БОРИС ЛЕВ

ОТ СЛЕДА К ДОКАЗАТЕЛЬСТВУ

Как доказать и оспорить в суде принадлежность криптоактивов



ПРАВО РОССИИ И БЕЛАРУСИ

КРИПТОВАЛЮТА И ПРАВО · КНИГА 4

Борис Лев

От следа к доказательству

«Автор»
2026

Лев Б.

От следа к доказательству / Б. Лев — «Автор», 2026

След в блокчейне показывает, куда ушли деньги. Кто их перевёл, он не показывает. Между графом трассировки и выводом суда о том, чей это адрес, лежит цепочка умозаключений, и другая сторона может атаковать любое её звено. Книга о том, как такую цепочку построить, оспорить и защитить в российском и белорусском процессе.Атрибуция разобрана по шагам: эвристики и где они дают сбой, метки аналитических платформ, доступ, знание, контроль и выгода. Пятиуровневая шкала и реестр допущений позволяют записать силу каждого вывода так, чтобы её можно было проверить. Отдельно разобраны экспертиза и заключение специалиста, обеспечение иска и арест, возражения и допрос эксперта.Через книгу проходит учебный кейс: хищение 1,4 млн USDT, двенадцать шагов, два эксперта с разными выводами, решение суда. В приложениях — задание эксперту, 49 возражений, 86 вопросов эксперту и методика экспертизы для России и Беларуси.Для судебных юристов, экспертов и комплаенс-специалистов.

© Лев Б., 2026
© Автор, 2026

Содержание

Выходные данные 6
Как читать эту книгу 8
Место в серии 9
Часть I. Почему след ещё не доказательство 10
Глава 1. Разрыв 10
1.1 Шесть статусов, один разрыв 11
1.2 Два вопроса, которые звучат одинаково 12
Типичные ошибки 13
1.3 Внутри ATTRIBUTED: доступ, знание, контроль, выгода 13
Как это делают на практике 14
Пример формулировки: вопросы аналитику или эксперту 15
1.4 Для кого эта книга и чего в ней нет 16
1.5 Карта книги 17
Глава 2. Анатомия атрибуции 20
2.1 Атрибуция как цепочка выводов 20
2.2 Четыре вида шагов 21
2.3 Разметка шага 22
Пример формулировки 23
2.4 Учебный кейс: двенадцать шагов, две разметки 24
2.5 Где эксперты расходятся и почему 27
Как это делают на практике 28
Пример формулировки: вопросы аналитику и проект вопросов для ходатайства о назначении экспертизы 29
Типичные ошибки 29
Глава 3. Эвристики и где они ломаются 32
3.1 Эвристика — допущение с историей 33
3.2 Общие входы 34
Как это делают на практике 35
Пример формулировки: вопросы эксперту 35
3.3 Сдача и цепочки отщипов (peel chains) 36
Пример формулировки: вопросы эксперту 37
3.4 Кастодиальные и омнибус-адреса 37
Пример формулировки: запрос бирже 38
Пример формулировки: вопросы эксперту 38
3.5 Сети со счётной моделью: Ethereum, Tron, стейблкоины 38
Как это делают на практике 41
3.6 Миксеры, мосты, DEX и приватные монеты 41
Пример формулировки: вопросы эксперту 42
3.7 Время и временные метки 42
Пример формулировки: приложение с временными метками 43
Пример формулировки: вопросы эксперту 44
3.8 Сводная таблица: эвристика, допущение, атака, как закрыть 44

Типичные ошибки 45
Глава 4. Метки аналитических платформ: чёрный ящик в зале суда 48
4.1 Что такое метка и откуда она 48
Российский и белорусский контекст 50
4.2 «Платформа показала» ещё не вывод аналитика 50
Как это делают на практике 51
Пример формулировки в заключении 51
Пример вопросов для ходатайства о назначении экспертизы 51
Как оспаривать метку в рецензии 52
4.3 Метки меняются: снимки и версии 52
Как это делают на практике: фиксация выгрузки платформы 53
Пример формулировки: перечень выгрузок (приложение к заключению) 53
Типичные ошибки 53
4.4 Sterlingov: платформа перед судом 54
Что утверждала защита 54
Что признал суд 54
Почему доказательства всё же допущены 54
Что было раскрыто 55
Апелляция 55
Что из этого следует для практики 55
Что это значит для российского и белорусского суда 55
4.5 Когда платформы расходятся 56
Для стороны, которая опирается на атрибуцию 56
Для стороны, которая её оспаривает 56
Пример формулировки: как объяснить расхождение 56
4.6 ИИ как новый источник ошибок 57
Что должен сделать аналитик 57
Что спросит другая сторона 57
4.7 Что требовать от метки 58
Пример формулировки: ходатайство об истребовании исходных данных заключения 58
Часть II. Степень уверенности 62
Глава 5. Шкала 62
5.1 Зачем нужна шкала 62
Типичные ошибки 63
5.2 Пять уровней: критерии и формулировки 63
Конец ознакомительного фрагмента. 64

Борис Лев
От следа к доказательству

Выходные данные

Борис Лев
Первое издание, 2026
© Борис Лев, 2026. Все права защищены.

Никакая часть этой книги не может быть воспроизведена, сохранена в информационно-поисковой системе или передана в какой-либо форме и какими-либо средствами (электронными, механическими, путём фотокопирования, записи или иными), включая размещение в интернете и в корпоративных сетях, без предварительного письменного разрешения правообладателя, за исключением случаев, прямо предусмотренных законом, в том числе цитирования в объёме, оправданном целью цитирования.

Предупреждение

Книга носит образовательный и информационный характер. Она не является юридической консультацией и не создаёт отношений между юристом и клиентом. Она не заменяет консультации юриста, который знает право страны, где рассматривается дело, и изучил обстоятельства этого дела.

Книга посвящена праву Российской Федерации и Республики Беларусь; английские и американские дела приводятся как сравнительный материал. Прежде чем опираться на нормы и судебные акты, которые цитируются в книге, их нужно прочитать полностью и в действующей редакции.

Процессуальные правила, законодательство о цифровых валютах и судебная практика в этой области меняются быстро. Право изложено по состоянию на ноябрь 2026 года, и перед применением его нужно проверить. В пределах, допускаемых законом, ни автор, ни издатель не несут ответственности за решения, принятые на основе материалов книги, и за прямой или косвенный ущерб, связанный с их использованием.

Книга написана для обеих сторон спора: для тех, кто строит атрибуцию, и для тех, кто её проверяет. Она не предназначена для того, чтобы помочь кому-либо скрыть имущество, уклониться от исполнения судебного акта или воспрепятствовать обращению взыскания.

Дело «Халдена» и другие учебные примеры составные: имена, названия организаций, суммы, адреса и биржи вымышлены, процессуальные события придуманы. Нормы и судебные акты, которые разбираются в книге, реальны и указаны в примечаниях к главам.

Компании, сервисы и программные продукты упоминаются только для справки. Товарные знаки принадлежат их владельцам. Автор не связан ни с одной из упомянутых компаний и не получает от них вознаграждения.

Об использовании технологий

Книга подготовлена при существенном использовании инструментов искусственного интеллекта, которые работали под руководством автора. Они применялись для поиска материалов, подготовки черновиков текста, проверочных прочтений и редактуры. Книга не является переводом. Замысел, структура, редакторские решения, сверка источников с первоисточниками и окончательное утверждение текста принадлежат автору.

Связаться с автором

Электронная почта: boris.lev.book@gmail.com
Telegram: t.me/LevBoris (@LevBoris)
Telegram-канал: t.me/lev_boris

LinkedIn: linkedin.com/in/borislev

Официальные контакты автора указаны выше. Любые другие аккаунты, использующие имя автора, к этой книге отношения не имеют.

Как читать эту книгу

Карта книги дана в конце главы 1 (раздел 1.5): таблица пяти частей и вопросов, на которые отвечает каждая. Начните с неё, а затем переходите к части, которая нужна вашему делу.

Шкала. Каждый вывод в книге имеет один из пяти уровней: «установлено», «весьма вероятно», «вероятно», «возможно», «не подтверждается». Глава 2 вводит шкалу, глава 5 даёт критерии каждого уровня и правила, по которым уровни применяются к цепочке шагов.

Дело «Халдена». Учебный кейс, который проходит через всю книгу. Глава 2 излагает его как цепочку из двенадцати шагов, глава 17 доводит до решения суда. Кейс составной.

Термины. Каждая глава открывается коротким списком терминов, а термин объясняется там, где он впервые встречается в главе. Поэтому главу можно читать отдельно от остальных. Определения собраны в глоссарии (приложение G).

Россия и Беларусь. Там, где правила двух стран совпадают по существу, они изложены вместе, со ссылками на нормы обеих. Там, где расходятся, у каждой страны свой раздел («Россия: …», «Беларусь»), а в главе 17 отличия белорусского процесса вынесены во врезки «РБ». Начиная с главы 7 английская и американская практика собрана в отдельных разделах «Сравнительный материал».

Приложение H. Методика проведения экспертизы дана в двух самостоятельных вариантах: для России и для Беларуси. Остальные приложения общие; где процесс различается, как в задании эксперту (приложение B), для каждой страны выделен свой раздел.

Место в серии

Это четвёртая книга серии «Криптовалюта и право».

• **«Криптовалютная криминалистика»** — о деле, в котором ваш клиент пострадавший: средства похищены, выведены через цепочку адресов, площадка исчезла.

• **«Поиск скрытых криптоактивов»** — об обратном случае: актив цел, у него есть владелец, и этот владелец — ваш оппонент, который не хочет, чтобы актив нашли.

• **«Происхождение цифровых активов»** — те же инструменты применительно к собственным активам: как доказать банку, налоговому органу, площадке и суду законность их происхождения.

• **Эта книга, «От следа к доказательству»,** — о том, что происходит, когда оспорена сама атрибуция и каждый шаг от данных к лицу должен выдержать проверку другой стороны и суда.

Метод у серии общий. В первых трёх книгах сила вывода обозначалась словами «установлено», «вероятно», «возможно». Эта книга сохраняет их как уровни 1, 3 и 4 пятиуровневой шкалы (глава 5). Где книга опирается на материал предыдущих, она называет книгу и главу.

Часть I. Почему след ещё не доказательство

Глава 1. Разрыв

Термины главы

• **Адрес**: строка из букв и цифр, на которую можно отправить криптоактивы. Похож на номер счёта, но имени владельца в нём нет.

• **Кошелёк**: программа или устройство, где хранятся ключи к одному или нескольким адресам. Кто владеет ключами, тот может перемещать активы.

• **Транзакция**: перевод между адресами, навсегда записанный в публичный реестр (блокчейн).

• **Трасса**: восстановленный путь средств от адреса к адресу, шаг за шагом; обычно изображается графом.

• **Депозитный адрес**: адрес, который биржа выдаёт одному клиенту, чтобы он пополнял свой счёт на бирже.

• **Горячий (сводный) кошелёк**: общий кошелёк биржи, в котором хранятся и из которого выплачиваются средства многих клиентов сразу. Похож на сводный счёт банка.

• **Атрибуция**: вывод о том, что адрес или транзакция принадлежит определённому лицу или совершена им.

• **Аналитическая платформа**: коммерческая программа (Chainalysis, TRM, Elliptic, Crystal), которая объединяет адреса в группы и присваивает им имена (метки).

Арбитражный суд в судебном заседании рассматривает ходатайство ответчика об отмене обеспечительной меры. Десятью днями раньше по заявлению истца, без извещения сторон, суд наложил арест на имущество ответчика. Основанием стало заключение аналитика с графом трассы. В графе сорок переходов (переход — один перевод с адреса на следующий адрес). Трасса проходит через три блокчейна и два моста (сервисы, которые переносят стоимость из одного блокчейна в другой), а также через один миксер (сервис, который смешивает монеты многих пользователей, чтобы разорвать связь между отправителем и получателем). В конце графа стоит адрес, который назван адресом ответчика. Заключение занимает 112 страниц. Представитель истца называет его «полной и непрерывной трассой».

У аналитика ответчика заключение на руках девять дней. Первые шестнадцать переходов она не оспаривает. Она просит суд посмотреть на семнадцатый. На нём средства поступают на адрес, который в заключении истца помечен как «промежуточный кошелёк, вероятно под контролем ответчика». Она показывает, что за тот же месяц этот адрес получил 41 000 входящих переводов более чем от 9 000 разных отправителей. Все исходящие переводы с него уходят на один горячий кошелёк лицензированной биржи. Это депозитный адрес. Биржа выдала его для одного клиентского счёта: всё, что на него поступает, зачисляется на этот счёт и пересылается на горячий кошелёк биржи. Клиентов у биржи, по её собственным данным, несколько сотен тысяч; девять тысяч отправителей позволяют предположить, что этот клиент сам является платёжным сервисом, который принимает деньги своих клиентов. Чей это счёт, может сказать только биржа.

Всё, что после семнадцатого перехода, по-прежнему верно описывает движение стоимости, но ничего не говорит о том, кто её перемещал. Суд отменяет арест имущества ответчика: истец не обосновал, что адрес, на который поступили средства, связан с ответчиком, а значит, не показал разумность и обоснованность своего требования именно к этому лицу. Истцу остаётся ходатайствовать об истребовании у биржи сведений о владельце счёта, если

биржа вообще ответит российскому суду. После работы ещё по двадцати трём переходам у истца против ответчика есть то же, что и до заключения: подозрение, а не доказательство.

Аналитик истца не был недобросовестен и проследил деньги верно. Его ошибка в том, что он написал «ответчик» там, где доказательства говорили только «кто-то».

1.1 Шесть статусов, один разрыв

Вторая книга серии, «Поиск скрытых криптоактивов», положила в основу метода формулу:

TRACED ≠ LOCATED ≠ ATTRIBUTED ≠ CONTROLLED ≠ PROVED ≠ RECOVERABLE

Определения те же; эта книга посвящена одному из шагов между статусами.

• **Traced (прослежен).** Движение стоимости прослежено до адреса, сервиса или счёта. Это делается по самому блокчейну или по записям, например по выпискам биржи.

• **Located (обнаружен).** Известно, где актив находится сейчас.

• **Attributed (атрибутирован).** Доказательства связывают это место с лицом или организацией, с указанным уровнем обоснованности.

• **Controlled (под контролем).** Кто-то фактически может переместить актив: у него есть ключи, право подписи или доступ к счёту. Контроль свидетельствует о владении, но сам по себе его не доказывает.

• **Proved (доказан).** Суд установил значимые для дела факты по применимому стандарту или может установить их на имеющихся доказательствах.

• **Recoverable (взыскиваем).** Есть правовой путь превратить актив или его стоимость в деньги или имущество в руках клиента.

Книга 1 учит первому статусу. Книга 2 ведёт дело от первого статуса к четвёртому и показывает, что собирать по пути к пятому. Книга 3 отвечает на другой вопрос: откуда актив взялся. Эта книга посвящена шагу от третьего статуса к пятому. Он начинается с атрибуции, которую готов подписать аналитик. Заканчивается он выводом, который готов сделать суд после того, как другая сторона попыталась этот вывод опровергнуть.

На этом шаге выигрывается или проигрывается большинство споров о криптоактивах, и о нём написано меньше всего. Трассировка — техническое ремесло со своими инструментами, вендорами (компаниями, которые продают аналитические платформы) и курсами. Судебный процесс — юридическое ремесло со своими нормами, судебной практикой и учебниками. Атрибуция находится между ними. Аналитик рассчитывает, что ею займётся юрист, а юрист считает, что ей уже занялось заключение. В заключении написано «вероятно под контролем ответчика», и никто не спрашивает, на чём основано «вероятно», пока об этом не спросит представитель другой стороны.

Открывающая сцена составная, но собрана из решённых дел, и не только российских. В английском деле *D'Aloia v Persons Unknown* у истца было больше, чем у истца в сцене: судебный запрет, раскрытие сведений биржей и трасса на четырнадцать переходов от его кошелька до депозитного кошелька на бирже Bitkub, привязанного к конкретному клиенту. Иск к бирже суд отклонил.

В вопросах права суд согласился с истцом. Он признал USDT (стейблкоин, то есть токен, курс которого привязан к доллару США) имуществом. Суд также признал, что по общему праву USDT в принципе можно проследить, пока его можно идентифицировать, а прослеживание через смешанный фонд допускается по праву справедливости (equity), но не по общему праву (в английском праве это две исторически разные ветви, и правила прослеживания в них различаются). С доказательствами всё было иначе. Суд указал, что экспертные доказательства были представлены хаотично и в итоге противоречиво. Две аналитические платформы дали

совершенно разные результаты, а доказательств того, как работает каждая из них, представлено не было. Суд не убедился, что хоть какая-то часть USDT истца вообще дошла до этого кошелька. Сбой произошёл на статус раньше, чем в сцене, на TRACED, а не на ATTRIBUTED, но причина та же: суду показали результаты платформ без рассуждения, которое к ним привело.

У разрыва между *attributed* и *proved* есть структура, и эта структура определяет план книги. Атрибуция состоит из цепочки утверждений. Каждое опирается на свои данные и своё правило их прочтения, и у каждого свой уровень обоснованности. Другая сторона может атаковать цепочку в любом звене. Защитить её можно в каждом звене, но только если знать, где звенья.

1.2 Два вопроса, которые звучат одинаково

Аналитик и судья могут смотреть на один граф и, казалось бы, задавать один и тот же вопрос. На деле вопросы разные, и большая часть проблем в этой области возникает из-за их смешения.

Аналитик спрашивает: **связаны ли эти адреса?** Её инструменты отвечают в терминах кластеров, потоков, времени операций и меток. Кластер — группа адресов, которую программа считает принадлежащей одному владельцу. Метка — имя, которое платформа присваивает адресу, например «Биржа K» или «мошенничество». Хороший ответ — хорошо обоснованный кластер, сходящийся поток или метка из источника, которому она доверяет. Единица её работы — адрес. Её стандарт сложился в профессии: сходится ли картина и пришёл бы ли другой компетентный аналитик с теми же данными к тому же кластеру.

Судья спрашивает: **доказал ли истец, что этот ответчик владел этим активом, распоряжался им или вывел его?** Единица его работы — лицо. Формально стандарт один: суд оценивает доказательства по внутреннему убеждению, основанному на их всестороннем, полном, объективном и непосредственном исследовании (ст. 67 ГПК РФ, ст. 71 АПК РФ; ч. 2 ст. 237 Кодекса гражданского судопроизводства Республики Беларусь). На практике порог меняется от стадии к стадии.

• Для обеспечения иска достаточно показать, что непринятие мер затруднит или сделает невозможным исполнение решения (ч. 2 ст. 139 ГПК РФ, ч. 2 ст. 90 АПК РФ, ст. 156 КГС РБ). Российский суд при этом проверяет разумность и обоснованность требования и связь меры с предметом иска, но не требует доказательств в объёме, нужном для решения по существу (пп. 14–15 постановления Пленума ВС РФ от 01.06.2023 № 15; подробно — глава 11).

• Для ареста имущества третьего лица в уголовном деле в России нужны достаточные основания полагать, что оно получено в результате преступных действий подозреваемого или обвиняемого либо использовалось или предназначалось как орудие или средство совершения преступления (ч. 3 ст. 115 УПК РФ). Для цифровой валюты с 3 марта 2026 г. действуют особые правила ареста и изъятия (ч. 7.1, 7.2 ст. 115, ст. 164.2 УПК РФ в ред. Федерального закона от 20.02.2026 № 38-ФЗ; глава 15). В Беларуси критерий иной: достаточные основания полагать, что имущество отчуждено подозреваемым или обвиняемым для сокрытия его принадлежности или источников (ст. 132 УПК РБ).

• Для решения по существу связь ответчика с активом должна быть установлена, а не предположена.

Судья не строит кластер сам. Он оценивает достоверность выводов заключения, в том числе вывода о кластере, и того, кто его подписал, по правилам о судебной экспертизе и о заключении специалиста (кто такой специалист и чем он отличается от эксперта — глава 9, конец 9.3).

Между двумя вопросами теряются три вещи.

1. Лица нет в блокчейне. Ни один блок не содержит имени. Переход от адреса к лицу всегда идёт через сведения вне блокчейна. Это может быть досье KYC (от англ. know your customer, «знай своего клиента»: документы, по которым биржа идентифицирует клиента при открытии счёта), устройство, банковский перевод, сообщение, поведение лица или признание. Граф аналитика заканчивается на адресе, а вопрос судьи с адреса начинается. То, что их соединяет, и есть настоящее доказательство атрибуции. Обычно это самая слабая часть материалов дела.

2. Уверенность не переводится сама собой. Слова «вероятно», «высокая степень уверенности», «сильная связь» внутри аналитической платформы означают результат скоринговой модели, то есть программы, которая оценивает связь в баллах. В заключении аналитика или эксперта те же слова означают его мнение о факте. Суд не примет уровень уверенности, если не видит его оснований, а представитель другой стороны спросит об основаниях первым делом. Глава 5 даёт словарь, который выдерживает такой перевод: пятиуровневую шкалу («установлено», «весьма вероятно», «вероятно», «возможно», «не подтверждается»), где у каждого уровня есть письменные критерии.

3. Порог движется, и атрибуция должна двигаться вместе с ним. Атрибуции, которой хватило для ареста имущества или для возбуждения уголовного дела, часто не хватает для решения по существу. Обеспечительные меры принимаются по материалам истца, без вызова ответчика (ч. 1.1 ст. 93 АПК РФ). Решение выносится после того, как ответчик представил свои возражения и рецензию, а нередко и после судебной экспертизы, которую суд поручает выбранному им эксперту. Поэтому цепочку выводов нужно либо с самого начала строить под более жёсткий тест (глава 14), либо перестраивать под возражения другой стороны. Разнице порогов посвящена глава 11.

