

ПОИСК СКРЫТЫХ КРИПТОАКТИВОВ

Как обнаружить, доказать
и взыскать то, что от вас прячут

Для семейных, банкротных
и корпоративных юристов

Борис Лев

Поиск скрытых криптоактивов

«Автор»

2026

Лев Б.

Поиск скрытых криптоактивов / Б. Лев — «Автор», 2026

Оппонент утверждает, что криптовалюты у него нет. Или что была, но он всё продал в убыток. Или что ключи утеряны. Проверить по реестру невозможно: криптоактив нигде не регистрируется. Эта книга - о том, что делать дальше. Как найти отправную точку, когда её нет. Как увидеть в банковской выписке покупку биткоина. Как вскрыть офшорный траст, мультисиг и цепочку номиналов. Как превратить данные блокчейна в доказательство, которое примет суд. И как получить деньги - потому что решение о взыскании криптоактива не исполняется само. Три сквозных дела - раздел имущества при разводе, банкротство предпринимателя, корпоративный конфликт - проходят через всю книгу от первого подозрения до полученных денег. Ни одно не заканчивается полной победой, и книга объясняет почему. 19 глав, 11 шаблонов процессуальных документов, разбор 15 юрисдикций, отдельные главы о наследовании и об этических границах. Законодательство по состоянию на сентябрь 2026 года, включая новый закон о цифровых валютах.

© Лев Б., 2026

© Автор, 2026

Содержание

Предисловие	6
Часть I. Разведка	8
Глава 1. Что лежит на столе: криптоактив как предмет спора	8
1.1. Зачем юристу эта книга именно сейчас	9
1.2. Таксономия: что именно ищем	11
1.3. Правовой статус: что говорит закон	13
Основной закон	14
Статус актива	15
Судебная защита: снятая ловушка	16
Что запрещено, а что нет	17
Контур законного оборота	18
Открытые вопросы: где я даю свой ответ	20
Что ещё осталось из прежней рамки	22
Международная рамка	23
1.4. Почему крипту сложно найти: анатомия невидимости	24
1.5. Что уже есть в арсенале юриста, и чего не хватает	25
1.6. Сквозной кейс № 1: вводная	26
1.7. Как пользоваться этой книгой	27
Вместо заключения	28
Глава 2. Ончейн-анализ: что видно в блокчейне и как это превратить в доказательство	29
2.1. Что такое блокчейн глазами юриста	30
Что видно	31
Чего не видно	32
Что из этого следует для доказывания	33
2.2. Инструменты: от бесплатного эксплорера до профессиональной платформы	34
Уровень 1. Публичные эксплореры	35
Уровень 2. Профессиональные аналитические платформы	37
Уровень 3. Расследователи и форензик-лаборатории	38
2.3. Методология: что делает аналитик и как читать его результат	39
Алгоритм трассировки	40
Что получает юрист на выходе	41
Чек-лист: как проверить результат аналитика	42
2.4. Пределы ончейн-анализа: где трассировка обрывается	43
Пять ситуаций, в которых ончейн-трассировка заходит в туннель	44
Что делать, когда трассировка оборвалась	45
2.5. Что нужно знать о технике, чтобы правильно ставить задачу	46
Две разные модели учёта	47
Сети второго уровня: где сегодня чаще всего обрывается след	48
Ложные связи: пылевые рассылки и отравление адресов	49
2.6. Допустимость ончейн-данных в российском процессе	50
Квалификация	50
Три способа введения в дело	51
Типовые возражения противной стороны и контраргументы	52
Практические рекомендации по допустимости	53

2.7. Как поставить задачу аналитику: шаблон технического задания	54
2.8. Сквозной кейс № 1, продолжение: первый след	55
Вместо заключения	56
Глава 3. Оффчейн-разведка: где искать отправную точку, если противник молчит	58
3.1. Проблема холодного старта	59
3.2. Банковские следы	60
Что искать в выписках	61
Как получить выписки	62
Практический приём	63
3.3. Устройства: телефон, компьютер, аппаратный кошелёк	64
Что можно найти на устройстве	65
Правовые механизмы доступа	66
Форензик-инструменты	67
Практический совет	68
3.4. Переписка: мессенджеры, почта, SMS	69
Где искать	70
Правовой доступ	71
Что именно искать в переписке	72
3.5. Свидетели	73
Кто может быть свидетелем	74
Как работать со свидетелями	75
Практический приём	76
3.6. Цифровой след: социальные сети, форумы, публичные данные	77
Где искать	78
Правовой статус	79
3.7. Процессуальные механизмы: как легально получить доступ	80
Гражданский и арбитражный процесс	81
Банкротство	82
Уголовное преследование	83
3.8. Регулируемый контур: новый слой источников	84
Почему это не отменяет остальную главу	85
Порядок: сначала дешёвое	86
Кому теперь можно писать	87
Банковский отказ как след	88
Майнеры: адреса уже в налоговой	89
Налоговый источник со 2 мая 2027 года	90
Что изменить в работе прямо сейчас	91
3.9. Как собрать всё воедино: чек-лист холодного старта	92
3.10. Сквозной кейс № 1, продолжение: второй след	93
Вместо заключения	94
Глава 4. Сквозной кейс № 1: от подозрения к доказанному факту	95
Конец ознакомительного фрагмента.	96

Поиск скрытых криптоактивов

Предисловие

Эта книга написана для юристов, которые сталкиваются с новой реальностью имущественных споров: криптоактивами.

Это вторая книга. Первая — «Криптовалютная криминалистика: расследование хищений, возврат средств и защита цифровых активов» — о ситуации, когда пострадал ваш доверитель: средства похищены, выведены, площадка исчезла. Здесь ситуация обратная: актив цел, у него есть владелец, и этот владелец — ваш оппонент, который не хочет, чтобы актив нашли.

Методика трассировки, работа с ончейн-аналитиком и техническое устройство блокчейна разобраны в первой книге подробнее, чем позволяет объём этой. Здесь они изложены в объёме, достаточном для имущественного спора; если нужен более глубокий разбор технической части — он там.

О сквозных делах. Книгу насквозь проходят три дела: раздел имущества при разводе, банкротство предпринимателя, корпоративный конфликт. Все три смоделированы. Имена, суммы, даты, адреса кошельков и содержание переписки условны; совпадения с реальными лицами и обстоятельствами случайны. Дела построены как типичные, а не как отчёт о конкретной практике, и приведённые в них исходы показывают, чем такие споры заканчиваются в среднем, а не гарантируют результат.

О подготовке издания. При работе над книгой применялись инструменты искусственного интеллекта — для поиска и систематизации источников, сверки ссылок на нормативные акты, редактуры и подготовки макета. Правовые позиции, оценки перспектив и практические выводы принадлежат автору и проверены им. Ответственность за изложенное несёт автор.

Законодательство приведено по состоянию на 4 сентября 2026 года. Правовая рамка обновилась 1 сентября 2026 года с вступлением в силу Федерального закона № 282-ФЗ «О цифровых валютах и цифровых правах»; практики его применения на момент подготовки книги не существует. Там, где ответа нет, автор приводит собственную позицию и обозначает её как позицию. Отдельные положения закона вступают в силу в 2027–2028 годах — соответствующие даты указаны в тексте. Перед подачей любого процессуального документа сверяйте действующую редакцию.

Ещё пять лет назад вопрос «а есть ли у оппонента криптовалюта?» звучал в зале суда как экзотика. Сегодня криптоактивы всплывают в делах о разводе, банкротстве, корпоративных конфликтах еженедельно. Суды признали крипту имуществом.

Но методологии её обнаружения, доказывания и взыскания не существовало — ни в законе, ни в учебниках, ни в статьях юридических фирм.

Эта книга заполняет пробел.

Она написана практиком для практиков. Здесь нет пересказов Википедии о том, как работает блокчейн. Здесь есть конкретные алгоритмы: как найти крипту, если противник молчит; как доказать, что она принадлежит именно ему; как арестовать, продать, взыскать; как договориться, не доводя до суда.

Книга построена вокруг трёх сквозных кейсов, которые проходят через все главы:

Кейс № 1 — развод Елены и Сергея К. (семейный спор).

Кейс № 2 — банкротство ИП Романа Т. (банкротное дело).

Кейс № 3 — корпоративный конфликт «КриптоВолна» (корпоративный спор).

Каждый кейс начинается с подозрения и заканчивается результатом. Вы видите не теорию, а живой процесс: разведку, структуры, доказывание, взыскание, переговоры.

Книга разделена на пять частей:

Часть I. Разведка — как найти криптоактивы, если противник молчит. Банковские следы, устройства, переписка, свидетели, ончейн-анализ.

Часть II. Соккрытие через структуры — как противник прячет активы через прямое владение, трасты, офшоры, мультисиги, DAO, миксеры. И как это вскрыть.

Часть III. Доказывание — как превратить найденные активы в доказательства для суда. Процессуальное закрепление, специфика семейных, банкротных и корпоративных дел.

Часть IV. Взыскание и исполнение — как арестовать, продать, передать, взыскать. Работа с ФССП, трансграничное исполнение.

Часть V. Практика и инструменты — переговоры, мировые соглашения, этика, риски, границы допустимого поведения.

Эта книга не заменит профессионального обучения. Но она даст вам карту местности. Вы будете знать, куда смотреть, что запрашивать, как формулировать ходатайства, какие доказательства приобщать, когда договариваться, а когда идти в суд.

Криптоактивы — это не экзотика. Это новая реальность имущественных споров. И в этой реальности выиграет тот, кто умеет работать с технологиями, не нарушая закон.

Начнём.

* * *

Часть I. Разведка

Глава 1. Что лежит на столе: криптоактив как предмет спора

* * *

В производстве мирового судьи участка № 318 лежит дело о расторжении брака и разделе совместно нажитого имущества. Ответчик — Сергей К., 46 лет, предприниматель. В отзыве на иск одна строчка, от которой у адвоката истицы, Елены К., всё сжимается: «В 2020–2021 годах приобретал цифровую валюту, однако в 2022 году продал её по цене ниже рыночной в связи с обвалом рынка. Денежные средства израсходованы на нужды семьи. Иных активов, подлежащих разделу, не имеется». Елена помнит, как муж сидел по ночам в телефоне, как в 2021-м говорил: «Мы теперь не бедные». Помнит переводы по 300–500 тысяч на карту, привязанную к какой-то бирже. Но ни названия биржи, ни суммы, ни документов. Судья смотрит на адвоката Елены и спрашивает: «Истец, вы настаиваете на запросе? Куда именно?» Адвокат молчит три секунды. В этих трёх секундах — вся эта книга.

* * *

1.1. Зачем юристу эта книга именно сейчас

Ещё пять лет назад вопрос «а есть ли у оппонента криптовалюта?» звучал в зале суда как экзотика. Судья поднимал бровь, адвокат противной стороны пожимал плечами, а само слово «биткоин» произносилось с интонацией человека, говорящего о коллекционных марках или монгольских тугриках.

Сегодня ситуация другая. Точной доли владельцев не знает никто: обследования дают расхождение в разы, поскольку одни считают тех, кто владеет активом сейчас, другие — тех, кто когда-либо совершал операции, третьи оценивают по косвенным признакам. Социологические опросы последних лет дают несколько процентов взрослого населения; оценки, построенные на данных площадок, — величины кратно большие. Банк России публикует не долю владельцев, а объёмы потоков и веб-трафик, и они устойчиво растут.

Для практики точная цифра и не нужна. Достаточно того, что криптоактив перестал быть редкостью в делах определённой категории: там, где у стороны есть свободные средства и техническая грамотность, вероятность встретить его в споре стала заметной. В делах о расторжении брака, в процедурах банкротства физических и юридических лиц, в корпоративных конфликтах криптоактивы всплывают еженедельно — не как курьёз, а как регулярная позиция в описи имущества или как подозрение, которое невозможно проверить стандартными средствами.

При этом суды уже признали: криптовалюта — это имущество. Отправной точкой стало дело Ильи Царькова: постановлением Девятого арбитражного апелляционного суда от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017 содержимое криптокошелька должника включено в конкурсную массу. За ним последовала линия арбитражной практики. Арбитражные суды включают биткоины в конкурсную массу. Районные суды делят эфириум при разводе.

Казалось бы, правовая рамка есть.

Но рамка — это не методология. Суд признал крипту имуществом. А дальше что? Куда направить запрос? Как доказать, что кошелёк принадлежит именно ответчику? Что делать, если актив выведен через миксер или спрятан в трасте на Британских Виргинских Островах? Как арестовать то, чего нет ни в одном реестре имущества?

На эти вопросы нет ни одного системного ответа — ни в законе, ни в разъяснениях, ни в учебниках.

Есть разрозненные статьи юридических фирм, где на двух страницах пересказывается общеизвестное: «запросите данные у биржи», «назначьте экспертизу». Но между «запросите» и реальным ответом биржи с Сейшельских островов лежит пропасть, которую ни одна статья не закрывает.

Эта книга — попытка закрыть. Она написана для практикующего юриста, который завтра идёт в заседание и ему нужен алгоритм, а не лекция по криптографии.

Три тезиса, на которых строится всё дальнейшее:

Первый. Криптоактив невидим для стандартных инструментов обнаружения имущества. Запрос в ФНС, Росреестр, ГИБДД, ПФР не даст ничего. Актив существует, но в правовом поле вашего дела его как бы нет — пока вы не докажете обратное.

Одна оговорка, без которой утверждение станет неточным. Реестр в этой сфере есть, но это реестр не активов, а посредников: Банк России ведёт перечень лицензированных участников, а цифровые депозитарии администрируют адреса и знают их владельцев. Актив, прошедший через этот контур, обнаружим по запросу (раздел 3.8).

