркнуть, что один лишь рост цены не является доказательством манипуляции; значимым становится сочетание координации, распределения выгод и последующего обвала.

MEV/sandwich является самым сложным паттерном, потому что злоупотребление заключено в порядке исполнения и экономическом результате. На уровне признаков нужно анализировать последовательность операций вокруг жертвы, одинаковые торговые пары, изменение цены до и после, прибыль атакующего и связь с bundle/validator-инфраструктурой. Для Solana это требует сбора данных с высокой временной точностью и аккуратного учета особенностей слотов.

Таблица 6. Паттерны подозрительных операций и объяснимые признаки

Паттерн	Наблюдаемые признаки	Риск ложного вывода	Что сохранять в evidence bundle
Dusting / фишинговая рассылка	Микросуммы, массовая отправка, новый/подозрительный токен, повторяемый отправитель.	Легитимные аирдропы и тестовые операции.	Mint, metadata, отправитель, список получателей, суммы, время, ссылки на транзакции.
Wash trading	Короткие циклы, самосделки, повторяемые контрагенты, близкие суммы, малое число независимых участников.	Маркет-мейкинг, арбитраж, ребалансировка.	Граф цикла, временное окно, суммы, токены, DEX/AMM-контекст.
Pump-and-dump	Предварительная концентрация токена, резкий рост объема/цены, последующая распродажа, новые адреса.	Органический рост интереса или новостной эффект.	Периоды до/после, распределение держателей, данные DEX/биржи, адреса выгодоприобретателей.
MEV / sandwich	Операции до и после сделки жертвы, одинаковая пара, изменение цены, прибыль атакующего.	Обычный арбитраж без вреда пользователю.	Последовательность в слоте/блоке, путь swap, pre/post balances, оценка прибыли.
Рассеивание средств	Многоходовая передача после инцидента, дробление суммы, переход к биржам/мостам/миксерам.	Казначейское управление или распределение ликвидности.	Дерево переводов, глубина, временная динамика, внешние метки сервисов.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Особую экономическую и техническую значимость в контексте Solana приобретает

механика dusting-атак, которая существенно отличается от аналогичного паттерна в сетях Bitcoin или Ethereum. В архитектуре Solana хранение любых данных on-chain (включая создание системных аккаунтов и токеновых счетов SPL) требует резервирования определенного объема нативной криптовалюты SOL для обеспечения rent-exempt баланса. Если баланс аккаунта падает ниже этого порога, он подлежит удалению при очистке слотов. При проведении массовых dusting-рассылок злоумышленники часто отправляют новые, мошеннические или низколиквидные SPL-токены на адреса пользователей. Для получения возможности распоряжаться или взаимодействовать с этими токенами на кошельке получателя должен быть инициализирован соответствующий ассоциированный токеновый счет (Associated Token Account, ATA). Инициализация ATA требует выделения rent-exempt баланса в SOL со стороны пользователя или самого отправителя. Таким образом, dusting-атаки в Solana преследуют не только классическую криминалистическую цель деанонимизации и связывания адресных кластеров, но и создают прямые экономические издержки (rent коллизии) либо маскируют вредоносные ссылки в метаданных токенов.

В данном разделе следует изложить основные результаты, полученные в ходе исследования. Представленные данные должны быть чётко структурированы, при необходимости дополнены таблицами, графиками, рисунками. Следует избегать излишнего описания и сосредоточиться на интерпретации ключевых наблюдений, измерений или расчетов. При необходимости результаты могут быть разделены на подпункты или тематические блоки.

Систематизация литературы позволяет сделать несколько выводов. Первый вывод: blockchain forensics находится на стыке технического анализа и доказательной интерпретации. Открытая транзакция сама по себе не является обвинением; она становится элементом доказательного набора только после корректной нормализации, сопоставления с контекстом и проверки альтернативных объяснений.

Второй вывод: Solana требует отдельной методики. Использование терминов «кошелек», «аккаунт» и «токеновый счет» как синонимов приводит к ошибкам. Для расследователя важно различать подпись транзакции, адрес fee payer, программные аккаунты, token account, owner, mint и фактическое изменение баланса. Ошибка на этом уровне не исправляется машинным обучением: модель будет обучаться на неправильно сконструированных признаках.