Вопрос аналитика при этом остаётся необходимым: суд не может ответить на свой вопрос без её ответа. Ошибка — считать хороший ответ на первый вопрос ответом на второй или отвечать на второй, добавляя к первому прилагательные.

Типичные ошибки

• В иске или в заявлении о преступлении утверждается, что актив принадлежит ответчику, хотя доказано только поступление средств на счёт на бирже. Поступление указывает на счёт, а не на его владельца. Владельца устанавливает ответ биржи.

• Метка платформы («вероятно под контролем ответчика») переносится в исковое заявление или в ходатайство как установленный факт.

• Переход, на котором средства попадают на биржу, считается концом трассы против ответчика. На самом деле с этого места нужен второй источник вне блокчейна.

• Слова об уверенности в заключении не сопровождаются письменными критериями.

• Атрибуцию строят под обеспечительные меры или арест и рассчитывают, что она выдержит рассмотрение дела по существу.

1.3 Внутри ATTRIBUTED: доступ, знание, контроль, выгода

За словом «атрибутирован» стоят четыре отдельных утверждения. Заключение, которое сводит их в одно слово, легко написать и легко опровергнуть. Заключение, которое держит их раздельно, труднее написать и гораздо труднее опровергнуть: другой стороне придётся выиграть четыре спора вместо одного.

1. **Доступ.** Лицо могло добраться до адреса. У него был ключ, сид-фраза (обычно 12 или 24 слова, по которым восстанавливаются ключи кошелька), логин, устройство с установленным кошельком или роль подписанта в мультиподписном кошельке (таком, для перевода из

которого нужны подписи нескольких лиц). Трасса чаще всего доказывает именно доступ, и это самое слабое из четырёх звеньев. Общий ноутбук даёт доступ двоим. Сид-фраза, попавшая к посторонним, даёт доступ вору.

2. **Знание.** Лицо знало, что актив там. Примеры доступа без знания: кошелёк, установленный супругом; корпоративный ключ, оставшийся у бывшего сотрудника; сид-фраза в сейфе, который никто не открывал. Знание доказывается вне блокчейна: перепиской, скриншотами, проверками баланса, признаниями, временем входа в аккаунт по сравнению с движением рынка.

3. **Контроль.** Лицо перемещало актив или могло переместить его по своей воле. Доказательства: подписанные транзакции, запросы на вывод, логи биржи, привязанные к верифицированной личности и устройству. В «Поиске скрытых криптоактивов» контроль — четвёртый статус, и большинство судов считает его сердцевиной владения. Но и контроль не равен владению: контролировать актив могут и доверительный управляющий, и кастодиан (хранитель чужих активов), и вор.

4. **Выгода.** Стоимость или её эквивалент дошли до лица или до того, кому оно указало. Примеры: вывод в фиат (обычные деньги) на счёт на его имя, покупки, погашение его долгов, переводы его семье. Выгода превращает техническую картину в юридическую. Во многих делах это единственное звено, которое суд признаёт решающим.

Цепочка идёт в одну сторону. Выгода обычно предполагает контроль, а контроль — доступ. Обратное неверно: из доступа ничего не следует о выгоде. Большинство оспоренных атрибуций проигрывается одинаково. Истец доказывает доступ, называет его контролем и просит суд вывести из этого выгоду. Во многих успешных защитах ответчик просто показывает суду, что произошло именно это.

Отсюда два следствия для всей книги.

1. Четыре звена показывают, что собирать. Если задание аналитику звучит «чей это адрес?», ответ будет дан в терминах кластеров и меток. Если задание звучит «какие у нас доказательства доступа, знания, контроля и выгоды и какое звено самое слабое?», заключение будет таким, которым юрист может пользоваться. Приложение В ставит этот вопрос аналитику (вопрос 7 задания в В.3).

2. Четыре звена показывают, где вас будут атаковать. Каждое типовое возражение из главы 12 направлено против одного из четырёх звеньев. Общее хранение, угнанные аккаунты, скомпрометированные ключи и номинальные держатели направлены против доступа или контроля. «Он не знал» направлено против знания, «деньги ушли в другое место» — против выгоды. Если вы знаете, от какого звена зависит дело, вы знаете, к какому возражению готовиться.

Как это делают на практике

Каждое звено обычно доказывается своим видом доказательств, и находятся они у разных лиц. В таблице упоминается образ устройства: точная копия содержимого телефона или компьютера, снятая так, чтобы потом можно было проверить её целостность.

Звено	Чем обычно доказывается	Как получить
Доступ	Досье KYC по счёту на бирже; логи входа с IP-адресами (сетевыми адресами, с которых заходили в аккаунт) и идентификаторами устройств	Запрос бирже через следователя в уголовном деле; истребование доказательств судом в гражданском или арбитражном (экономическом) деле
Знание	Переписка, письма, скриншоты, где упоминается кошелёк или баланс; входы в аккаунт, совпадающие по времени со спорными переводами	Изъятие и осмотр устройств в уголовном деле; компьютерно-техническая экспертиза; логи биржи
Контроль	Подписанные транзакции из кошелька; запросы на вывод и их подтверждения; программа-кошелёк или сид-фраза, найденные на устройстве	Блокчейн; ответ биржи; компьютерно-техническая экспертиза изъятого устройства
Выгода	Банковские выписки о выводе средств с биржи на счёт на имя ответчика (обвиняемого); покупки и погашение долгов за счёт этих средств	Запрос в банк через следователя; истребование выписки судом

Порядок работы обычно такой.

1. Найти переход, на котором трасса входит в сервис, знающий своих клиентов, чаще всего в биржу. С этого места становятся доступны доказательства вне блокчейна.

2. Получить сведения биржи о счёте-получателе: досье KYC, логи входа и IP-адреса, историю выводов, привязанные банковские счета. В уголовном деле запрос направляет следователь. В гражданском и арбитражном деле сторона заявляет ходатайство об истребовании доказательств (ч. 1 ст. 57 ГПК РФ, ч. 4 ст. 66 АПК РФ; ст. 180, ч. 2 ст. 234, ч. 5 ст. 235 КГС РБ). Определение российского или белорусского суда иностранную биржу ни к чему не обязывает, и это нужно учитывать при выборе между гражданским и уголовным путём. Доказательства от неё получают через судебное поручение иностранному суду в порядке международного договора либо через материалы уголовного дела (уголовный путь при неустановленном лице разобран в главе 15). Если биржа не отвечает ни суду, ни следователю, атрибуция остаётся на уровне счёта, и требование к конкретному лицу на этих доказательствах заявлять преждевременно.

3. Проследить вывод в фиат до банка и получить выписки по счёту-получателю.

4. Если есть доступ к устройствам, добиться компьютерно-технической экспертизы: поиск программ-кошельков, сид-фраз и переписки.

5. Поставить аналитику или эксперту вопросы по каждому звену отдельно.

Пример формулировки: вопросы аналитику или эксперту

1. Имеются ли в представленных материалах сведения о том, что [лицо] имело доступ к адресу […] (ключам, сид-фразе, учётной записи на бирже, устройству с установленным кошельком)? Если да, какие именно и из какого источника (блокчейн, ответ биржи, сведения банка, материалы сторон)?

2. Имеются ли сведения о том, что [лицо] знало о нахождении активов на адресе […]? Если да, какие именно?

3. Имеются ли сведения о том, что переводы с адреса […] совершались [лицом] или по его распоряжению (подписанные транзакции, запросы на вывод, логи биржи, привязанные к его учётной записи и устройству)?

4. Поступали ли средства с адреса […] или их эквивалент на счета [лица] или указанных им лиц? Если да, когда, в каком размере и на основании каких документов это установлено?

5. По каждому из вопросов 1–4: каков уровень обоснованности вывода, по каким критериям и какие дополнительные сведения могли бы его изменить? Если материалов для ответа недостаточно, укажите это.

Вопросы в такой форме можно включить в задание аналитику стороны, предложить суду при назначении судебной экспертизы или, в уголовном деле, заявить в ходатайстве следователю. Вопрос «принадлежит ли адрес ответчику» в такой перечень не включают: ответ на него даёт суд. Вопросы эксперту и заключение по ним не могут выходить за пределы его специальных знаний; вопросы права перед экспертом не ставятся (п. 4 постановления Пленума ВС РФ от 21.12.2010 № 28 — по уголовным делам; п. 8 постановления Пленума ВАС РФ от 04.04.2014 № 23 — в арбитражном процессе). Раздельные ответы позволяют суду проверить каждое звено, а стороне заранее увидеть, какое звено нужно подкрепить.

Открывающая сцена проваливается на первом звене. Семнадцатый переход доказал, что *кто-то* со счётом на бирже имел доступ к средствам, но не что доступ имел ответчик. Поэтому до знания, контроля и выгоды дело не дошло, что бы ни говорили слова «вероятно под контролем ответчика». Пробел обнаружился в судебном заседании, хотя его можно было увидеть при подготовке заключения.

1.4 Для кого эта книга и чего в ней нет

Книга написана для четырёх читателей, которые встречаются в одном процессе и редко говорят на одном языке.

• **Судебный юрист**, у которой есть заключение о трассировке и предстоит заседание. Ей нужно знать, что заключение доказывает на самом деле, где его будут атаковать и что спросить у аналитика раньше, чем спросит другая сторона.

• **Аналитик или эксперт**, который собирается подписать заключение. Ему нужен способ формулировать выводы так, чтобы они выдержали вопросы другой стороны и суда. Ещё ему нужно фиксировать каждый шаг, чтобы честная уступка по одному шагу не обрушила остальные.

• **Расследователь из комплаенса** банка или биржи, который делает атрибуции каждую неделю и теперь видит, как они попадают в суд. Его внутренний стандарт («достаточно, чтобы подать отчёт») не совпадает с судебным, а соответствовать судебному ему придётся всё чаще.

• **Фонд судебного финансирования**, которому предлагают профинансировать криптоиск и показывают граф. Ему нужно уметь читать граф как риск. Ещё ему нужно знать, какие вопросы отличают иск, который закончится мировым соглашением, от иска, который рассыплется на семнадцатом переходе.

Три ограничения удерживают книгу в её предмете.

Она не учит трассировке. Кластеризация, эвристики (правила, по которым программа решает, что у адресов один владелец), мосты и миксеры объяснены в книге 1 и применены в книге 2. Глава 3 этой книги возвращается к ним только для того, чтобы показать, где каждый из этих приёмов даёт сбой: каждый сбой даёт другой стороне основание для возражения.

Она не учит процессу. Как фиксировать ончейн-данные (данные из самого блокчейна), как ставить задачу аналитику и как добиваться обеспечительных мер, изложено в «Криптовалютной криминалистике» (главы 15 и 20) и в «Поиске скрытых криптоактивов» (главы 9 и 14). Главы 8–11 этой книги опираются на тот материал и разбирают вопросы, которые там остались открытыми: что происходит, когда оспорен метод, спорны данные, суд назначил свою экспертизу или порог оказался выше, чем тот, под который строилась атрибуция.

Она не обещает возврата активов. Серия с первой страницы держится одной позиции: честная оценка того, что можно доказать и взыскать, стоит для клиента больше, чем уверенная.

В этой книге позиция особенно значима, потому что её предмет — расстояние между уверенностью и доказательством. Глава 16 даёт метод, как сказать клиенту «нет» и сказать это рано.

Юрисдикции. Право в этой книге — право Российской Федерации и Республики Беларусь по состоянию на дату, указанную на странице с выходными данными. Рассматриваются: гражданский, арбитражный и уголовный процесс России; гражданский процесс Беларуси (с 1 января 2026 г. он единый для общих и экономических судов и регулируется Кодексом гражданского судопроизводства) и её уголовный процесс; законодательство о судебно-экспертной деятельности; Федеральный закон № 282-ФЗ «О цифровых валютах и цифровых правах», правила ареста и изъятия цифровой валюты в УПК РФ (Федеральный закон от 20.02.2026 № 38-ФЗ) и белорусский режим цифровых знаков (токенов) по Декрету № 8 и последующим указам. Английские и американские дела приводятся как сравнительный материал. Споры об атрибуции там начались на несколько лет раньше, и их ошибки дешевле изучить по чужим решениям, чем повторить в своих. Ничто в этой книге не заменяет консультации юриста по вашему делу в вашем суде.

1.5 Карта книги

Через всю книгу проходит один учебный кейс, дело ООО «Халден Логистик» (далее — дело «Халдена»). Глава 2 вводит его как цепочку из двенадцати выводов, размеченную двумя экспертами, которые расходятся во мнениях. К нему возвращается каждая следующая глава, а в главе 17 цепочка доходит до суда.

Часть	Главы	На какой вопрос отвечает
I. Почему след ещё не доказательство	1–4	Из чего состоит атрибуция и где ломается каждая часть?
II. Степень уверенности	5–7	Насколько сильно каждое звено, как об этом сказать и как это записать?
III. Доказательство в суде	8–11	Что требуют российские и белорусские суды на каждой стадии, прежде чем действовать?
IV. Атака и защита	12–15	Как атрибуцию ломают, как её удерживают и что делать, если ответчика нет?
V. От доказательства к решению	16–17	Стоит ли вести этот иск, и как выглядит оспоренная атрибуция от иска до решения?

Каждая глава открывается коротким списком терминов и сценой из практики. В конце главы идут три врезки (для стороны истца, стороны ответчика и для аналитика или эксперта) и короткий список «Что проверить». В приложениях — рабочие документы: реестр допущений (приложение A), задание эксперту (B), чек-лист возражений (C), банк вопросов (D), таблица дел (E), структура заключения (F), глоссарий (G) и методика проведения экспертизы (H).

* * *

Для истца. Прежде чем представлять заключение, прочитайте его так, как прочитает другая сторона. Найдите первый переход, на котором средства поступают на адрес, которым ответчик не распоряжается единолично: биржа, платёжный провайдер, общий кошелёк. Всё после этого перехода требует второго источника вне блокчейна. Если его нет, ходатайство нужно нацеливать на истребование сведений о владельце счёта (ст. 57 ГПК РФ, ст. 66 АПК РФ) или на уголовный путь, где запрос бирже направит следователь. Просить на таких доказательствах арест имущества лица, которое, по вашему мнению, стоит за счётом, преждевременно.

Для ответчика. Не оспаривайте грамотную трассу. Спор с её арифметикой тратит доверие суда, которое понадобится позже. Найдите переход, на котором «кто-то» стал «ответчиком», и спросите, какое доказательство обосновало эту замену. В большинстве заключений это метка, совпадение по времени или круглое число. Глава 12 описывает, что делать с каждым из этих оснований, а глава 13 — как изложить это в рецензии на заключение и в вопросах эксперту.

Для эксперта. Пишите о четырёх звеньях раздельно: доступ, знание, контроль, выгода. Укажите, какие из них подтверждаются вашими материалами, а какие нет. Если заключение само называет свои пределы, рецензент другой стороны не найдёт в них ничего нового. Если оно заявляет все четыре звена при одном доказанном, вопросы в заседании будут именно об этом.

* * *

Что проверить

• ☐ Какого из шести статусов дело достигло на самом деле — по доказательствам, а не по исковому заявлению?

• ☐ На каком переходе трасса покидает адрес, которым ответчик распоряжается единолично?

• ☐ По доступу, знанию, контролю и выгоде — по одной строке: что это доказывает или «пока ничего».

• ☐ Поставлены ли аналитику или эксперту вопросы по каждому звену отдельно (пример — в 1.3)?

• ☐ Что решается на следующем заседании (обеспечение, арест по ст. 115 УПК или существо спора) и строилась ли атрибуция под этот порог или под более низкий?

• ☐ Есть ли за каждым словом об уверенности в заключении («вероятно», «высокая») письменные критерии?

• ☐ Кто подпишет заключение (аналитик стороны или судебный эксперт) и прочитал ли он его глазами рецензента другой стороны?

* * *

Примечания к главе 1

• Формула шести статусов и определения: Лев Б., «Поиск скрытых криптоактивов», глава 1 (в английском издании *Tracing Hidden Crypto Assets* — та же глава). Уровни атрибуции в предыдущей книге: Лев Б., «Криптовалютная криминалистика», глава 12; в этой книге их заменяет пятиуровневая шкала главы 5.

• Оценка доказательств по внутреннему убеждению: ч. 1 ст. 67 ГПК РФ, ч. 1 ст. 71 АПК РФ; ч. 2 ст. 237 Кодекса гражданского судопроизводства Республики Беларусь от 11.03.2024 № 359-З (в силе с 01.01.2026; ГПК 1999 г. и ХПК 1998 г. утратили силу). Обеспечение иска: ч. 2 ст. 139, ст. 140 ГПК РФ; ч. 2 ст. 90, ст. 91 АПК РФ; ст. 156–164 КГС РБ. Арест имущества в уголовном деле: ч. 3, 7.1, 7.2 ст. 115 УПК РФ (ч. 7.1 и 7.2 введены Федеральным законом от 20.02.2026 № 38-ФЗ); ст. 132 УПК РБ (критерий для имущества третьих лиц отличается от российского — см. 1.2). Истребование доказательств: ч. 1 ст. 57 ГПК РФ, ч. 4 ст. 66 АПК РФ; ст. 234–235 КГС РБ. *Сверено по consultant.ru (РФ) и по текстам КГС и УПК РБ в редакции Закона от 20.07.2026 № 173-З (последнее изменение по карточкам pravo.by; полный текст — зеркало prg.kz).*

• Судебная экспертиза и заключение специалиста: ст. 79–87 ГПК РФ (исследование заключения и вопросы эксперту в заседании — ст. 187), ст. 82–87 АПК РФ (вызов эксперта — ч. 3 ст. 86), Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»; постановление Пленума ВАС РФ от 04.04.2014 № 23 «О некоторых вопросах практики применения арбитражными судами законодательства об экспертизе», п. 8 (вопросы права и правовых последствий оценки доказательств не могут быть

поставлены перед экспертом); в Беларуси — ст. 218, 222, 227–228 КГС и Закон от 18.12.2019 № 281-З «О судебно-экспертной деятельности». Глава 9.

• Федеральный закон от 04.08.2026 № 282-ФЗ «О цифровых валютах и цифровых правах»: в силе с 01.09.2026, отдельные положения — с 01.07.2027 и 01.09.2027. Беларусь: Декрет Президента от 21.12.2017 № 8 «О развитии цифровой экономики» (действует), Указы № 367 от 17.09.2024 «Об обращении цифровых знаков (токенов)» и № 19 от 16.01.2026 «О криптобанках…». Сверено по вторичным источникам и разъяснениям государственных органов; перед применением сверьте с официальной публикацией.

• *Fabrizio D'Aloia v Persons Unknown Category A & Ors* [2024] EWHC 2342 (Ch), Высокий суд Англии, судья Ричард Фарнхилл (в качестве заместителя судьи Высокого суда), 12 сентября 2024 г.: USDT признан имуществом (п. 5); USDT в принципе можно проследить, прослеживание через смешанный фонд допускается по праву справедливости, но не по общему праву (п. 7); иск к Bitkub отклонён, потому что истец не доказал поступление хотя бы части своих средств на кошелёк 82e6 (пп. 6, 8). Экспертные доказательства были представлены «хаотично и в итоге противоречиво» (п. 58; в оригинале: chaotic and, ultimately, contradictory); TRM и Crystal дали «совершенно разные результаты» (п. 59; quite different results). Сверено по тексту решения на сайте Национального архива Великобритании (caselaw.nationalarchives.gov.uk/ewhc/ch/2024/2342).

• Открывающая сцена — составная. Цифры, количества и биржа вымышлены; схема взята из решённых дел.

Глава 2. Анатомия атрибуции

Термины главы

• **Вывод**: заключение, которое аналитик делает из данных, в отличие от того, что данные фиксируют напрямую.

• **Эвристика**: практическое правило чтения данных блокчейна, например «адреса, потраченные в одной транзакции, принадлежат одному владельцу». Обычно оно верно, но не всегда.

• **Кластер**: группа адресов, которые аналитик или платформа считают принадлежащими одному владельцу.

• **Метка**: запись в базе аналитической платформы о том, кому принадлежит адрес, например «Биржа K».

• **KYC** («знай своего клиента»): проверка личности, которую биржа проводит при открытии счёта, и досье клиента, которое она хранит.

• **Мост**: сервис, переносящий стоимость из одного блокчейна в другой, примерно как банк-корреспондент переводит деньги между двумя банковскими системами.

• **Газ**: небольшая плата сети за каждую транзакцию. В Ethereum комиссия платится в ETH; в Tron ей соответствуют энергия и пропускная способность, которые получают стейкингом TRX, делегированием от другого адреса или сжиганием TRX. Каждый адрес сам платит комиссию за свои транзакции и обычно не может отправить токены, пока у него нет нужного для неё. Другой адрес может только обеспечить его этим: прислать ETH или TRX, активировать новый адрес Tron (его активирует перевод TRX, перевод USDT не активирует), делегировать или сдать в аренду энергию. Кто это сделал, видно в блокчейне.

• **USDT в сети Tron**: долларовый стейблкоин компании Tether (один токен должен стоить один доллар США), учитываемый в блокчейне Tron.

Два заключения по одной краже поступают к судебному юристу с разницей в неделю. Оба написаны грамотными аналитиками. Оба начинаются с одного кошелька и ведут те же 1,4 млн USDT по тем же двенадцати шагам к одному биржевому счёту на имя человека по фамилии Реннер. Первое заключение делает вывод, что Реннер «контролировал средства на всём протяжении и является выгодоприобретателем хищения». Второе — что Реннер «получил часть похищенного на биржевой счёт на своё имя; контроль над промежуточными адресами не установлен».