Актив, который туда не заходил, не значится нигде. А тот, кто решил спрятать, в контур и не пойдёт: он для того и создан, чтобы владельца было видно.

Второй. Бремя доказывания наличия криптоактивов лежит на той стороне, которая на них ссылается. Если ваш клиент говорит: «У него точно есть биткоины», — суд ответит: «Докажите». И это бремя не снимается ни одним ходатайством об истребовании, если вы не знаете, *куда именно* истребовать.

Третий. Противник, который прячет криптоактивы, находится в структурном преимуществе. У него нет обязанности их декларировать (в большинстве случаев). У него нет реестровой записи, которую можно арестовать. У него есть время, анонимность и множество способов усложнить трассировку.

Книга даёт инструмент, чтобы это преимущество сломать.

* * *

1.2. Таксономия: что именно ищем

Прежде чем искать, нужно понять, что искать. Криптоактив для юриста — не технологическое понятие, а процессуальное. Нас интересует не хеш-функция и не консенсусный алгоритм, а ответ на три вопроса: *где лежит, кто контролирует, можно ли достать*.

По этим трём осям выстроена таблица, к которой вы будете возвращаться в каждой последующей главе.

Монеты в прямом владении (холодный кошелёк). Примеры — BTC, ETH на Ledger, Trezor, бумажном носителе; Где лежит — Устройство, сейф, голова владельца; Кто контролирует — Только владелец (ключи); Обнаружимость — Крайне низкая; Правовой статус в РФ — Имущество (ст. 128 ГК).

Монеты на централизованной бирже. Примеры — Счёт на Binance, Bybit, OKX, HTX; Где лежит — Серверы биржи; Кто контролирует — Биржа (кастодиан); Обнаружимость — Средняя: есть юрилицо, есть KYC; Правовой статус в РФ — Имущество; зависит от юрисдикции биржи.

Стейблкоины. Примеры — USDT (Tether), USDC; Где лежит — Кошелёк или биржа; Кто контролирует — Владелец / биржа; Обнаружимость — Средняя; Правовой статус в РФ — Спорный; на практике — имущество.

Токенизированные реальные активы. Примеры — Токены на недвижимость, золото, акции; Где лежит — Платформа-эмитент; Кто контролирует — Эмитент / смарт-контракт; Обнаружимость — Средняя; Правовой статус в РФ — цифровые права по ФЗ-282 либо иное имущество.

DeFi-позиции: стейкинг, лендинг, пулы ликвидности. Примеры — Lido, Aave, Uniswap, Curve; Где лежит — Смарт-контракт в блокчейне; Кто контролирует — Никто единолично; протокол децентрализован; Обнаружимость — Низкая; Правовой статус в РФ — Не урегулировано.

NFT. Примеры — Токены на OpenSea, Rarible, маркетплейсы; Где лежит — Кошелёк владельца; Кто контролирует — Владелец (ключи); Обнаружимость — Низкая; Правовой статус в РФ — Имущество / цифровое право.

Активы в частных структурах. Примеры — Траст, мультисиг-кошелёк, DAO, офшорный SPV; Где лежит — Зависит от структуры; Кто контролирует — Номинал, совет, смарт-контракт; Обнаружимость — Очень низкая; Правовой статус в РФ — Зависит от оболочки.

Монеты после миксера / бриджа. Примеры — Пропущенные через Tornado Cash, THORChain, Wormhole; Где лежит — Размыты по блокчейну; Кто контролирует — Формально — владелец, фактически — не установлены; Обнаружимость — Крайне низкая; Правовой статус в РФ — Имущество, но трассировка затруднена.

Два вывода из этой таблицы, которые нужно зафиксировать сразу.

Вывод первый. Чем дальше актив от централизованной биржи с процедурой KYC (Know Your Customer — процедура идентификации клиента) и ближе к децентрализованному протоколу, холодному кошельку или миксеру, тем сложнее его обнаружить и тем дороже обойдётся доказывание. Запрос на биржу может стоить ноль рублей и две недели ожидания. Расследование цепочки через миксер — десятки тысяч долларов и месяцы работы ончейн-аналитика. Книга ведёт от простого к сложному, но не обманывайте себя: противник, который знает, что его ищут, будет двигаться вниз по этой таблице.

Вывод второй. Правовой статус криптоактива в России — «имущество». Этого достаточно для раздела, для включения в конкурсную массу, для обращения взыскания. Не нужно доказывать суду, что биткоин — это «вещь» или «право требования». Достаточно сослаться

на статью 128 ГК РФ и позицию Верховного Суда. Проблема не в квалификации. Проблема в обнаружении и доказывании принадлежности.

* * *

1.3. Правовой статус: что говорит закон

Этот параграф — не академический обзор. Это рабочий минимум, который вы вставите в ходатайство, исковое заявление или апелляционную жалобу.

Оговорка о времени. Правовая рамка в этой области меняется быстрее, чем выходят книги. Основной массив действующего регулирования применяется с сентября 2026 года, судебной практики по нему пока нет, а часть норм вступает в силу в 2027–2028 годах. Там, где ответа не существует, я привожу собственную позицию и помечаю её как позицию. Проверяйте актуальность перед подачей любого документа.

Основной закон

Оборот цифровой валюты в России регулируется Федеральным законом от 4 августа 2026 г. № 282-ФЗ «О цифровых валютах и цифровых правах» и сопутствующим ему Федеральным законом № 283-ФЗ. Это первый комплексный акт в этой сфере — около 290 страниц.

Параллельно доживает свой срок Федеральный закон № 259-ФЗ: он утрачивает силу частями, окончательно — с 1 сентября 2028 года. Практическое следствие: в процессуальных документах указывайте, на какую дату вы ссылаетесь, иначе оппоненту будет за что зацепиться.

Для имущественного спора устройство регулирования сводится к двум вещам. В вашу пользу: цифровая валюта прямо названа имуществом, и доказывать это не требуется. В сторону осторожности: законный оборот замкнут на контур лицензированных посредников, и что суд скажет об активе за пределами этого контура, пока неизвестно.

Статус актива

Цифровая валюта по Закону № 282-ФЗ — имущество в виде совокупности электронных данных в информационной системе, которое может использоваться как инвестиция или средство платежа. При этом она не является рублём, иностранной валютой или международной денежной либо расчётной единицей.

Формулировка «имущество» стоит прямо в законе. Это снимает необходимость выводить статус актива через ст. 128 ГК и судебную практику, как приходилось делать раньше. В процессуальных документах теперь достаточно ссылки на закон.

Дополнительно статус подтверждён с двух других сторон:

-

Налоговое право.

Федеральный закон от 29.11.2024 № 418-ФЗ признал цифровую валюту, в том числе полученную в результате майнинга, имуществом для целей налогообложения. Доход от продажи облагается по общей ставке для физических лиц.

-

Уголовное право.

С марта 2026 года цифровая валюта имеет статус имущества и в уголовно-правовом смысле, что делает возможным её арест и конфискацию. Практическое значение этого для взыскания разобрано в разделе 14.7.

Судебная защита: снятая ловушка

До 2026 года в Законе № 259-ФЗ содержалось условие, о котором многие юристы узнавали слишком поздно: требования, связанные с владением цифровой валютой, подлежали судебной защите только при условии, что владелец проинформировал о ней налоговый орган. При этом самого механизма такого информирования не существовало.

Постановление Конституционного Суда РФ от 20 января 2026 г. № 2-П (по жалобе гражданина Тимченко) разрешило эту коллизию, но не так, как принято пересказывать. Норму целиком неконституционной суд не признал.

Разграничение проведено по способу получения актива:

-

Для тех, кто получил цифровую валюту в результате майнинга,

требование об информировании признано соответствующим Конституции: для этой категории механизм передачи сведений в налоговый орган существует. Работает он по двум каналам — оператор майнинговой инфраструктуры обязан сообщать сведения о лице, которому оказывает услуги (ст. 86.5 НК РФ), и сам майнер сообщает сведения о полученной валюте и об адресе-идентификаторе (ч. 11 ст. 3 Закона № 282-ФЗ).

-

Для тех, кто приобрёл её иными способами,

установленного порядка уведомления не существует, а потому впредь до внесения изменений действующее регулирование не может считаться препятствующим судебной защите.

И здесь ключевое условие, которое чаще всего опускают в пересказах. Защита предоставляется, если в суд представлены сведения, подтверждающие, что цифровая валюта получена и использовалась на допустимых законом основаниях.

Практический вывод: возражение «истец не декларировал актив, следовательно, требование не подлежит судебной защите» само по себе больше не работает. Но оно превращается в другое, более трудное для вас: «истец не доказал законность приобретения актива». Готовьте цепочку происхождения средств заранее — банковскую выписку, источник дохода, документы о приобретении.

По делам, где ваш доверитель майнил, проверяйте отдельно, исполнялась ли обязанность по ст. 86.5 НК РФ: для него послабление КС не действует.

Позиция автора. Обязанность информировать налоговые органы об операциях с цифровой валютой в зарубежных информационных системах вводится для физических лиц — резидентов со 2 мая 2027 года. Я исхожу из того, что после появления работающего механизма законодатель попытается вернуть условие о судебной защите в том или ином виде. Если это произойдёт, ловушка вернётся, но уже с реальной возможностью её избежать. Следите за этим сроком: он важнее, чем кажется, и для ваших доверителей, и для оценки перспектив спора.

Что запрещено, а что нет

Начну с того, что запрета нет, потому что именно этот вопрос задаёт доверитель первым.

Владеть криптоактивом можно. Приобретать, хранить, продавать, дарить, передавать по наследству — всё это закон не ограничивает. Для имущественного спора вывод простой: предмет спора существует, он законен, и защищать в суде вы будете правомерный интерес, а не сомнительный.

Запрет касается другого — использования актива в качестве денег внутри страны. Расплатиться криптовалютой за товар, работу, услугу или результат интеллектуальной деятельности нельзя, и формулировка закона охватывает не только прямую оплату, но и любой способ, из которого следует, что расчёт производится именно так (ч. 6 ст. 1).

Из этого правила закон делает четыре изъятия, и перечень исчерпывающий: внешнеторговые расчёты резидента с нерезидентом; получение валюты за майнинг, включая вознаграждение участника пула; уплата комиссий сети, без которых транзакция технически невозможна; приобретение за цифровую валюту ценных бумаг, других цифровых валют либо цифровых прав (ч. 7 ст. 1).

Третье изъятие стоит запомнить отдельно. Комиссия сети — не расчёт по сделке, а плата за саму возможность провести операцию, и попытка оппонента подвести под запрет любое движение средств этим изъятием снимается.

Запрет на распространение сведений. К запрету расчётов примыкает норма, о которой чаще забывают: распространять информацию об использовании цифровой валюты как средства платежа тоже нельзя, и реклама здесь лишь частный случай (ч. 9 ст. 1). Применительно к тем же четырём изъятиям запрет не действует (ч. 10).

Для практикующего юриста это ближе, чем кажется. Публикация, объясняющая, как принимать оплату криптовалютой, подпадает под норму независимо от того, оказывались ли услуги фактически.

Отдельно — содействие обходу. Часть 2 статьи 30 запрещает помогать резидентам совершать сделки в нарушение закона, и в перечень запрещённого прямо включены информирование о способах их совершения и предоставление программных средств.

Эта норма уже работает, тогда как обязанность проводить сделки через лицензированных посредников отложена до 1 июля 2027 года. Для юриста, который консультирует, пишет и ведёт публичные каналы, из всего закона это положение самое чувствительное. Разбор — в разделе 19.5.

И одно полномочие на будущее. Правительство по согласованию с Банком России и органом безопасности вправе установить особый режим, отличающийся от общего (ч. 18 ст. 1). Отслеживайте: именно так, вероятнее всего, будут вводиться исключения для отдельных отраслей.

Контур законного оборота

Закон вводит несколько видов лицензированных участников рынка. Как устроена их деятельность, для розыска активов почти безразлично. Важно одно: это юридические лица под надзором, у которых есть обязанности перед клиентом и перед регулятором. **Значит, им можно направить запрос и рассчитывать на ответ.**

Участник

Функция

Что у него можно запросить

Организатор торговли

Организация сделок

Сведения о сделках участника

Брокер

Исполнение поручений клиентов

Идентификация клиента, история поручений

Управляющий

Доверительное управление

Состав и стоимость переданного имущества

Цифровой депозитарий

Учёт цифровых валют и прав, **доступ к адресам-идентификаторам**

Принадлежность адреса, остатки, история

Обменная организация

Обмен цифровых валют

Данные клиента, операции обмена

Строка про цифровой депозитарий — самая важная в этой таблице и, возможно, во всей главе.

Существует лицензированное лицо, которое администрирует адреса и знает, кому они принадлежат. Глава 2 этой книги построена на том, что адрес анонимен и связь с личностью устанавливается косвенно. Внутри регулируемого контура эта задача косвенной быть перестаёт — единственное место во всей методике, где короткий путь существует.

Переход растянут во времени, и до 1 июля 2027 года обменные сервисы вправе работать, не входя в реестр Банка России. После этой даты картина меняется дважды: сделки резидентов должны идти через участников реестра, а банк обязан отказать в переводе, если получатель организует оборот цифровой валюты, не имея на то полномочий.

Второй элемент для нас интереснее первого. Отказ фиксируется, а зафиксированный отказ — это след, о работе с которым речь в разделе 3.8.

Позиция автора о том, что это значит для розыска активов. Я ожидаю расслоения рынка на два контура. В регулируемом контуре розыск станет проще банковского: у депозитария есть и адрес, и личность, и история, и обязанность отвечать. В нерегулируемом всё останется как описано в этой книге, и именно туда уйдут те, кто прячет. То есть регулирование

не отменяет методику этой книги, а очерчивает область её применения: дела, где противник прячется намеренно. А это и есть те дела, ради которых книга написана.

