Анатомия ончейн-пампа: криминалистическое руководство по выявлению и отслеживанию рыночных манипуляций

Раздел 1: Идентификация архитекторов: классификация кошельков на этапе генерации токенов (TGE)

Основа любого криминалистического ончейн-анализа, направленного на выявление рыночных манипуляций, закладывается в самый ранний момент существования актива — в момент его создания и первоначального распределения. Событие генерации токенов (Token Generation Event, TGE) представляет собой не хаотичный, а тщательно спланированный процесс, управляемый смарт-контрактами и документацией по токеномике.[1] Эта предсказуемость создает уникальные ончейн-паттерны, анализ которых позволяет с высокой степенью уверенности идентифицировать и классифицировать кошельки ключевых инсайдеров: основателей, ранних инвесторов, казначейства (Treasury) и эдвайзеров. Создание такой карты основных участников является первым и решающим шагом, поскольку их последующие действия становятся главным объектом нашего расследования.

1.1. След TGE: деконструкция паттернов первоначального распределения

Анализ начинается с транзакции создания токен-контракта. Адрес, развернувший контракт (deployer), является отправной точкой. От него или от специально назначенного

адреса-дистрибьютора исходят первые транзакции, формирующие первоначальное распределение токенов.

Анализ последовательности транзакций

Тщательное изучение первых транзакций после TGE позволяет выявить четкие категории получателей:

- **Кошельки казначейства и экосистемных фондов:** Как правило, это первые и самые крупные получатели токенов. Характерным признаком является получение значительной доли от общего предложения (например, 20-40%) в рамках одной транзакции. Эти средства часто переводятся на вновь созданные смарт-контракты с мультиподписью (например, Gnosis Safe) для повышения безопасности. Такие кошельки нередко помечаются соответствующими тегами на аналитических платформах, таких как Nansen или Arkham Intelligence, что упрощает их идентификацию.[3] Ончейн-аналитик должен искать крупные переводы с круглыми суммами (например, 100 000 000 токенов) на адреса, которые являются не стандартными кошельками (Externally Owned Accounts, EOA), а смарт-контрактами.
- **Кошельки основателей, команды и инвесторов:** Распределение токенов для этих групп обычно происходит в виде серии последующих транзакций от основного дистрибьютора. Здесь проявляются следующие паттерны:
    - **Временная близость:** Транзакции происходят в быстрой последовательности, часто в пределах нескольких блоков друг от друга, что указывает на скоординированный, автоматизированный или полуавтоматизированный процесс распределения.
    - **Иерархия объемов:** Объемы переводов часто сгруппированы в четкие уровни, соответствующие различным раундам инвестирования или статусу участников. Например, кошельки инвесторов посевного раунда могут получить по 5 000 000 токенов каждый, в то время как участники приватного раунда — по 1 000 000 токенов.
    - **Возраст адресов-получателей:** В целях операционной безопасности и анонимности инсайдеры почти всегда получают свои аллокации на новые, специально созданные для этого кошельки (EOA). Перевод значительной аллокации на уже существующий, активный кошелек с богатой историей транзакций является крайне редким явлением.

1.2. Вестинг-контракты как поведенческие маркеры

Вестинг-схемы (vesting schedules) являются фундаментальным элементом токеномики, предназначенным для согласования интересов команды и инвесторов с долгосрочным

успехом проекта.[5] Предотвращая немедленную продажу больших объемов токенов, вестинг обеспечивает стабильность рынка. С точки зрения ончейн-анализа, вестинг-контракты — это один из самых надежных инструментов для идентификации инсайдеров. Они создают предсказуемую, заблокированную во времени ончейн-связь между кошельком и проектом.

Идентификация транзакций вестинга

Анализ транзакций от основного дистрибьютора выявляет переводы на адреса смарт-контрактов, которые не являются децентрализованными биржами (DEX) или известными DeFi-протоколами. Это, как правило, кастомные вестинг-контракты. Последующие транзакции, в которых кошельки-бенефициары запрашивают (claim) токены из этих контрактов, окончательно подтверждают их статус инсайдеров.

Ончейн-сигнатуры различных схем вестинга

- **Линейный вестинг (Linear Vesting):** Характеризуется регулярными, периодическими транзакциями получения токенов из вестинг-контракта.[6] Кошелек-бенефициар будет иметь историю транзакций, напоминающую работу часового механизма, например, получение ровно 1/36 от общей суммы каждый месяц в течение трех лет.
- **Вестинг с клиффом (Cliff Vesting):** Отличается полным отсутствием транзакций получения токенов в течение определенного начального периода (например, 12 месяцев), за которым следует одна крупная транзакция, когда значительная часть токенов (например, 25%) становится доступной для вывода.[5] Мониторинг первой транзакции получения средств после истечения клиффа является ключевым моментом для аналитика.
- **Событийный вестинг (Event-driven Vesting):** Этот тип сложнее отследить предиктивно, но его можно подтвердить ретроспективно. Если дорожная карта проекта предполагает разблокировку токенов после запуска основной сети (mainnet), аналитик может сопоставить дату этого события с ончейн-транзакциями получения средств из вестинг-контракта.[8]