Юрист читает оба дважды и не находит места, где они расходятся. Графы одинаковые, хеши транзакций (уникальные номера переводов) совпадают. Ни одно заключение не называет ложным то, что утверждает другое. Но первое даёт ей ответчика, а второе только свидетеля.

Данные одни и те же. Различается другое: что каждый аналитик вывел из них в каждой из двенадцати точек и сколько из своих рассуждений записал. Первый делал выводы смело и записал только итог, второй делал их осторожно и записал каждый шаг. В заседании по шагам можно проверить только второе заключение, поэтому у него больше шансов устоять.

2.1 Атрибуция как цепочка выводов

Английское издание книги «Поиск скрытых криптоактивов» (*Tracing Hidden Crypto Assets*) дало серии лестницу из пяти ступеней, которая показывает, насколько сильно можно сформулировать вывод: наблюдение, связь, вывод, подтверждённый вывод, заключение.

• **Наблюдение**: то, что записано в реестре (публичной записи всех транзакций блокчейна).

• **Связь**: то, что добавляют записи третьего лица. Например, биржа сообщает, что депозитный адрес принадлежит конкретному клиенту.

• **Вывод**: то, что добавляет аналитик. Например: судя по характеру переводов, этот адрес, вероятно, контролировало то же лицо, что и тот.

• **Подтверждение**: второй, независимый источник, говорящий то же самое.

• **Заключение**: то, что всё это в совокупности поддерживает. Его нельзя формулировать сильнее, чем позволяют ступени под ним.

Первым двум ступеням посвящены книги 1 и 2. Эта книга начинается с третьей. Атрибуции строятся и рушатся на последних трёх ступенях.

Атрибуция любой реальной сложности состоит из цепочки выводов. Каждый вывод берёт какие-то данные, применяет к ним правило прочтения и даёт утверждение. На этом утверждении строится следующий вывод.

В цепочке из открывающей сцены двенадцать звеньев. В большинстве оспоренных атрибуций их от восьми до двадцати. В каждом звене аналитик что-то решил, и в каждом другая сторона может спросить, на каком основании.

Для всего дальнейшего имеют значение три свойства такой цепочки.

1. Слабость передаётся вперёд, а не назад. Если звено шесть опирается на эвристику, верную в четырёх случаях из пяти, эту неопределённость наследуют все следующие звенья, как бы сильны они ни были сами по себе. Безупречное совпадение по KYC на звене десять не исправляет сомнительный кластер на звене шесть. Оно доказывает, что счёт, на который пришли средства на десятом звене, принадлежит Реннеру. Что он распоряжался ими на шестом, оно не доказывает.

2. Звенья не равнозначны. В большинстве цепочек весь вес атрибуции несут два-три звена, остальные их поддерживают. В главе 14 поиск таких звеньев назван анализом чувствительности. Автор, не разобравший цепочку по звеньям, не знает, какие из них важны, и поэтому не может их защитить.

3. Цепочку можно проверить лишь в той мере, в какой она записана. Два аналитика могут прогнать одну цепочку в голове и прийти к разным выводам, как в открывающей сцене, потому что ни один не записал шаги так, чтобы их можно было сравнить. Цепочку, существующую только в виде итогового вывода, нельзя проверить, а ошибку в ней нельзя исправить, не отбросив всю цепочку.

2.2 Четыре вида шагов

Каждое звено цепочки атрибуции относится к одному из четырёх видов. Вид показывает, что в звене может оказаться неверным и кого о нём спрашивать.

Ончейн-шаги читают реестр. Например: этот перевод пополнил тот адрес; эти адреса потратили средства вместе, в одной транзакции; вызов смарт-контракта (программы, работающей в блокчейне) перевёл токены с A на B; этот адрес отправил средства через мост в другую сеть. Данные публичны, и прочтение может повторить любой.

Непубличным остаётся правило, по которому данные читают, то есть эвристика. Глава 3 показывает, где каждое правило отказывает. Ончейн-шаг оспаривают, показывая, что правило к этой транзакции не подходит или что другое прочтение тех же данных не хуже.

Оффчейн-шаги связывают реестр с внешним миром. Например: запись биржи о том, что депозитный адрес принадлежит верифицированному клиенту; метка платформы о том, что адрес принадлежит известному сервису; IP-лог (журнал сетевых адресов, с которых входили в аккаунт); образ устройства с установленным кошельком; ответ на дастинг (крошечный проб-

ный перевод, рассчитанный на реакцию владельца адреса; судебный эксперт такой перевод не делает, потому что это сбор материалов, а аналитик стороны делает его только по прямому поручению: это контакт с возможной стороной спора, который может насторожить её до обращения за обеспечительными мерами); OSINT-совпадение (найденное по открытым источникам) адреса с аккаунтом в соцсети.

Каждую такую запись кто-то хранит, и надёжность этого держателя входит в шаг. Оффчейн-шаг оспаривают вопросами: откуда запись, как она получена, на какую дату верна и подтвердит ли её держатель в суде, дав подписку об ответственности за заведомо ложные показания.

Документальные шаги опираются на письменные доказательства: банковские выписки о выводе средств с биржи на банковский счёт; счета; договор, в тексте которого указан адрес кошелька; переписку, где адрес отправляют или обсуждают. Это самые сильные доказательства звеньев «знание» и «выгода» из главы 1. Их оспаривают обычным порядком: подлинность, полнота и разрыв между тем, что документ показывает, и тем, что им пытаются доказать.

Свидетельские шаги основаны на чьих-то словах: признании в переписке, объяснении следователю, показаниях соучастника, собственной позиции ответчика в отзыве. Для суда они самые убедительные. Опираться на них при этом рискованнее всего: свидетель может отказаться от своих слов, а реестр нет.

Виды шагов нужно держать раздельно. Если цепочка идёт от ончейн-кластера к названному лицу, в ней обязательно есть оффчейн-шаг, который совершает этот переход, и другая сторона будет проверять его первым. Частая ошибка заключений об атрибуции: имя просто появляется в конце ончейн-цепочки, взятое из метки без указанного источника. Разметка каждого шага по виду сразу обнаруживает такую ошибку.

2.3 Разметка шага

Каждый шаг записывается в шести полях. Формат намеренно простой. В главе 7 и приложении А он развёрнут в рабочий документ, реестр допущений.

Поле	Что туда писать	Для чего
Утверждение	Одно предложение: что утверждает этот шаг	Чтобы шаг можно было процитировать и оспорить отдельно
Данные	На чём держится утверждение (хеш транзакции, запись, документ, показания) и где это хранится	Чтобы любой мог это найти
Метод	Правило, применённое к данным: названная эвристика, запрос записи, сравнение двух дат	Чтобы правило можно было сверить с его известными пределами
Допущение	Что должно быть верно, чтобы метод дал здесь правильный ответ	Именно это другая сторона будет отрицать
Альтернатива	Лучшее объяснение тех же данных, которое не поддерживает утверждение	Шаг должен оказаться убедительнее этого объяснения
Обоснованность	Уровень от 1 до 5 по шкале книги (см. ниже), с одной строкой обоснования	Честный вес шага

Чаще всего аналитики пропускают четвёртое и пятое поля, а именно они решают исход спора. Если допущение записано, автор его обдумал. Если оно осталось неявным, другая сторона обычно находит его первой.

То же с альтернативой. Альтернатива, которую заключение называет и отвергает с обоснованием, почти ничего не даёт другой стороне. Альтернатива, впервые появившаяся в рецензии ответчика, уже нанесла ущерб.

В поле «Обоснованность» ставится один из пяти уровней шкалы книги:

1. **Установлено**: шаг прямо наблюдается или надёжно зафиксирован в записях либо все реальные альтернативы исключены.

2. **Весьма вероятно**: шаг подтверждают два независимых источника, основная альтернатива рассмотрена и признана маловероятной.

3. **Вероятно**: шаг объясняет данные лучше альтернатив, но опирается на один источник или метод либо основную альтернативу исключить нельзя.

4. **Возможно**: шаг совместим с данными, но хотя бы одна альтернатива объясняет их не хуже.

5. **Не подтверждается**: данных в пользу шага нет или данные говорят против него (аналитик указывает, что именно).

Критерии каждого уровня и правила их применения к цепочке изложены в главе 5. Метки *установлено*, *вероятно* и *возможно* из книг 1–3 (с небольшими расхождениями в формулировках) соответствуют уровням 1, 3 и 4.

Как уровни шкалы соотносятся с категорическими и вероятными выводами эксперта, показано в главе 5 (раздел 5.3).

Разметку держат честной два правила.

1. Одно утверждение на шаг. «Средства ушли на адрес X, который контролирует Реннер» содержит два шага: движение средств и атрибуцию. У них разные данные, разные методы и разная уверенность. Если записать их одним шагом, сильная половина скроет слабую.

2. Уверенность не может расти вдоль цепочки. Шаг не может быть увереннее самого слабого шага, от которого зависит. Если шаг отмечен уровнем 4 (возможно), то любой последующий шаг, использующий его результат, не выше уровня 4, как бы хорош ни был его собственный метод. Повысить уверенность может только подтверждение: второй шаг из независимых данных, приходящий к тому же утверждению. Это новый шаг со своими шестью полями, а не исправление старого.

Пример формулировки

Так шаг 7 учебного кейса (раздел 2.4) мог бы выглядеть в заключении, составленном по шести полям. Формулировка следует разметке эксперта Б. Многоточия обозначают сведения, которые в реальном заключении будут заполнены.

Шаг 7. E2 — промежуточный кошелёк, «связанный с» биржей K

Утверждение. Адрес E2 (сеть Ethereum, 0x…) является промежуточным кошельком, связанным с биржей K.

Данные. Метка «Биржа K — промежуточный», присвоенная адресу E2 аналитической платформой, в том виде, как она приведена в заключении аналитика истца (с. …). Дата получения метки и источник, на котором платформа её основала, в заключении не указаны. История транзакций адреса E2 за период с … по … (приложение …).

Метод. Использование метки платформы (оффчейн-шаг). Сведений о проверке метки по другим данным заключение аналитика истца не содержит.

Допущение. Метка обозначает кошелёк, используемый для одного клиента биржи K, и была верна на дату мартовских переводов.

Альтернатива. E2 принадлежит посреднику, например OTC-дилеру (дилеру, который покупает и продаёт криптоактивы для клиентов вне биржи) или иному сервису, зачисляющему

средства своих клиентов на биржу K, а не отдельному клиенту биржи. Метка не указывает, какой из этих вариантов верен. Если E2 является адресом посредника, шаг ничего не говорит о том, кто контролировал средства до D1. На шаг 8 это не влияет: перевод с E2 на D1 является обычным ончейн-переводом, который может проверить любой.

Обоснованность. Уровень 4 (возможно). Источник и дата метки неизвестны, метка не говорит, чей это адрес, поэтому адрес посредника объясняет данные не хуже клиентского кошелька. Уровень повысится, если биржа K в ответе на запрос подтвердит назначение адреса E2.

Каждое поле здесь можно проверить отдельно. Суд видит, почему шаг весит мало и какое доказательство его усилит.

2.4 Учебный кейс: двенадцать шагов, две разметки

Кейс составной. Все имена, суммы и адреса вымышлены. Схема повторяется в делах о хищении стейблкоинов (токенов, стоимость которых привязана к фиксированной сумме, обычно к одному доллару США).

Фабула. ООО «Халден Логистик» (далее — «Халден»), экспедитор, держала оборотные средства в USDT в сети Tron. Ключи от кошелька (секретные коды, которыми подписываются переводы) хранились на ноутбуке финансового директора. 3 марта ноутбук был заражён через вложение с поддельным счётом. 4 марта в 02:14 UTC 1 400 000 USDT ушли из кошелька одной транзакцией. Из этой суммы около 1,05 млн USDT позднее прошли через миксер или иной сервис, на котором след теряется. Поэтому след подтверждает только 348 000 USDT, поступившие на D1 (депозитный адрес биржи K), и 340 000 USDT, выведенные на банковский счёт Реннера.

Аналитик «Халдена» (эксперт А, привлечён истцом) и аналитик ответчика (эксперт Б) согласны в том, какие данные лежат в основе двенадцати шагов ниже. Они расходятся в том, что эти данные доказывают.

№	Утверждение	Вид	Данные	Эксперт А	Эксперт Б
1	1,4 млн USDT ушли с кошелька «Халдена» на адрес T1	Ончейн	Хеш, блок [высота]	1 (Установлено)	1 (Установлено)
2	Перевод с кошелька «Халдена» на T1 состоялся; то, что он не был санкционирован, следует из заявления директора и оценивается судом	Документ / показания	Отчёт об инциденте, образ ноутбука, объяснение директора	1 (Установлено)	1 (Установлено), не оспаривается
3	T1 за 40 минут разделил средства на четыре адреса T2–T5	Ончейн	Четыре хеша	1 (Установлено)	1 (Установлено)
4	T1–T5 контролировало одно лицо	Ончейн	Время переводов, равные доли; на все пять адресов TRX переведены и энергия делегирована с одного обычного кошелька, который их и активировал (не с сервиса аренды энергии)	1 (Установлено)	**3 (Вероятно)**: паттерн совместим и с одним лицом, и с дрейнер-сервисом, делящим выручку нескольких клиентов
5	T3 перевёл через мост 350 000 USDT на адрес E1 в Ethereum	Ончейн	Внесение средств в межсетевой обменный сервис в Tron и выплата этого сервиса в Ethereum, связанные его идентификатором перевода, записанным в обеих частях	1 (Установлено)	1 (Установлено)

Продолжение таблицы, строки 6–12 из 12

№	Утверждение	Вид	Данные	Эксперт А	Эксперт Б
6	E1 и E2 (позже получивший средства с моста) входят в один кластер	Ончейн	ETH на газ получены обоими адресами из общего источника; метка кластера на платформе	**1 (Установлено)**	**4 (Возможно)**: тот же источник присылал ETH и множеству несвязанных адресов (картина ретранслирующего сервиса, исключить его нельзя); источник метки не указан
7	E2 — промежуточный кошелёк, «связанный с» биржей K	Офчейн	Метка платформы «Биржа K — промежуточный»	1 (Установлено)	**4 (Возможно)**: метка не говорит, чей это кошелёк: клиента или посредника; дата снимка не указана
8	348 000 USDT прошли с E1 через E2 на депозитный адрес D1 биржи K	Ончейн	Хеш	1 (Установлено)	1 (Установлено)
9	D1 принадлежит клиентскому счёту K-7731	Офчейн	Ответ биржи K на запрос	1 (Установлено)	1 (Установлено), при условии ознакомления с ответом
10	Счёт K-7731 открыт на Мариуса Реннера	Офчейн	KYC-досье биржи K	1 (Установлено)	1 (Установлено)
11	Реннер контролировал T1–T5	Вывод	Шаги 4, 6, 7, 10	**1 (Установлено)**	**5 (Не подтверждается)**: ничто не связывает Реннера ни с чем до шага 8
12	Реннер — выгодоприобретатель хищения	Вывод	Шаги 1–11; вывод эквивалента 340 000 USDT на банковский счёт Реннера	**1 (Установлено)**	**3 (Вероятно)** для 348 000; **5 (Не подтверждается)** для 1,4 млн

Пояснения к таблице. *Хеш* — уникальный номер транзакции, *блок* — пакет транзакций, в котором она записана в реестр. *Дрейнер-сервис* похищает средства по заказу нескольких клиентов и делит между ними выручку. *Ретранслирующий сервис (relay)* снабжает средствами на комиссии множество не связанных между собой пользователей (присылает им ETH или TRX или делегирует энергию), поэтому общий источник средств на комиссии сам по себе не означает общего владельца. *Депозитный адрес* биржа выдаёт конкретному клиенту для пополнения счёта; горячий кошелёк и кошелёк-сборщик — общие кошельки биржи (глава 3, раздел 3.4). *Ответ на запрос* означает ответ биржи на запрос следователя или суда.

Tether выпускает USDT отдельно в сети Tron и в сети Ethereum, и сторонний мост не может создать USDT в Ethereum. Поэтому «мост» на шаге 5 означает межсетевой обменный сервис, мост в широком смысле: он получил 350 000 USDT от T3 в сети Tron и выплатил E1 в сети Ethereum USDT из собственного пула за вычетом своей комиссии 2 000 USDT (около 0,57%). Так на E1 поступило 348 000 USDT, та же сумма, что позднее поступила на D1. E1 получил не те токены, которые отправил T3, поэтому совпадение сумм не связывает две части перевода. Их связывает идентификатор перевода сервиса, записанный в обеих частях, или записи самого сервиса. В деле «Халдена» сервис записывает идентификатор перевода в обеих сетях, поэтому связь может проверить каждый по блокчейну, и шаг 5 оценён уровнем 1. Если бы сервис был кастодиальным (принимает депозит на адрес, выданный под одну заявку, и выплачивает со своего кошелька без общего идентификатора в блокчейне), связь опиралась

бы на его записи, и уровень зависел бы от них, как на шаге 9. С E1 348 000 USDT ушли на E2, а с E2 на D1; оба перевода записаны в блокчейне и учтены в шаге 8.

В столбце А все шаги сверху донизу отмечены уровнем 1 (установлено). В столбце Б цепочка рвётся в трёх местах.

В столбце «Данные» у эксперта А шаги 11 и 12 ссылаются на предыдущие шаги, а не на новые доказательства. Для вывода это нормально, но значит, что шаги 11 и 12 не могут быть сильнее самого слабого шага, на который ссылаются. А отметил их уровнем 1, хотя они держатся на шагах 4, 6 и 7, которым Б поставила уровни 3, 4 и 4. Новых доказательств итоговый вывод А к этим шагам не добавляет, только уверенность, а правило 2 из раздела 2.3 этого не допускает.

Шаг 12 приведён здесь так, как его отметила Б. В главе 5 (раздел 5.7) он уточнён и разделён на три утверждения: получение 348 000 USDT (уровень 1), извлечение выгоды из них (уровень 2) и осведомлённость Реннера о происхождении средств, которая остаётся открытым вопросом.

Шаги 2 и 10 опираются на материалы вне специальных знаний аналитиков: объяснение директора о том, что перевод не был санкционирован, и KYC-досье биржи K. Оба эксперта оценивают их только по тому, что показывают материалы дела. Правдивы ли объяснения директора и подлинны ли документы KYC, решает суд. На шаге 9 Б ставит уровень при условии ознакомления с ответом биржи. Аналитик стороны так поступить может, судебный эксперт — нет (глава 5, 5.7).

2.5 Где эксперты расходятся и почему

Эксперты расходятся в трёх звеньях: 4, 6 и 7. Все три расхождения устроены одинаково. А применил правило, не записав его допущение. Б записала допущение и установила, что оно не доказано.

Шаг 4. Правило: почти одновременное деление средств на равные доли с одного адреса, когда TRX и энергия для всех адресов получены с одного обычного кошелька, указывает на одного владельца. Допущение: сторонний сервис не участвовал.

Альтернатива: оператор «дрейнер-как-сервис», который похищает средства для нескольких клиентов и делит выручку с одного горячего кошелька (кошелька, из которого постоянно уходят платежи). Тогда T1 принадлежит сервису, а T2–T5 его клиентам, и утверждение об «одном лице» неверно именно в том смысле, который важен для иска.

А эту альтернативу не упомянул. Б упомянула и проверила то, что может показать блокчейн: подписан ли перевод на шаге 1 собственным ключом «Халдена» или сделан адресом, которому «Халден» ранее разрешил распоряжаться средствами (так работают многие дрейнеры), и получал ли T1 средства от других потерпевших. Исключить альтернативу по этим данным она не смогла и поставила шагу уровень 3 (вероятно). Недобросовестности здесь нет ни у кого; разметка Б полнее.

Шаг 6. Правило: адреса, получившие ETH на газ из общего источника, связаны между собой. Допущение: этот источник — собственный кошелёк злоумышленника. Данные показывают, что тот же источник присылал ETH на газ ещё тысячам адресов, не связанных ни с E1 и E2, ни друг с другом. Это картина ретранслирующего сервиса (например, моста, который присылает получателям немного ETH для первых транзакций), и эксперт Б не смогла исключить, что источник — такой сервис. Разрешить вопрос помогло бы сравнение времени: пришли ли ETH на E1 в той же транзакции, что выплата моста, или через несколько секунд после неё. Довод Б подкрепляет и практика 2026 года: ряд кошельков позволяет платить комиссию токенами, которые уже лежат на том же адресе, а саму транзакцию отправляет и оплачивает в ETH сервис поставщика кошелька, общий для тысяч пользователей (глава 3, раздел 3.5). Тогда

никакой внешний кошелёк не снабжает адрес средствами на газ, а общий плательщик комиссии ничего не связывает. Уровень шага от этого не меняется.

Метка кластера на платформе совпадает с выводом A, но в заключении не сказано, на чём эта метка основана. Если она основана на той же эвристике общего источника средств на комиссии, это не второй источник, а первый, учтённый дважды. В главе 6 это названо двойным счётом. Б поставила шагу уровень 4 (возможно) и указала, что второе, независимое основание для кластера повысило бы уровень.

Шаг 7. Метка платформы гласит: «Биржа K — промежуточный», то есть адрес связан с биржей K. А прочитал её как клиентский кошелёк. Б указала, что адрес может быть «связан с» биржей, не принадлежа её клиенту: им может пользоваться посредник, например OTC-дилер или иной сервис, зачисляющий средства своих клиентов на биржу. Метка не говорит, какой вариант верен, и в заключении нет её даты.