Открытые вопросы: где я даю свой ответ

Практики нет. Ниже — вопросы, которые возникнут у вас в первом же деле, и мои ответы на них. Это позиция, а не разъяснение закона; используйте как отправную точку для собственной аргументации, а не как ссылку.

Первый. Остаётся ли имуществом актив на адресе, не администрируемом цифровым депозитарием, после 1 июля 2027 года?

Да, остаётся, и это следует не из общих соображений, а из текста закона.

Определение цифровой валюты (п. 1 ч. 1 ст. 2) построено на природе актива, а не на способе хранения: имущество в виде совокупности электронных данных, содержащихся в информационной системе. Оговорки о нахождении в регулируемом контуре в нём нет.

Дальше существеннее. Требование совершать сделки через лицензированных посредников относится к **обращению** цифровых валют, а это понятие закон определяет узко (п. 3 ч. 1 ст. 2). Обращением признаются сделки, влекущие переход валюты от одного обладателя к другому, совершаемые с участием субъекта национальной платёжной системы либо предусматривающие встречное предоставление в виде денежных средств, ценных бумаг, цифровых валют и цифровых прав на цифровых счетах и **на адресах-идентификаторах, администрируемых цифровыми депозитариями**, либо иного имущества на территории России.

Перечень закрытый. Сделка, встречным предоставлением по которой выступает цифровая валюта на адресе, депозитарием не администрируемом, под определение обращения не подпадает, а значит, и требование о посреднике к ней не относится.

Практическое следствие: требование о разделе или о включении в конкурсную массу актива, лежащего на самостоятельно контролируемом адресе, заявляется на общих основаниях. На возражение «актив находится вне законного оборота» отвечайте пунктом 3 части 1 статьи 2: вне регулируемого обращения не значит вне права.

Второй. Влияет ли нарушение оппонентом порядка приобретения на возможность взыскания в вашу пользу?

Моя позиция: не влияет и не должно.

Иное означало бы, что нарушитель извлекает преимущество из собственного нарушения — прямо вопреки ст. 10 ГК. Более того, я ожидаю, что сам факт приобретения актива в обход установленного порядка станет самостоятельным доводом о недобросовестности, полезным при постановке вопроса об отступлении от равенства долей (раздел 10.6) и о неосвобождении от обязательств (раздел 11.5).

Третий. Что с активами, приобретёнными до 1 сентября 2026 года?

Моя позиция: они не становятся незаконными. Обратная сила ухудшающих норм — исключение, требующее прямого указания. Но их дальнейший оборот подчиняется новым правилам, и это создаёт практическую проблему для взыскания в натуре: передать актив по решению суда после 1 июля 2027 года, минуя регулируемый контур, будет затруднительно.

Практическое следствие, и оно существенное: **конструкция «передать в натуре, при неисполнении — денежный эквивалент» из главы 15 приобретает дополнительное обоснование**. Денежная компенсация, которую я и раньше рекомендовал как вариант по умолчанию, становится ещё предпочтительнее.

Четвёртый. Где граница между разъяснением закона доверителю и запрещённым информированием о способах обхода?

Самый неприятный вопрос, и он адресован лично вам. Моя позиция изложена в разделе 19.5; коротко: разъяснение содержания и последствий нормы — профессиональная обязанность и не может быть запрещено, а описание конкретного порядка действий, позволяющего требования не соблюсти, находится по другую сторону границы.

Практики нет, формулировка закона широкая, и до появления первых дел я рекомендую держаться от границы дальше, чем кажется необходимым.

Что ещё осталось из прежней рамки

Нормы, действующие независимо от специального регулирования и применяемые вами в каждом деле.

Семейный кодекс, статьи 34–39. Актив, приобретённый в период брака за счёт общих средств, — совместная собственность. Не имеет значения, на чьё имя открыт аккаунт и в какой юрисдикции. Значение имеют источник средств и момент приобретения.

Закон о банкротстве, статья 213.25. В конкурсную массу включается всё имущество должника. Практика начиная с дела Царькова (постановление Девятого ААС от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017) исходит из обязанности управляющего разыскивать и включать в массу цифровые активы. Отдельного разъяснения Верховного Суда по криптоактивам в банкротстве нет; ссылайтесь на акты арбитражных судов своего округа, проверенные по картотеке.

Майнинг. Легализован Федеральным законом от 08.08.2024 № 221-ФЗ с 1 ноября 2024 года. Действуют региональные ограничения, установленные постановлениями Правительства и продлённые до 2032 года в ряде регионов. Для имущественного спора значимо одно: доход от майнинга — имущество, и он подлежит разделу и включению в массу наравне с приобретённым активом.

Международная рамка

Один абзац, чтобы снять страх «а вдруг в другой стране это не имущество».

•

Европейский союз.

Регламент MiCA (Regulation 2023/1114) устанавливает единый режим для криптоактивов. Директива DAC8 вводит автоматический обмен информацией между налоговыми органами стран ЕС. Биржа, работающая в ЕС, обязана раскрывать данные по запросу компетентного органа.

•

Великобритания.

Практика с 2019 года устойчиво признаёт криптоактивы имуществом (

AA v Persons Unknown

[2019] EWHC 3556 (Comm);

Ion Science Ltd v Persons Unknown

, решение судьи Батчера от 21.12.2020, официально не опубликовано).

•

США.

Квалификация зависит от регулятора: для SEC это может быть security, для CFTC — commodity, для IRS — property. В имущественных спорах применяется режим property.

•

ОАЭ, Сингапур, Швейцария.

Лицензионные режимы, биржи обязаны хранить данные клиентов и отвечать на запросы регуляторов.

•

Беларусь.

Криптовалюта легализована с 2017 года Декретом Президента № 8, оборот сосредоточен в контуре Парка высоких технологий, площадки идентифицируют клиентов. Для российского юриста это самая достигаемая из зарубежных юрисдикций — подробно в разделе 16.7.

Практический вывод: в подавляющем большинстве юрисдикций криптоактив — имущество. Проблема не в правовом статусе. Проблема в том, чтобы найти его и доказать принадлежность конкретному лицу. Этим занимается вся остальная книга.

Врезка. Формулировка для искового заявления или ходатайства

«Цифровая валюта в силу прямого указания Федерального закона от 04.08.2026 № 282-ФЗ «О цифровых валютах и цифровых правах» является имуществом. Требования, связанные с владением цифровой валютой, подлежат судебной защите. Согласно Постановлению Конституционного Суда РФ от 20.01.2026 № 2-П, в отношении лиц, приобретших цифровую валюту способами, не связанными с майнингом, действующее регулирование не может считаться препятствующим судебной защите при представлении сведений, подтверждающих, что актив получен и использовался на допустимых законом основаниях. Такие сведения представлены в материалы дела [перечислить].

На основании ст. 128 ГК РФ, ст. 34 СК РФ (вариант: ст. 213.25 Федерального закона «О несостоятельности (банкротстве)») прошу признать, что цифровая валюта [наименование, при возможности — адрес кошелька либо идентификатор аккаунта] является имуществом, подлежащим разделу / включению в конкурсную массу / обращению взыскания.

В целях установления факта наличия и объёма указанных активов прошу направить запрос в [цифровую депозитарий / обменную организацию / оператора].»

1.4. Почему крипто сложно найти: анатомия невидимости

Стандартный имущественный спор построен на реестрах.

Квартира — в Росреестре. Автомобиль — в ГИБДД. Доля в ООО — в ЕГРЮЛ. Счёт в банке — в ФНС через запрос по ИНН. Криптоактив внутри регулируемого контура — у цифрового депозитария. Криптоактив вне его — нигде. Акции — у депозитария. Пенсия — в ПФР. Юрист привык к парадигме: *есть объект → есть реестр → есть запрос → есть ответ*.

С криптоактивом эта парадигма рассыпается. Четыре причины, по которым стандартный инструментариум бессилен:

Первая. Реестра владельцев нет. Не существует государственного реестра, в котором записано: «Адресу 0x7a3f...b21e принадлежит Иван Петров, 1983 г. р., ИНН такой-то». Блокчейн фиксирует транзакции между адресами, но не идентифицирует владельцев. Адрес — строка из 42 символов, и без привязки к внешнему миру она анонимна.

Исключение одно, и оно узкое. Цифровой депозитарий администрирует адреса и знает их владельцев, поэтому запрос к нему на такой вопрос ответ дать может. Но только по тому, что заходило в регулируемый контур. Запрос в ФНС, Росреестр или МВД не вернёт ответ «у данного лица есть кошелек с 47 биткоинами» ни при каких обстоятельствах.

Вторая. Нет посредника. Банковский счёт можно арестовать одним определением суда, направленным в банк. Недвижимость — запретом регистрационных действий. А холодный кошелек — это флешка в кармане пиджака, стальная пластина в сейфе или 24 слова, выученные наизусть. Нет юрлица, которому можно направить предписание. Нет кнопки «заморозить». Есть только сам владелец и его ключи.

Третья. Псевдонимность и множественность. Один человек может создать неограниченное число кошельков за секунды, без регистрации, без паспорта, без привязки к личности. Он может разбить актив на десять кошельков, отправить часть на децентрализованную биржу, часть — в стейкинг, часть — через мост в другой блокчейн. Каждая операция добавляет слой, за которым всё сложнее разглядеть связь с конкретным человеком.

Четвёртая. Трансграничность. Биржа может быть зарегистрирована на Сейшельских Островах, серверы — в Сингапуре, домен — в зоне .io, а поддержка отвечать из Дубая. С какой юрисдикцией вы будете взаимодействовать? Есть ли договор о правовой помощи? Признается ли ваш судебный запрос? На практике запрос российского суда на биржу, зарегистрированную в офшоре, чаще всего остаётся без ответа. Не потому что биржа злая. Потому что у неё нет юридической обязанности отвечать на запрос иностранного суда, не подкреплённый международным договором.

Совокупность этих четырёх факторов создаёт ситуацию, в которой противник, желающий скрыть актив, тратит на это часы. А юрист, желающий его найти, — недели и месяцы. Асимметрия колоссальная.

Но она не абсолютна. В каждой из четырёх причин есть уязвимость. У адреса есть история транзакций, которая публична. У кошелька есть точки входа и выхода — моменты конвертации в фиат, привязанные к бирже с KYC. У псевдонимности есть границы: человек оставляет цифровые следы в мессенджерах, почте, социальных сетях.

У трансграничности есть обходные пути: запрос через международную правовую помощь, через регулятора юрисдикции биржи, через косвенные данные.

Методология поиска строится на эксплуатации этих уязвимостей. Этому посвящены главы 2–4.

* * *

1.5. Что уже есть в арсенале юриста, и чего не хватает

Будем честны: у практикующего юриста в России есть инструменты, которые формально применимы и к криптоактивам. Проблема в том, что они спроектированы для другого мира.

Что есть:

-

Ходатайство об истребовании доказательств

(ст. 57 ГПК РФ, ст. 66 АПК РФ). Работает, если вы знаете, у кого истребовать. «Прошу истребовать у ПАО “Сбербанк”...» — работает. «Прошу истребовать у лица, управляющего кошельком 0x7a3f...b21e...» — не работает, потому что суд не знает, кому направить запрос.

-

Адвокатский запрос

(ст. 6.1 ФЗ «Об адвокатской деятельности и адвокатуре»). Направляется бирже, если вы знаете, какой. Биржа может ответить, может не ответить. Обязанности отвечать у неё нет, если она не в российской юрисдикции.

-

Обеспечительные меры

(ст. 139–140 ГПК, ст. 91–92 АПК). Арест имущества. Применимы к криптоактивам в теории. На практике: суд не может арестовать то, что не может идентифицировать. Если вы не укажете конкретный адрес кошелька или аккаунт на бирже, определение об аресте будет неисполнимым.

-

Судебная экспертиза

. Можно назначить экспертизу для анализа транзакций в блокчейне. Но нужно сначала получить эти транзакции и поставить эксперту правильные вопросы.

-

Объяснения сторон, показания свидетелей

. Работают как вспомогательный инструмент: «Я видела, как он покупал биткоины», «Он говорил мне, что у него есть кошелёк». Но как самостоятельное доказательство — слабы.

Чего не хватает:

- Понимания,

куда именно

направлять запрос. Какие биржи работают с клиентами из РФ, где они зарегистрированы, как сформулировать запрос, чтобы его не проигнорировали.

- Методики работы с ончейн-данными как доказательством. Как извлечь историю транзакций, как заверить, как представить суду, чтобы это не выглядело распечаткой с неизвестного сайта.

- Алгоритма действий при обнаружении миксера, мультисига, траста. Что делать, когда трассировка обрывается на Tornado Cash или на кошельке, подписанном тремя ключами из пяти.

- Знания о том, как исполнить решение, если актив на зарубежной платформе. Как физически передать биткоины взыскателю. Как оценить волатильный актив на дату исполнения.

Именно эти пробелы закрывают оставшиеся 17 глав. Книга построена как последовательный алгоритм: **разведка → структуры → доказывание → взыскание**. Каждый шаг опирается на предыдущий. Пропустить разведку и сразу просить суд арестовать кошелёк — всё равно что просить арестовать квартиру, не зная адреса.

* * *

1.6. Сквозной кейс № 1: вводная

С этого момента и до конца Части I нас будет сопровождать одно дело. Смоделированное, но типичное: обстоятельства собраны из того, что встречается в этой категории споров постоянно. Вы встретите его в главах 2, 3, 4, 10 и 16 — каждый раз на новой стадии.

Дело о разводе С.

Елена и Сергей К. состояли в браке 14 лет.