Идентификация кошелька, получающего токены из вестинг-контракта, позволяет с практически стопроцентной уверенностью присвоить ему тег «Команда», «Основатель» или «Ранний инвестор». Любое последующее движение средств с этого кошелька, особенно в сторону централизованной биржи (CEX), приобретает чрезвычайно важное сигнальное значение. Таким образом, механизм, созданный для финансового контроля и стабильности, становится невольным источником ценнейшей разведывательной информации.

1.3. Продвинутая кластеризация кошельков и картирование

сущностей

Инсайдеры редко ограничиваются одним адресом. Для построения полной картины их ончейн-активности необходимо применять методы кластеризации, которые объединяют псевдонимные адреса в единую сущность, контролируемую одной группой лиц.[10]

Фундаментальные эвристики

- **Эвристика общего владения входами (Common Input Ownership Heuristic):** Основополагающий принцип кластеризации. Если несколько адресов используются в качестве входов (inputs) в одной транзакции, предполагается, что все они контролируются одним владельцем, поскольку для авторизации такой транзакции требуются приватные ключи от всех этих адресов.[10]
- **Анализ адресов для сдачи (Change Address Analysis):** В UTXO-блокчейнах, таких как Bitcoin, транзакции часто генерируют «сдачу», которая отправляется на новый адрес. Алгоритмы кластеризации могут идентифицировать эти адреса, связывая их с исходным кластером.[10]

Продвинутые и поведенческие эвристики

По мере того как аналитические инструменты становятся все более совершенными, злоумышленники адаптируют свои методы, избегая очевидных связей. Это приводит к необходимости использования более сложных эвристик:

- **Скоординированное пополнение газа:** Мощный, но тонкий сигнал. Когда центральный кошелек рассылает небольшие суммы ETH (для оплаты комиссий за транзакции) на несколько новых кошельков в течение короткого промежутка времени, это с высокой вероятностью указывает на подготовку этих кошельков к скоординированным действиям одной сущностью.
- **Эвристика стейкинга (на примере Cardano):** На PoS-блокчейнах, таких как Cardano, все платежные адреса, делегирующие свои средства на один и тот же стейкинг-ключ, могут быть объединены в один кластер. Это связано с тем, что владелец приватного ключа от стейкинг-адреса контролирует все полученные вознаграждения.[11]
- **Атрибуция депозитных адресов:** Как отмечают исследователи из Merkle Science, сущности часто используют одни и те же депозитные адреса для взаимодействия с CEX. Отслеживая потоки средств с этих адресов, можно идентифицировать основные горячие кошельки биржи и, как следствие, другие депозитные адреса, связанные с ними, создавая петлю обратной связи для идентификации сущностей.[12]

Анализ на основе графов

Конечная цель кластеризации — перейти от простого списка адресов к сетевому графу,

где адреса являются узлами, а транзакции — ребрами. Визуализация и анализ этого графа с помощью алгоритмов (например, выявление сообществ) позволяют обнаруживать плотно связанные группы кошельков, которые представляют собой операционную сеть одной сущности.[13] Платформы, такие как Arkham, предоставляют инструменты для визуализации этих связей, делая сложные схемы движения средств наглядными.[4]

Эта эволюция аналитических методов породила своего рода «гонку вооружений». Если раньше для сокрытия следов было достаточно использовать несколько несвязанных кошельков, то теперь, перед лицом мощных алгоритмов кластеризации и AI-систем деанонимизации [4], манипуляторы вынуждены прибегать к гораздо более сложным схемам, включающим десятки промежуточных «транзитных» кошельков и дробление средств, чтобы разорвать ончейн-связи и усложнить работу аналитиков.

Тип кошелька	Источник средств	Паттерн транзакций	Временные характеристики	Объем	Адрес назначения	Взаимодействие с вестингом
Основатели/Команда	Deployer/ Дистрибьютор	Серия транзакций с близкими по объему суммами	Пакетная отправка в течение нескольких блоков после TGE	Значительный, но не крупнейший % от общего предложения	Новый EOA	Часто через вестинг-контракт
Ранний инвестор	Deployer/ Дистрибьютор	Серия транзакций с четко выраженными уровнями и объемов	Пакетная отправка после транзакций для команды	Зависит от раунда (Seed, Private)	Новый EOA	Часто через вестинг-контракт
Казначе	Deployer/	Одна или	Обычно	Крупней	Новый	Прямой