Если E2 — адрес посредника, шаг 7 ничего не говорит о том, кто контролировал средства до D1; шаг 8, обычный ончейн-перевод, который видит любой, остаётся в силе в любом случае. Метки такого рода разобраны в главе 4.

После понижения шагов 4, 6 и 7 под шагом 11 (*Реннер контролировал T1–T5*) не остаётся ничего на уровне 1, и Б ставит ему уровень 5 (не подтверждается). С хищением Реннера связывают только шаги 9 и 10. Они связывают его с поступлением 348 000 USDT, а не с выводом 1,4 млн.

Такое требование всё равно стоит заявлять, но оно уже того, которое поддерживает заключение А. Юрист, заявивший требование по заключению А, к судебному заседанию, скорее всего, будет защищать требование по заключению Б.

Из этого не следует, что Б права, а А ошибся. По фактам, которые выяснятся в главе 17, А может оказаться прав насчёт Реннера. Трудность в том, что заключение А не показывает, *почему* оно верно. Поэтому его нельзя исправить там, где оно ошибочно, и нельзя защитить там, где его оспаривают, а заключение Б это позволяет.

Следующие пять глав оставляют учебный кейс в этой точке и излагают инструменты, которые позволят двинуть его дальше: эвристики за шагами 4 и 6 (глава 3), метки за шагом 7 (глава 4), критерии пяти уровней обоснованности и правила их применения к цепочке (глава 5), правила сложения шагов без двойного счёта (глава 6) и реестр, в котором всё это ведётся (глава 7).

Как это делают на практике

Таблицу шагов проще всего получить до того, как аналитик сформулировал выводы. В российском и белорусском процессе для этого есть два пути.

Если сторона сама привлекает аналитика, требование о таблице шагов включают в задание аналитику (в договор или техническое задание). Если суд назначает экспертизу, сторона предлагает свои вопросы в ходатайстве о назначении экспертизы; окончательный круг вопросов определяет суд, а отклонение предложенных вопросов обязан мотивировать (ч. 2 ст. 79 ГПК РФ, ч. 2 ст. 82 АПК РФ). В Беларуси стороны вправе представить вопросы эксперту по п. 3 ст. 221 КГС, а отклонение их суд мотивирует (ч. 3 ст. 222 КГС). Это даёт стороне рычаг, но ограниченный: вопрос о форме исследования суд может счесть не требующим специальных знаний. Надёжнее просить суд указать в определении, что исследование по каждому шагу должно быть описано так, чтобы его обоснованность можно было проверить (ч. 2 ст. 86 ГПК РФ, ч. 2 ст. 86 АПК РФ; ст. 8 Федерального закона от 31.05.2001 № 73-ФЗ, которая в силу ч. 2 ст. 41 этого закона применяется и к негосударственным экспертам).

1. Попросите аналитика изложить атрибуцию пронумерованными шагами в шести полях раздела 2.3 до того, как он напишет заключение.

2. Просмотрите проект таблицы вместе с аналитиком: задавайте вопросы и делайте замечания, но не предлагайте уровни и обоснования. Отметьте каждый шаг, у которого в поле «Данные» только ссылки на предыдущие шаги, и каждый шаг, основанный на метке платформы.

3. По каждому слабому или спорному шагу спросите, какое доказательство повысит его уровень. Для шага 7 в деле «Халдена» это подтверждение биржи о назначении кошелька. Решите, запрашивать ли его через следователя или ходатайством об истребовании доказательств.

4. Заявляйте требование в пределах того, что поддерживают установленные шаги. Уточняйте его, когда новые доказательства повышают уверенность шага.

5. Попросите приложить итоговую таблицу к заключению или воспроизвести её в исследовательской части.

Таблица шагов прямо отвечает требованию ч. 2 ст. 86 ГПК РФ (в арбитражном процессе — ч. 2 ст. 86 АПК РФ: содержание и результаты исследований с указанием применённых методов, оценка результатов, обоснование выводов): заключение должно содержать подробное описание проведённого исследования, сделанные в результате его выводы и ответы на поставленные судом вопросы. Она полезна и суду. Заключение эксперта для суда необязательно, а несогласие с ним суд должен мотивировать (ч. 3 ст. 86 ГПК РФ). Разметка по шагам позволяет суду принять или отвергнуть вывод по конкретному шагу и сослаться на него в мотивировке. Нормы КГС Республики Беларусь о заключении эксперта разобраны в главе 9.

Пример формулировки: вопросы аналитику и проект вопросов для ходатайства о назначении экспертизы

Многоточия заменяются данными дела.

1. Какие транзакции и в какой последовательности связывают адрес … (кошелёк ООО «Халден Логистик») с адресом …? Каждый шаг изложите отдельно и пронумеруйте.

2. На каких данных основан каждый шаг (хеш транзакции, ответ биржи, иной документ) и где эти данные находятся?

3. Какой метод применён на каждом шаге и при каких условиях он даёт верный результат?

4. Какие иные объяснения тех же данных возможны для каждого шага и по каким основаниям они исключены либо не могут быть исключены?

5. В какой форме сделан вывод по каждому шагу (категорической, вероятной, вывод о невозможности ответить на вопрос) и почему? Для вероятного вывода: на каких данных он основан и какое иное объяснение не исключено?

6. Если шаг основан на метке аналитической платформы: какая это платформа, на какую дату получена метка и на каком источнике она основана?

7. Какие шаги основаны только на результатах других шагов, без новых данных?

Вопросы 3 и 4 соответствуют полям «Допущение» и «Альтернатива». Без них заключение обычно сообщает только итог. Вопросы 5 и 7 касаются формы заключения, а не обстоятельств, требующих специальных знаний, и суд может не включить их в определение; тогда их задают эксперту в судебном заседании (ст. 187 ГПК РФ, ч. 3 ст. 86 АПК РФ).

Типичные ошибки

• Сначала просят итоговый вывод, а шаги потом. Когда вывод уже написан, таблицу подгоняют под него, и шаги, которые его ослабляют, в неё не попадают.

• В ходатайстве ставят только вопрос о конечной принадлежности средств конкретному лицу. Эксперт отвечает на поставленный вопрос, и промежуточные шаги в заключение не попадают.

• Принимают заключение, где итоговые шаги ссылаются только на предыдущие шаги, но отмечены уровнем 1 (установлено). Это ошибка разметки А на шагах 11 и 12.

• Считают метку платформы подтверждением эвристики аналитика, хотя метка основана на той же эвристике (шаг 6).

• Оставляют поле «Альтернатива» пустым или пишут «отсутствует». Альтернативу предложит рецензия другой стороны.

• Ссылаются на метку платформы без даты и источника (шаг 7).

• Заявляют требование по итоговому выводу заключения, а не по тому, что поддерживают установленные шаги.

* * *

Для истца. Просите у аналитика таблицу шагов до заключения, а не после; для этого подойдут вопросы из раздела 2.5. Если в поле «Данные» шаг ссылается только на предыдущие шаги, это вывод, и вам нужно знать, на чём он держится, до того как вы заявите его в иске. Заявляйте требование, которое поддерживают установленные шаги: здесь это получение 348 000 USDT. Большее требование держите в резерве, пока шаги 4, 6 и 7 не подтверждены: увеличить требование на новых доказательствах проще, чем защищать его после рецензии ответчика.

Для ответчика. Постройте встречную таблицу сами, по заключению истца, до того как привлекать своего аналитика. Отметьте каждый шаг, который ссылается на метку без источника, на эвристику без допущения или на предыдущий шаг без новых данных. Выберите два-три шага, где альтернативное объяснение сильнее всего, а остальные не оспаривайте. Спор с явно установленными шагами расходует терпение суда, а в рецензии выглядит придиркой.

Для эксперта. Не подписывайте вывод, пока не выписали его цепочку в шести полях. Если альтернативное объяснение шага нельзя исключить по имеющимся данным, так и напишите и отметьте шаг соответственно. Тогда заказчик сможет искать данные, которые эту альтернативу исключат. Шаг, поднятый с уровня 3 до уровня 1 на новых данных, свидетельствует о строгости метода. Если же шаг, отмеченный уровнем 1, приходится понижать, отвечая на вопросы в заседании, суд обычно перестаёт доверять заключению в целом.

* * *

Что проверить

• ☐ Каждое звено цепочки — одно предложение, один вид, одно утверждение?

• ☐ Какие шаги являются выводами (в поле «Данные» только ссылки на предыдущие шаги) и какой самый слабый шаг под каждым из них?

• ☐ Для каждого ончейн-шага: эвристика названа, допущение записано?

• ☐ Для каждого оффчейн-шага: кто хранит запись, на какую дату она верна, подтвердит ли её держатель в суде?

• ☐ Где цепочка переходит от адреса к лицу и какой единственный шаг совершает этот переход?

• ☐ У каждого ли шага есть уровень от 1 до 5 с одной строкой обоснования? Нет ли шага с более высоким уровнем (меньшим номером), чем у шага, от которого он зависит?

• ☐ Альтернативное объяснение каждого спорного шага записано и отвергнуто с обоснованием или просто не упомянуто?

• ☐ Включено ли требование о таблице шагов в задание аналитику или в вопросы ходатайства о назначении экспертизы?

* * *

Примечания к главе 2

• Лестница утверждений (наблюдение → связь → вывод → подтверждённый вывод → заключение) и метки *установлено / вероятно / возможно*: Лев Б., «Поиск скрытых криптоактивов»; в английском издании (*Tracing Hidden Crypto Assets*) — глава 9, врезка «How strongly

to state a finding». Близкие метки: Лев Б., «Криптовалютная криминалистика», глава 15. Пятиуровневая шкала, которая заменяет их в этой книге, и её критерии: глава 5.

• Разметка шага шестью полями разворачивается в реестр допущений: глава 7 и приложение А.

• Дело «Халдена» — составное; все имена, суммы, адреса и биржа вымышлены. Механика USDT в сети Tron и мостов, которую он предполагает, описана в «Криптовалютной криминалистике», главы 4 и 13.

• Право сторон представить суду вопросы эксперту и обязанность суда мотивировать отклонение предложенных вопросов: ч. 2 ст. 79 ГПК РФ. Содержание заключения эксперта (подробное описание проведённого исследования, сделанные в результате его выводы и ответы на поставленные судом вопросы): ч. 2 ст. 86 ГПК РФ. Необязательность заключения для суда и обязанность мотивировать несогласие с ним: ч. 3 ст. 86 ГПК РФ. Тексты статей сверены по действующей редакции ГПК РФ, 01.11.2026. Процессуальный статус «специалиста» и «эксперта» в РФ и РБ, нормы КГС: глава 9. Других ссылок на нормативные акты и судебных решений глава не содержит.

Глава 3. Эвристики и где они ломаются

Термины главы

• **Вход и выход (модель UTXO).** Bitcoin не ведёт остатков по счетам. Кошелёк хранит отдельные неизрасходованные выходы прежних транзакций (UTXO). Как купюру, каждый можно потратить только целиком: транзакция берёт один или несколько из них как входы и создаёт новые выходы.

• **Сдача.** Выход, который возвращает плательщику неизрасходованный остаток, как магазин даёт сдачу с купюры.

• **Кластер.** Группа адресов, которую аналитик или платформа считает принадлежащей одному владельцу.

• **CoinJoin.** Одна транзакция, которую собирают много не связанных между собой пользователей, каждый со своими входами, чтобы нельзя было понять, чей выход чей.

• **Счётная модель.** Ethereum и Tron ведут остаток по каждому адресу, как банк по каждому счёту. Транзакция списывает с одного счёта и зачисляет на другой; входов для объединения и сдачи нет.

• **Газ (Ethereum), энергия (Tron).** Плата сети за исполнение транзакции в собственной монете сети (ETH, TRX). Адрес, на котором есть только USDT, обычно не может их перевести, пока кто-то не обеспечит эту плату, если только он не пользуется «безгазовым» сервисом, который платит комиссию за него и удерживает её в USDT (3.5).

• **Миксер; мост.** Миксер собирает депозиты многих пользователей в общий пул и выплачивает выводы так, что по реестру не видно, какой депозит оплатил какой вывод. Мост переносит стоимость между двумя блокчейнами: блокирует или сжигает её в одной сети и высвобождает или выпускает в другой либо принимает её в собственный пул в одной сети и выплачивает из своего пула в другой.

• **Время блока.** Время, записанное в блоке, который включил транзакцию. Оно показывает, когда создан блок, а не когда транзакцию подписали или отправили.

В кластере было 2 300 адресов, и заключение специалиста, приобщённое к уголовному делу, относило их все к обвиняемому. Совокупный остаток по кластеру составлял чуть больше 41 биткоина. Потерпевший лишился шести. Следователь ходатайствовал об аресте имущества третьих лиц, а именно биржевых счетов, на которые за два года уходили средства кластера. Районный суд ходатайство удовлетворил.

Защита попросила одно: перечень транзакций, по которым платформа объединила кластер. Их было 1 900. Специалист защиты отсортировала их по числу входов. Почти наверху оказалась транзакция с 94 входами, среди выходов которой несколько десятков были одинакового номинала. Это был CoinJoin: одна транзакция, собранная десятками незнакомых друг другу пользователей ровно для того, чтобы инструмент, читающий её так, как читал этот, решил, что они одно лицо. Платформа так и прочла. Десятки посторонних людей были присоединены к обвиняемому, а через них все, с кем они когда-либо совершали операции.

Суд апелляционной инстанции отменил арест в части счетов третьих лиц. В постановлении не было слова «CoinJoin». В нём было сказано, что следствие не представило сведений, на основании которых указанное имущество отнесено к обвиняемому, а выводы специалиста в этой части не содержат описания применённой методики.

Сцена составлена из ситуаций, которые встречаются в практике, и не описывает конкретное дело.

3.1 Эвристика — допущение с историей

Блокчейн редко показывает, кому принадлежит адрес. Аналитик это выводит. Каждый ончейн-шаг (шаг анализа по данным самого блокчейна), выходящий за пределы чтения одной транзакции, опирается на **эвристику**: практическое правило вида «если виден такой паттерн, вероятнее всего объяснение такое-то».

Три примера. Два входа, потраченные в одной транзакции, вероятно, принадлежат одному владельцу. Выход на свежий адрес того же типа, что и входы, вероятно, сдача. Четыре равных перевода за сорок минут, вероятно, сделало одно лицо.

Ни одно из этих правил не входит в протокол (технические правила, которым обязана следовать программа каждого участника сети). Каждое обобщает то, как обычно ведут себя люди и программы. Каждое верно, пока кто-то не поведёт себя иначе: случайно, намеренно или чтобы правило обойти.

Юристу удобно думать об эвристике как о допущении с историей. Допущение — то, что должно быть истинно, чтобы правило дало верный ответ в данной транзакции. История показывает, как часто на похожих транзакциях это допущение выполняется. Хорошее заключение называет и то, и другое. Слабое не называет ничего и подаёт результат правила как наблюдение.

Три вопроса проверяют любую эвристику в заключении, и это те же вопросы, которые рано или поздно задаст суд. Формально заключение эксперта для суда необязательно: оно оценивается наравне с другими доказательствами, и ни одно доказательство не имеет заранее установленной силы. На практике судья специальными познаниями не обладает и почти всегда опирается на заключение — если эксперт или аналитик достаточно компетентен, чтобы объяснить свой метод и защитить вывод на вопросах сторон. Закон это учитывает: несогласие с заключением суд обязан мотивировать. Поэтому спор об атрибуции в российском и белорусском суде выигрывается не доводом «суд не обязан принимать заключение», а тем, чьё заключение выдержит допрос, рецензию и ходатайство о повторной экспертизе. Американский суд проводит ту же проверку раньше и открыто — оценивает надёжность метода до того, как допустить показания.

1. Применимо ли правило к этой транзакции? У каждой эвристики есть область применения, то есть круг транзакций, для которых она создана. Правило общих входов (3.2) создано для обычных кошельков Bitcoin. К CoinJoin, PayJoin или пакетному выводу средств биржей оно не применимо. Определение сдачи (3.3) предполагает, что кошелёк плательщика ведёт себя определённым образом, и не работает для кошельков, которые ведут себя иначе. Первая линия атаки на любую эвристику — показать, что транзакция лежит вне её области.

2. Какова частота ошибок и кто её измерял? Аналитические компании редко публикуют частоту ошибок своей кластеризации. В американском деле *United States v. Sterlingov* суд признал, что ведущий вендор не собирал и не учитывал централизованно свои ложноположительные и ложноотрицательные результаты. Тем не менее доказательства были допущены, потому что их подтверждали другие источники. Для большинства судов отсутствие частоты ошибок не решает дело, но переносит вес на подтверждение, и аналитик без подтверждения уязвим. Академические исследования измеряли некоторые эвристики на эталонных данных (транзакциях, действительный владелец которых известен), и для одних правил результаты лучше, чем для других. Аналитика, который опирается на эвристику и не может сказать, как часто она ошибается, об этом спросят, и этот пункт он проиграет, какова бы ни была истинная цифра.

3. Применена ли она одна или подтверждена чем-то независимым? Результат эвристики — гипотеза. Больше чем гипотезой он становится, только когда в ту же сторону указывает независимое доказательство: другая эвристика с другим допущением, оффчейн-запись

(сведения вне блокчейна), документ. Что считать независимым, разбирает глава 6. Кластер, построенный одной эвристикой и «подтверждённый» меткой платформы, построенной той же эвристикой, — одно доказательство, а не два.

Ниже разобраны эвристики, которые чаще всего встречаются в заключениях об атрибуции, в том порядке, в каком их обычно применяют: механизм, допущение, способы отказа и то, что должен сделать аналитик, чтобы закрыть пробел.

3.2 Общие входы

Чтобы заплатить, кошелёк Bitcoin берёт один или несколько неизрасходованных выходов как **входы**, примерно как платят несколькими купюрами, и создаёт новые **выходы**: один получателю и, как правило, один с остатком обратно плательщику. Каждый вход подписывается **закрытым ключом** своего адреса (секретным кодом, который даёт контроль над адресом).

Отсюда и правило. Если транзакция тратит несколько входов, все их контролировало одно лицо, потому что одно лицо должно было подписать каждый. Аналитик объединяет адреса входов в один кластер. Правило повторяется на каждой транзакции с несколькими входами, и кластеры растут, часто до тысяч адресов.

Правило — ровесник Bitcoin. Сам whitepaper (исходное описание системы 2008 года) в разделе о приватности признаёт, что транзакции с несколькими входами раскрывают принадлежность входов одному владельцу. Академические работы 2011–2013 годов превратили это признание в метод. Он до сих пор лежит в основе коммерческой кластеризации в сетях с UTXO (Bitcoin и сети, устроенные так же).

Допущение: одна транзакция — один подписант. В 2009 году это было почти правдой. Сейчас оно нарушается достаточно часто, чтобы иметь значение, и в трёх повторяющихся формах.

1. **CoinJoin.** Много не связанных между собой пользователей собирают одну транзакцию; каждый подписывает только свои входы, а выходы делаются одного номинала. Конструкция рассчитана на то, чтобы правило общих входов дало неверный ответ. Применённое к CoinJoin, оно сливает всех участников в один кластер, и ошибка расходится по всем последующим транзакциям этих участников. Открывающая сцена показывает именно эту ошибку.

2. **PayJoin.** Получатель платежа добавляет свой вход рядом со входом отправителя. Для читающего по правилу общих входов отправитель и получатель становятся одним лицом. PayJoin сделан так, чтобы выглядеть обычным платежом. Поэтому его труднее заметить, чем CoinJoin, а ложное слияние труднее обнаружить постфактум.

3. **Пакетные транзакции кастодиальных сервисов.** Биржа или платёжный провайдер тратит депозиты многих клиентов или выплачивает выводы многим клиентам одной транзакцией. Подписант один, это сервис. Но для любых правовых целей входы принадлежат разным клиентам. Правило верно в том, кто подписал, и неверно в том, кто владеет.

Прежде чем объединять адреса по транзакции с несколькими входами, аналитик должен проверить её на признаки совместной сборки: выходы одного номинала, необычно большое число входов и выходов, комиссия известному координатору (серверу, который собирает CoinJoin), известные шаблоны программ CoinJoin. Некоторые реализации взимают комиссию координатора в подготовительной транзакции, а не в самом CoinJoin, а некоторые используют несколько стандартных номиналов вместо одного, поэтому проверка одной лишь смешивающей транзакции может упустить и то, и другое. Если кошелёк и координатор известны, в заключении их нужно назвать. Если кластер слит через транзакцию, которую нельзя исключить как совместную, аналитик должен разделить кластер по этой транзакции и рассматривать части как отдельные гипотезы. В заключении должно быть указано, сколько сливающих транзакций проверено и как. Фраза «платформа кластеризовала эти адреса» методикой не является.

С 2024 года ряд самых известных CoinJoin-сервисов закрылся или стал объектом уголовного преследования (см. примечания). Некоторые аналитики считают это поводом не учитывать риск. Риск от этого не исчезает. Исторические CoinJoin остаются в реестре, независимые реализации продолжают работать, и атрибуция, проходящая через CoinJoin 2021 года, уязвима сегодня так же, как тогда.

Как это делают на практике

Юрист может поручить аналитику следующую проверку одной транзакции: той, которая включила адрес ответчика (обвиняемого) в кластер (**сливающая транзакция**).

1. Получить перечень сливающих транзакций, на которых построен кластер. Некоторые платформы позволяют его посмотреть или выгрузить; у других его приходится запрашивать у вендора (глава 10). Если аналитик не может его представить, кластер проверить нельзя (глава 4).