Сергей — владелец небольшой строительной компании. Елена не работала последние шесть лет, занималась детьми. В 2020 году Сергей начал «интересоваться инвестициями». Елена помнит: он купил ноутбук, поставил программу, по ночам сидел в телефоне. В 2021-м сказал: «Мы теперь не бедные. Я заработал больше, чем за три года в стройке». Показал экран телефона — цифры, графики. Елена не вникала.

В 2022-м начались конфликты. В 2024-м Елена подала на развод и раздел имущества. В ходе подготовки дела адвокат запросил у Сергея сведения обо всех активах. Сергей предоставил выписки по банковским счетам (три счёта, на всех — не больше 200 тысяч рублей), свидетельство о собственности на квартиру (приобретена до брака), ПТС на автомобиль. На вопрос о криптоактивах ответил: «Покупал биткоин в 2020-м и эфир в 2021-м. Вложил около двух миллионов. В 2022-м, когда рынок рухнул, продал с убытком. Осталось около трёхсот тысяч, потратил на жизнь. Больше ничего нет».

Документов, подтверждающих покупку и продажу, не предоставил. Название биржи не назвал. Сказал: «Не помню, всё делал через приложение, оно уже удалено».

Адвокат Елены знает: в 2021-м биткоин стоил 60 с лишним тысяч долларов.

Если Сергей действительно купил на два миллиона рублей и не продавал — на пике это могло быть 15–20 миллионов. А если он не продал, а перевёл на холодный кошелёк? А если купил не на два, а на десять миллионов? А если вывел через структуру, о которой жена не подозревала?

Вопросы, на которые предстоит ответить в следующих главах:

- Как проверить, была ли крипто, если ответчик отрицает?

(Глава 2: ончейн-анализ и косвенные данные.)

- Куда направить запрос, если неизвестно, какая биржа?

(Глава 3: оффчейн-разведка.)

- Что делать, если средства выведены на холодный кошелёк или через миксер?

(Главы 5–8: структуры.)

- Как оценить актив, если ответчик утверждает, что продал в убыток?

(Главы 10 и 14: доказывание и взыскание.)

Ответы придут по порядку. Пока зафиксируем: на этом этапе у адвоката Елены нет ничего, кроме устного утверждения и косвенных воспоминаний клиентки. Книга начинается именно отсюда — из точки, где нет ни адреса кошелька, ни названия биржи, ни документов. Из точки, в которой находится большинство ваших клиентов.

* * *

1.7. Как пользоваться этой книгой

Книга написана для трёх категорий юристов, и каждая может читать её по-разному.

Семейный юрист найдёт основное содержание в главах 1–4 (разведка), 10–12 (доказывание в гражданском процессе) и 17 (тактика переговоров). Корпоративные кейсы и детали банкротных процедур можно пропускать, хотя логика обнаружения структур универсальна.

Банкротный юрист будет работать с главами 1–3 (ввод и разведка), 5–9 (сокрытие через структуры — ядро книги), 13–16 (доказывание в арбитраже и взыскание). Семейные кейсы — для понимания логики, но не для прямого применения.

Корпоративный юрист сосредоточится на главах 1–2, 5–9 (структуры, мультисиги, DAO, офшорные оболочки) и 14–16 (арест и взыскание в арбитражном процессе).

Сквозные кейсы (их в книге три: развод, банкротство, корпоративный конфликт) можно читать как самостоятельные истории — они содержат все ключевые правовые решения в контексте. Прикладные шаблоны — ходатайства, запросы, чек-листы — вынесены в Приложения в конце книги, чтобы не разрывать нарратив.

Каждая глава самодостаточна: в ней есть минимум контекста, необходимый для понимания, даже если вы пропустили предыдущую. Но последовательное чтение даёт больше: методология наслаивается, и к главе 10 вы уже мыслите как ончейн-аналитик.

* * *

Вместо заключения

Вернёмся в зал суда. Судья спрашивает: «Куда направить запрос?» Адвокат Елены молчит.

К концу этой книги он не будет молчать. Он будет знать, что первым делом нужно проверить косвенные следы: банковские выписки на предмет переводов в адрес бирж, переписку в мессенджерах, историю браузера на устройствах, показания свидетелей. Он будет знать, как поставить вопрос перед судом так, чтобы получить определение об истребовании данных у конкретной биржи. Он будет знать, что делать, если биржа в офшоре и не отвечает.

Он будет знать, как читать ончейн-граф, если дело дойдёт до экспертизы.

Но это — следующая глава. А сейчас — закройте эту, откройте блокнот и запишите три вопроса, которые вы зададите клиенту на первой встрече, когда он скажет: «Мне кажется, у него есть крипта». Если вы не знаете, какие это три вопроса, — книга написана для вас.

* * *

Примечания

Данные о распространённости криптоактивов в РФ: опрос НАФИ (2024), аналитический доклад Банка России «Криптовалюты: тенденции и риски» (2025). Конкретные цифры варьируются в зависимости от методики; в тексте указан консервативный диапазон.

Дело Царькова: постановление Девятого арбитражного апелляционного суда от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017 (определение Арбитражного суда г. Москвы от 05.03.2018 отменено) — включение криптовалюты в конкурсную массу. Последующую практику сверять по kad.arbitr.ru.

Сводного разъяснения Верховного Суда по квалификации цифровой валюты как имущества на момент подготовки книги не издано.

Regulation (EU) 2023/1114 of the European Parliament and of the Council (MiCA).

Council Directive (EU) 2023/2226 (DAC8) — расширение автоматического обмена информацией на криптоактивы.

AA v Persons Unknown [2019] EWHC 3556 (Comm); *Ion Science Ltd v Persons Unknown* (Commercial Court, 21.12.2020, неопубликованное решение судьи Батчера).

Налоговый кодекс США, IRC § 1031 (исключена крипта с 2018), IRS Notice 2014-21.

* * *

Глава 2. Ончейн-анализ: что видно в блокчейне и как это превратить в доказательство

* * *

Адвокат Елена Морозова сидит напротив клиентки. Та протягивает телефон: «Вот, он мне это показывал. Говорил, что тут два миллиона». На экране — скриншот. Тёмный фон, зелёные и красные цифры, какой-то график. Ни названия приложения, ни логотипа, ни привязки к аккаунту. Елена смотрит на картинку и понимает: она не знает, что это. Биржевой терминал? Кошелёк? Скриншот из браузера? Она не знает, можно ли это приобщить к делу. Не знает, как заверить. Не знает, докажет ли это хоть что-нибудь. Клиентка смотрит на неё с надеждой. Елена говорит: «Давайте разберёмся». И не знает, с чего начать.

Эта глава — ответ на вопрос, с чего начать.

* * *

2.1. Что такое блокчейн глазами юриста

Забудьте всё, что вы слышали о майнинге, нодах и консенсусных алгоритмах. Для ваших целей блокчейн — это одна конкретная вещь: **публичный реестр транзакций, который невозможно подделать задним числом.**

Представьте банковскую выписку. В ней записано: кто, кому, сколько, когда. Выписка хранится в банке. Банк может её потерять, исказить, отказать в выдаче. Теперь представьте ту же выписку, но записанную одновременно на тысячах компьютеров по всему миру, защищённую криптографически так, что изменение одной строчки потребует переписывания всей последующей истории, а это вычислительно невозможно. Это блокчейн.

Что видно

Каждая транзакция в блокчейне содержит:

-

Адрес отправителя.

Строка из 34–62 символов в зависимости от сети. Пример для Bitcoin:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

. Пример для Ethereum:

0x7a3f...b21e

(полный адрес — 42 символа).

-

Адрес получателя.

Та же строка.

-

Сумма.

В базовых единицах сети (сатоши для Bitcoin, wei для Ethereum).

-

Дата и время.

С точностью до секунды.

-

Хеш транзакции.

Уникальный идентификатор — цифровая подпись конкретной операции. По хешу транзакцию можно найти в любом эксплорере и убедиться, что она существовала.

-

Комиссия.

Сколько заплатили за проведение операции.

Для смарт-контрактов (взаимодействие с децентрализованными протоколами) дополнительно видно: с каким контрактом взаимодействовали, какую функцию вызвали, сколько токенов внесли или вывели.

Чего не видно

Имени владельца. Адрес не привязан к ФИО, паспортным данным, ИНН. Адрес — это псевдоним. Один человек может создать тысячу адресов. Один адрес может использоваться несколькими людьми. Привязка адреса к конкретной личности появляется только через внешние данные: регистрацию на бирже с KYC (Know Your Customer — процедура идентификации клиента), переписку, показания свидетелей, данные устройства.

Что из этого следует для доказывания

Ончейн-данные доказывают **факт перемещения средств между адресами**. Они показывают: в такую-то дату с адреса А на адрес Б ушло столько-то монет. Это объективный, верифицируемый, неизменяемый факт.

Ончейн-данные **не доказывают принадлежность адреса конкретному лицу**. Этого в блокчейне нет. Принадлежность устанавливается отдельно — через данные биржи, переписку, показания, косвенные улики. Этому посвящена глава 3.

Аналогия, которую можно использовать в суде: блокчейн — это камера видеонаблюдения, установленная над дорогой, по которой перемещаются деньги. Камера сняла, как мешок переехал из точки А в точку Б. Запись точная, нестираемая, доступная всем. Но лиц на записи не видно. Чтобы связать мешок с конкретным человеком, нужны другие доказательства. Камера говорит «что» и «когда». Не говорит «кто».

Врезка. Три мифа о блокчейне, которые мешают юристу

Миф 1: «Блокчейн полностью анонимен». Нет. Он псевдонимен и при этом абсолютно прозрачен. Каждая транзакция видна любому. Задача аналитика — привязать псевдоним к личности. Это сложно, но не невозможно.

Миф 2: «Если крипто ушла на другой кошелёк, она потеряна навсегда». Нет. История транзакций сохраняется в блокчейне навечно. Даже если средства прошли через десять адресов, цепочку можно восстановить. Другое дело, что она может оборваться на миксере или наличном выводе, но это вопрос трассировки, а не исчезновения данных.

Миф 3: «Ончейн-данные нельзя подделать». Сами данные в блокчейне — нельзя. Но *интерпретацию* данных — можно исказить. Неподготовленный человек может неверно прочитать граф, перепутать адреса, не учесть миксер. Поэтому нужен квалифицированный аналитик или эксперт. И поэтому суду нужен не просто скриншот, а заключение с методологией.

* * *

2.2. Инструменты: от бесплатного эксплорера до профессиональной платформы

Юристу не нужно покупать лицензию на профессиональное аналитическое ПО за десятки тысяч долларов в год. Но ему нужно понимать, что существует на каждом из трёх уровней и какой инструмент на каком этапе применяется.

Уровень 1. Публичные эксплореры

Это бесплатные веб-сайты, которые позволяют любому человеку ввести адрес или хеш транзакции и увидеть все данные. Никакой регистрации, никаких платных подписок.

Основные эксплореры по сетям:

Сеть

Эксплорер(ы)

Что покажет

Bitcoin

Blockchain.com, Blockchair, Mempool.space

Баланс адреса, все входящие и исходящие транзакции, контрагенты, время

Ethereum и токены ERC-20

Etherscan.io

Аналогично + взаимодействие со смарт-контрактами

Solana

Solscan.io

Транзакции, токены, программы

Tron

Tronscan.org

Транзакции TRC-20 (популярен для USDT)

BNB Chain

BscScan.com

Транзакции в сети Binance Smart Chain

Что юрист может сделать сам, без аналитика:

- Если клиент называет адрес кошелька — ввести его в эксплорер и увидеть текущий баланс и историю операций. Это занимает тридцать секунд.

- Если клиент называет хеш транзакции — увидеть, откуда и куда ушли средства, в каком объёме.

- Увидеть, взаимодействовал ли адрес с известными протоколами: стейкинг (Lido, Rocket Pool), децентрализованные биржи (Uniswap, Curve), лендинг (Aave, Compound).

Практический совет. На первой встрече с клиентом, если он называет хотя бы один адрес или хеш, откройте эксплорер прямо при нём, на своём ноутбуке. Введите данные. Покажите цифры. Это превращает абстрактное «у него где-то есть крипта» в конкретный баланс на экране. Эффект для клиента огромный: он видит, что вы работаете не вслепую. Эффект для вас: вы сразу понимаете масштаб — там триста тысяч рублей или тридцать миллионов.

Чего нельзя делать на уровне эксплорера:

- Деанонимизировать владельца адреса. Эксплорер покажет транзакции, но не скажет, кому принадлежит адрес.

- Построить граф связей через цепочку из десяти и более промежуточных адресов. Вручную это нечитаемо.

- Отличить миксер от обычного кошелька, если вы не знаете заранее, как выглядит адрес миксера.
- Сделать отчёт, пригодный для суда. Скриншот с эксплорера — это начало, но не доказательство в полном смысле.

Уровень 2. Профессиональные аналитические платформы

Это платные сервисы с базами данных, в которых размечены миллионы адресов: какой принадлежит бирже, какой — миксеру, какой — санкционному лицу. Аналитик загружает адрес, и платформа автоматически строит граф, помечает узлы, показывает связи.

Платформа
Ключевые возможности
Когда применяется

Chainalysis Reactor / Investigations

Построение графов транзакций, автоматическая привязка адресов к биржам, миксерам, санкционным спискам. Стандарт индустрии.