При реализации детерминированного сопоставления входящих и исходящих потоков по точной сумме (`amount`) в атомарных единицах возникает критический риск ложноположительных связей (коллизий). В условиях сверхвысокой пропускной способности Solana и доминирования на рынке высокочастотных торговых ботов (MEV-ботов, арбитражных и маркет-мейкинг алгоритмов) в рамках одного и того же слота или узкого временного окна неизбежно генерируются сотни транзакций с идентичными или крайне близкими объемами передаваемых активов. В этих обстоятельствах совпадение сумм переводов перестает служить надежным уникальным идентификатором связи между контрагентами. Детерминированный алгоритм сопоставления может ошибочно связывать независимые транзакции ботов в единый мошеннический граф (например, ложно классифицируя их как паттерны wash trading или циклическое рассеивание средств). Для нивелирования данного ограничения forensic-движок не должен опираться на сумму как на единственный изолированный признак: детерминированное выделение связей по `amount` должно проходить обязательную кросс-валидацию сопутствующими метаданными — включая верификацию путей исполнения инструкций (`instruction traces`), идентификаторов DEX-пулов, временных интервалов слотов и истории адресов отправителей.

Третий вывод: открытый self-hosted движок имеет научную ценность, если он не имитирует закрытые корпоративные платформы, а делает ставку на воспроизводимость. Коммерческие системы могут использовать недоступные внешние метки, собственные базы адресов и закрытые правила. Открытая исследовательская система должна компенсировать это прозрачностью: показывать исходные транзакции, параметры правил и границы уверенности.

Четвертый вывод: Rust полезен как инженерная основа, но не должен использоваться как аргумент вместо методики. Безопасность памяти, строгая типизация и конкурентная обработка важны для высоконагруженного парсинга. Но ложные срабатывания, неверные пороги, неполная база фишинговых адресов и ошибочная интерпретация DeFi-событий остаются проблемами методологии. Поэтому будущая эмпирическая часть должна измерять не только скорость, но и precision, recall, объяснимость, устойчивость к шуму и стоимость ручной проверки.

Пятый вывод связан с этикой. Криптовалютная криминалистика может помогать расследованиям, комплаенсу и защите пользователей, но она также создает риск чрезмерной деанонимизации и ошибочного присвоения адресов конкретным лицам. В статье предлагается использовать осторожную лексику: «подозрительный кластер», «вероятная связь», «требует проверки», «технический индикатор», а не «доказанный мошенник», если нет дополнительных подтверждений.

Главное ограничение обзора состоит в неравномерности научной базы. Bitcoin и Ethereum исследуются более десяти лет, тогда как Solana только недавно стала объектом системного графового анализа. Поэтому часть требований к Solana-forensics выводится не только из прямых Solana-исследований, но и из адаптации более зрелых методов к новой архитектуре. Такая адаптация должна проверяться экспериментально.

Второе ограничение связано с отсутствием открытого размеченного набора данных для Solana-мошенничества. Без такого набора трудно сравнивать алгоритмы и утверждать превосходство одного подхода над другим. Перспективным направлением является формирование benchmark-корпуса: подтвержденные атаки, обычные переводы, DEX-операции, ботовые транзакции, failed transactions и нулевые операции, снабженные прозрачной схемой разметки.

Третье направление - разработка объяснимых правил для MEV/sandwich в Solana. Здесь нельзя механически копировать Ethereum-эвристики, поскольку механизмы распространения транзакций, bundle-инфраструктура и исполнение по слотам отличаются. Нужны измерительные исследования, которые связывают порядок исполнения, изменение цены, прибыль и роль валидаторной инфраструктуры.

Четвертое направление - интеграция Rust-движка с формальными инвариантами. Для парсера можно проверять свойства «сумма в raw-единицах не теряется при конвертации», «одна signature не обрабатывается дважды», «токеновый счет не отождествляется с owner без явной связи». Такие инварианты ближе к безопасности by design, чем простой перечень библиотек.

Наконец, дальнейшая работа должна включать эмпирическую оценку. Для публикации исследовательского результата желательно представить воспроизводимый протокол: датасет, период сбора, RPC-источники, правила очистки, метрики, baseline-методы, код или псевдокод, а также анализ ошибок. Без этого forensics-движок остается технической идеей, а не проверенным научным инструментом.

ЗАКЛЮЧЕНИЕ

Обзор показал, что криминалистический анализ транзакций в высокопроизводительных блокчейнах требует перехода от простого просмотра адресов к

воспроизводимой аналитической системе. Методы, разработанные для Bitcoin и Ethereum, дают важную основу: адресная кластеризация, транзакционные графы, машинное обучение, анализ DeFi-атак и экономических манипуляций. Однако Solana предъявляет дополнительные требования, связанные с account model, SPL-токенами, instruction traces и параллельной моделью исполнения.