йство (Treasury)	Дистрибьютор	несколько очень крупных транзакций	первая транзакция после TGE	ший % от общего предложения (20-50%+)	контракт с мультиподписью	перевод, без вестинга
Эдвайзеры	Deployer/ Дистрибьютор	Небольшие, часто единичные транзакции	Могут быть распределены во времени	Небольшой % от общего предложения	Новый EOA	Может быть как прямой перевод, так и через вестинг

Таблица 1: Сигнатуры распределения токенов на этапе TGE

Раздел 2: Подготовительная фаза: обнаружение самых ранних ончейн-сигналов

Этот раздел посвящен выявлению неочевидных ончейн-действий, которые предшествуют активным рыночным манипуляциям. Эти сигналы, подобно «подсказкам» в карточной игре, выдают намерения инсайдеров переместить активы на биржу для последующей продажи. Обнаружение этих подготовительных шагов позволяет предвидеть будущую волатильность задолго до того, как она станет очевидной для широкого рынка.

2.1. Сигнатура «тестового депозита»: след осторожности

Централизованные биржи (CEX), находясь под давлением регуляторов, обязаны внедрять процедуры AML (противодействие отмыванию денег) и KYC (знай своего клиента).[16] Одним из следствий этих требований является необходимость верификации или добавления в «белый список» (whitelisting) внешних кошельков перед осуществлением крупных депозитов или выводов средств.[18] Эта операционная

необходимость вынуждает инсайдеров совершать «тестовый депозит» — действие, которое оставляет четкий и предсказуемый след в блокчейне.

Анатомия тестового депозита

- **Цель:** Проверить контроль над собственным кошельком и убедиться в правильности адреса для депозита перед отправкой основной, крупной суммы. Биржи, такие как Coinbase и Gemini, открыто описывают эту процедуру как метод верификации.[20]
- **Сумма:** Транзакция имеет незначительный, неэкономический характер. Обычно это небольшое количество нативного токена сети (например, 0.001–0.01 ETH) или стейблкоина. В некоторых случаях, как, например, в «тесте Сатоши» от Coinbase, требуется отправить очень точную, некруглую сумму (например, 1.268 ADA), что делает такую транзакцию еще более заметной.[20]
- **Последовательность:** Тестовый депозит является *первым* взаимодействием между кошельком инсайдера и депозитным адресом CEX. За ним, после определенной задержки, следует основной депозит токена, предназначенного для продажи.
- **Временная задержка:** Интервал между тестовой и основной транзакцией является важным параметром. Он может варьироваться от нескольких минут до нескольких часов или даже дней. Короткий интервал свидетельствует о высокой степени готовности инсайдера к немедленным действиям.

Таким образом, регуляторные требования, направленные на повышение безопасности и прозрачности, парадоксальным образом создают один из самых надежных опережающих индикаторов для ончейн-аналитиков. Процедура комплаенса заставляет инсайдеров совершать предсказуемое и публично наблюдаемое действие, превращая функцию безопасности в сигнал для разведки.

2.2. Пробуждение: интерпретация реактивации «спящих» кошельков

Феномен «спящего кошелька» — это мощный рыночный сигнал. Кошелек, который был неактивен в течение длительного периода и внезапно проявляет активность, привлекает пристальное внимание всего рынка. Это связано с тем, что такие кошельки часто принадлежат ранним инвесторам или долгосрочным держателям, чьи действия считаются стратегическими и хорошо продуманными.[22]

Определение «спячки» и «активации»

- **Период неактивности:** Для того чтобы сигнал был сильным, период неактивности должен составлять не менее 6-12 месяцев. Кошельки, бездействовавшие несколько лет (3+ года), считаются особенно значимыми, так как они могут принадлежать

участникам ICO или даже «эпохи Сатоши».[23]

- **Тип транзакции активации:** Значимость пробуждения кошелька определяется не столько самим фактом движения средств, сколько *характером первой транзакции* после долгого периода бездействия.
    - **Сигнал высокой вероятности:** Получение ETH или стейблкоинов с миксера (например, Tornado Cash) или другого протокола для повышения конфиденциальности. Это преднамеренное и затратное действие, направленное на разрыв ончейн-связи с источником средств, и часто является прелюдией к финансированию новых кошельков для рыночных операций.
    - **Сигнал средней вероятности:** Получение средств с крупной CEX или перевод активов с другого блокчейна через мост. Это указывает на то, что владелец кошелька консолидирует активы и готовится к ончейн-активности.
    - **Подготовительный сигнал:** Первой транзакцией является вызов функции approve для смарт-контракта DEX или отправка небольшого тестового депозита. Это прямое и недвусмысленное указание на намерение взаимодействовать с CEX или DeFi-протоколами.

Анализ активации «спящих» кошельков требует перехода от простого наблюдения («кошелек переместил средства») к вероятностной оценке намерений, основанной на характере первого действия. Иерархия сигналов (миксер > approve > перевод с CEX > перевод на собственный адрес) позволяет с большей точностью прогнозировать будущие действия владельца кошелька.