Полноценное расследование; формирование заключения для экспертизы

Elliptic

Аналогично, с акцентом на санкционный скрининг и отчёты по конкретным схемам (миксеры, группа Lazarus)

Если в деле есть миксер или санкционный элемент

Crystal Intelligence

Платформа, выросшая из разработок Bitfury. Поддержка отчётности на нескольких языках, развитые базы по площадкам Восточной Европы

Когда нужен инструмент с разметкой площадок, работавших с российскими пользователями

Arkham Intelligence

Деанонимизация через открытые данные: привязка кошельков к фондам, биржам, публичным лицам

Быстрая первичная проверка: кому *может* принадлежать адрес

Nansen

Поведенческие метки кошельков: «кит», «сма́рт-мани», «бот», «долгосрочный держатель»

Понимание паттернов: адрес активного трейдера или «копилка»

Bubblemaps

Визуализация связей между кошельками в виде наглядного графа

Иллюстрация для суда; презентация клиенту

Ключевой тезис: вы не обязаны покупать лицензию. Ваша задача как юриста — знать, что эти инструменты существуют, понимать логику их работы и уметь поставить задачу тому, кто ими владеет: аналитику, эксперту, консалтинговой фирме.

Уровень 3. Расследователи и форензик-лаборатории

Когда трассировка сложная, уходит через миксеры, кросс-чейн мосты, приватные монеты или когда нужен отчёт, который выдержит перекрёстный допрос, — привлекают специалистов.

•

Частные ончейн-аналитики.

Работают на базе Chainalysis или Elliptic. Стоимость исследования: от 80 000 до 500 000 руб. в зависимости от сложности. Срок: от двух дней до нескольких недель.

•

Форензик-лаборатории при консалтинговых фирмах.

Комплексные расследования: ончейн + оффчейн + финансовая аналитика. Дорого (от 1 млн руб.), но для крупных дел — оправданно.

•

Судебные эксперты.

Аккредитованные специалисты, которые дают заключение по определению суда. Назначаются в рамках процесса. Результат — самый весомый с процессуальной точки зрения.

Когда привлекать: если сумма спора превышает стоимость расследования; если трассировка уходит через пять и более промежуточных адресов; если противная сторона будет оспаривать данные и нужен процессуально безупречный документ.

* * *

2.3. Методология: что делает аналитик и как читать его результат

Юрист не обязан строить граф сам. Но он обязан понимать, что происходит на каждом этапе, чтобы правильно поставить задачу и критически оценить результат.

Алгоритм трассировки

Шаг 1. Отправная точка. Аналитик получает то, что вы ему даёте: адрес кошелька, хеш транзакции, название биржи. Если у вас ничего нет — отправной точки нет, и аналитик не сможет начать. Сначала ищем точку входа через оффчейн-разведку (глава 3).

Шаг 2. Построение графа. Аналитик отслеживает, куда ушли средства с исходного адреса. Каждая транзакция — ветка. Если средства разделились на три адреса — три ветки. Если с каждого из них ушли дальше — граф растёт. Для простых случаев это 3–5 узлов. Для сложных — сотни.

Шаг 3. Маркировка узлов. Каждый адрес в графе получает метку из базы данных платформы: «биржа», «миксер Tornado Cash», «DEX Uniswap», «стейкинг Lido», «неизвестный кошелек». Метка вида «белорусский обменник, резидент ПБТ» встречается чаще, чем принято думать, и стоит дороже прочих: за ней стоит юридическое лицо, обязанное идентифицировать клиента. Метка — это не догадка аналитика, а результат сопоставления с базой из миллионов размеченных адресов.

Шаг 4. Поиск точек привязки. Ключевой момент. Аналитик ищет в графе узел, который привязан к личности. Это может быть: депозит на биржу с КИС, вывод с биржи на банковскую карту, взаимодействие с сервисом, требующим регистрации. В этом месте псевдоним превращается в имя.

Шаг 5. Фиксация результата. Аналитик формирует отчёт: граф, таблица транзакций, текстовые выводы. Если трассировка оборвалась — фиксирует, где именно и почему.

Что получает юрист на выходе

-

Визуальный граф.

Схема с узлами и стрелками. Можно приобщить к делу как иллюстрацию. Судья видит структуру, не вникая в хеши.

-

Таблицу транзакций.

Каждая строка: дата, хеш, адрес отправителя, адрес получателя, сумма, метка узла. Это основной доказательный документ.

-

Текстовое заключение.

Аналитик описывает, что обнаружено, каким методом, с какой степенью уверенности.

-

Перечень адресов для запросов.

Если в цепочке есть биржа — аналитик укажет, какая именно. Это основание для судебного запроса.

Чек-лист: как проверить результат аналитика

Прежде чем нести заключение в суд, проверьте:

- ☐ У каждой транзакции указан

хеш

. Без хеша данные не верифицируются. Любой человек может зайти в эксплорер, ввести хеш и убедиться, что транзакция существовала.

- ☐ Указана

сеть

(блокчейн). Не «где-то в крипте», а конкретно: сеть Ethereum, блок № 18 432 901, хеш 0x7f3a...

- ☐ Все узлы графа

помечены

. Если 7 из 10 адресов — «неизвестно», результат слабый и для суда недостаточный.

- ☐ Указана

степень уверенности

. Аналитик обязан разграничивать: «установлено», «с высокой вероятностью», «предположительно». Если всё написано как факт без оговорок — это некачественная работа.

- ☐ Зафиксированы

разрывы в цепочке

. Если трассировка оборвалась на миксере или наличном выводе — это указано прямо, с объяснением почему.

- ☐ Указаны

инструменты и версии баз данных

, использованные при анализе. Это нужно для воспроизводимости и для ответа на возражения.

* * *

2.4. Пределы ончейн-анализа: где трассировка обрывается

Это критически важный параграф. Юрист должен чётко понимать, в какой момент аналитика бессильна. Чтобы не тратить бюджет клиента впустую. Чтобы не обещать суду невозможного. Чтобы знать: обрыв трассировки — это не провал, а информация.

Пять ситуаций, в которых ончейн-трассировка заходит в туннель

Первая. Миксеры и сервисы CoinJoin. Tornado Cash, Wasabi Wallet, Samourai Wallet (последний прекратил работу после уголовного преследования его основателей в США). Принцип: сотни пользователей вносят монеты в общий пул, а выводят их с другого адреса. Связь между конкретным входом и конкретным выходом детерминированно не устанавливается. Аналитик может сказать: «Средства вошли в миксер такого-то числа в таком-то объёме». Дальше — по-разному, и разница техническая.

В протоколах на доказательствах с нулевым разглашением, к которым относится Tornado Cash, соответствие между конкретным входом и конкретным выходом не вычисляется в принципе: криптографическая конструкция построена именно на этом. Любая цифра вида «с вероятностью 78 % выходной адрес связан с входным» здесь недостоверна, и эксперт противной стороны это покажет.

В схемах объединения платежей (CoinJoin) анализ подмножеств может дать **множество адресов-кандидатов** при совпадении сумм и времени — но именно множество, а не установленное соответствие и не откалиброванный процент.

Требуя от аналитика формулировки в этих терминах. Заключение, содержащее конкретную вероятность связи входа с выходом, ослабляет вашу позицию сильнее, чем честное «установить соответствие не представляется возможным».

Вторая. Кросс-чейн мосты. Wormhole, THORChain, Stargate и аналогичные протоколы (состав действующих мостов быстро меняется: часть, включая Multichain, прекратила работу). Средства переходят из одного блокчейна в другой. Адрес в сети Ethereum и адрес в сети Solana — это разные сущности в разных реестрах. Связь между ними неочевидна и требует специализированных инструментов, которые есть не у каждого аналитика.

Третья. Наличный вывод через P2P. Крипта продаётся за наличные через P2P-площадку (LocalBitcoins в прошлом, аналоги в настоящем) или через офлайн-обменник без KYC. После конвертации в наличные цифровой след обрывается полностью. Монеты становятся деньгами в кармане.

Четвёртая. Холодный кошелёк без исходящих транзакций. Если средства лежат на адресе и никуда не двигались, история пуста. Граф строить не из чего. Адрес виден, баланс виден, но движения нет. Доказывать можно только факт наличия средств на дату, если есть основание полагать, что адрес принадлежит ответчику.

Пятая. Приватные монеты. Monero (XMR), Zcash в режиме shielded transactions. Блокчейн этих сетей не показывает ни отправителя, ни получателя, ни сумму. Трассировка невозможна в принципе. Если ответчик конвертировал биткоин в Monero и вывел — цифровой след обрывается.

Что делать, когда трассировка оборвалась

Обрыв — это не конец дела. Это смена инструмента.

Прежде чем строить на обрыве следа довод о недобросовестности, исключите безобидное объяснение: переход в сеть второго уровня выглядит в основном блокчейне так же, как исчезновение, но сокрытием не является (раздел 2.5). Проверьте это первым.

Во-первых, сам факт использования миксера или приватной монеты фиксируется. Аналитик пишет: «Такого-то числа средства в объёме 2,4 BTC были направлены на адрес, ассоциированный с миксером Tornado Cash». Это объективный факт.

Во-вторых, этот факт можно использовать в суде как косвенное доказательство намерения скрыть актив. Логика: законопослушный владелец не использует миксер. Миксер нужен тому, кто хочет разорвать связь между собой и средствами. Использование миксера в период имущественного спора или накануне него — свидетельство недобросовестности.

В-третьих, после обрыва ончейн-трассировки включается оффчейн-разведка: анализ устройств, переписки, показаний свидетелей, банковских операций. Об этом — глава 3.

Врезка. Что сказать суду, когда трассировка оборвалась

«Ончейн-анализ фиксирует, что [дата] средства в объёме [X монет] были направлены с адреса [A] на адрес, ассоциированный с сервисом смешивания [название]. Дальнейшая трассировка технически невозможна ввиду особенностей протокола. Сам факт использования миксера свидетельствует о целенаправленных действиях ответчика по сокрытию актива и подтверждает его недобросовестность. Прошу суд учесть данное обстоятельство при оценке поведения ответчика и распределении бремени доказывания».

* * *

2.5. Что нужно знать о технике, чтобы правильно ставить задачу

Три вещи, о которых юристы не спрашивают, а зря: из-за них аналитик даёт ответ не на тот вопрос, а оппонент получает возражение, к которому вы не готовы.

Две разные модели учёта

Биткоин и Ethereum устроены принципиально по-разному, и слово «адрес» означает в них не одно и то же.

Аккаунтная модель (Ethereum и большинство более новых сетей). У адреса есть баланс, как у банковского счёта. Пришло — прибавилось, ушло — убавилось. Адрес обычно используется долго, часто он единственный у человека. Читается просто: открыли эксплорер, увидели всю историю в одном месте.

Модель непотраченных выходов, UTXO (биткоин). Баланса как числа не существует. Есть «кусочки» полученных средств, и при трате кошелёк собирает из них нужную сумму, а остаток отправляет обратно — **на новый адрес сдачи**, который принадлежит тому же владельцу. Один кошелёк порождает десятки и сотни адресов.

Отсюда практические следствия, которые определяют постановку задачи.

Первое. В биткоине бессмысленно спрашивать «какой баланс на адресе ответчика». Правильный вопрос — какие адреса относятся к одному кошельку и каков совокупный остаток по ним.

Второе. Объединение адресов в один кошелёк делается по эвристикам, а не по достоверным данным. Основная — эвристика общего входа: если в одной транзакции несколько адресов выступили источниками одновременно, ими, вероятно, распоряжается одно лицо. Вторая — определение адреса сдачи. Обе дают вероятный, а не установленный результат, и в заключении это должно быть написано прямо.

Третье. Возражение оппонента «кластеризация не доказывает принадлежность» технически справедливо. Отвечать нужно не спором о методе, а совокупностью: кластер плюс извлечённый с устройства адрес плюс переписка плюс банковская выписка.

Сети второго уровня: где сегодня чаще всего обрывается след

Это самый частый практический разрыв в делах последних лет, и его регулярно принимают за использование миксера.

Сети второго уровня — Arbitrum, Optimism, Base, zkSync и подобные — работают поверх основной сети. Транзакции совершаются в них, а в основную сеть попадает лишь сжатый результат. Комиссия при этом составляет центы вместо десятков долларов, поэтому туда переместилась основная масса розничных операций.

Что видит юрист. Средства ушли с адреса в основной сети на контракт моста — и исчезли. В эксплорере основной сети дальше ничего нет.

Что произошло на самом деле. Средства продолжают существовать, на том же или другом адресе, но в другой сети, и смотреть надо в её собственном эксплорере. Это не сокрытие. Это переход в другую систему координат.

Как ставить задачу. В техническом задании аналитику (раздел 2.7) перечисляйте сети прямо и добавляйте пункт: «При обнаружении перехода средств в сеть второго уровня или в другой блокчейн продолжить трассировку в соответствующей сети, указав использованный мост и хеши транзакций на обеих сторонах».

Почему это важно процессуально. Разница между «средства ушли в миксер» и «средства ушли в Arbitrum» огромна. Первое — довод о намеренном сокрытии со всеми последствиями раздела 8.5. Второе — обычная операция, которую совершают миллионы людей ради экономии на комиссии, и выдавать её за сокрытие нельзя: эксперт оппонента объяснит суду разницу, и пострадает доверие ко всему вашему заключению.

Проверьте это прежде, чем заявлять о недобросовестности.

Ложные связи: пылевые рассылки и отравление адресов

Возражение, к которому надо быть готовым, потому что оно техническое и звучит убедительно.

Пылевая рассылка. На адрес приходят ничтожные суммы от посторонних лиц — без ведома и согласия владельца. Отправить средства на любой адрес может кто угодно; согласия получателя не требуется. В графе транзакций такие поступления выглядят как связи с отправителем.

Отравление адресов. Злоумышленник создаёт адрес, визуально похожий на тот, с которым жертва уже работала — совпадают первые и последние символы, — и отправляет с него мелкую транзакцию, рассчитывая, что жертва скопирует адрес из истории. В графе возникает связь с адресом, к которому владелец не имеет отношения.

Что из этого следует. Входящая транзакция сама по себе не свидетельствует о связи между владельцами адресов. Свидетельствует **исходящая**: чтобы отправить средства, нужен доступ к ключу.