2. Найти транзакцию, которая первой присоединила адрес ответчика к остальному кластеру, её идентификатор (уникальный номер, аналог номера платёжного поручения) и дату.

3. Попросить аналитика открыть её в публичном блок-эксплорере (бесплатном сайте, который показывает любую транзакцию) и зафиксировать число входов и выходов. Обычный платёж, как правило, имеет от одного до нескольких входов и два выхода. Десятки с каждой стороны — тревожный признак.

4. Попросить зафиксировать суммы выходов. Несколько выходов строго одинаковой суммы — типичный признак CoinJoin.

5. Попросить проверить, не ушла ли комиссия на адрес, известный как адрес координатора CoinJoin, и не совпадает ли транзакция с шаблоном известной реализации CoinJoin.

6. Если любой из пунктов 3–5 указывает на совместную транзакцию, попросить пересчитать кластер без этого слияния и указать, сколько адресов и какой остаток остаются связанными с ответчиком.

Результат в заключении удобно привести короткой таблицей: идентификатор транзакции, дата, число входов, число выходов, выходы одного номинала (да/нет), координатор найден (да/нет), вывод.

Пример формулировки: вопросы эксперту

В гражданском и арбитражном процессе, а в Беларуси также в экономическом суде, сторона предлагает такие вопросы в ходатайстве о назначении экспертизы; окончательный круг вопросов определяет суд. В уголовном деле защита может ходатайствовать перед следователем о внесении в постановление о назначении экспертизы дополнительных вопросов эксперту (ст. 198 УПК РФ). Если заключение уже получено, те же вопросы задают эксперту или специалисту при допросе в судебном заседании.

1. Какая транзакция первой присоединила адрес … к кластеру? Укажите её идентификатор и дату.

2. Сколько у этой транзакции входов и выходов и сколько выходов имеют одинаковую сумму?

3. Проверялась ли эта транзакция на признаки CoinJoin, PayJoin и пакетной транзакции сервиса? Что именно проверялось и с каким результатом?

4. Сколько адресов и какой остаток останутся в кластере, если исключить эту транзакцию?

5. Изучил ли эксперт перечень сливающих транзакций сам или опирался на кластеризацию платформы?

3.3 Сдача и цепочки отщипов (peel chains)

Выход в Bitcoin можно потратить только целиком, как купюру. Плательщик, который должен 0,3 BTC и располагает одним выходом в 1 BTC, тратит его целиком и создаёт два новых: 0,3 BTC получателю и 0,7 BTC на свой же адрес. Второй выход и есть **сдача**. Блокчейн не помечает, какой выход какой.

Если аналитик может определить сдачу, трасса (цепочка прослеживания средств) переходит за плательщиком на его следующий адрес. Для этого используют набор сигналов. Сдача обычно уходит на свежий, ранее не использованный адрес. У неё тот же тип адреса (технический формат, так называемый тип скрипта), что и у входов. При круглой сумме платежа сдача составляет некруглую сумму. Это тот выход, который создал бы кошелёк, минимизируя комиссию. У него тот же программный отпечаток, что у входов.

Допущение: кошелёк плательщика ведёт себя так, как ожидают сигналы. Значит, определение сдачи — прогноз о поведении программы.

Правило ломается в четырёх повторяющихся случаях.

• **Круглые суммы не там.** Биржи и продавцы считают цены в фиатной валюте, поэтому покупка часто оказывается некруглой суммой, а сдача круглой. Правило «круглый выход — платёж» отказывает ровно тогда, когда платёж — покупка.

• **Выходы одного типа.** Если плательщик и получатель используют один кошелёк и один тип адреса, сигнал типа ничего не говорит.

• **Намеренный уход от сдачи.** Некоторые кошельки подбирают входы так, чтобы сдачи не было вовсе, или дробят её на несколько выходов. Кошельки, ориентированные на приватность, перемешивают порядок выходов и суммы.

• **Одна ошибка, перенесённая дальше.** Неверно определённая сдача уводит трассу по пути получателя, и каждый следующий шаг идёт за посторонним. Одно из первых систематических исследований (Meiklejohn et al., 2013) обнаружило, что его собственное неуточнённое правило сдачи слило несколько крупных сервисов в один кластер более чем из миллиона адресов; его пришлось исправлять вручную. Исследование 2022 года, проверившее распространённые правила сдачи на эталонных данных, показало, что несколько из них по отдельности ошибались примерно в половине случаев или чаще. Тщательно ограниченные правила и их комбинации работали гораздо лучше (цифры приведены в примечаниях).

Определением сдачи пользоваться можно, но его правильность не очевидна. Заключение, которое подаёт определение сдачи как наблюдение, его переоценивает.

Peel chain (цепочка отщипов) — последовательность транзакций, в которой крупный остаток переходит через ряд свежих адресов, а на каждом шаге от него «отщипывается» небольшой платёж. Это похоже на пачку купюр, от которой на каждой остановке отдают одну, а остальное несут дальше. Это классический паттерн отмывания, и аналитики считают распознанную peel chain сильным доводом в пользу того, что крупный выход на каждом шаге остаётся у того же лица.

Сложность в том, что так же выглядит обычная биржа. **Горячий кошелёк** биржи (общий кошелёк, из которого она платит клиентам), выплачивающий выводы по одному, даёт ровно ту же форму. Принадлежит ли цепочка отмывателю или сервису, обычно решается тем, откуда она началась и куда ушли «отщипы». Если они ушли сотням не связанных между собой клиентов бирж, цепочка может оказаться просто биржей.

Аналитик должен называть сигналы для каждого решения о сдаче, а не только вывод. Если два сигнала расходятся, в заключении нужно это указать и объяснить, какой предпочтён и почему. Для каждого шага, где трасса зависит от решения о сдаче, аналитик должен проверить альтернативу: если решение неверно, приходит ли трасса в то же место другим путём? Если

нет, шаг становится кандидатом на анализ чувствительности (глава 14) и должен быть отмечен не выше уровня 3 (*вероятно*), пока его не подтвердит что-то независимое.

Пример формулировки: вопросы эксперту

1. Какой выход транзакции на шаге … принят за сдачу и по каким сигналам?
2. Указывал ли какой-либо сигнал на другой выход?
3. Куда ведёт трасса, если сдачей считать другой выход?

Аналитик, который уже прогнал альтернативу и может сказать, что она не ведёт ни к чему значимому, на вопрос ответил. Аналитику, который этого не сделал, придётся делать это при допросе в заседании.

3.4 Кастодиальные и омнибус-адреса

Каждая цепочка атрибуции, которая заканчивается на лице, рано или поздно доходит до сервиса: биржи, платёжного провайдера, кастодиального кошелька, OTC-деска (брокера, совершающего крупные сделки вне биржевого стакана, то есть списка заявок на покупку и продажу). В этой точке эвристики из 3.2 и 3.3 перестают работать. Причина в том, как сервисы хранят деньги, а не в технологии.

Кастодиальный сервис хранит активы клиентов на адресах, которые контролирует сам. Это похоже на банк: деньги клиентов не лежат в отдельных ячейках, а у клиента есть только запись на его счёте. Каждому клиенту выдаётся **депозитный адрес**. Поступившие депозиты затем сметаются (автоматически переводятся) в кошельки-сборщики, объединяются в горячих кошельках для выплат, уходят в холодное хранение (офлайн-кошельки) и снова выплачиваются из горячих. Ничто в этом процессе не связывает монеты одного клиента с последующим выводом того же клиента. **Омнибус-адрес** — адрес, на котором вместе хранятся средства многих клиентов.

Поэтому по записям сервиса депозитный адрес закреплён за одним клиентом, а всё после сметания принадлежит сервису. Для атрибуции из этого следуют три вещи.

Во-первых, на депозитном адресе трасса меняет природу. До него трасса — цепочка выводов о том, кто что контролировал. После него она лишь описывает внутреннее казначейство сервиса. Проследить средства из горячего кошелька до «следующего адреса» ничего не говорит о клиенте: сервис оплатил бы этот вывод из того же пула, кто бы из клиентов ни внёс депозит. Открывающая сцена главы 1 — трасса, которая не остановилась на депозитном адресе.

Во-вторых, атрибуция уходит в оффчейн. На вопрос, чей счёт получил средства, отвечают только записи сервиса, полученные через истребование доказательств или запрос следователя. На вопрос, куда клиент отправил их дальше, отвечают те же записи: внутренние проводки, заявки на вывод, привязанные банковские счета.

В-третьих, юридическое прослеживание и аналитическое расходятся. Можно ли проследить имущественное право в смешанный фонд биржи, решает право. В деле *D'Aloia* английский суд признал прослеживание через смешанный фонд возможным по праву справедливости (equity) (п. 7), но истец проиграл, потому что не доказал, что его стоимость вообще попала в этот фонд (глава 1, 1.1). Суд также признал, что истец не ограничен методами FIFO, pari passu и rolling charge: допустимы и другие методы, «если они методологически обоснованы и надлежаще доказаны» (п. 7(iii)). Эксперт истца этому требованию не отвечал: его описание применённого метода менялось между заключением, совместным заявлением экспертов и перепиской незадолго до процесса (пп. 58–60). В российском и белорусском процессе вопрос ставится иначе, через предмет доказывания по иску о неосновательном обогащении или о возмещении вреда, но доказательственная проблема та же.

Для каждого сервиса, которого касается трасса, аналитик должен определить, какие адреса депозитные, а какие внутренние. Ончейн-трасса должна остановиться на депозитном адресе, и в заключении это нужно указать. Затем следует перечислить, какие записи нужны от сервиса, чтобы продолжить, и от кого. Заключение, показывающее ровную линию через биржу и дальше, следует считать ошибочным, пока оно не объяснит, как это сделано.

Пример формулировки: запрос бирже

«Просим сообщить, является ли адрес … депозитным адресом, выданным [биржей], и если да, указать аккаунт, за которым он был закреплён на [дата]. По каждому депозиту из прилагаемого перечня (идентификатор транзакции, сумма, время в UTC) просим представить соответствующую запись о зачислении на этот аккаунт, а также сведения обо всех выводах с этого аккаунта за период с [дата] по [дата] с указанием адресов назначения или банковских реквизитов и времени в UTC».

Тот же перечень сведений можно включить в запрос следователя (глава 10) и в ходатайство об истребовании доказательств. В ходатайство к нему добавляют то, чего требует процессуальный закон: какие обстоятельства эти сведения подтвердят, почему сторона не может получить их сама и где они находятся (ч. 2 ст. 57 ГПК РФ, ч. 4 ст. 66 АПК РФ; образец — в 4.7). Письмо стороны биржу ни к чему не обязывает. Адвокатский запрос (ст. 6.1 Федерального закона от 31.05.2002 № 63-ФЗ) обязывает отвечать российские организации, но не иностранную биржу.

Пример формулировки: вопросы эксперту

1. Является ли адрес … депозитным адресом или кошельком сервиса? На каком основании сделан вывод: метка платформы, паттерн сметания, записи самого сервиса?

2. На каком основании после сметания утверждается, что данный вывод сделал данный клиент, а не что он оплачен из общего пула?

3.5 Сети со счётной моделью: Ethereum, Tron, стейблкоины

Большая часть похищенной и скрываемой стоимости в нынешних спорах — не биткоин. Это USDT в сетях Tron и Ethereum и USDC — главным образом в Ethereum (в Tron компания Circle прекратила выпуск USDC в феврале 2024 г.), то есть **стейблкоины**: токены, которые выпускает компания и курс которых привязан к доллару США. Эвристики из 3.2 и 3.3 на эти сети не переносятся.

Ethereum и Tron используют **счётную модель**, поэтому в транзакции нет нескольких входов для слияния и нет выхода-сдачи. Аналитику, применяющему правило общих входов к сети со счётной моделью, просто не к чему его применять. Звучит очевидно, но это повторяющаяся ошибка заключений, написанных по шаблонам для Bitcoin.

Кластеризация в счётной модели опирается на другой, более узкий набор сигналов, у каждого своё допущение. **Разрешение на токены** (approve), упомянутое в таблице, — разрешение, которое счёт даёт смарт-контракту (программе, работающей в блокчейне) или другому адресу тратить свои токены.

Сигнал	Правило	Допущение	Как ломается
Повторное использование депозитного адреса	Счета, отправляющие на один депозитный адрес биржи, принадлежат одному клиенту	Каждый депозитный адрес выдан одному клиенту	Общие или перепроданные биржевые аккаунты; биржи, переназначающие адреса; третьи лица, платящие на депозитный адрес клиента (клиенты платёжного сервиса или OTC-дилера, потерпевшие, переводящие средства на счёт мошенника)
Оплата газа	Счёт, получивший первые средства на комиссии со счёта X, контролирует владелец X	Никто не оплачивает комиссии чужому	Ретранслирующие, paymaster- и «безгазовые» сервисы (в Tron — провайдеры Gas-Free и рынки аренды энергии), пополнение газа мостами, краны, выводы с бирж, дрейнер-киты, оплачивающие сметание с кошельков жертв
Разрешения на токены (approve)	Счёт, разрешивший другому тратить свои токены, ему доверяет	Разрешение отражает общий контроль	Разрешения DEX-роутерам, мостам и фишинговым контрактам; при краже это самый частый случай
Поведенческий тайминг	Счета, активные в одни и те же секунды по одному паттерну, имеют одного контролёра	Такой паттерн создаёт только одно лицо	Боты, дрейнер-как-сервис, общие скрипты
Аирдропы и мультиучастие	Счета, получившие один аирдроп и сводящие его на один адрес, принадлежат одному лицу	Сведение означает владение	Сибил-фермы на заказ; сведение на сервис

В таблице ретранслирующими (relay) и paymaster-сервисами названы сервисы, которые оплачивают комиссии сети за пользователей. Кран (faucet) бесплатно раздаёт небольшие суммы монет. Дрейнер-кит означает вредоносную программу, которую продают мошенникам для опустошения кошельков жертв. DEX-роутером называют контракт децентрализованной биржи, исполняющий обмены (3.6). Аирдроп означает бесплатную раздачу токенов многим адресам, а сибил-ферма означает набор адресов под управлением одного оператора, созданный, чтобы получить раздачу много раз.

Чтобы перевести USDT в Tron, счёту нужны энергия и пропускная способность. Их получают стейкингом TRX (монеты блокируются в обмен на ресурсы, а вывести их можно только после периода ожидания), сжиганием TRX (монеты расходуются на оплату ресурсов) либо через делегирование ресурсов от другого счёта. Поэтому свежесозданный адрес с похищенными USDT должен быть активирован и получить TRX или энергию, прежде чем сможет что-либо перевести. Перевод USDT адрес Tron не активирует; его активирует первый поступивший TRX или вызов создания счёта. Обозреватели показывают адрес, который активировал счёт («activated by»), и его нужно фиксировать для каждого адреса в цепочке. Тот, кто их дал, — естественная зацепка, но не естественный вывод: рынки аренды энергии, выводы с бирж и дрейнер-сервисы снабжают чужих. В деле ООО «Халден Логистик» (далее — дело «Халдена») правило об общем источнике средств на комиссию лежит в основе шага 6 в сети Ethereum (адреса E1 и E2) и шага 4 в Tron (T1–T5); шаг 4 опирается также на поведенческий тайминг и равные доли переводов. Эксперт Б оценила шаг 6 как возможный (уровень 4), а шаг 4 как вероятный (уровень 3), потому что нельзя исключить соответственно ретранслирующий сервис и дрейнер-сервис (глава 2, 2.5).

На 2026 год ряд кошельков позволяет платить комиссию сети токенами, которые лежат на том же адресе. В Ethereum и других сетях, работающих на его программном обеспечении, Trust Wallet (FlexGas), MetaMask (транзакции «gas included») и аппаратный кошелёк Tangem (Smart Gas) используют EIP-7702. Это изменение протокола Ethereum, действующее с мая 2025 года: оно позволяет обычному адресу действовать в транзакции как счёт со смарт-контрактом. Пользователь подписывает перевод, ретранслятор поставщика (служебный адрес, который отправляет транзакции за других) отправляет транзакцию и платит ETH, а комиссия удерживается с пользователя в USDT или другом токене. Paymaster-сервисы работают похоже. В Tron то же делает сервис GasFree: пользователь подписывает разрешение, провайдер отправляет перевод с отдельного адреса GasFree, связанного с адресом пользователя, и оплачивает энергию, а комиссия удерживается в USDT. GasFree поддерживают, в частности, TronLink, Guarda и Klever; похожие услуги предлагают и другие кошельки. Набор функций и сетей меняется, поэтому аналитик должен сверяться с текущей документацией кошелька.

Для атрибуции из этого следует четыре вещи. Во-первых, пользователю не нужен другой кошелёк, чтобы получить средства на комиссию, поэтому обычной связи через источник комиссии нет. Во-вторых, общий ретранслятор или плательщик комиссии ничего не связывает: им пользуются тысячи не связанных лиц. В-третьих, сам след служит признаком: делегирование по EIP-7702 на известный контракт кошелька или адрес GasFree показывает, каким кошельком или сервисом пользовались, но почти никогда — кто именно. Некастодиальный кошелёк не хранит данных о личности клиента, а по опубликованным политикам (в редакциях 2025–2026 годов; проверьте действующую) IP-адреса хранятся недолго или не хранятся вовсе (Trust Wallet: не сохраняются; Tangem: IP-адреса и адреса кошельков не собираются; RPC-провайдер MetaMask: IP-адрес и адрес кошелька, срок хранения в 2022 году объявлен около 7 дней). Запрос о сохранении данных, направленный сразу, почти ничего не стоит, но рассчитывать на него не стоит. Полезные сведения обычно находятся в другом месте: у биржи или у сервиса покупки криптовалюты за деньги внутри кошелька (при покупке картой через встроенного провайдера тот проверяет личность покупателя). В-четвёртых, при GasFree средства в блокчейне движутся с адреса GasFree, а не с собственного адреса пользователя; аналитик должен связать их, и это возможно, потому что адрес GasFree вычисляется из адреса пользователя.

Адрес Tron и адрес Ethereum могут иметь один закрытый ключ. Шестнадцатеричный адрес Tron — это адрес Ethereum с добавленным префиксом 41, поэтому для каждого адреса Tron в цепочке аналитик может вычислить соответствующий адрес Ethereum и проверить, использовался ли он. Большинство кошельков получает два адреса из разных ключей, так что неиспользованный двойник ничего не доказывает; активный двойник, связанный с делом, — сильное доказательство общего контроля.

У стейблкоинов к тому же есть эмитент. Эмитенты USDT и USDC могут заморозить токены на уровне контракта, то есть заблокировать токены на определённом адресе так, чтобы их нельзя было перевести. Заморозка — средство защиты, а не доказательство. Однако сама заморозка записана в блокчейне: контракт вносит адрес в чёрный список и фиксирует событие, а последующее уничтожение замороженного остатка фиксируется так же. Записи эмитента о том, кто и на каком основании запросил заморозку, — оффчейн-факты. И то и другое может подтвердить или опровергнуть атрибуцию. Заключение, не учитывающее, действовал ли эмитент, упускает источник.

Для каждого шага кластеризации в сети со счётной моделью в заключении нужно назвать сигнал, его допущение и объяснить, почему известные способы отказа здесь не действуют. Для оплаты газа или энергии нужно установить плательщика и сказать, сервис ли это.

Как это делают на практике

Проверка плательщика газа или энергии состоит из трёх шагов.

1. Найти адрес, который активировал данный адрес (Tron) или прислал ему первые ETH (Ethereum), и любой адрес, делегировавший ему энергию, с транзакцией каждого.

2. Проверить, отмечен ли отправитель как биржа, сервис аренды энергии, «безгазовый» сервис, мост или ретранслирующий сервис, и не пришёл ли его перевод в той же транзакции, что выплата какого-либо сервиса, или через несколько секунд после неё. Подсчитать, сколько других новых адресов он снабдил за тот же период. Если адрес сам комиссию не платил, проверить, нет ли делегирования по EIP-7702, известного ретранслятора или paymaster или адреса GasFree.

3. Если он снабдил сотни или тысячи не связанных между собой адресов, шаг ничего не говорит об общем контроле. Его следует исключить или отметить не выше уровня 4 (*возможно*), если его не подтверждает что-то независимое.

3.6 Миксеры, мосты, DEX и приватные монеты

В этих точках трасса рвётся по замыслу. Каждая теряет информацию по-своему. Каждую иногда можно перекрыть выводом, но любой такой переход — эвристический шаг с той же уязвимостью.

В **миксер** пользователи вносят фиксированные суммы, а позже выводят средства на новые адреса. Аналитики восстанавливают связь по времени (вывод вскоре после депозита), по сумме (тот же номинал за вычетом комиссии) и по поведенческим отпечаткам (цена газа, кошелёк, адрес вывода, использованный где-то ещё). Всё это вероятностно. Сила вывода зависит от того, сколько других пользователей было в пуле в то время; это число называют **множеством анонимности**. Совпадение в пуле из пяти — сильный вывод; то же совпадение в пуле из пяти тысяч — едва зацепка. Заключение, связывающее стороны миксера, должно называть размер множества анонимности на соответствующий момент.