2.3. Вспомогательные подготовительные сигналы: цифровая «разведка»

Помимо тестовых депозитов и активации «спящих» кошельков, существуют и другие, менее очевидные ончейн-действия, которые указывают на подготовку к манипуляциям.

- **Превентивное одобрение контрактов (Approve):** Прежде чем продать токен на DEX (например, Uniswap) или внести его в определенные смарт-контракты, владелец должен выполнить транзакцию approve, которая дает контракту разрешение на перемещение токенов от его имени. Мониторинг транзакций approve для целевого токена, особенно с кошельков, ранее идентифицированных как инсайдерские, является прямым сигналом о намерении совершить сделку.
- **Скоординированное пополнение газа:** Как уже упоминалось, этот паттерн является не только эвристикой для кластеризации, но и подготовительным сигналом. Наблюдение за тем, как известный инсайдерский кошелек распределяет ETH на серию новых кошельков, является сильным индикатором подготовки к распределенной операции покупки или продажи.

- **Взаимодействие с депозитными адресами бирж:** Даже до совершения депозита аналитик может отслеживать любые взаимодействия (включая транзакции с нулевой стоимостью) с известными депозитными адресами CEX. Иногда такие действия могут использоваться для запуска процессов верификации или добавления в белый список на стороне биржи.

Раздел 3: Зажигание и выход: анализ активных фаз манипуляции

Этот раздел посвящен анализу двух наиболее динамичных и критически важных этапов пампа: скоординированной скупки, которая инициирует рост цены («зажигание»), и тщательно организованной продажи, которая обрушивает рынок («выход»). Ключевая задача здесь — установить четкие ончейн-критерии, позволяющие отличить манипулятивную активность от органического поведения рынка.

3.1. Зажигание: скоординированная скупка инсайдеров против одиночного кита

Крупная покупка на рынке может быть как первым шагом в скоординированном пампе, так и действием одиночного «кита» — крупного инвестора, действующего на основе собственной уверенности в проекте.[25] Различение этих двух сценариев имеет первостепенное значение для правильной оценки ситуации. Для этого используется многофакторная аналитическая модель.

- **Временная корреляция (Тайминг):** Скоординированный памп характеризуется серией покупок с нескольких, на первый взгляд, независимых кошельков, происходящих в очень сжатые сроки (от нескольких минут до нескольких часов). Покупка одиночного кита, как правило, представляет собой одну крупную транзакцию или несколько транзакций от одной кластеризованной сущности.
- **Анализ источника средств:** Это наиболее важный отличительный признак.
    - **Скоординированные инсайдеры:** Средства для покупок часто можно проследить до общего источника (например, вывод с одной и той же CEX, один кошелек-финансист, который распределил ETH или стейблкоины) или они поступают с серии недавно созданных и пополненных кошельков.
    - **Органический кит:** Средства, как правило, поступают с уже существующего, давно активного кошелька с разнообразной историей ончейн-активности.

- **Соотношение объема и ликвидности:** Инсайдеры, организующие памп, часто совершают покупки, размер которых намеренно рассчитан так, чтобы «подтолкнуть цену вверх», не исчерпывая при этом всю ликвидность за одну сделку. Анализ размера каждой покупки относительно глубины пула ликвидности DEX в момент сделки показывает, что серия покупок, каждая из которых поглощает 5-10% доступной ликвидности, более характерна для скоординированного пампа, чем одна транзакция, поглощающая 50%.
- **Обнаружение фиктивной торговли (Wash Trading):** Для создания иллюзии высокого объема и привлечения органических покупателей инсайдеры могут прибегать к фиктивной торговле — одновременной покупке и продаже актива самим себе.[27] Ончейн это можно обнаружить, выявив адреса, которые выступают и покупателем, и продавцом в одной и той же транзакции (или в тесном цикле транзакций) без чистого изменения позиции. Такие сделки часто выполняются ботами с высокой скоростью.[28]

Таким образом, ключевое различие между скоординированным пампом и органической покупкой кита заключается не столько в *объеме* транзакций, сколько в *структуре и хореографии* предшествующих им потоков капитала. Если покупке предшествовала сложная, многоадресная и скоординированная по времени подготовка, это с высокой вероятностью указывает на манипулятивное намерение.

3.2. Подготовка к выходу: ончейн-паттерны, предшествующие дампу

Инсайдеры прекрасно понимают, что прямой перевод большого количества токенов с известного кошелька «Команды» на CEX вызовет панику на рынке и обрушит цену до того, как они успеют продать свои активы.[29] Поэтому для сокрытия потоков средств перед продажей они используют сложные методы.