Держите это разграничение в голове в обе стороны. Если ваш аналитик строит вывод на входящих поступлениях — заключение уязвимо. Если на входящих поступлениях строит вывод эксперт оппонента — у вас есть готовое возражение.

2.6. Допустимость ончейн-данных в российском процессе

Квалификация

Ончейн-данные в российском гражданском и арбитражном процессе — это **письменные или электронные доказательства** (ст. 71 ГПК РФ, ст. 75 АПК РФ). Они не являются «вещественными доказательствами» и не являются «экспертизой» сами по себе. Это документ, полученный из источника, который может быть общедоступным (публичный блокчейн) или запрашиваемым (биржа).

Три способа введения в дело

Способ 1. Самостоятельная фиксация с нотариальным заверением.

Адвокат или клиент открывает эксплорер, вводит адрес, делает скриншоты или распечатки. Затем обращается к нотариусу для обеспечения доказательств (ст. 102–103 Основ законодательства РФ о нотариате). Нотариус фиксирует: дату, время, URL, содержание страницы. Протокол осмотра приобщается к делу.

Когда подходит: простые случаи — один адрес, одна-две транзакции, баланс. Когда сумма спора невелика и нет смысла нанимать аналитика.

Ограничение: нотариус фиксирует то, что видит. Он не строит граф, не размечает адреса, не делает выводов. Для суда это будет доказательством того, что на дату осмотра на адресе был такой-то баланс. Не больше.

Способ 2. Заключение специалиста.

Привлекается ончейн-аналитик, который составляет письменное заключение. Основание: ст. 188 ГПК РФ (консультация специалиста) или ст. 55.1 АПК РФ. Это не судебная экспертиза — специалист не назначается судом, а привлекается стороной. Но заключение является допустимым доказательством и оценивается судом наряду с другими.

Когда подходит: средняя сложность дела, есть конкретные адреса, нужен граф и выводы, но нет необходимости в назначении экспертизы. Стоимость: 30 000–150 000 руб. Срок: 3–10 дней.

Способ 3. Судебная экспертиза.

Назначается определением суда по ходатайству стороны. Эксперт предупреждается об уголовной ответственности за дачу заведомо ложного заключения (ст. 307 УК РФ). Отвечает на вопросы, поставленные судом. Самый весомый вариант с процессуальной точки зрения.

Когда подходит: противная сторона оспаривает данные; граф сложный; сумма спора значительна; суд сам сомневается и хочет заключение от назначенного эксперта.

Ограничение: долго (1–3 месяца), дорого (100 000–500 000 руб.), не все экспертные учреждения имеют специалистов по блокчейну.

Типовые возражения противной стороны и контраргументы

Возражение

Контраргумент

«Блокчейн можно подделать»

Данные в блокчейне защищены криптографически. Изменение записи требует переписывания всей последующей цепи, что вычислительно невозможно для сетей с достаточной мощностью. Хеш транзакции верифицируется любым публичным эксплорером. Прошу суд проверить: ввести хеш [указать] в эксплорер [указать] и убедиться в наличии записи.

«Не доказано, что адрес принадлежит ответчику»

Признаю. Ончейн-данные доказывают движение средств. Принадлежность адреса устанавливается совокупностью доказательств: данные биржи, переписка, показания, косвенные улики. Прошу оценить в совокупности.

«Скриншот не является надлежащим доказательством»

Данные зафиксированы протоколом нотариального осмотра от [дата] / получены в рамках судебной экспертизы / извлечены из общедоступного публичного реестра с фиксацией хеша транзакции.

«Заключение специалиста — не экспертиза»

Закон не требует обязательного назначения экспертизы для приобщения доказательства. Специалист привлечён в порядке ст. 188 ГПК РФ. Суд оценивает доказательство по внутреннему убеждению (ст. 67 ГПК РФ).

«Аналитик не имеет лицензии / сертификата»

Закон не устанавливает лицензионных требований для ончейн-аналитиков. Квалификация подтверждается опытом, публикациями, использованными инструментами.

Практические рекомендации по допустимости

Фиксируйте данные до обращения в суд. Адрес может быть очищен. Аккаунт на бирже — удалён. Биржа — ликвидирована. То, что вы зафиксировали сегодня, завтра может быть недоступно. Правило: заподозрили — зафиксировали.

Нотариальное заверение — минимум. Если сумма спора больше 500 тысяч рублей, не ограничивайтесь скриншотом. Заказывайте заключение аналитика. Разница в стоимости — 50 тысяч. Разница в убедительности для суда — пропасть.

Формулируйте вопросы эксперту конкретно. Не «установить, есть ли у ответчика криптоактивы». А: «Установить, поступали ли на адрес [0x7a3f...b21e] средства в период с 01.01.2020 по 31.12.2022. Если да — в каком объёме, от каких адресов, на какие адреса были перенаправлены, с указанием хешей транзакций и дат».

* * *

2.7. Как поставить задачу аналитику: шаблон технического задания

Аналитик не сыщик. Он не ищет «крипту ответчика». Он работает с конкретными адресами и хешами. Ваша задача — дать ему отправную точку. Его задача — развить её в граф. Чтобы не было разговора «найдите мне всё», используйте шаблон.

* * *

ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА ОНЧЕЙН-ИССЛЕДОВАНИЕ

1. Объект исследования.

Адрес(а) кошелька(ов): [указать].

Хеш(и) транзакции(й): [при наличии].

Период исследования: [с... по...].

Сеть (блокчейн): [указать, если известно; если нет — определить в ходе исследования].

2. Целевой вопрос.

Установить движение средств с адреса [А]: направление, объём, промежуточные адреса, привязка к известным сервисам (биржи, миксеры, протоколы). Вариант: установить источник поступления средств на адрес [Б].

3. Формат результата.

— Граф транзакций (визуализация в формате, пригодном для приобщения к делу).

— Таблица транзакций: дата, хеш, адрес отправителя, адрес получателя, сумма, метка узла.

— Текстовое заключение с выводами и указанием степени уверенности по каждому выводу.

— Перечень адресов, ассоциированных с биржами или иными сервисами, для последующего запроса.

4. Ограничения.

При переходе средств в сеть второго уровня (роллап) либо в другой блокчейн — продолжить трассировку в соответствующей сети, указав использованный мост и хеши транзакций на обеих сторонах перехода.

Если трассировка прерывается на миксере или приватной монете — зафиксировать точку разрыва, идентифицировать сервис, указать причину невозможности продолжения.

5. Требования к допустимости.

Заключение должно содержать: наименование использованных инструментов и версий баз данных; описание методологии; указание на степень уверенности; подпись исполнителя с указанием квалификации. Документ должен быть пригоден для представления в суд в качестве заключения специалиста.

6. Конфиденциальность.

Данные по настоящему делу не используются для публичных отчётов, публикаций и маркетинговых материалов.

7. Сроки и стоимость.

Срок: [указать]. Стоимость: [указать]. Порядок оплаты: [указать].

* * *

Этот шаблон можно адаптировать. Главное — не просите «найти крипту». Давайте адрес, хеш, период. Если адреса нет — сначала глава 3.

* * *

2.8. Сквозной кейс № 1, продолжение: первый след

Вернёмся к делу Елены и Сергея К.

Адвокат Елены, вооружившись знаниями из главы 1, понимает: просто спросить суд «есть ли у ответчика крипто?» — бессмысленно. Суд не знает, куда направить запрос. Нужно дать суду конкретный адрес для истребования.

Первый шаг — банковские выписки. Адвокат заявляет ходатайство об истребовании выписок по всем счетам и картам Сергея за 2020–2022 годы. Суд удовлетворяет. Банки предоставляют данные.

Из выписок видно:

- Март 2021: перевод 487 000 руб. на расчётный счёт российского юридического лица, аффилированного с крупной криптобиржей. Назначение: «Пополнение счёта по договору оферты № [номер]».

- Апрель 2021: перевод 312 000 руб. туда же.

- Июнь 2021: перевод 150 000 руб. туда же.

- Июль–август 2021: четыре перевода на общую сумму 620 000 руб. на тот же счёт.

Итого: около 1 570 000 руб. за шесть месяцев. Не два миллиона, о которых говорил Сергей. Но и не ноль. И главное — есть привязка к конкретной бирже и к конкретному аккаунту. Номер договора оферты в назначении платежа — это идентификатор клиента.

Что это даёт:

Во-первых, опровергается версия Сергея о том, что он «вложил около двух миллионов и всё потерял». Переводов на 1 570 000, а не на 2 000 000. И это только один банк. Могли быть другие.

Во-вторых, появляется точка для запроса. Биржа. Конкретное юрлицо. Конкретный договор.

В-третьих, появляется основа для ончейн-анализа. Если удастся получить данные аккаунта — адреса кошельков, историю операций, — можно будет построить граф и проследить, куда ушли средства.

Но есть проблема. Российское юридическое лицо биржи ликвидировано. Данные переданы иностранному оператору. Запрос российского суда на иностранную биржу может остаться без ответа. Как быть — разберём в главе 3. А пока зафиксируем: первый след найден. Он не в блокчейне. Он в банковской выписке. Ончейн-анализ начнётся тогда, когда мы получим адрес.

А адрес мы получим через оффчейн-разведку.

* * *

Вместо заключения

Ончейн-анализ — не магия и не хакерство. Это чтение публичного реестра с правильными инструментами и правильной методологией. Юристу не нужно уметь строить граф самому. Ему нужно понимать три вещи: что граф покажет, чего не покажет и как превратить его в строку в судебном решении.

Но есть проблема, которую ончейн-анализ не решает сам по себе. Ему нужна отправная точка. Адрес. Хеш. Название биржи. Что-то, за что можно зацепиться. Если у вас нет ни одного адреса — ончейн-анализ не начнётся.

Где взять отправную точку, если противник молчит? Из переписки. Из устройств. Из банковских выписок. Из показаний свидетелей. Из цифровых следов, которые человек оставляет в обычной жизни. Это не блокчейн. Это детективная работа. О ней — следующая глава.

* * *

Примечания

Гражданский процессуальный кодекс РФ, ст. 71 (письменные доказательства), ст. 188 (консультация специалиста), ст. 67 (оценка доказательств).

Арбитражный процессуальный кодекс РФ, ст. 75 (письменные доказательства), ст. 55.1 (заключение специалиста).

Основы законодательства РФ о нотариате, ст. 102–103 (обеспечение доказательств).

Уголовный кодекс РФ, ст. 307 (заведомо ложное заключение эксперта).

Федеральный закон от 04.08.2026 № 282-ФЗ «О цифровых валютах и цифровых правах»: ст. 1 (предмет регулирования, ч. 6 — запрет расчётов, ч. 7 — исключения, ч. 9–10 — запрет распространения информации, ч. 18 — особый режим), ст. 2 (основные понятия: п. 1 ч. 1 — цифровая валюта, п. 3 ч. 1 — обращение цифровых валют, п. 5–6 ч. 1 — адрес-идентификатор и адреса, администрируемые цифровыми депозитариями), ст. 3 (майнинг), ст. 6 (деятельность оператора), ст. 14–18 (участники рынка), ст. 30 (совершение сделок и операций), ст. 56 (порядок вступления в силу). Федеральный закон от 04.08.2026 № 283-ФЗ. 5.1. Федеральный закон от 31.07.2020 № 259-ФЗ — применяется в части, не утратившей силу; полностью прекращает действие с 01.09.2028. 5.2. Постановление Конституционного Суда РФ от 20.01.2026 № 2-П по делу о проверке конституционности ч. 6 ст. 14 Федерального закона № 259-ФЗ в связи с жалобой гражданина Тимченко Д. И. Статья 86.5 НК РФ — обязанность оператора майниговой инфраструктуры сообщать в налоговый орган сведения о лице, которому оказываются услуги по предоставлению инфраструктуры (введена Федеральным законом № 418-ФЗ); формат и состав сведений — приказ ФНС России от 28.04.2025 № ЕД-7-15/429@. 5.3. Федеральный закон от 29.11.2024 № 418-ФЗ — цифровая валюта как имущество для целей налогообложения. Федеральный закон от 08.08.2024 № 221-ФЗ — майнинг.

Дело Царькова: постановление Девятого ААС от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017.

Tornado Cash: внесён OFAC в список SDN 08.08.2022 (Executive Order 13694), повторно обозначен в ноябре 2022 года со ссылкой на EO 13722. Исключён из списка SDN 21.03.2025 после решения Апелляционного суда пятого округа США от 26.11.2024 по делу *Van Loon v. Department of the Treasury*. **На момент подготовки книги протокол под санкциями США не находится.** Роман Семёнов, один из разработчиков протокола, внесён в список SDN в августе 2023 года отдельным решением и при делистинге протокола из него не исключён. Санкционный статус любого сервиса проверять по актуальному списку SDN на дату подготовки документа.

Данные об объёмах средств, проходящих через миксеры и кросс-чейн мосты, публикуются в ежегодных отчётах аналитических компаний (Chainalysis, Elliptic, TRM Labs). Конкретный отчёт и год указывать по актуальной публикации на дату вёрстки.

Методические рекомендации по обеспечению доказательств нотариусами (утв. решением Правления Федеральной нотариальной палаты, протокол от 26.06.2023 № 10/23) — в том числе обеспечение доказательств в сети «Интернет» (осмотр сайта) как случай, не терпящий отлагательства; письмо ФНП от 13.01.2012 № 12/06-12; п. 22 постановления Пленума Верховного Суда РФ от 26.12.2017 № 57. Перечень форм обеспечения доказательств по ст. 103 Основ законодательства о нотариате является закрытым.