Мост либо блокирует или сжигает токены в одной сети и высвобождает или выпускает ту же стоимость в другой, либо, будучи межсетевым обменным сервисом (сервисом ликвидности, мостом в широком смысле), выплачивает тот же токен за вычетом комиссии из собственного пула в другой сети. Перевод, который начинается как USDT в сети Tron и заканчивается обычными USDT в сети Ethereum, проходит через сервис второго вида, потому что выпускать USDT в обеих сетях может только Tether. Мосты-протоколы оставляют твёрдую техническую связь между сторонами: сообщение, идентификатор транзакции или запись события (event log, то есть запись, которую контракт моста делает в блокчейне). Кастодиальные обменные сервисы, которые принимают депозит на адрес, выданный под одну заявку, и выплачивают со своего кошелька, обычно такой связи в блокчейне не оставляют: связью служит запись сервиса о заявке, а это оффчейн-доказательство, которое нужно получить у сервиса. Проход через мост по такой связи — наблюдение. Если же аналитик сопоставил стороны по сумме и времени, шаг — вывод и должен быть отмечен как вывод. Шаг 5 дела «Халдена» («Т3 перевёл через мост 350 000 USDT на E1») *установлен* (уровень 1), потому что опирается на идентификатор перевода сервиса, записанный в обеих сетях, а не на совпадение сумм; суммы в любом случае не совпадают, так как на E1 поступило 348 000 USDT за вычетом комиссии сервиса (глава 2, 2.4).

Децентрализованная биржа (DEX) — смарт-контракт, который обменивает один токен на другой без посредника, хранящего средства клиентов. Обмен полностью виден в реестре: токены вошли, токены вышли, тот же счёт. Проследить стоимость через обмен обычно просто. Сложнее в двух случаях. Обмен может идти через агрегатор или роутер, дробящий его

по нескольким пулам; тогда нужно внимательно прочитать вызовы контракта. Либо результат уходит на другой счёт, и это уже новый шаг атрибуции.

Приватные монеты, например Monero, и **экранированные пулы** (части сети, где суммы и стороны зашифрованы) скрывают связь между отправителем и получателем. Когда стоимость уходит в них, ончейн-прослеживание, как правило, останавливается. Некоторые выводы сохраняются, например суммы и время входа и выхода на прозрачной стороне. Но они того же слабого, временного типа, что описан выше. Заключение, утверждающее, что проследило стоимость через приватный протокол, нужно попросить пошагово показать, какая информация уцелела и по какому правилу её соединили.

Использование миксера, приватной монеты или цепочки мостов само по себе факт, и «Поиск скрытых криптоактивов» рассматривает его как факт. В споре о сокрытии он может поддержать вывод об умысле. Вывод о личности он поддержать не может. «Средства прошли через миксер, а ответчик — из тех, кто пользуется миксерами» — не шаг цепочки атрибуции.

Пример формулировки: вопросы эксперту

1. На чём основан переход через мост на шаге …: на собственном сообщении или записи события моста либо на совпадении сумм и времени? Укажите идентификаторы транзакций в обеих сетях.

2. Сколько депозитов того же номинала поступило в пул миксера между депозитом и выводом, сопоставленными на шаге …?

3. Был ли другой вывод, столь же хорошо совпадающий по сумме и времени?

3.7 Время и временные метки

Когда другие доказательства заканчиваются, атрибуция опирается на время: два события, близкие по времени, считаются связанными. Именно эту эвристику чаще всего применяют небрежно, потому что временная метка выглядит как факт.

Время блока не совпадает со временем события. Транзакции записываются в **блоки**, то есть пакеты, которые сеть добавляет в цепочку через промежутки времени: в среднем около десяти минут в Bitcoin, около двенадцати секунд в Ethereum и три секунды в Tron. Время, показанное для транзакции, записано в её блок производителем блока в пределах допуска протокола. В Bitcoin допуск широк: время блока должно быть лишь позже медианы времени одиннадцати предыдущих блоков и не более чем на два часа опережать сетевое время, поэтому оно может расходиться с действительным на час и больше, а более поздний блок может показывать более раннее время. В Ethereum и Tron время блока привязано к фиксированным слотам и гораздо точнее; транзакция в Tron, кроме того, должна попасть в блок до истечения срока действия (по умолчанию 60 секунд, не более 24 часов), иначе она отпадает. В Bitcoin между подписанием и включением в блок могут пройти минуты или часы, а подписать транзакцию можно за несколько дней до отправки. В быстрых сетях разрыв короче, но не нулевой. Заключение, где сказано «обвиняемый перевёл средства в 03:41», на самом деле говорит «блок с транзакцией был создан около 03:41», а это другое и более слабое утверждение.

Записи ведут время в разных поясах и форматах. Блок-эксплореры показывают UTC или местное время смотрящего, в зависимости от настроек. Записи биржи могут быть в местном времени биржи, в UTC или в поясе, выбранном в аккаунте пользователя. Банковские выписки обычно содержат местную дату банка без времени. У логов устройств, выгрузок мессенджеров и серверных логов свои соглашения. Каждая атрибуция, сопоставляющая ончейн-событие с оффчейн-событием (входом в аккаунт, выводом, сообщением), сравнивает разные часы, и

пересчёт нужно указать, а не предположить. В российских делах отдельный источник ошибок — протоколы осмотра, в которых время с экрана переписано без указания часового пояса.

Близость во времени нужно оценивать относительно **базовой частоты**, то есть того, как часто такие события происходят и без всякой связи между ними. Депозит на биржу через одиннадцать минут после кражи наводит на мысль, если биржа получила в тот час мало депозитов такого размера. Если таких депозитов были тысячи, он почти ничего не значит. То же относится ко входу в аккаунт за двадцать минут до вывода, если пользователь заходит в аккаунт каждый час. Поэтому временному выводу нужна оценка того, как часто столь же близкое совпадение случается случайно (подробно о базовых частотах — глава 6).

Аналитик должен указать источник и часовой пояс каждой временной метки, привести все метки к одной шкале (UTC) в таблице и отделить время блока от времени оффчейн-событий. Для каждого временного вывода нужно назвать окно и, где возможно, базовую частоту сопоставимых событий в этом окне.

Пример формулировки: приложение с временными метками

Ниже показано, в каком виде временные метки следует приводить в заключении. Данные условные и к делу «Халдена» не относятся.

№	Событие	Источник	Время в источнике	Часовой пояс источника	UTC	Время блока или время события
1	Вход в аккаунт клиента на бирже M	Ответ биржи M на запрос, лист «Logins»	2026-03-14T03:30:17Z	UTC (суффикс «Z» в записи)	14.03.2026 03:30:17	Время события (серверный лог биржи)
2	Исходящий перевод USDT с адреса потерпевшего (tx 7f3…a1)	Tronscan, страница транзакции, сохранена 20.03.2026	14 Mar 2026 03:41:09	UTC (настройка эксплорера видна на скриншоте)	14.03.2026 03:41:09	Время блока
3	Сообщение «готово» в мессенджере	Выгрузка с телефона обвиняемого (образ устройства)	14.03.2026 06:43	Местное время устройства, UTC+3 (настройки устройства зафиксированы в протоколе осмотра)	14.03.2026 03:43	Время события (часы устройства)
4	Зачисление депозита на аккаунт № … на бирже M	Ответ биржи M, лист «Deposits»	14.03.2026 11:52:40	UTC+8 (указано в сопроводительном письме биржи)	14.03.2026 03:52:40	Время события (учёт биржи)
5	Зачисление на банковский счёт обвиняемого	Банковская выписка	14.03.2026	Местная дата банка, UTC+3; время не указано	13.03.2026 21:00 – 14.03.2026 20:59	Только дата события

Под таблицей в заключении следует указать, как установлен часовой пояс каждого источника, и ссылаться на таблицу из каждого временного вывода. Абзац заключения может выглядеть так:

«Всё время в заключении указано в UTC. Время ончейн-транзакций — время блока по данным Tronscan; оно показывает, когда создан блок с транзакцией, а не когда транзакция подписана. Записи биржи M о депозитах, согласно её сопроводительному письму от [дата],

ведутся по UTC+8 и пересчитаны. Банковская выписка содержит только даты. Источники и пересчёт приведены в приложении 3».

Пример формулировки: вопросы эксперту

1. Это время в UTC или местное, и как это установлено?
2. Это время блока или время создания транзакции?
3. Сколько ещё депозитов такого размера поступило на эту биржу в тот же час?

3.8 Сводная таблица: эвристика, допущение, атака, как закрыть

Эвристика	Допущение	Типовая атака	Как аналитик закрывает
Общие входы (UTXO)	Одна транзакция — один подписант	Сливающая транзакция — CoinJoin, PayJoin или пакетная транзакция сервиса	Перечислить сливающие транзакции; проверить каждую; делить кластер на сомнительных слияниях
Определение сдачи (UTXO)	Кошелёк ведёт себя так, как ожидают сигналы	Сигнал круглой суммы или типа адреса указывает не туда; трасса идёт за посторонним	Называть сигналы для каждого решения; прогнать альтернативу; решения по одному сигналу — не выше уровня 3 (*вероятно*)
Peel chain	Крупный выход остаётся у одного лица	Цепочка — сервис, выплачивающий выводы	Установить начало цепочки и получателей «отщипов»; исключить поведение сервиса
Повторный депозитный адрес (счётная модель)	Один клиент на депозитный адрес	Общие, перепроданные или переназначенные аккаунты	Получить записи биржи по адресу; не опираться на один паттерн
Оплата газа или энергии (счётная модель)	Никто не платит комиссии за чужого	Плательщик — ретранслирующий сервис, «безгазовый» сервис, рынок аренды, биржа, дрейнер	Установить плательщика; сказать, сервис ли это; не использовать в одиночку
Поведенческий тайминг	Паттерн создаёт только одно лицо	Боты и дрейнер-сервисы создают тот же паттерн для многих клиентов	Назвать базовую частоту; искать независимый сигнал
Прослеживание внутри сервиса	Движения после сметания отражают клиента	Сервис платит из пула; ничто после сметания не связано с клиентом	Остановиться на депозитном адресе; продолжать только по записям сервиса
Сопоставление сторон миксера	Время и сумма связывают стороны	Множество анонимности велико; много равноценных совпадений	Назвать размер множества; без независимого подтверждения — не выше уровня 4 (*возможно*)
Сопоставление моста по сумме и времени	Совпадающие суммы — те же средства	Сообщение моста говорит другое, или совпадает несколько переводов	Опираться на сообщение или запись события моста; совпадение сумм — лишь вывод
Временная связка ончейн и оффчейн	Часы совпадают, близость означает связь	Ошибка пояса; время блока принято за время события; высокая базовая частота	Всё в UTC в приложении; указать источник и базовую частоту

Таблица — не чек-лист для дискредитации аналитиков. Каждая эвристика в ней полезна, и большинству атрибуций нужны несколько. Таблица перечисляет допущения, которые анали-

тик делает, используя эти эвристики. Аналитик, записавший допущения до заседания, получит вопросы о них на своих условиях, а не на условиях другой стороны.

Типичные ошибки

1. Применение эвристик Bitcoin (общие входы, сдача) к переводам USDT в Tron или Ethereum, где нет ни входов для слияния, ни сдачи.

2. Ходатайство об аресте всего остатка кластера вместо суммы, которую поддерживает трасса.

Остальные типичные ошибки соответствуют столбцу «Типовая атака» таблицы в 3.8.

* * *

Для истца. Запросите у аналитика перечень сливающих транзакций за каждым кластером, на который опирается дело, и решения о сдаче за каждой трассой, которая от них зависит. Если такого перечня нет, кластер или трасса — продукт платформы, а не мнение аналитика, и глава 4 объясняет, чего это стоит. Не просите арестовать остаток кластера, который не разложен на сливающие транзакции. Просите ту сумму, которую поддерживает трасса.

Для ответчика. Самая дешёвая и действенная атака на большой кластер — обычно одна транзакция: та, что присоединила к нему вашего доверителя. Запросите её через ходатайство об истребовании, а в уголовном деле через ходатайство следователю о предоставлении исходных данных заключения, и проведите проверку из 3.2. Если в ней много входов и выходы одного номинала или газ либо энергию на первый адрес доверителя оплатил сервис, у вас есть первое возражение. В Tron и Ethereum проверьте, не применялись ли эвристики Bitcoin вообще. Если применялись, остальное в заключении, возможно, атаковать не придётся.

Для эксперта. Для каждого эвристического шага записывайте допущение в разметке из главы 2 и прогоняйте очевидную альтернативу до подписания. Если использован кластер платформы, либо разложите его на сливающие транзакции, либо прямо скажите, что не раскладывали. Переведите все временные метки в UTC в приложении к заключению по форме из 3.7 и укажите источник каждой.

* * *

Что проверить

• ☐ Для каждого кластера: сколько сливающих транзакций и проверена ли каждая на CoinJoin, PayJoin и пакетную транзакцию сервиса?

• ☐ Для транзакции, которая присоединила ответчика (обвиняемого) к кластеру: число входов и выходов, выходы одного номинала, известный координатор?

• ☐ Для каждого решения о сдаче: какие сигналы и куда ведёт трасса, если решение неверно?

• ☐ Применялась ли UTXO-эвристика к Ethereum, Tron или другой сети со счётной моделью?

• ☐ Для каждого плательщика газа или энергии, на который опирается вывод: это сервис и скольким ещё адресам он платил?

• ☐ Останавливается ли трасса на первом депозитном адресе биржи или идёт дальше по внутренним кошелькам сервиса?

• ☐ Для каждого прохода через миксер или мост: твёрдая техническая связь (сообщение, идентификатор перевода, запись события) или совпадение суммы и времени? Каков был размер множества анонимности?

• ☐ Каждая временная метка — с источником, в UTC в приложении и с пометкой «время блока» или «время события»?

* * *

Примечания к главе 3

• Правило общих входов в исходном замысле: Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), разд. 10 «Privacy».

• Ранняя кластеризация: Reid F., Harrigan M., «An Analysis of Anonymity in the Bitcoin System», IEEE PASSAT/SocialCom 2011, с. 1318–1326 (расширенная версия — Springer, 2013). Meiklejohn S. et al., «A Fistful of Bitcoins», ACM IMC ’13 (Барселона, октябрь 2013 г.), doi:10.1145/2504730.2504747: неуточнённая эвристика сдачи дала около 13% ложных срабатываний и один кластер из 1,6 млн адресов, объединивший несколько крупных сервисов; после уточнений оценка снизилась примерно до 0,17% (по последующему переиспользованию адресов, а не по эталонным данным).

• Проверка на эталонных данных: Kappos G. et al., «How to Peel a Million: Validating and Expanding Bitcoin Clusters», USENIX Security 2022 — доля ложных обнаружений у ранее распространённых эвристик сдачи: 64,19% (Androulaki), 51,64% (Meiklejohn), 48,7% (Goldfeder), 12,7% (Ermilov); у ограниченной эвристики peel chain авторов — 0,62% (0,02% в строгом варианте). Möser M., Narayanan A., «Resurrecting Address Clustering in Bitcoin», Financial Cryptography 2022 — отдельные эвристики находят 10–30% выходов-сдачи; комбинированная модель — 82% при ~0,06% ложных срабатываний; наивное слияние даёт суперкластер из 223,9 млн адресов.

• CoinJoin: Maxwell G., тема 279249 на bitcointalk.org, 22 августа 2013 г. PayJoin: Dorier N., BIP 78 (2019) — прямо указывает, что payjoin ломает эвристику общих входов.

• CoinJoin-сервисы после 2024 г.: координатор Wasabi (zkSNACKs) остановлен 1 июня 2024 г.; основатели Samourai Wallet (*United States v. Rodriguez and Hill*, No. 1:24-cr-82 (S.D.N.Y.)) признали вину 30 июля 2025 г. в сговоре с целью ведения бизнеса по переводу денег, заведомо переводившего преступные доходы, и в ноябре 2025 г. приговорены к пяти и четырём годам (пресс-релизы прокуратуры Южного округа Нью-Йорка). Tornado Cash: *Van Loon v. Department of the Treasury*, 122 F.4th 549 (5th Cir. 2024); исключение из санкционного списка OFAC 21 марта 2025 г.; *United States v. Storm*, No. 1:23-cr-430 (KPF) (S.D.N.Y.) — вердикт 6 августа 2025 г. (виновен по сговору о переводе денег, по отмыванию и санкциям присяжные не пришли к решению); по состоянию на дату, указанную на странице с выходными данными, ходатайство об оправдании не разрешено, повторный процесс по двум пунктам назначен на апрель 2027 г.; по этим пунктам вина не установлена.

• Сети со счётной моделью: Victor F., «Address Clustering Heuristics for Ethereum», Financial Cryptography 2020. Ресурсы Tron: TRON Developer Hub, «Bandwidth and Energy» — перевод TRC-20 расходует Energy, бесплатной квоты у которой нет.

• *United States v. Sterlingov*, No. 1:21-cr-399 (RDM) (D.D.C.), определение от 29 февраля 2024 г. (судья Мосс), ECF 259, 719 F. Supp. 3d 65: ходатайство защиты об исключении доказательств Chainalysis Reactor отклонено; суд признал, что Chainalysis не вела централизованного учёта ложных срабатываний, но счёл инструмент надёжным с учётом подтверждающих доказательств. Вердикт 12 марта 2024 г.; приговор 8 ноября 2024 г. — 150 месяцев. Подтверждено апелляцией, No. 24-3161 (D.C. Cir. 25.09.2026) (судья Уилкинс, состав: Миллетт, Пиллард, Уилкинс): допуск показаний о Reactor признан правомерным, хотя частота ошибок неизвестна, поскольку факторы Daubert не являются исчерпывающими. Главы 4 и 10.

• *D’Aloia v Persons Unknown Category A* [2024] EWHC 2342 (Ch) (судья Richard Farnhill), 12 сентября 2024 г.: прослеживание через смешанный фонд возможно по праву справедливости, но не по общему праву; по общему праву USDT можно проследить, пока его можно идентифицировать; кроме FIFO, pari passu и rolling charge допустимы другие методы, если они методологически обоснованы и надлежаще доказаны (п. 7); описание метода экспертом менялось (пп. 58–60); истец не доказал, что хотя бы часть его средств поступила на депозитный кошелёк («82e6 wallet») (п. 6). Подробнее — примечания к главе 1.

• В российской и белорусской опубликованной практике не найдено решений, в которых суд оценивал бы надёжность конкретных эвристик кластеризации; поэтому глава опирается на зарубежные дела и академические исследования. Заключение эксперта необязательно для суда и оценивается по общим правилам; несогласие с ним суд мотивирует в решении: ч. 3 ст. 86 ГПК РФ; ч. 5 и 7 ст. 71 АПК РФ (никакие доказательства не имеют для арбитражного суда заранее установленной силы; мотивы принятия или отказа в принятии доказательств отражаются в судебном акте); ч. 5 ст. 228 и ч. 3 ст. 237 КГС РБ. Подробно — глава 9.

• Приложение с временными метками (3.7) и запрос бирже (3.4) — условные примеры; идентификаторы транзакций, время и биржа вымышлены. Порядок постановки вопросов эксперту описан в 3.2 в общем виде, нормы о постановке вопросов эксперту: ч. 2 ст. 79 ГПК РФ; ч. 2 ст. 82 АПК РФ; ст. 198 УПК РФ; п. 3 ст. 221 и ч. 3 ст. 222 КГС РБ. Истребование доказательств: ч. 2 ст. 57 ГПК РФ, ч. 4 ст. 66 АПК РФ; адвокатский запрос: ст. 6.1 Федерального закона от 31.05.2002 № 63-ФЗ. Политики кошельков в 3.5 (в редакциях 2025–2026 годов; проверьте действующую): уведомление о конфиденциальности Trust Wallet, trustwallet.com/en/privacy-notice (IP-адрес используется кратковременно и не сохраняется; сведения властям раскрываются лишь в той мере, в какой этого требует закон); блог Tangem от 05.11.2025 со ссылкой на его справочный центр (IP-адреса, балансы и транзакции пользователей не собираются); заявление Consensys о сборе данных через Infura (ноябрь 2022 года) и The Block от 06.12.2022 (срок хранения сокращается до 7 дней).

• *Сверено по первоисточникам или дословным копиям там, где исходные сайты были недоступны.*

Глава 4. Метки аналитических платформ: чёрный ящик в зале суда

Термины главы

• **Вендор**: компания, которая продаёт аналитическую платформу для блокчейна (Chainalysis, Crystal, TRM, Elliptic).

• **Метка**: запись в базе вендора о том, кому принадлежит адрес, например «биржа Binance» или «мошенничество».

• **Кластер**: группа адресов, которые платформа считает принадлежащими одному владельцу.

• **Выгрузка (снимок)**: файл, сохранённый из платформы, который показывает, что она отображала на определённую дату. Это похоже на выписку из реестра по состоянию на конкретный день.

• **Хеш**: короткий код, вычисленный из содержимого файла, своего рода отпечаток пальца файла. Если в файле изменится хотя бы один символ, изменится и хеш, поэтому совпадение хеша подтверждает, что файл тот же, что был сохранён.

• **Депозитный адрес**: адрес, который биржа выдаёт конкретному клиенту для пополнения его счёта.

• **Горячий кошелёк**: общий кошелёк биржи, из которого она выплачивает средства клиентам.

• **Защитный приказ** (protective order): распоряжение суда в США или Англии, по которому конфиденциальные материалы можно показывать только названным лицам, например представителям сторон и экспертам, и только для целей дела. В российском и белорусском процессе прямого аналога нет; ближе всего к нему рассмотрение сведений, составляющих охраняемую законом тайну, в закрытом заседании.

Первое заключение аналитика истец приобщил в марте. В нём говорилось, что средства поступили на адрес «Биржа М — промежуточный кошелёк». Второе заключение истец представил в сентябре, в ответ на рецензию ответчика. В нём тот же адрес назывался «Биржа М — горячий кошелёк».

В блокчейне ничего не изменилось: адрес совершил те же транзакции. Между двумя выгрузками вендор переметил адрес в своей базе, а аналитик перенёс новую метку в заключение, не заметив этого.