Для безопасного Rust-движка Solana-forensics в статье предложены ключевые требования: read-only доступ к данным, отсутствие приватных ключей, нормализация сумм в атомарных единицах, явное различение wallet/token account/mint/owner, построение временного мультиграфа, объяснимые правила детектирования и evidence bundle для повторной проверки. Такой подход позволяет рассматривать движок не как закрытый скоринговый черный ящик, а как научно проверяемый инструмент поддержки расследования.

Наиболее перспективной исследовательской повесткой является создание открытого benchmark-набора Solana-транзакций, адаптация графовых и ML-методов к Solana-данным, формализация признаков MEV/sandwich-атак и оценка влияния ошибок нормализации на качество расследования. До получения эмпирических метрик все утверждения о производительности и точности должны формулироваться осторожно. Это повышает не только научную добросовестность статьи, но и практическую ценность будущего инструмента для кибербезопасности и цифровой криминалистики.

КОНФЛИКТ ИНТЕРЕСОВ: Авторы заявляют об отсутствии конфликта интересов.

ФИНАНСИРОВАНИЕ: Исследование не получало внешнего финансирования.

ЗАЯВЛЕНИЕ ОБ ОДОБРЕНИИ ИНСТИТУЦИОНАЛЬНЫМ ЭТИЧЕСКИМ КОМИТЕТОМ (IRB): Этическое одобрение не требовалось, поскольку статья представляет обзор литературы и не включает эксперименты с участием людей или персональными данными.

ЗАЯВЛЕНИЕ ОБ ИНФОРМИРОВАННОМ СОГЛАСИИ: Не применимо.

ЗАЯВЛЕНИЕ О ДОСТУПНОСТИ ДАННЫХ: Новые экспериментальные данные в рамках данной обзорной статьи не создавались. Все рассмотренные материалы доступны в опубликованных источниках, указанных в списке литературы.

БЛАГОДАРНОСТИ: Автор благодарит разработчиков открытых блокчейн-инструментов и исследователей, чьи публикации сформировали основу настоящего обзора.

УВЕДОМЛЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: При подготовке рукописи использовались AI-инструменты для языкового редактирования.

СПИСОК ЛИТЕРАТУРЫ

Alizadeh, S., & Khabbazian, M. (2025). Solana's transaction network: Analysis, insights, and comparison. EPJ Data Science, 14, Article 48. https://doi.org/10.1140/epjds/s13688-025-00561-x

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. Electronics, 13(17), 3568. https://doi.org/10.3390/electronics13173568

Bartoletti, M., Carta, S., Cimoli, T., & Saia, R. (2020). Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact. Future Generation Computer Systems, 102, 259-277. https://doi.org/10.1016/j.future.2019.08.014

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and

Informatics, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Chen, W., Zheng, Z., Cui, J., Ngai, E. C. H., Zheng, P., & Zhou, Y. (2018). Detecting Ponzi schemes on Ethereum: Towards healthier blockchain technology. In Companion Proceedings of the Web Conference 2018 (pp. 1409-1418). ACM. https://doi.org/10.1145/3178876.3186046

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (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

Cui, S., Zhao, G., Gao, Y., Tavu, T., & Huang, J. (2022). VRust: Automated vulnerability detection for Solana smart contracts. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 639-652). ACM. https://doi.org/10.1145/3548606.3560552

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash Boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In 2020 IEEE Symposium on Security and Privacy (pp. 910-927). IEEE. https://doi.org/10.1109/SP40000.2020.00040

Hamrick, J. T., Rouhi, F., Mukherjee, A., Feder, A., Gandal, N., Moore, T., & Vasek, M. (2021). An examination of the cryptocurrency pump-and-dump ecosystem. Information Processing & Management, 58(4), 102506. https://doi.org/10.1016/j.ipm.2021.102506

Hasan, M., Rahman, M. S., Janicke, H., & Sarker, I. H. (2024). Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis. Blockchain: Research and Applications, Article 100207. https://doi.org/10.1016/j.bcra.2024.100207

Jung, R., Jourdan, J. H., Krebbers, R., & Dreyer, D. (2018). RustBelt: Securing the foundations of the Rust programming language. Proceedings of the ACM on Programming Languages, 2(POPL), Article 66. https://doi.org/10.1145/3158154

Kamps, J., & Kleinberg, B. (2018). To the moon: Defining and detecting cryptocurrency pump-and-dumps. Crime Science, 7, Article 18. https://doi.org/10.1186/s40163-018-0093-5

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841-853. https://doi.org/10.1016/j.future.2017.08.020