Технические особенности: модель непотраченных выходов (UTXO) и аккаунтная модель учёта; эвристика общего входа и определение адреса сдачи как основа кластеризации; сети второго уровня (роллапы) и мосты между сетями; пылевые рассылки и отравление адресов. Специальной правовой литературы по этим вопросам нет; при подготовке заключения опираться на пояснения привлечённого специалиста. 10.1. **Санникова Л. В., Харитонова Ю. С.** Цифровые активы: правовой анализ: монография. — М.: 4 Принт, 2020. — 304 с. Первое отечественное исследование криптоактивов как объекта права: классификация, признаки, сопоставление с режимами США, Японии, Швейцарии, Германии, Беларуси и других юрисдикций. 10.2. **Карцхия А. А.** Гражданско-правовая модель регулирования цифровых технологий. — М., 2019. — общая рамка гражданско-правовой квалификации цифровых объектов.

Лев Б. Криптовалютная криминалистика: расследование хищений, возврат средств и защита цифровых активов. — методика ончейн-трассировки, устройство блокчейн-эксплореров и работа с аналитическими платформами изложены там развёрнуто; в настоящей главе — в объёме, необходимом для имущественного спора.

* * *

Глава 3. Оффчейн-разведка: где искать отправную точку, если противник молчит

* * *

Адвокат Морозова возвращается в офис после заседания. Судья удовлетворил ходатайство об истребовании банковских выписок — это победа. Но выписки пришли, и в них пусто. Ни одного перевода на биржу. Ни одной подозрительной операции. Клиентка уверена: крипта есть, муж её прячет. Но как доказать, если в официальных каналах — тишина? Ответчик сидит на заседании с каменным лицом и говорит: «Никогда ничем подобным не занимался». Ни адреса кошелька, ни названия биржи, ни хеши транзакции. Ончейн-анализ не запустить — нечего вводить в эксплорер. Нужно искать в другом месте. В телефоне. В переписке. В показаниях. В цифровом мусоре, который человек оставляет за собой, даже когда думает, что всё удалил.

* * *

3.1. Проблема холодного старта

Глава 2 закончилась на выводе: ончейн-анализ не работает без отправной точки. Ему нужен адрес, хеш, название биржи — хоть что-то конкретное. Но в большинстве реальных дел противник не предоставляет ничего. Он не обязан. Он говорит: «У меня нет криптоактивов», и формально бремя доказывания обратного ложится на вас.

Это и есть **холодный старт**: вы подозреваете, что криптоактивы существуют, но у вас нет ни одной зацепки в блокчейне. Нет адреса. Нет хеша. Нет названия биржи. Есть только уверенность клиента и косвенные обстоятельства.

Задача оффчейн-разведки — превратить эту уверенность в конкретную отправную точку, которую можно передать ончейн-аналитику. Найти ниточку, за которую можно потянуть.

Ниточек шесть. Перечислю их, а затем разберу каждую:

Банковские следы. Переводы, платежи, операции с контрагентами.

Устройства. Телефоны, компьютеры, аппаратные кошельки.

Переписка. Мессенджеры, электронная почта, SMS.

Свидетели. Люди, которые видели, слышали, знают.

Цифровой след. Социальные сети, форумы, публичные данные.

Процессуальные механизмы. Судебные запросы, осмотр, выемка.

Не в каждом деле сработают все шесть. Но в каждом деле хотя бы одна из них даст результат. Ваша задача — проверить каждую последовательно, от самой простой к самой сложной.

* * *

3.2. Банковские следы

Это первый и самый простой шаг. Мы уже видели его в деле Елены и Сергея К.: переводы на юрлицо биржи в назначении платежа. Но это — идеальный случай. В реальности следы могут быть менее очевидными.

Что искать в выписках

Прямые переводы на биржи. Назначение платежа содержит слова: «пополнение», «депозит», «покупка криптовалюты», «по договору оферты». Контрагент — юридическое лицо, связанное с криптоплощадкой или обменником, в том числе белорусское: обменниками из Парка высоких технологий пользуются и российские клиенты, и такой платёж в выписке — сильный след, потому что белорусская площадка отвечает на запросы (раздел 16.7). Учтите, что состав действующих площадок быстро меняется: часть площадок, обслуживавших российских пользователей в 2020–2022 годах, к моменту вашего дела уже ликвидирована или заблокирована, а их наименования сохранились только в выписках. Отсутствие площадки сегодня не означает отсутствия операции вчера. Это самый простой и сильный след.

P2P-переводы. Человек покупает крипту не напрямую у биржи, а у другого физлица через P2P-площадку. В выписке это выглядит как обычный перевод физическому лицу: «Иванову И.И.». Никаких слов о крипте. Но: сумма круглая (100 000, 500 000), переводы регулярные, получатели разные и не связаны с должником родственными или деловыми отношениями. Это косвенный признак P2P-покупки.

Переводы на карты, привязанные к обменникам. Некоторые обменники принимают оплату на карты подставных лиц. В выписке — перевод физлицу, но сумма и паттерн указывают на обмен криптовалюты.

Платежи в пользу процессинговых компаний. Некоторые биржи принимают оплату через платёжных агрегаторов. В назначении — «оплата услуг по договору №...» с контрагентом, который является процессингом.

Обратные переводы. Если крипта продавалась, деньги должны были куда-то прийти. Входящие переводы от биржи, от физлиц (P2P-продажа), от обменника. Если ответчик утверждает, что «всё потерял», а на счёт поступали крупные суммы — это противоречие.

Как получить выписки

-

Ходатайство об истребовании

(ст. 57 ГПК, ст. 66 АПК). Просите суд запросить выписки по всем счетам ответчика за интересующий период. Указывайте конкретные банки, если знаете. Если не знаете — просите запросить в ФНС перечень открытых счетов, а затем по каждому.

-

Запрос финансового управляющего

в деле о банкротстве. У управляющего полномочия шире: он запрашивает все банки по ст. 213.9 ФЗ-127.

-

Запрос адвоката.

Менее эффективен: банк вправе отказать. Но попробовать стоит, особенно если клиент — ваш доверитель и даёт согласие на получение собственных выписок.

Практический приём

Запрашивайте выписки за **расширенный период**. Не только за время брака или за год до банкротства. Минимум три года. Криптоинвестор часто начинает с малых сумм, наращивает постепенно, а выводит крупно. Если вы возьмёте только последний год, можете пропустить вход.

* * *

3.3. Устройства: телефон, компьютер, аппаратный кошелёк

Если банковские следы не дали результата или дали недостаточно, следующий источник — устройства ответчика. Это самый богатый, но и самый сложный с правовой точки зрения канал.

Что можно найти на устройстве

-

Приложения бирж и кошельков.

Иконки на экране телефона: Binance, Bybit, OKX, MetaMask, Trust Wallet, Ledger Live, Trezor Suite. Даже если приложение удалено, в настройках телефона, в облачном бэкапе, в истории покупок в App Store / Google Play могут остаться следы установки.

-

Аппаратный кошелёк.

Устройство размером с флешку (Ledger, Trezor, SafePal, Keystone). Если оно есть у ответчика — это прямой доступ к средствам. Но для извлечения ключей нужен PIN или seed-фраза.

-

История браузера.

Посещения сайтов бирж, эксплореров, форумов о крипте. Даже если история очищена, в кэше, в закладках, в файлах cookie могут остаться данные.

-

Скриншоты и фотографии.

Снимки экрана с балансом, с графиками, с адресами кошельков. Фотографии seed-фразы, записанной на бумаге. Люди фотографируют экран и забывают удалить.

-

Файлы.

Документы с названиями «кошелёк», «биткоин», «крипта», «seed», «private key». Текстовые файлы, заметки, таблицы.

-

Облачные бэкапы.

Резервные копии телефона в iCloud или Google. В них — удалённые приложения, переписка, фотографии.

Правовые механизмы доступа

Добровольное предоставление. В идеале ответчик сам передаёт устройство. В семейных делах это возможно, если сторона готова к сотрудничеству. В банкротстве финансовый управляющий вправе требовать передачи устройств должника (ст. 213.9 ФЗ-127).

Судебный осмотр. Ходатайство о осмотре устройства в заседании (ст. 58 ГПК, ст. 78 АПК). Суд осматривает телефон или компьютер, фиксирует содержимое. Работает, если устройство физически доступно.

Судебная экспертиза. Назначение экспертизы с вопросом: «Имеются ли на устройстве [модель, серийный номер] данные, свидетельствующие о владении криптоактивами: приложения, адреса кошельков, транзакции, переписка». Эксперт извлекает данные с помощью форензик-инструментов.

Уголовно-процессуальные механизмы. Если в деле есть признаки преступления (мошенничество, преднамеренное банкротство, злостное уклонение от исполнения), возможен обыск и выемка в рамках уголовного дела (ст. 182–183 УПК РФ). Это крайняя мера, но в крупных делах о сокрытии активов — рабочая.

Форензик-инструменты

Для извлечения данных с устройств специалисты используют:

Инструмент

Что делает

Cellebrite UFED / Physical Analyzer

Извлечение данных с мобильных устройств: приложения, переписка, файлы, удалённые данные

Magnet AXIOM

Комплексная форензика: телефоны, компьютеры, облачные хранилища

XRY (MSAB)

Альтернатива Cellebrite; популярна в государственных структурах РФ

EnCase / FTK

Компьютерная форензика: жёсткие диски, образы, восстановление удалённых файлов

Юристу не нужно владеть этими инструментами. Нужно знать, что они существуют, и правильно поставить задачу эксперту: не просто «посмотрите телефон», а «установите наличие приложений, связанных с криптобиржами и кошельками; извлеките адреса кошельков, хеши транзакций, историю посещений соответствующих сайтов; проверьте облачные бэкапы».

Практический совет

Если вы подозреваете, что у ответчика есть аппаратный кошелёк, **заявите об этом в суде как можно раньше.**

Устройства легко уничтожить: разбить, выбросить, перепрошить. Если суд не примет обеспечительных мер (изъятие, запрет на отчуждение), к моменту экспертизы устройства уже не будет. В банкротстве управляющий должен включить аппаратные кошельки в опись имущества должника.

* * *

3.4. Переписка: мессенджеры, почта, SMS

Переписка — второй по богатству источник после устройств. Люди обсуждают инвестиции. Отправляют друг другу адреса кошельков. Пересылают скриншоты балансов. Жалуются на убытки. Хвастаются прибылью. Всё это — доказательства.

Где искать

Мессенджеры. Telegram, WhatsApp, Signal, Viber. Telegram — самый популярный для обсуждения крипты в русскоязычном пространстве. В нём же работают P2P-обменники, боты для покупки, каналы с сигналами.

Электронная почта. Письма от бирж: верификация аккаунта, подтверждения операций, уведомления о входе. Письма от кошельков, от DeFi-протоколов. Если ответчик регистрировался на бирже, на его почте есть письмо «Подтвердите ваш аккаунт на [название биржи]».

SMS. Уведомления о входе в аккаунт, коды верификации, оповещения о транзакциях. Даже если тело сообщения удалено, метаданные (отправитель, время) могут сохраниться.

Правовой доступ

Переписка на устройстве ответчика. Извлекается в рамках осмотра или экспертизы устройства (см. параграф 3.3). Это законно, если устройство получено легально.

Переписка на серверах мессенджеров и почтовых сервисов. Запрос к оператору связи или к владельцу сервиса. В России: запрос через суд на основании ст. 57 ГПК / ст. 66 АПК. На практике: российские операторы отвечают; иностранные мессенджеры (WhatsApp, Signal) — почти никогда. Почтовые сервисы (Mail.ru, Яндекс) отвечают на судебный запрос. Gmail, Outlook — только через международную правовую помощь.

Переписка, которую клиент видел сам. Если ваш клиент (например, супруга) видел переписку на телефоне мужа, может пересказать её содержание или показать скриншот. Скриншот заверяется нотариально. Показания даются в суде. Это не идеально, но лучше, чем ничего.

Что именно искать в переписке

- Названия бирж и обменников.
- Адреса кошельков (строки, начинающиеся с 0x, bc1, T...).
- Хеши транзакций.
- Seed-фразы (12 или 24 слова).
- Обсуждения сумм: «купил на 500 тысяч», «перевёл два битка».
- Инструкции: «отправь на этот адрес», «вот мой кошелёк».
- Скриншоты балансов, графиков, подтверждений операций.

* * *

3.5. Свидетели

Когда цифровых следов недостаточно или к ним нет доступа, включается человеческий фактор. Люди говорят. Люди хвастаются. Люди жалуются. Люди обсуждают инвестиции за ужином, в офисе, в баре.

Кто может быть свидетелем

-

Супруг / супруга.

Видел(а), как ответчик торговал, слышал(а) разговоры, видел(а) экран.

-

Дети, родственники.

Случайно видели приложение на телефоне, слышали разговоры.

-

Друзья, знакомые.

Ответчик рассказывал об инвестициях, показывал результаты, просил совета.

-

Коллеги, партнёры.

Обсуждали крипту на работе, ответчик хвастался доходностью.

-

Бухгалтер, финансовый консультант.

Если ответчик пользовался услугами по управлению активами.

Как работать со свидетелями

Подготовка. Не ведите свидетеля в суд неподготовленным. Встретьтесь заранее. Выясните: что именно он видел или слышал, когда, при каких обстоятельствах. Не подсказывайте, не навязывайте. Но помогите структурировать: «Что вы видели на экране?», «Какие суммы назывались?», «Были ли упомянуты названия бирж или приложений?».

Допрос в суде. Заявите ходатайство о вызове свидетеля (ст. 69 ГПК, ст. 88 АПК). Сформулируйте вопросы заранее. Ключевые:

- Видели ли вы, как ответчик совершал операции с криптовалютой?
- Называл ли он конкретные суммы, названия бирж, приложений?
- Показывал ли он экран устройства с данными о балансе или транзакциях?
- Обсуждал ли он покупку, продажу, хранение криптоактивов? Когда именно?