Представитель ответчика это заметила. Когда аналитика вызвали в заседание для пояснений, она первым делом спросила: «Какое из ваших двух заключений верное?» Честный ответ был таким: ни одна из меток не была его собственным выводом, каждая лишь повторяла то, что база вендора показывала в день выгрузки.

Метка имела значение. В горячем кошельке хранятся средства многих клиентов, а промежуточный может принадлежать одному. От этой разницы зависел один из шагов цепочки истца. Суд не решал, какая метка верна. Он указал, что и аналитик этого не решил.

4.1 Что такое метка и откуда она

Метка — утверждение платформы, что адрес или кластер принадлежит названной организации или относится к категории: «депозит Binance», «даркнет-рынок», «лицо под санкциями», «миксер» (сервис, который смешивает монеты многих пользователей, чтобы скрыть их происхождение), «мошенничество». Ради меток аналитики и покупают коммерческие инструменты. Метки превращают граф из анонимных строк в карту с названиями.

Большинство названий в заключении об атрибуции поставил вендор. Аналитик, который подписал заключение, обычно их не создавал.

Вендоры строят метки из нескольких видов источников, которые сильно различаются по тому, может ли их проверить другая сторона.

Источник	Пример	Может ли другая сторона проверить?
Прямое взаимодействие	Аналитики вендора делают депозит и вывод в сервисе и записывают использованные адреса	Частично: транзакции видны в блокчейне, а заметки вендора о его действиях нет
Данные самого сервиса	Биржа или кастодиан передаёт вендору список своих адресов	Редко: список обычно конфиденциален
Расследования и данные правоохранителей	Адреса из изъятий, обвинительных заключений, судебных актов	Иногда, если назван публичный источник
Открытые источники	Адреса, опубликованные самой организацией, на форумах, в утечках, в санкционных списках	Да, если источник назван
Эвристическое расширение	Метка с исходного (подтверждённого) адреса переносится на все адреса, которые правила кластеризации платформы слили с ним	Только если представлены сливающие транзакции (глава 3)
Сообщения пользователей	Жалобы на мошенничество от публики или других клиентов; метки блок-эксплореров (name tags); метки, купленные или собранные у пользователей на площадках разведданных; собственные метки учётной записи пользователя, которые видит только он и которые не являются атрибуцией платформы	Редко, и это самый ненадёжный источник

Две последние строки важнее всего в споре об атрибуции и менее всего заметны. Метка может начаться с одного адреса, подтверждённого прямым взаимодействием. После эвристического расширения она может покрывать десять тысяч адресов. Все они носят то же имя, но исходного подтверждения нет ни у одного из них.

Метка может держаться и на одном лишь сообщении человека, который потерял деньги.

Из этого не следует, что метки ненадёжны как класс. Метки из прямого взаимодействия или из списков самих сервисов часто очень хороши, и у вендоров есть серьёзные коммерческие причины держать их точными.

Трудность в том, что метка часто не сообщает, на каком источнике она основана. Вендоры здесь расходятся. Один крупный вендор заявляет, что его метки не имеют вероятностной оценки, потому что он ставит их только консервативно. Другой показывает источник и уровень уверенности для каждой метки. В любом случае заключение, которое цитирует метку без источника, повторяет вывод вендора без его оснований.

Уровень уверенности, который показывает вендор, — не оценка шага аналитиком. Шаг, который держится на метке, аналитик сам оценивает по пятиуровневой шкале книги (глава 5), какую бы оценку ни показывала платформа.

Российский и белорусский контекст

В делах российских и белорусских судов к коммерческим зарубежным платформам добавляется государственная. Систему Росфинмониторинга «Прозрачный блокчейн» представили в 2021 году. К 2023 году, по словам руководителя ведомства, ею пользовались МВД, ФСБ и Следственный комитет. В декабре 2025 года завершился пилотный проект с банками.

По оценке автора, для доказывания у этой системы та же проблема, что у коммерческих инструментов, и даже острее. Официальной публикации методики и источников меток мы не нашли (см. примечания), и, насколько известно автору, доступа к системе у защиты и у частного аналитика нет. Если в материалах уголовного дела адрес отнесён к лицу «по данным мониторинга», это метка с неизвестным источником. Вопросы из 4.7 задаются к ней так же, как к метке вендора.

По наблюдениям автора, из коммерческих платформ в заключениях для российских и белорусских судов часто встречается Crystal. Её начали разрабатывать в Bitfury в 2015 году; сейчас это Crystal Intelligence (Crystal Blockchain B.V., Амстердам). Кроме неё аналитики используют AML-сервисы, работающие на российском рынке, например ШАРД, КоинКИТ (CoinKYT), AMLCrypto и BitOK, а также бесплатные версии обозревателей с метками. Перечень приведён только для ориентира и не является рекомендацией: автор эти сервисы не сравнивал, их методики и покрытие меток не опубликованы, а состав рынка быстро меняется. Всё сказанное в этой главе о метках вендоров относится и к ним, и к обозревателям. Какой инструмент использован и на каком основании получен доступ (лицензия, учётная запись, договор), указывается в заключении (приложение F, F.3).

4.2 «Платформа показала» ещё не вывод аналитика

Во многих заключениях встречается фраза: «По данным Crystal, адрес принадлежит бирже X». По форме это вывод аналитика, по сути — пересказ того, что записано в базе вендора. Суд эту базу проверить не может, другая сторона обычно тоже. Аналитик часто не знает, на чём метка основана.

Пользоваться платформой можно и нужно: эксперты всегда опираются на справочники, базы данных и приборы. Но заключение эксперта должно содержать подробное описание проведённого исследования, сделанные в результате его выводы и ответы на поставленные судом вопросы (ч. 2 ст. 86 ГПК РФ). Если в заключении написано только «платформа показала», описания исследования в этой части нет.

Отсюда три правила.

1. За метку отвечает аналитик. Платформу в суд не вызовут. Вызовут аналитика или эксперта, и спрашивать будут его. Если он перенёс метку в заключение, он должен уметь её объяснить. Ответ «так показывает программа» суд обычно понимает так: сам аналитик этот вопрос не исследовал.

2. Нужно указать, откуда взялась метка. Для каждой метки, на которой держится важный шаг, аналитик пишет, из какого источника она получена (виды источников — в таблице раздела 4.1). Если платформа источник не раскрывает, так и пишут: «источник метки платформой не раскрывается». Заключение от этого не становится негодным, но суд видит, что этот шаг нуждается в подтверждении.

3. Метку нужно проверить по самому блокчейну. Это может сделать любой аналитик, даже без доступа к платформе. Например:

• **депозитный адрес** биржи обычно переводит поступившее на общий кошелёк биржи, часто после того, как биржа прислала ему TRX, энергию или ETH на этот перевод, иногда

только по достижении порога, а в Ethereum иногда внутренним переводом из пересылающего контракта;

• **горячий кошелёк** биржи получает средства, собранные с множества депозитных адресов самой биржи, и отправляет тысячи выплат не связанным между собой людям;

• **адрес мошенника** часто получает много небольших переводов от разных отправителей и быстро их выводит.

Если поведение адреса совпадает с меткой, это нужно написать в заключении: такая проверка не зависит от вендора, и повторить её может любой. Если не совпадает, метку нельзя принимать без дополнительных данных.

Как это делают на практике

Самая простая проверка — та, которую сделал аналитик ФБР в деле *Sterlingov* (4.4): сопоставить метку с записями самой биржи.

В российском и белорусском деле ответ биржи на запрос следователя или на запрос суда об истребовании доказательств можно сопоставить с меткой платформы и указать результат в заключении. Если ответа биржи ещё нет, аналитик может прямо написать, какой запрос подтвердит метку и кому его направить. В Беларуси физические лица вправе покупать и продавать токены за деньги только через резидентов Парка высоких технологий (операторов криптоплатформ и операторов обмена) по Указу Президента Республики Беларусь от 17.09.2024 № 367. Поэтому сведения о покупке токенов за деньги и о выводе в деньги находятся у белорусского оператора, и суд может истребовать их в Беларуси, без запроса за рубеж. Обмен токенов на токены на зарубежных площадках указ не запрещает, поэтому у белорусского клиента может быть и счёт на иностранной бирже; его операции там в записи белорусского оператора не попадают. В России с 01.07.2027 организацию обращения цифровых валют смогут осуществлять только лица, названные в законе (ч. 3 ст. 1 Федерального закона от 04.08.2026 № 282-ФЗ «О цифровых валютах и цифровых правах»). Сведения таких российских организаций суд сможет истребовать в общем порядке (ст. 57 ГПК РФ, ст. 66 АПК РФ).

Пример формулировки в заключении

«Адрес TQ7…k2 отмечен на платформе [наименование] (выгрузка от 12.03.2026, хеш файла SHA-256: …) как депозитный адрес биржи M. Источник метки платформой не раскрывается. История транзакций адреса соответствует депозитному: все 37 входящих переводов за период с 01.02 по 10.03.2026 в течение 2–40 минут переведены на адрес TR9…x4, который на той же платформе отмечен как горячий кошелёк биржи M. В ответе биржи M от 02.04.2026 на запрос следователя адрес TQ7…k2 указан как депозитный адрес счёта № … Вывод о принадлежности адреса бирже M основан на совокупности этих данных».

Суд видит, откуда метка и на какую дату, что аналитик проверил сам и какое независимое подтверждение получено.

Пример вопросов для ходатайства о назначении экспертизы

Если нужно проверить чужое заключение, в ходатайстве можно предложить такие вопросы:

1. На каком источнике основана метка платформы, согласно которой адрес … принадлежит …?

2. Соответствует ли история транзакций адреса … такой принадлежности?

3. Подтверждается ли принадлежность адреса данными другой аналитической платформы или другими материалами дела?

Как оспаривать метку в рецензии

В деле ООО «Халден Логистик» (дело «Халдена», глава 2) шаг 7 держится на метке «Биржа K — промежуточный» без источника и без даты. Эксперт Б не утверждала, что метка неверна. Она указала три обстоятельства:

• других доказательств для этого шага в заключении нет;

• метка не уточняет, в чём состоит связь с биржей K: принадлежит ли адрес клиенту биржи или посреднику, который переводит на неё средства;

• по истории транзакций адрес так же похож на адрес посредника, например OTC-дилера (дилера, который покупает и продаёт криптоактивы для клиентов вне биржи), который зачисляет средства своих клиентов на биржу K.

На этих основаниях эксперт Б оценила шаг 7 как возможный: уровень 4 по пятиуровневой шкале (4.1, глава 5). История транзакций совместима с меткой, но так же хорошо объясняется адресом посредника. Рецензия, построенная так, не обвиняет аналитика другой стороны в ошибке. Она показывает суду, что вывод не обоснован, и даёт основание для ходатайства о повторной или дополнительной экспертизе.

4.3 Метки меняются: снимки и версии

База данных платформы постоянно меняется. Вендоры добавляют метки по мере появления сведений. Они сливают и делят кластеры, когда улучшают свои правила, переименовывают организации, исправляют ошибки и снимают метки, которые больше не могут подтвердить. Адрес, который в прошлом году был «неизвестным», сегодня может быть «Биржа M», а через месяц «Биржа M, горячий кошелёк».

Для заключения это риск, потому что заключение опирается на то, что база показывала в один конкретный день. Отсюда четыре следствия.

1. Заключение говорит по состоянию на дату. У каждой метки в заключении должна быть дата её получения. Если вендор сообщает номер версии платформы или набора данных, его тоже нужно указать. Без даты метку нельзя воспроизвести, а её позднейшее изменение нельзя объяснить.

2. Выгрузки нужно сохранять. Аналитик сохраняет нужный экран платформы, граф или отчёт по адресу в момент анализа и хранит его вместе с рабочими материалами. Исходная выгрузка с метаданными (сведениями, которые файл хранит о себе, например дата создания) лучше скриншота. Скриншот лучше, чем ничего. Если метка потом изменится, аналитик сможет показать, что платформа отображала в тот день, когда он на неё опирался.

3. Изменившаяся метка тоже доказательство. Если метка разная в заключении истца и в рецензии ответчика, суду нужно знать, какая верна и почему вендор её изменил. Журналы изменений по отдельным адресам вендоры публикуют редко. Некоторые объясняют изменение по запросу своего клиента, но не обязаны; другой стороне вендор отвечать не обязан. Аналитик, который спросил до заседания, в гораздо лучшем положении, чем тот, кто узнал об изменении из вопроса представителя другой стороны.

4. Повторный запрос не равен воспроизведению. Если через год запросить платформу снова и получить ту же метку, это покажет лишь, что метка всё ещё там. Это не покажет, что она верна или что тогда она держалась на том же источнике, что и сейчас.

Открывающая сцена главы — ошибка снимка: две выгрузки с интервалом в несколько месяцев дали две разные метки, и обе аналитик подал как свой вывод. Если бы он датировал

каждую выгрузку и заметил изменение, он мог бы спросить вендора о причине, записать ответ и объяснить изменение во втором заключении.

Как это делают на практике: фиксация выгрузки платформы

1. **Выгрузить.** В момент анализа выгрузите отчёт по адресу, граф или страницу организации в исходном формате платформы (CSV, JSON или PDF, что она предлагает). Сделайте скриншот того же экрана так, чтобы были видны дата и учётная запись. Так поступают с каждым адресом, от которого зависит ключевой шаг.

2. **Посчитать хеш.** Вычислите хеш SHA-256 каждого файла. Это делают стандартные средства: в Windows команда certutil -hashfile <файл> SHA256, в macOS и Linux shasum -a 256 <файл>.

3. **Записать дату и обстоятельства.** Укажите дату и время выгрузки с часовым поясом, платформу и модуль, учётную запись и номер версии, если платформа его показывает.

4. **Хранить с рабочими материалами.** Храните файлы в неизменном виде вместе с коротким перечнем, где для каждого файла указан его хеш. Не открывайте и не пересохраняйте файлы: любое изменение меняет хеш.

5. **Приложить или перечислить.** Приложите перечень выгрузок к заключению или укажите файлы среди использованных материалов, чтобы другая сторона могла их запросить. Заранее проверьте, разрешает ли лицензия платформы представлять её выгрузки в суд; если нужно согласие вендора, получите его до того, как заключение будет представлено.

6. **Нотариальный протокол осмотра, если выгрузка нужна как самостоятельное доказательство.** В российской практике обычный путь здесь — нотариальный протокол осмотра информации. Он фиксирует, что платформа показывала в конкретный день. Порядок подробно разобран в книге 1, глава 15.

7. **Проверить снова перед заседанием.** Незадолго до заседания запросите основные адреса ещё раз. Если метка изменилась, выгрузите её заново, посчитайте хеш и объясните изменение в дополнительном заключении или письменных пояснениях.

Пример формулировки: перечень выгрузок (приложение к заключению)

«Приложение 3. Выгрузки аналитической платформы, использованные при подготовке заключения.

1. Файл TQ7k2_address_report.csv. Платформа [наименование], модуль [ ]. Выгрузка выполнена [ФИО] с учётной записи [идентификатор] 12.03.2026 в 14:05 UTC. Хеш SHA-256: [64 символа]. Метка на платформе: «Биржа М, депозитный адрес». Источник метки платформой не раскрывается.

2. Файл TQ7k2_screen.png. Скриншот того же экрана, 12.03.2026, 14:06 UTC. Хеш SHA-256: [значение].

Файлы хранятся в неизменном виде в рабочих материалах аналитика и будут представлены по запросу суда или сторон. Подлинность любой представленной копии проверяется по указанным значениям хеша».

Типичные ошибки

• Метка приведена в заключении без даты получения.

• Сохранён только скриншот, обрезанный так, что не видны дата, платформа и учётная запись.

• Выгрузку открыли и сохранили заново (например, в табличном редакторе), и хеш больше не совпадает.

• Аналитик через несколько месяцев снова запросил платформу, получил другую метку и без пояснений перенёс её в новое заключение, как в открывающей сцене.

• Метка, унаследованная через кластер, приведена так, будто подтверждён сам адрес.

• Две совпадающие платформы представлены как независимые, хотя никто не проверил, нет ли у них общего источника (4.5).

4.4 *Sterlingov*: платформа перед судом

Опубликованных российских или белорусских решений, в которых суд подробно разбирал бы надёжность коммерческой аналитической платформы, найти не удалось. Самое подробное такое исследование на сегодня проведено в американском деле *United States v. Sterlingov*. Обвиняемого судили в федеральном суде округа Колумбия как предполагаемого оператора миксера Bitcoin Fog. Доказательства обвинения по блокчейну были построены в основном на Chainalysis Reactor.

Защита просила исключить эти доказательства как ненадёжные по правилу 702 Федеральных правил о доказательствах США. Суд применил тест *Daubert* (критерии Верховного суда США, по которым судья решает, достаточно ли надёжно заключение эксперта, чтобы его исследовать). 29 февраля 2024 года судья Мосс ходатайство отклонил.

Что утверждала защита

Защита утверждала, что атрибуции платформы нельзя проверить. Программа проприетарная, а её эвристики (эмпирические правила, по которым платформа решает, что у адресов один владелец) никто независимо не проверял.

Кроме того, вендор не собирал и не учитывал централизованно собственные ложноположительные результаты (ошибочные атрибуции) и ложноотрицательные (пропущенные). Поэтому известной частоты ошибок, которую можно было бы представить суду, не было.

Что признал суд

Суд не оспаривал, что частота ошибок не учитывалась и что рецензирования не было. Свидетель самого вендора под присягой заявила, что ложные срабатывания в едином реестре не собирались. Суд признал, что ни то, ни другое не исключает допуска доказательств.

Почему доказательства всё же допущены

Суд счёл частоту ошибок одним из факторов, а не обязательным условием допуска. Доказательства поддержало то, что было вокруг платформы:

• **собственные проверки аналитика**: аналитик ФБР сверил атрибуции платформы с ответами бирж на запросы (в ответах были названы владельцы счетов) и ложных срабатываний в этой сверке не нашёл;

• **независимые инструменты**: вторая коммерческая платформа, TRM, подтвердила все 144 адреса, с которых пополнялись счета обвиняемого, а сотрудница CipherTrace, которую защита сначала заявила своим экспертом, а затем отозвала, сошлась с Chainalysis почти по 400 000 адресов и не нашла ни одного ложного срабатывания;

• **характер ошибок**: свидетель вендора пояснила, что платформа скорее пропускает адреса, чем ошибочно их помечает, поэтому кластеры получаются скорее меньше, чем больше;

• **другие доказательства по делу**, включая данные обвиняемым под присягой на досудебном заседании показания о том, что биткоины на его биржевой счёт поступили через Bitcoin Fog.

Перед судом была и цифра 99,9146% точности кластеризации. Её привёл сотрудничавший со следствием обвиняемый по другому делу, который просматривал кластеры. Это не измеренная частота ошибок, и ссылаться на неё как на частоту ошибок не следует.

Что было раскрыто

Защита требовала исходный код платформы. Суд раскрыть его не обязал. Доступ к коду поставили в зависимость от того, обоснует ли квалифицированный эксперт конкретную потребность в нём, а такого обоснования не последовало.

Вместо кода обвинение передало подробности спорной эвристики под защитным приказом. Их могли видеть защитники и эксперты, но не сам обвиняемый. Суд также предложил защите государственное финансирование лицензии на инструмент или привлечения эксперта. К этой модели раскрытия мы вернёмся в главе 10.

Апелляция

25 сентября 2026 года Апелляционный суд США по округу Колумбия оставил решение в силе. Он признал, что допуск доказательств не был злоупотреблением усмотрением. Суд также указал, что факторы *Daubert* не являются перечнем, которому обязан соответствовать каждый метод, и что ограничения раскрытия были законны. Довод о праве на очную ставку со свидетелями обвинения (Confrontation Clause) суд отклонил: выходные данные программы не являются ни показаниями с чужих слов, ни свидетельскими показаниями, поэтому Шестая поправка не требовала раскрывать исходный код вендора. Часть доводов проверялась лишь на явную ошибку (plain error), потому что в суде первой инстанции их не заявляли. Суд сослался также на общее признание платформы правоохранительными органами и отраслью.

Что из этого следует для практики

1. Доказательства выдержали проверку благодаря подтверждениям. *Sterlingov* иногда цитируют как одобрение платформы, а апелляционное решение будут цитировать так ещё чаще. Вернее читать оба решения как одобрение совокупности доказательств, в которой платформа была одним из нескольких независимых источников. Атрибуция, которая держится на одной метке одного вендора без независимой опоры, выглядела бы совсем иначе.

2. Значение имеют собственные проверки аналитика. Суд придал вес тому, что аналитики сделали для проверки результатов платформы. Аналитику, который не может описать ни одной собственной проверки, нечего предложить суду взамен.

3. Допустимость не означает достоверности. Решение о том, что доказательство достаточно надёжно, чтобы его исследовать, не означает, что оно верно. Защита по-прежнему могла оспаривать каждую атрибуцию перед присяжными.

Что это значит для российского и белорусского суда

Отдельной стадии проверки допустимости метода, как в *Daubert*, у нас нет. Заключение приобщается к делу и оценивается вместе с остальными доказательствами.

Вопросы при этом те же: каков метод, проверен ли он, что известно о его ошибках, что ещё подтверждает результат. Только задают их в рецензии на заключение, в вопросах эксперту

в заседании и в ходатайстве о повторной экспертизе в связи с сомнениями в обоснованности заключения.

Судья специальными познаниями не обладает и на заключение опирается (глава 3). Поэтому заключение, которое отвечает на эти вопросы заранее, обычно оказывается убедительнее.