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A fistful of Bitcoins: Characterizing payments among men with no names. Communications of the ACM, 59(4), 80-87. https://doi.org/10.1145/2896384

Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. Electronic Markets, 33, Article 37. https://doi.org/10.1007/s12525-023-00654-3

Qin, K., Zhou, L., & Gervais, A. (2022). Quantifying blockchain extractable value: How dark is the forest? In 2022 IEEE Symposium on Security and Privacy. IEEE. https://doi.org/10.1109/SP46214.2022.9833734

Solana Foundation. (2026). Tokens on Solana. https://solana.com/docs/tokens

Solana Foundation. (2019). Sealevel - Parallel processing thousands of smart contracts. https://solana.com/news/sealevel---parallel-processing-thousands-of-smart-contracts

Victor, F., & Hagemann, T. (2019). Cryptocurrency pump and dump schemes: Quantification and detection. In 2019 IEEE International Conference on Data Mining Workshops (ICDMW) (pp. 244-251). IEEE. https://doi.org/10.1109/ICDMW.2019.00045

Victor, F., & Weintraud, A. M. (2021). Detecting and quantifying wash trading on decentralized cryptocurrency exchanges. In Proceedings of the Web Conference 2021 (pp. 23-32). ACM. https://doi.org/10.1145/3442381.3449824

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2022). SoK: Decentralized finance (DeFi). In Proceedings of the 4th ACM Conference on Advances

in Financial Technologies (pp. 30-46). ACM. https://doi.org/10.1145/3558535.3559780

Xu, J., & Livshits, B. (2019). The anatomy of a cryptocurrency pump-and-dump scheme. In 28th USENIX Security Symposium (pp. 1609-1625). USENIX Association. https://doi.org/10.48550/arXiv.1811.10109

Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2023). SoK: Decentralized finance (DeFi) attacks. In 2023 IEEE Symposium on Security and Privacy. IEEE. https://doi.org/10.1109/SP46215.2023.10179435

Yakovenko, A. (2017). Solana: A new architecture for a high performance blockchain v0.8.13. https://solana.com/solana-whitepaper.pdf

Tobias Cloosters, Pascal Winkler, Jens-Rene Giesen, Ghassan Karame, Lucas Davi SseRex: Practical Symbolic Execution of Solana Smart Contracts(2026) https://doi.org/10.48550/arXiv.2603.16349

Sven Smolka, Jens-Rene Giesen, Pascal Winkler, Oussama Draissi, Lucas Davi, Ghassan Karame, Klaus Pohl Smolka S. et al. *Fuzz on the Beach: Fuzzing Solana Smart Contracts* (2023) https://doi.org/10.1145/3576915.3623178

Sébastien Andreina, Tobias Cloosters, Lucas Davi, Jens-Rene Giesen, Marco Gutfleisch, Ghassan Karame, Alena Naiakshina, Houda Naji Xie J. et al. *Defying the Odds: Solana's Unexpected Resilience in Spite of the Security (2024)* https://doi.org/10.1145/3658644.3670333

XIANGFAN WU, JU XING, XIAOQI LI Exploring Vulnerabilities and Concerns in Solana Smart Contracts (2025) https://arxiv.org/abs/2504.07419

Jakub Sliwinski, Quentin Kniep, Roger Wattenhofer, Fabian Schaich Halting the Solana Blockchain with Epsilon Stake(2024) https://dl.acm.org/doi/10.1145/3631461.3631553

Ziwei Li, Zigui Jiang, Member, IEEE, Ming Fang, Jiaxin Chen, Zhiying Wu, Jiajing Wu, Senior Member, IEEE, Lun Zhang, Zibin Zheng, Fellow, IEEE SolPhishHunter: Towards Detecting and Understanding Phishing on Solana(2025) https://arxiv.org/pdf/2505.04094

XIAOYE ZHENG, ZHIYUAN WAN, DAVID LO, DIFAN XIE, XIAOHU YANG, Why Does My Transaction Fail? A First Look at Failed Transactions on the Solana Blockchain(2025) https://arxiv.org/pdf/2504.18055

Boqin Qin, Yilun Chen, Haopeng Liu, Hua Zhang, Qiaoyan Wen, Linhai Song, Yiying Zhang Understanding and Detecting Real-World Safety Issues in Rust(2024) https://dl.acm.org/doi/abs/10.1109/TSE.2024.3380393

Paul C. van Oorschot Memory Errors and Memory Safety: A Look at Java and Rust(2023) https://dl.acm.org/doi/abs/10.1109/MSEC.2023.3249719