Ключевые паттерны сокрытия

- **Фрагментация / «Очистка» (Peel Chaining):** Крупный пакет токенов (например, 10 млн) не отправляется единовременно. Вместо этого он дробится на множество более мелких, часто неровных сумм (например, 137 456 токенов, 89 211 токенов) и рассылается на серию вновь созданных кошельков. Это делается для того, чтобы обойти простые системы оповещения о «крупных переводах».
- **Промежуточные «транзитные» кошельки:** Фрагментированные суммы не отправляются напрямую на CEX. Сначала они поступают на один или несколько промежуточных кошельков. Эти «транзитные» или «перевалочные» кошельки существуют только для того, чтобы получить средства из нескольких источников и

затем перенаправить их в конечный пункт назначения, разрывая прямую связь между инсайдером и биржей.[30] Типичная схема выглядит так:
Кластер инсайдера -> 10-20 новых кошельков -> 1-3 транзитных кошелька -> Депозитные адреса CEX.

- **Распределенные по времени и биржам депозиты:** Чтобы не создавать единого крупного всплеска притока токенов на CEX, инсайдеры распределяют свои депозиты во времени (в течение нескольких часов или дней) и между несколькими биржами (например, Binance, KuCoin, OKX). Это затрудняет анализ для тех, кто отслеживает потоки только на одной бирже.

Эти методы, используемые инсайдерами для подготовки к дампу, функционально идентичны техникам отмывания денег, таким как «слоение» (layering) и «структурирование» (structuring/smurfing).[16] Это означает, что аналитические инструменты и эвристики, разработанные для борьбы с отмыванием денег и финансированием терроризма (AML/CFT), могут быть эффективно применены для обнаружения подготовки к рыночным манипуляциям. Платформы, такие как Chainalysis и Elliptic, которые специализируются на отслеживании незаконных средств для правоохранительных органов, обладают необходимыми возможностями для выявления таких схем.[10]

Окончательным подтверждением дампа является резкое увеличение предложения токена на CEX, которое отслеживается аналитическими платформами, за которым следует быстрое падение цены, сопровождающееся высоким объемом торгов.[29] Описанные выше ончейн-паттерны являются опережающими индикаторами этого события.

Раздел 4: От теории к практике: создание системы мониторинга в реальном времени

Этот заключительный раздел переводит аналитические концепции в плоскость практической реализации. Он представляет собой руководство по основным инструментам и передовым практикам для создания надежной автоматизированной системы обнаружения ончейн-пампов, с особым акцентом на максимизацию целостности сигнала и минимизацию ложных срабатываний.

4.1. Инструментарий аналитика: сравнительный обзор

Основой любой системы мониторинга является надежный и своевременный доступ к данным блокчейна. Существует несколько уровней доступа к этим данным, каждый со своими преимуществами и недостатками.

- **Уровень доступа к данным:**
  - **Прямой доступ к ноде / Публичные API:** Базовый уровень, предоставляющий необработанные данные. Требует значительных инженерных усилий для обработки, индексации и анализа. API обозревателей блоков, таких как Etherscan, являются хорошей отправной точкой, но имеют ограничения по скорости запросов.[26]
  - **Платформы ончейн-аналитики (Freemium/Платные):** Эти сервисы предоставляют уже проиндексированные, помеченные и легко запрашиваемые данные через API, что является наиболее эффективным решением.
    - **Nansen:** Специализируется на маркировке кошельков (например, «Smart Money», «Airdrop Pro») и предоставляет дашборды в реальном времени для мониторинга потоков на биржи. Сильная сторона Nansen — идентификация того, *кто* совершает действия.[3]
    - **Arkham Intelligence:** Мощная платформа для картирования сущностей и визуализации транзакционных потоков с помощью инструмента Visualizer. API предоставляет программный доступ к данным о сущностях, портфелях и истории транзакций.[4]
    - **Glassnode:** Предлагает глубокие и сложные ончейн-метрики (например, Realized Profit/Loss, SOPR), доступные через высокопроизводительный API, что идеально подходит для количественного анализа и построения предиктивных моделей.[35]
    - **Dune Analytics:** Гибкая платформа на основе SQL, где аналитики могут создавать и делиться собственными дашбордами. Хотя это в меньшей степени инструмент для оповещений в реальном времени, он незаменим для глубоких, кастомизированных исследований и исторического анализа.[36]
- **Библиотеки с открытым исходным кодом:** Для разработчиков, создающих собственные решения, необходимы такие библиотеки, как web3.py (Python) или ethers.js (JavaScript), для взаимодействия с нодами блокчейна и API.