4.5 Когда платформы расходятся

Платформы могут расходиться, и насколько часто, никто не измерял. У них разные исходные данные, разные правила и пороги кластеризации, и метки они добавляют с разной скоростью. Один и тот же адрес может быть «Биржей K» на одной платформе, «неизвестным» на второй и частью кластера другой биржи на третьей.

В английском деле *D'Aloia* суд отметил, что результаты, полученные экспертом истца с помощью двух платформ (Crystal и TRM), расходились, эксперт не объяснил почему, а методики платформ не были представлены; о надёжности самих инструментов суд выводов не делал. Это стало одной из причин, по которым трассировка истца не была принята.

При правильном обращении расхождение полезно обеим сторонам.

Для стороны, которая опирается на атрибуцию

Согласие платформ подтверждает метку, только если они пришли к ней независимо. Две платформы могли купить один и тот же список адресов биржи. Они могли расширить один и тот же исходный адрес через одну и ту же транзакцию совместного расходования (транзакцию, в которой тратятся монеты сразу с нескольких адресов; платформы считают это признаком одного владельца). Тогда это один источник, посчитанный дважды (глава 6).

Аналитик, который ссылается на согласие платформ, должен объяснить, почему считает его независимым. Аналитик, который обнаружил расхождение, должен указать его в заключении. Необъяснённое расхождение, найденное другой стороной, вредит гораздо больше, чем расхождение, раскрытое и объяснённое самим аналитиком.

Для стороны, которая её оспаривает

Вторая платформа — самая дешёвая из доступных независимых проверок. Прогнать основные адреса истца через другого вендора стоит недорого, и в результате часто получается другая метка или никакой.

Это ещё не доказывает, что метка истца неверна. Но это показывает, что метка требует объяснения, и перекладывает на аналитика истца обязанность обосновать, почему его источник предпочтительнее. Если до сих пор в деле было только заключение аналитика одной стороны, расхождение платформ даёт наглядное основание для ходатайства о назначении судебной экспертизы.

Пример формулировки: как объяснить расхождение

«Платформа A относит адрес … к горячему кошельку биржи M. Платформа B метки для него не содержит. Платформа C включает его в кластер биржи L. История транзакций адреса совместима с меткой A: адрес получал средства, собранные с сотен депозитных адресов биржи M, выплачивал выводы не связанным между собой получателям и регулярно переводил средства на известный холодный кошелёк биржи M (кошелёк для хранения средств вне сети). С меткой C эта история несовместима. В ответе на запрос биржа M подтвердила, что адрес

принадлежит ей. Поэтому для этого шага принимается метка A, а метка C рассматривается как ошибка кластеризации».

4.6 ИИ как новый источник ошибок

Аналитические вендоры уже предлагают ИИ-ассистентов. Они пересказывают историю кошелька, предлагают вероятного владельца, пишут текст отчёта и подсказывают, какие потоки средств важны. Аналитики и сами пользуются языковыми моделями: просят объяснить транзакции, написать код для разбора выгрузок, подготовить черновики разделов заключения.

При небрежном использовании появляются ошибки трёх видов. Об ответственности юриста за такие ошибки подробно говорится в книге «Кто платит за ошибку ИИ».

1. Убедительный вымысел. Языковая модель, которую спросили об адресе, может уверенно выдать атрибуцию, метку, число транзакций или ссылку на судебное решение, которых не существует. Такой текст ничем не отличается от остального заключения и не показывает, откуда он взялся. Аналитик, который его вставил, добавил в цепочку шаг без всяких данных.

2. Невоспроизводимый результат. Один и тот же вопрос, заданный одной и той же модели дважды, может дать два разных ответа. Версию модели, её настройки и текст запроса фиксируют редко. Шаг, который нельзя повторить, нельзя и проверить. А если выводы заключения нельзя проверить, это прямое основание для сомнений в его обоснованности.

3. Скрытая опора. Некоторые платформы предлагают кластеры и метки с помощью машинного обучения. Аналитик может не знать, что метку сгенерировала модель и аналитики вендора её не подтверждали. Это та же проблема, что в 4.1, только острее: в категорию «эвристическое расширение» теперь входит модель, правила которой никто не может назвать.

Зарубежные суды уже реагируют. Юристов штрафуют за выдуманные ИИ ссылки на судебную практику. В деле *Matter of Weber* (2024) суд штата Нью-Йорк не придал никакого веса расчётам эксперта. Среди прочих недостатков эксперт перепроверял расчёты с помощью ИИ-ассистента и не смог сказать, какие данные в него вводил и на какие источники тот опирался. Суд также указал, что использование ИИ в доказательствах нужно раскрывать.

В США подготовлен проект нового правила 707 Федеральных правил о доказательствах. Оно распространило бы стандарт надёжности на машинно-сгенерированные доказательства, представленные без эксперта. Проект был опубликован для обсуждения в 2025–2026 годах и на момент написания не принят.

В России и Беларуси специальных правил нет, но действуют общие. Заключение должно содержать подробное описание исследования и обоснованные выводы, а эксперт отвечает за заключение лично.

Что должен сделать аналитик

• Не включать в заключение метку, атрибуцию или число, предложенные моделью, пока они не проверены по блокчейну или по первичному документу.

• Фиксировать каждый использованный ИИ-инструмент, его версию и цель использования и указывать это в заключении.

• Считать результат платформы, который вендор описывает как сгенерированный моделью, отдельной категорией источника. До подтверждения он весит не больше, чем эвристическое расширение.

Что спросит другая сторона

• Использовали ли вы ИИ-инструменты при подготовке заключения?

• Какие именно, для чего и как вы проверили их результат?

• Эта метка подтверждена аналитиками вендора или предложена моделью?

4.7 Что требовать от метки

Для каждой метки, от которой зависит шаг цепочки атрибуции, заключение должно ответить на семь вопросов. Если оно на них не отвечает, вопросы можно поставить в рецензии, задать аналитику или эксперту в заседании либо включить в ходатайство о назначении экспертизы. В скобках указано, почему вопрос важен.

1. Какая платформа и какой её продукт или модуль дали метку для адреса […]? (Разные продукты одного вендора могут опираться на разные данные.)

2. На какую дату и время получена метка, сохранена ли выгрузка, указан ли её хеш, составлялся ли нотариальный протокол осмотра? (Метки меняются: 4.3.)

3. На каком виде источника основана метка: прямое взаимодействие, данные самого сервиса, данные правоохранительных органов, открытые источники, эвристическое расширение или сообщения пользователей? (Первые два надёжны, последние два слабы: 4.1.)

4. Метка стоит на самом адресе или унаследована через кластер? Если унаследована, какие транзакции объединили адрес с кластером? (Унаследованная метка надёжна ровно настолько, насколько надёжно объединение, которое её перенесло: глава 3.)

5. Соответствует ли метке история транзакций самого адреса и что именно аналитик проверил? (Это единственная проверка, доступная без вендора: 4.2.)

6. Что показывают по этому адресу другие платформы и независимы ли их источники от источника первой платформы? (Совпадение подтверждает метку, только если оно независимо: 4.5.)

7. Создана ли метка или решение аналитика опереться на неё с помощью ИИ-инструмента? (Новый источник неназванных ошибок: 4.6.)

Если на эти вопросы ответить нельзя, шаг нужно оценивать не выше уровня 4 (*возможно*). В заключении следует указать, что могло бы повысить оценку: подтверждение самой биржи, вторая независимая платформа или публичный документ.

Пример формулировки: ходатайство об истребовании исходных данных заключения

«В [наименование суда] по делу № […]

Ходатайство об истребовании доказательств

Истец представил заключение [ФИО] от [дата] (документ озаглавлен «[название, например «Заключение специалиста»]», т. [ ], л. д. [ ]; далее — заключение аналитика истца). В разделе […] заключения вывод о связи адреса […] с биржей K (шаг 7 цепочки) основан на метке платформы [название]. Выгрузки платформы, на которые ссылается аналитик, к заключению не приложены. Без них нельзя проверить, что показывала платформа, на какую дату и на каком источнике основана метка.

Эти материалы имеют значение для установления принадлежности адреса […]. Они находятся у истца и аналитика. Ответчик получить их самостоятельно не может, так как доступа к платформе и к рабочим материалам аналитика у него нет.

На основании ст. 57 ГПК РФ прошу истребовать у истца:

1. выгрузки платформы [название] по адресам […] в исходном формате с указанием даты и времени выгрузки и хеша SHA-256 каждого файла;

2. скриншоты тех же экранов, на которых видны дата и учётная запись;

3. документы, переданные аналитику для подготовки заключения (задание, перечень исходных данных), и журнал хода исследования, если он вёлся».

Истребовать можно только существующие документы и предметы. Вопрос об использовании ИИ-инструментов включите в вопросы эксперту, если назначена экспертиза. Аналитика другой стороны можно вызвать только в процессуальном качестве, например как свидетеля о том, как он получал и сохранял данные (ч. 1 ст. 69 ГПК РФ, ст. 56 АПК РФ). Оценку доказательств он в этом качестве не даёт.

В арбитражном суде такое ходатайство подают по ч. 4 ст. 66 АПК РФ, в Беларуси по ч. 2 ст. 234 КГС (ходатайство о процессуальных действиях, направленных на сбор доказательств, которые сторона не может представить самостоятельно). Если по делу назначается судебная экспертиза, семь вопросов из списка выше можно предложить для постановки перед экспертом (ч. 2 ст. 79 ГПК РФ, ч. 2 ст. 82 АПК РФ, п. 3 ст. 221 КГС), переформулировав их применительно к спорным адресам (см. также примеры вопросов в 4.2). Глава 10 разбирает, что ещё можно получить от другой стороны и от вендора.

* * *

Для истца. До приобщения заключения добейтесь, чтобы аналитик ответил на семь вопросов из 4.7 по каждой метке, на которой держится существенный шаг. Сами проверьте основные адреса на второй платформе. Если она расходится с первой, лучше узнать об этом сейчас и включить объяснение в заключение. В запросе бирже (через следователя или через истребование судом) просите подтвердить принадлежность адреса: одна строка от биржи весит больше любой метки вендора. Верховный Суд РФ отменил апелляционное определение, в котором не было сказано, каким образом установлена принадлежность ответчику криптокошелька, на который переводилась криптовалюта (определение СК по гражданским делам от 16.04.2024 № 69-КГ24-3-К7; Приложение Е, Е.2.3).

Для ответчика. Требуйте датированные выгрузки по каждой метке, а не только само заключение (образец ходатайства в 4.7). Проверьте основные адреса истца на другой платформе. Включите в вопросы эксперту вопрос об использовании ИИ. Метка без источника, без даты и без независимого подтверждения обычно самый слабый шаг цепочки, и оспорить его в рецензии проще всего.

Для эксперта. Не принимайте метку, которую не можете обосновать как собственный вывод. Датируйте и сохраняйте каждую выгрузку, считайте её хеш. Сверяйте каждую существенную метку с поведением адреса в блокчейне и пишите в заключении, что сверили. Раскрывайте расхождения платформ и объясняйте их. Указывайте, использовался ли ИИ и как вы проверили его результат.

* * *

Что проверить

• ☐ По каждой метке для существенного шага: платформа, продукт, дата получения, сохранённая выгрузка с хешем или нотариальный протокол осмотра?

• ☐ На каком виде источника основана каждая метка? Если он неизвестен, оценён ли шаг не выше уровня 4 (*возможно*)?

• ☐ Метка стоит на самом адресе или унаследована через кластер?

• ☐ Ведёт ли себя адрес в блокчейне так, как предсказывает метка?

• ☐ Проверена ли вторая платформа и независимо ли её согласие?

• ☐ Менялась ли метка между заключениями и объяснено ли изменение?

• ☐ Использовался ли ИИ, для чего и как проверен результат?

* * *

Примечания к главе 4

• Требования к содержанию заключения эксперта (подробное описание исследования, выводы, ответы на поставленные судом вопросы): ч. 2 ст. 86 ГПК РФ (сверено 01.11.2026); ст. 8 (заключение должно позволять проверить обоснованность и достоверность выводов на

базе общепринятых научных и практических данных) и ст. 25 (содержание заключения, в том числе оценка результатов исследований, обоснование и формулировка выводов) Федерального закона от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». Повторная экспертиза при сомнениях в правильности или обоснованности заключения: ч. 2 ст. 87 ГПК РФ, ч. 2 ст. 87 АПК РФ. В Беларуси повторная экспертиза: ч. 2 ст. 229 КГС; подробнее о белорусских нормах — глава 9. Номера статей сверены 01.11.2026.

• Истребование доказательств по ходатайству стороны: ст. 57 ГПК РФ (ч. 1 — содействие суда в собирании и истребовании доказательств; ч. 2 — требования к содержанию ходатайства), сверено по consultant.ru. Арбитражный процесс: ч. 4 ст. 66 АПК РФ (ходатайство об истребовании доказательства). Беларусь: ч. 2 ст. 234 КГС (ходатайства о процессуальных действиях, направленных на сбор доказательств, когда сторона не может представить их самостоятельно); истребование доказательств от других лиц и организаций как способ обеспечения доказательств: ч. 5 ст. 235 КГС. Вопросы для эксперта: ч. 2 ст. 79 ГПК РФ, ч. 2 ст. 82 АПК РФ, п. 3 ст. 221 КГС; вопросы эксперту в заседании: ч. 3 ст. 228 КГС.

• Беларусь: Указ Президента Республики Беларусь от 17.09.2024 № 367 «Об обращении цифровых знаков (токенов)» (покупка и продажа токенов физическими лицами за деньги только через резидентов ПВТ; обмен токенов на токены на зарубежных площадках не запрещён); сверено по обзорам REVERA (2025), myfin.by и разъяснению на gomelisp.gov.by (wp-content/uploads/2025/03/tokeny.pdf). Россия: ч. 3 ст. 1 Федерального закона от 04.08.2026 № 282-ФЗ «О цифровых валютах и цифровых правах» (организацию обращения цифровых валют осуществляют только лица, указанные в ст. 14–18; вступает в силу с 01.07.2027); сверено по тексту закона на base.spinform.ru.

• «Прозрачный блокчейн»: «Коммерсантъ», 19.02.2021 (представление системы); «Интерфакс», 09.03.2023 (использование МВД, ФСБ, СК); завершение пилота с банками — декабрь 2025 г. (ТАСС). Официальной публикации методики на fedsfm.ru не найдено; опубликованных судебных решений с оценкой её данных не обнаружено. Crystal: crystalintelligence.com (история компании).

• В опубликованной российской и белорусской практике не найдено решений, в которых суд оценивал бы заключение специалиста на основе Chainalysis, Crystal или «Прозрачного блокчейна»; поиск по состоянию на дату, указанную на странице с выходными данными.

• Принадлежность криптокошелька ответчику как факт, который суд должен установить и мотивировать: Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 16.04.2024 № 69-КГ24-3-К7 (текст на vsrf.ru). Заключение специалиста в этом деле не оценивалось; см. Приложение Е, Е.2.3.

• *United States v. Sterlingov*, No. 1:21-cr-399 (RDM) (D.D.C.), определение от 29.02.2024 (судья Мосс), ECF 259, 719 F. Supp. 3d 65; определение (Memorandum Opinion) от 30.11.2023, ECF 213, о том, что обвиняемый лично не знакомится с данными об эвристике, 704 F. Supp. 3d 176; подтверждено апелляцией, No. 24-3161 (D.C. Cir. 25.09.2026). Показания свидетеля вендора об отсутствии централизованного учёта ложных срабатываний: Declaration of Elizabeth Bisbee, ECF 149-1 (18.07.2023).

• Описания источников меток самими вендорами: Chainalysis, «Chainalysis data accuracy» (16.01.2024); TRM Labs, «Defensible blockchain attribution»; Elliptic, «How Elliptic scales intelligence» (17.06.2026). Независимая оценка покрытия меток одного вендора: Lubbertsen, van Eeten, van Wegberg, «Ghost Clusters», USENIX Security 2025. Опубликованных исследований, системно сравнивающих метки разных вендоров, не найдено. Расхождение результатов TRM и Crystal: D’Aloia v Persons Unknown Category A [2024] EWHC 2342 (Ch), пп. 59–60.

• AML-сервисы на российском рынке: перечень по обзору рынка крипторасследований — Г. Осипов, РБК Крипто, 28.06.2026; сведения о сервисах — их собственные сайты (shard.ru, coinkyt.com, amlcrypto.io, bitok.org; проверены 15.11.2026).

• ИИ и заключение эксперта: *Matter of Weber*, 2024 NY Slip Op 24258 (Sur. Ct., Saratoga County, 10.10.2024). Проект Fed. R. Evid. 707: обсуждение 15.08.2025–16.02.2026; в мае 2026 г. не одобрен, работа продолжается.

• Открывающая сцена — составная; смена метки и биржа вымышлены.

Часть II. Степень уверенности

Глава 5. Шкала

Термины главы

• **Утверждение**: отдельное высказывание, которое может быть истинным или ложным, например «адреса E1 и E2 принадлежат одному владельцу».

• **Уровень обоснованности**: насколько доказательства подтверждают утверждение, по шкале с письменными критериями.

• **Альтернативное объяснение**: другое толкование тех же данных, при котором утверждение оказывается ложным.

• **Независимое подтверждение**: подтверждение того же утверждения из источника, который не опирается на те же данные или то же допущение.

• **Категорический и вероятный вывод**: две формы вывода эксперта, принятые в российской и белорусской экспертной практике. Категорический вывод утверждает факт без оговорок, вероятный допускает, что факт мог быть иным.

• **Отношение правдоподобия**: число, которое показывает, во сколько раз данные вероятнее при одной версии, чем при другой. Применяется в некоторых видах экспертиз (например, ДНК), для блокчейн-анализа почти недоступно.

• **Правило слабого звена**: вывод не может быть сильнее самого слабого шага, на котором он основан.

В заключении аналитика, представленном истцом, было написано, что ответчик «с высокой степенью вероятности» контролировал кошелёк, на который поступили средства. В судебном заседании представитель ответчика спросил аналитика, что означает «высокая». Аналитик ответил, что он почти уверен. Представитель спросил, означает ли «почти уверен» категорический вывод или вероятный. Аналитик ответил, что вывод вероятный, но вероятность высокая. На вопрос, какие данные сделали бы вывод категорическим и какие снизили бы его до «возможно», ответа не последовало.

Суд не исключил заключение из числа доказательств. В решении он указал, что выражение «высокая степень вероятности» не раскрыто, что аналитик не смог объяснить, чем она отличается от обычной, и что поэтому вывод оценивается не выше, чем позволяют изложенные в заключении данные. Эти данные подтверждали, что ответчик получил часть средств. Контроль над кошельком из них не следовал.

Сцена составлена из ситуаций, которые встречаются в практике, и не описывает конкретное дело.

5.1 Зачем нужна шкала

В заключениях по атрибуции в блокчейне используется много слов для степени уверенности: «вероятно», «с высокой вероятностью», «связан», «соответствует», «указывает на». Аналитические платформы добавляют свои обозначения: оценки риска, цветовые метки, проценты. Ни одно из этих слов не имеет закреплённого значения. Два эксперта могут употребить одно слово для разной степени подтверждения, а один эксперт в одном заключении может обозначить одно и то же разными словами.

Для суда это создаёт две трудности. Судья не может понять, насколько сильным должен быть вывод. Другая сторона всегда может заявить, что слово слишком сильное для имеющихся данных, и эксперту не на что опереться в ответ.

В российской и белорусской практике часть этой задачи решает деление выводов на категорические и вероятные. Но вероятный вывод охватывает очень разные ситуации: от вывода, подтверждённого двумя независимыми источниками, до вывода, который с тем же успехом объясняется иначе. Суду такой вывод мало что говорит о его силе.

Шкала решает эти задачи. В ней немного уровней, и у каждого есть письменные критерии: что должны показывать данные, чтобы уровень применялся, и что может повысить или понизить вывод. Эксперт указывает уровень для каждого утверждения и объясняет его. Суд может сопоставить заявленный уровень с данными, а другая сторона может оспорить уровень, только показав, что критерий не выполнен.

Книга использует одну шкалу и для каждого шага цепочки атрибуции (глава 2), и для вывода в целом. Так суду проще следить за рассуждением, и сразу видно, где сильный вывод держится на слабом шаге.

На практике суд нередко опирается на заключение эксперта, хотя оно для него необязательно (ч. 3 ст. 86 ГПК РФ, ч. 5 ст. 228 КГС РБ). Специальных знаний у суда нет, для того и назначается экспертиза. Положить заключение в основу решения суд может, если эксперт объяснил и обосновал выводы так, что их можно проверить. Шкала с критериями даёт суду то, на что можно сослаться в мотивировке: какую обоснованность эксперт приписал каждому выводу и на каких основаниях.

Типичные ошибки

• В выводах используется слово для степени уверенности, которого нет больше нигде в заключении и которое не раскрыто.

• Оценка риска платформы или её цвет («высокий риск», «красный») переносится в заключение как уровень обоснованности вывода эксперта. Оценка риска показывает связь адреса с помеченной активностью. О том, кому принадлежит адрес, она ничего не говорит.

• Указан процент («уверенность 90%»), который ни из каких данных не рассчитывался.

• В резюме указан один уровень, а в исследовательской части для того же утверждения другой.

5.2 Пять уровней: критерии и формулировки

В шкале пять уровней. Они применяются к отдельному утверждению. Утверждение может быть положительным («E1 и E2 принадлежат одному владельцу») или отрицательным («Реннер не контролировал T1»); шкала работает одинаково.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, купив полную легальную версию на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.