Ayushi Sharma, Shashank Sharma, Sai Ritvik Tanksalkar, Santiago Torres-Arias Rust for Embedded Systems: Current State and Open Problems (Extended Report) (2024)

Detian Liu, Jianbiao Zhang, Yifan Wang, Hong Shen, Zhaoqian Zhang, Tao Ye Blockchain Smart Contract Security: Threats and Mitigation Strategies in a Lifecycle Perspective (2025) https://dl.acm.org/doi/10.1145/3769013

Авторлар туралы мәліметтер
Информация об авторах
Information about authors

	**Рохас-Криулько Наталья Педровна** – «Д. Серікбаев атындағы Шығыс Қазақстан техникалық университеті» КеАҚ «Цифрлық технологиялар және жасанды интеллект мектебі» оқытушы, Өскемен қ., Қазақстан **Рохас-Криулько Наталья Педровна** – преподаватель Школы цифровых технологий и искусственного интеллекта НАО «Восточно-Казахстанский технический университет им. Д. Серикбаева», г. Усть-Каменогорск, Казахстан **Rokhas Kriulko Natalia Pedrovna** – NAO "D. Serikbaev East Kazakhstan Technical University" lecturer at Lecturer at the School of Digital Technologies and Artificial Intelligence of the NAO "D. Serikbayev East Kazakhstan Technical University", Ust-Kamenogorsk, Kazakhstan e-mail: nrohas@edu.ektu.kz, ORCID: https://orcid.org/0009-0006-6841-0593,
	**Еремеев Владислав Алексеевич** – «Д. Серікбаев атындағы Шығыс Қазақстан техникалық университеті» КеАҚ «Цифрлық технологиялар және жасанды интеллект мектебі» студенті, Өскемен қ., Қазақстан **Еремеев Владислав Алексеевич** – студент Школы цифровых технологий и искусственного интеллекта НАО «Восточно-Казахстанский технический университет им. Д. Серикбаева», г. Усть-Каменогорск, Казахстан **Yeremeev Vladislav** – student of the School of Digital Technologies and Artificial Intelligence of the NAO "D. Serikbayev East Kazakhstan Technical University", Ust-Kamenogorsk, Kazakhstan, e-mail: yeremeyevvladislav918@gmail.com, ORCID: https://orcid.org/0009-0009-9390-698X
	**Попов Данил Андреевич** – «Д. Серікбаев атындағы Шығыс Қазақстан техникалық университеті» КеАҚ «Цифрлық технологиялар және жасанды интеллект мектебі» студенті, Өскемен қ., Қазақстан **Попов Данил Андреевич** студент Школы цифровых технологий и искусственного интеллекта НАО «Восточно-Казахстанский технический университет им. Д. Серикбаева», г. Усть-Каменогорск, Казахстан **Popov Danil** – student of the School of Digital Technologies and Artificial Intelligence of the NAO "D. Serikbayev East Kazakhstan Technical University", Ust-Kamenogorsk, Kazakhstan, e-mail: danilppv@gmail.com, ORCID: https://orcid.org/0009-0006-7966-461X

	**Киричёк Кирилл Николаевич** – «Д. Серікбаев атындағы Шығыс Қазақстан техникалық университеті» КеАҚ «Цифрлық технологиялар және жасанды интеллект мектебі» студенті, Өскемен қ., Қазақстан **Киричёк Кирилл Николаевич** - студент Школы цифровых технологий и искусственного интеллекта НАО «Восточно-Казахстанский технический университет им. Д. Серикбаева», г. Усть-Каменогорск, Казахстан **Kirichyok Kirill** – student of the School of Digital Technologies and Artificial Intelligence of the NAO "D. Serikbayev East Kazakhstan Technical University", Ust-Kamenogorsk, Kazakhstan, e-mail: kirichek331@gmail.com, ORCID: https://orcid.org/0009-0003-3095-3582
	**Черных Тимур Равильевич** – «Д. Серікбаев атындағы Шығыс Қазақстан техникалық университеті» КеАҚ «Цифрлық технологиялар және жасанды интеллект мектебі» студенті, Өскемен қ., Қазақстан **Черных Тимур Равильевич** – студент Школы цифровых технологий и искусственного интеллекта НАО «Восточно-Казахстанский технический университет им. Д. Серикбаева», г. Усть-Каменогорск, Казахстан **Chernykh Timur** – student of the School of Digital Technologies and Artificial Intelligence of the NAO "D. Serikbayev East Kazakhstan Technical University", Ust-Kamenogorsk, Kazakhstan, e-mail: rewvtrew@gmail.com, ORCID: https://orcid.org/0009-0006-2645-3421