Платформа	Ключевая особенность	Оповещения в реальном времени	Доступ по API	Гибкость запросов	Ценовая модель	Оптимальное применение
Nansen	Маркиро	Да	Да, с	Огранич	Подписк	Идентиф

	вка кошельков («Smart Money»)		ограничениями	енная	а	икация и отслеживание влиятельных игроков
Arkham Intelligence	Визуализатор связей, картирование сущностей	Да	Да	Средняя	Freemium / Платная	Криминалистический анализ, отслеживание потоков
Glassnode	Продвинутые ончейн-метрики	Да (через API)	Да, высокопроизводительный	Низкая (предустановленные метрики)	Подписка	Количественное моделирование, бэктестинг
Dune Analytics	Кастомные SQL-запросы и дашборды	Нет (запланированные обновления)	Да (для результатов запросов)	Высокая (SQL)	Freemium / Платная	Глубокие кастомизированные исследования
Etherscan API	Базовый доступ к данным транзакций	Нет	Да, с ограничениями по скорости	Низкая (предустановленные эндпоинты)	Бесплатно / Платные уровни	Простые скрипты и базовый мониторинг

Таблица 2: Сравнительный анализ платформ ончейн-аналитики

4.2. Целостность сигнала: система фильтрации шума и ложных

срабатываний

Основная проблема ончейн-анализа заключается в том, что блокчейн по своей природе является «шумной» средой. Один и тот же ончейн-сигнал может быть как признаком манипуляции, так и результатом легитимной деятельности. Надежная система должна уметь отличать одно от другого.[37]

- **Корреляция нескольких сигналов:** Наиболее эффективная стратегия — это создание скоринговой системы, в которой оповещение генерируется только тогда, когда для одной и той же сущности или токена в определенный промежуток времени фиксируется несколько независимых сигналов. Например: (Активация спящего кошелька с пополнением с миксера) + (Скоординированное пополнение газа) + (Серия небольших покупок на DEX) = Оповещение о высокой вероятности начала пампа.
- **Контекстуальная фильтрация:** Необработанные ончейн-данные должны быть помещены в контекст.
    - **Различение депозитов на CEX (продажа vs. стейкинг):** Это критически важная задача фильтрации. Крупный перевод на CEX может быть как подготовкой к продаже, так и участием в стейкинг-программе биржи. **Решение:** Необходимо вести базу данных известных адресов стейкинг-контрактов CEX. Анализируя адрес назначения, можно сделать вывод о цели перевода. Если токены отправляются на известный стейкинг-контракт, оповещение подавляется. Если на общий депозитный адрес горячего кошелька — приоритет оповещения повышается. Это требует сопоставления ончейн-данных с оффчейн-информацией (анонсы бирж о запуске стейкинг-программ).
    - **Фильтрация транзакций, связанных с работой протокола:** Крупные перемещения токенов могут быть связаны с легитимными операциями, такими как диверсификация казначейства, предоставление ликвидности для нового моста или выделение грантов, одобренных DAO. Такие транзакции следует фильтровать, сверяя их с публичными предложениями по управлению и официальными анонсами проекта.
- **Динамические пороги и скоринг рисков:** Вместо бинарных оповещений («да/нет») следует внедрить динамическую систему оценки рисков. Единичный крупный перевод на CEX может получить оценку 3/10. Если этому переводу предшествовала фрагментация с известного инсайдерского кошелька, оценка может вырасти до 7/10. Если, кроме того, была зафиксирована тестовая транзакция, оценка повышается до 9/10, генерируя оповещение с высоким приоритетом.[39] Такой подход, основанный на оценке рисков, позволяет сосредоточить внимание аналитика на наиболее вероятных событиях.

Эффективные системы ончейн-мониторинга работают не как детекторы отдельных событий, а как движки, отслеживающие «изменение состояний». Они сначала

устанавливают базовое состояние сущности (Состояние А: «спящий инсайдер»), а затем оповещают о *последовательности действий*, которые указывают на переход в новое состояние (Состояние Б: «подготовка к продаже»). Одна транзакция в вакууме неоднозначна. Истинный сигнал заключается в повествовательной последовательности действий. История начинается с идентификации инсайдерского кошелька на этапе TGE (Раздел 1). Затем происходит «пробуждение» и подготовка (Раздел 2). Наконец, наступает фаза активной манипуляции (Раздел 3). Система, отслеживающая эти переходы состояний, по своей сути более надежна и менее подвержена ложным срабатываниям.

Кроме того, проблема «сигнал против шума» в ончейн-анализе — это, по сути, проблема недостатка контекста. Решение заключается не только в улучшении алгоритмов, но и в систематической интеграции оффчейн-данных (анонсы бирж, предложения по управлению, активность в социальных сетях) для правильной интерпретации ончейн-событий. Продвинутая система ончейн-аналитики не может быть исключительно «ончейн». Она должна включать компонент, который систематически собирает и сопоставляет оффчейн-данные с ончейн-событиями, обеспечивая необходимый контекст и превращая шум в сигнал.

Выводы

Анализ ончейн-пампов представляет собой сложную, многоуровневую задачу, требующую комплексного подхода, выходящего за рамки простого отслеживания крупных транзакций. Как показывает данное исследование, скоординированные рыночные манипуляции оставляют в блокчейне отчетливый криминалистический след, который можно выявить и проанализировать на каждом этапе жизненного цикла схемы.

1. **Идентификация инсайдеров начинается с TGE.** Структурированный характер первоначального распределения токенов и использование вестинг-контрактов предоставляют наиболее надежные ончейн-маркеры для картирования сети кошельков, принадлежащих основателям, команде и ранним инвесторам.
2. **Подготовительные действия являются ключевыми опережающими индикаторами.** Такие сигналы, как «тестовые депозиты» на CEX (являющиеся непреднамеренным следствием регуляторных требований), активация «спящих» кошельков с пополнением через миксеры и превентивные вызовы функции approve, выдают намерения манипуляторов до начала активных действий.
3. **Различие между манипуляцией и органической активностью лежит в структуре, а не в объеме.** Скоординированную скупку отличает не столько размер покупок, сколько их временная корреляция и общий источник финансирования. Аналогично, подготовка к дампу характеризуется сложными схемами сокрытия

(фрагментация, транзитные кошельки), которые зеркально отражают методы отмывания денег.

4. **Эффективный мониторинг требует контекста и многофакторного анализа.** Для минимизации ложных срабатываний необходимо отказаться от анализа изолированных событий в пользу системы, которая отслеживает последовательность действий («изменение состояний») и обогащает ончейн-данные оффчейн-контекстом (анонсы проектов, биржевые программы).

В конечном счете, прозрачность блокчейна, которая часто воспринимается как гарантия честности, на самом деле является инструментом двойного назначения. Для манипуляторов она создает операционные сложности, вынуждая их прибегать ко все более изощренным методам сокрытия. Для аналитиков же она предоставляет беспрецедентный объем данных, позволяющий при наличии правильных инструментов и методологии не только реагировать на манипуляции постфактум, но и предвидеть их, защищая целостность рынка и активы инвесторов.

Works cited

1. Token Generation Events - Meegle, accessed on September 28, 2025, https://www.meegle.com/en_us/topics/tokenomics/token-generation-events
2. Token Generation Event (TGE) Marketing | Top TGE Agencies - LKI Consulting, accessed on September 28, 2025, https://lkiconsulting.io/marketing/token-generation-event-marketing/
3. What Is Address Labeling in Crypto? Complete Guide | Nansen, accessed on September 28, 2025, https://www.nansen.ai/post/what-is-address-labeling-in-crypto
4. On-Chain Analysis: What is it, how to do it, and the best blockchain analysis tools (2025) - Arkham, accessed on September 28, 2025, https://info.arkm.com/research/on-chain-analysis-guide
5. Understanding Vesting Schedules in Cryptocurrency | Magna Blog, accessed on September 28, 2025, https://www.magna.so/blog-posts/understanding-vesting-schedules-in-cryptocurrency
6. Exploring Vesting Schedules: Types and Tips - Rock'n'Block, accessed on September 28, 2025, https://rocknblock.io/blog/exploring-vesting-schedules-types-and-tips
7. Token Vesting - Everything you need to know - Eqvista, accessed on September 28, 2025, https://eqvista.com/company-valuation/valuation-crypto-assets/token-vesting/
8. Two ways of understanding Event-driven Vesting | by Nomiks - Medium, accessed on September 28, 2025, https://medium.com/@Nomiks/two-ways-of-understanding-event-driven-vesting-a7b11360184e
9. Vesting : the Good Practices.. This article has been produced by... | by Nomiks - Medium, accessed on September 28, 2025,

https://medium.com/@Nomiks/vesting-the-good-practices-6a189b408131
10. What Is Transaction Clustering in Crypto? Address Analysis | Nansen, accessed on September 28, 2025, https://www.nansen.ai/post/what-is-transaction-clustering-in-crypto-address-analysis
11. arxiv.org, accessed on September 28, 2025, https://arxiv.org/html/2503.09327v1
12. Transforming Blockchain Security: Introducing Our Advanced Clustering Algorithms and Heuristics for Bitcoin and Smart Contract Chains such as Ethereum and Tron - Merkle Science, accessed on September 28, 2025, https://www.merklescience.com/blog/transforming-blockchain-security-introducing-our-advanced-clustering-algorithms-and-heuristics-for-bitcoin-and-smart-contract-chains-such-as-ethereum-and-tron
13. [PDF] Bitcoin Transaction Graph Analysis - Semantic Scholar, accessed on September 28, 2025, https://www.semanticscholar.org/paper/Bitcoin-Transaction-Graph-Analysis-Fleder-Kester/a13134639194d3b41f04625d66713b5019bcda9d
14. Know Your Account: Double Graph Inference-based Account De-anonymization on Ethereum | Request PDF - ResearchGate, accessed on September 28, 2025, https://www.researchgate.net/publication/386335395_Know_Your_Account_Double_Graph_Inference-based_Account_De-anonymization_on_Ethereum
15. What Is Crypto Wallet Tracking? Complete Guide & Tools - Nansen, accessed on September 28, 2025, https://www.nansen.ai/post/what-is-crypto-wallet-tracking-complete-guide-tools
16. Introduction to Cryptocurrency Exchange Compliance - Chainalysis, accessed on September 28, 2025, https://www.chainalysis.com/blog/introduction-to-cryptocurrency-exchange-compliance-crypto-businesses-2024/
17. Crypto Exchange For KYC Verification - Meegle, accessed on September 28, 2025, https://www.meegle.com/en_us/topics/crypto-exchange/crypto-exchange-for-kyc-verification
18. How to withdraw cryptocurrency from my Crypto.com Exchange wallet (To: External Wallet Address), accessed on September 28, 2025, https://help.crypto.com/en/articles/3511870-how-to-withdraw-cryptocurrency-from-my-crypto-com-exchange-wallet-to-external-wallet-address
19. Whitelisting withdrawal addresses on the Crypto.com Exchange, accessed on September 28, 2025, https://help.crypto.com/en/articles/9233923-whitelisting-withdrawal-addresses-on-the-crypto-com-exchange
20. Small deposit test - Coinbase Help, accessed on September 28, 2025, https://help.coinbase.com/en/coinbase/trading-and-funding/sending-or-receiving-cryptocurrency/small-deposit-test
21. Verifying my wallet via Small Deposit Test - Gemini Support, accessed on September 28, 2025,

https://support.gemini.com/hc/en-us/articles/35261795002779-Verifying-my-wallet-via-Small-Deposit-Test
22. 8 Biggest Dormant BTC Wallets 2025 - Webopedia, accessed on September 28, 2025, https://www.webopedia.com/crypto/learn/dormant-bitcoin-wallets/
23. 10+ Year Dormant Bitcoin Whales Come to Life in 2024 - Bitquery, accessed on September 28, 2025, https://bitquery.io/blog/dormant-bitcoin-wallets-reactivated-insights-market-impact
24. Dormant Bitcoin Wallets Move 20,000 BTC After 14 Years - Bitbo, accessed on September 28, 2025, https://bitbo.io/news/dormant-bitcoin-wallets-move/
25. What Are Crypto Whales and How Can You Spot Them? - Binance TH, accessed on September 28, 2025, https://www.binance.th/en/faq/latest-release/1647b29d23be42a8a240316bba712302
26. What are the top crypto whales buying? How to track and find them - Nansen, accessed on September 28, 2025, https://www.nansen.ai/guides/what-are-the-top-crypto-whales-buying-how-to-track-and-find-them
27. Crypto Patterns That May Suggest Pump and Dump Schemes, accessed on September 28, 2025, https://www.chainalysis.com/blog/crypto-crime-2024-pump-and-dump/
28. Crypto Market Manipulation 2025: Suspected Wash Trading, Pump and Dump Schemes - Chainalysis, accessed on September 28, 2025, https://www.chainalysis.com/blog/crypto-market-manipulation-wash-trading-pump-and-dump-2025/
29. Onchain Signals: Key Indicators of Investor Dumping Activity | Nansen, accessed on September 28, 2025, https://www.nansen.ai/post/onchain-signals-key-indicators-of-investor-dumping-activity
30. Insider Trading Detected in 56% of Token Listings - Solidus Labs, accessed on September 28, 2025, https://www.soliduslabs.com/reports/crypto-insider-trading
31. How to Identify Suspicious Crypto Wallets Using Onchain Data - Nansen, accessed on September 28, 2025, https://www.nansen.ai/post/how-to-identify-suspicious-crypto-wallets-using-onchain-data
32. Elliptic: Blockchain Analytics & Crypto Compliance Solutions, accessed on September 28, 2025, https://www.elliptic.co/
33. Labels & Watchlists 101 - Nansen Academy, accessed on September 28, 2025, https://academy.nansen.ai/articles/2149924-labels-and-watchlists-101
34. Unofficial Arkham API, accessed on September 28, 2025, https://cipher-rc5.github.io/UnofficialArkhamAPI/
35. Glassnode - On-chain market intelligence, accessed on September 28, 2025, https://glassnode.com/
36. Welcome to Dune Docs - Dune Docs, accessed on September 28, 2025, https://docs.dune.com/

37. Data Analysis: 8 Tips For Finding Signals Within Noise | Blast Analytics, accessed on September 28, 2025, https://www.blastanalytics.com/blog/data-analysis-8-tips-finding-signals-within-noise
38. What are On-chain Analytics in Cryptocurrency? - Remitano, accessed on September 28, 2025, https://remitano.com/learn/br/14172-what-are-on-chain-analytics-in-cryptocurrency-noise-vs-signal-theory-explained
39. Reduce False Positives in AML: Best Practices and Examples in 2025 - FOCAL, accessed on September 28, 2025, https://www.getfocal.ai/blog/reduce-false-positives-in-aml