Нотариальное обеспечение показаний. Если есть риск, что свидетель не явится в суд или изменит показания, можно обеспечить показания нотариально (ст. 102 Основ о нотариате). Нотариус допрашивает свидетеля и фиксирует протокол.

Практический приём

В семейных делах свидетельские показания часто воспринимаются судьями скептически: «Это жена, она заинтересована». Усиливайте показания цифровыми следами. Жена говорит: «Я видела, как он покупал биткоин», — это слабо. Жена говорит: «Я видела, как он переводил 300 тысяч на карту, привязанную к приложению “Бинанс”, вот скриншот перевода из моего банка» — это сильно.

Свидетель + документ = убедительно.

* * *

3.6. Цифровой след: социальные сети, форумы, публичные данные

Человек, который инвестирует в крипту, часто оставляет следы в открытом доступе. Не всегда, но чаще, чем кажется.

Где искать

Социальные сети. Посты, репосты, комментарии о крипте. Подписки на криптоканалы. Аватарки с ссылкой к NFT. ВКонтакте, Telegram-каналы, X (Twitter). Люди хвастаются: «Купил свой первый биткоин», «Портфель вырос на 300 %». Это не доказательство владения конкретным адресом, но косвенное подтверждение интереса и, возможно, владения.

Форумы и сообщества. Русскоязычные форумы: bits.media, Bitcointalk (русскоязычные ветки), каналы в Telegram. Если ответчик регистрировался под ником и обсуждал свои операции — это след.

GitHub, NPM, доменные регистрации. Для технически подкованных: если ответчик разработчик или предприниматель в сфере крипты, его публичные репозитории, домены, смарт-контракты могут содержать адреса кошельков.

Публичные эксплореры. Если вы нашли хотя бы один адрес (из переписки, из показаний, из браузера), вы можете ввести его в эксплорер и увидеть историю. Это уже ончейн-анализ (глава 2), но отправная точка найдена оффчейн.

Правовой статус

Публичные данные — общедоступная информация. Скриншот поста в социальной сети, заверенный нотариально, является допустимым доказательством. Согласие автора поста на фиксацию не требуется, если пост публичный.

* * *

3.7. Процессуальные механизмы: как легально получить доступ

Все описанные источники бесполезны, если данные получены незаконно. Запись разговора без согласия, взлом телефона, несанкционированный доступ к переписке — это не доказательства, а основание для уголовного дела против вас. Поэтому фиксация должна быть процессуально чистой.

Гражданский и арбитражный процесс

-

Ходатайство об истребовании доказательств

(ст. 57 ГПК, ст. 66 АПК). Просите суд запросить: выписки у банков, данные у операторов связи, информацию у бирж. Указывайте конкретные данные и объясняйте, почему сами получить не можете.

-

Обеспечение доказательств

(ст. 64–66 ГПК, ст. 72 АПК). Если есть риск, что данные будут уничтожены (ответчик удалит переписку, отформатирует диск), просите суд обеспечить доказательства до или во время процесса. Нотариальный осмотр, экспертиза, изъятие.

-

Обеспечительные меры

(ст. 139–140 ГПК, ст. 91–92 АПК). Арест устройств, запрет на отчуждение аппаратных кошельков.

-

Нотариальное обеспечение

(ст. 102–103 Основ о нотариате). Фиксация переписки, скриншотов, содержимого сайтов — до обращения в суд или параллельно.

Банкротство

Финансовый управляющий имеет широкие полномочия:

- Запрашивать любые данные у должника, банков, операторов связи (ст. 213.9 ФЗ-127).
- Требовать передачи устройств, документов, ключей.
- При отказе — ходатайствовать перед судом о принудительном истребовании.
- Оспаривать сделки по выводу активов, включая конвертацию в крипту.

Уголовное преследование

Если есть признаки преступления (ст. 159 УК — мошенничество; ст. 196 — преднамеренное банкротство; ст. 315 — неисполнение решения суда):

- Обыск и выемка устройств (ст. 182–183 УПК).
- Осмотр места жительства.
- Изъятие аппаратных кошельков, бумажных носителей с ключами.
- Доступ к переписке по решению суда (ст. 186 УПК).

Это крайняя мера. Но в делах с крупными суммами и явным сокрытием — рабочая.

* * *

3.8. Регулируемый контур: новый слой источников

У оффчейн-разведки есть источник, которого не знала вся предыдущая история этой работы: лицо, которое по закону знает, кому принадлежит адрес, и обязано отвечать на запросы. Это цифровой депозитарий.

Прежде чем разбирать его, зафиксирую то, что важнее самого источника.

Почему это не отменяет остальную главу

Соблазн понятен: раз есть депозитарий, знающий владельца адреса, зачем банковские выписки, устройства, переписка и свидетели.

Затем, что регулируемый контур покрывает малую часть того, с чем вы столкнётесь.

Вне контура остаётся:

- всё, что приобреталось до появления контура, а это подавляющая часть активов в делах, которые вы ведёте сегодня;

- самостоятельное хранение: холодный кошелёк, аппаратное устройство, мнемоническая фраза в сейфе. Ни один депозитарий об этом ничего не знает;

- иностранные площадки, не имеющие обязательств в российской юрисдикции;

- расчёты между физическими лицами напрямую;

- всё, что противник переместил намеренно, узнав о споре.

Последний пункт решающий. **Человек, который прячет актив, уходит из регулируемого контура первым** — по определению, потому что контур создан, чтобы его было видно. Значит, в тех делах, ради которых написана эта книга, новый источник даст меньше всего.

Правильная модель — не замена, а слой. Регулируемый контур отвечает на вопрос «есть ли актив там, где его видно». Всё остальное в этой главе отвечает на вопрос «где он, если его не видно». Второй вопрос интереснее, но начинать надо с первого, потому что он дешевле.

Порядок: сначала дешёвое

Практическое правило, которое стоит встроить в работу с первого дня.

Шаг 1. Проверьте регулируемый контур. Это один запрос, он либо даёт готовый ответ, либо не даёт ничего. Стоимость проверки — время на подготовку ходатайства.

Шаг 2. Если ответ отрицательный — это не пустой результат. Официальное подтверждение того, что у оппонента нет активов в лицензированном контуре, при наличии ончейн-данных о его операциях становится доказательством того, что он держит активы вне контура. То есть намеренно. Это довод о недобросовестности, готовый к использованию в разделах 10.6 и 11.5.

Шаг 3. Дальше работайте по разделам 3.2–3.7. Ничего из описанного там не устарело.

Кому теперь можно писать

Адресат

Что знает

Что запрашивать

Цифровой депозитарий

Связь адреса-идентификатора с личностью, остатки, история

Принадлежность конкретного адреса; перечень адресов, администрируемых для лица; остатки на даты

Обменная организация

Данные клиента, операции обмена

Идентификация, история операций, встречные реквизиты

Брокер

Поручения клиента

История поручений, состав активов

Управляющий

Переданное в управление имущество

Состав, стоимость, сроки

Организатор торговли

Сделки участников

Сведения о сделках

Банк

Отказы в переводах в пользу лиц вне реестра

Сведения об отказах и их основаниях

Строка про депозитарий переворачивает логику главы 2. Там связь адреса с личностью устанавливается косвенно — через устройство, переписку, поведение. Здесь она устанавливается прямо, по запросу. Это принципиально новая возможность, и в тех делах, где она работает, она экономит месяцы.

Формулировка запроса:

Прошу истребовать у [наименование цифрового депозитария] сведения о том, администрируется ли адрес-идентификатор [указать полностью] в интересах [ФИО, дата рождения], а также перечень адресов-идентификаторов, администрируемых указанным лицом, с указанием остатков по состоянию на [даты] и истории операций за период с [дата] по [дата].

Дополнительно прошу истребовать сведения о наличии у указанного лица договорных отношений с иными лицами, включёнными в реестр Банка России.

Второй абзац важнее первого: он снимает необходимость угадывать, к какому именно депозитарию обращаться.

Банковский отказ как след

Отдельный механизм, который стоит держать в голове.

С 1 июля 2027 года банки обязаны отказывать в переводах в пользу лиц, не включённых в реестр Банка России. Каждый такой отказ фиксируется.

Для розыска это означает следующее: отказ банка в переводе оппонента — свидетельство того, что он пытался совершить операцию с нелегализованным контрагентом. Само по себе это не доказывает наличия актива, но указывает и на направление поиска, и на характер поведения.

Позиция автора. Я ожидаю, что сведения об отказах станут одним из самых продуктивных источников в делах после 2027 года — по той же причине, по которой сегодня продуктивна банковская выписка: они фиксируют намерение, а не только результат. Запрашивайте их отдельным пунктом, не полагаясь на то, что они попадут в обычную выписку.

Майнеры: адреса уже в налоговой

Отдельный источник, который работает не с 2027 года, а сейчас, и о котором почти не пишут.

Часть 11 статьи 3 Закона № 282-ФЗ обязывает лицо, осуществляющее майнинг, предоставлять в налоговый орган сведения о получении цифровой валюты **и об адресе-идентификаторе**, включая адрес майнинг-пула, в порядке и сроки, установленные Правительством. Часть 12 предусматривает передачу этих сведений в Росфинмониторинг и Банк России.

Практически это означает следующее. Если оппонент майнил как индивидуальный предприниматель или юридическое лицо, он состоит в реестре лиц, осуществляющих майнинг, который ведёт ФНС, и его адреса налоговому органу известны. Это единственный случай, когда связь адреса с личностью зафиксирована государственным органом напрямую.

Что из этого следует для запроса: истребуйте у налогового органа сведения о включении оппонента в реестр лиц, осуществляющих майнинг, и об адресах-идентификаторах, представленных им в порядке части 11 статьи 3. Отсутствие оппонента в реестре при наличии доказательств майнинга — самостоятельное нарушение и довод о недобросовестности.

Граждане, не являющиеся предпринимателями, вправе майнить в пределах лимитов энергопотребления, установленных Правительством (ч. 2 ст. 3), и в реестр не включаются. Для них этот источник не работает.

Налоговый источник со 2 мая 2027 года

Со 2 мая 2027 года у физических лиц — резидентов возникает обязанность информировать налоговые органы об операциях с цифровыми валютами в зарубежных информационных системах.

Практическое значение для розыска трудно переоценить: впервые появляется государственный орган, у которого могут находиться сведения об активах на иностранных площадках, то есть там, где сейчас запросы упираются в стену (глава 16).

Как этим пользоваться:

- истребуйте сведения через суд наравне с данными о счетах;
- в банкротстве запрос направляется управляющим напрямую в порядке ст. 20.3 и 213.9 Закона о банкротстве;

• отсутствие поданного уведомления при наличии ончейн-данных об операциях — самостоятельный довод о недобросовестности и, вероятно, основание для налоговой ответственности оппонента.

Позиция автора, и она сдержанная. Обязанность информировать не создаёт механизма проверки. Тот, кто скрывает актив от супруга или кредиторов, не станет декларировать его перед налоговым органом — риски для него несопоставимы. Поэтому я ожидаю, что этот источник будет давать результат в делах, где оппонент вёл себя добросовестно и просто не раскрыл актив по невнимательности, и не будет давать ничего там, где сокрытие умышленное. То есть по той же логике, что и весь регулируемый контур: он помогает найти забытое, а не спрятанное.

Что изменить в работе прямо сейчас

Три пункта, которые стоит внести в свои шаблоны сегодня.

Первый. В ходатайство об истребовании добавьте отдельный пункт о цифровых депозитариях и организациях из реестра Банка России. Стандартная формулировка «о счетах и вкладах» их не охватывает.

Второй. В запрос финансового управляющего должнику (шаблон В.8) добавьте вопрос о наличии договорных отношений с лицензированными участниками рынка цифровых валют. Отрицательный ответ при наличии ончейн-данных — зафиксированная ложь.

Третий. В протокол первой встречи (Приложение А) добавьте вопрос: пользовался ли оппонент российскими лицензированными сервисами. Ответ «нет, он всё держал сам» — это уже направление поиска.

3.9. Как собрать всё воедино: чек-лист холодного старта

Когда у вас нет ни одной зацепки, действуйте по алгоритму:

Шаг 1. Банковские выписки. Запросите за 3 года. Ищите переводы на биржи, обменники, P2P-контрагентов. Ищите входящие от тех же лиц.

Шаг 2. Опрос клиента. Что видел, что слышал, какие приложения, какие суммы, какие названия. Запишите. Структурируйте.

Шаг 3. Свидетели. Определите 2–3 человек, которые могут подтвердить интерес ответчика к крипте. Подготовьте. Заявите в суд.

Шаг 4. Ходатайство об осмотре / экспертизе устройств. Если есть основания полагать, что устройство содержит данные. Просите суд назначить экспертизу с конкретными вопросами.

Шаг 5. Нотариальная фиксация. Всё, что доступно сейчас: скриншоты, переписка, посты. Зафиксируйте до того, как это удалят.

Шаг 6. Цифровой след. Проверьте соцсети, форумы, публичные данные. Зафиксируйте.

Шаг 7. Передача аналитику. Как только появился хотя бы один адрес, хеш или название биржи — передавайте в ончейн-анализ (глава 2). Холодный старт завершён.

* * *

3.10. Сквозной кейс № 1, продолжение: второй след

Вернёмся к делу Елены и Сергея К.

Банковские выписки дали первый след: переводы на юрлицо биржи. Но российское юрлицо ликвидировано, данные переданы иностранному оператору. Запрос суда уходит в пустоту: ответ не приходит.

Адвокат Елены меняет тактику. Заявляет ходатайство об осмотре телефона Сергея в судебном заседании. Суд удовлетворяет. В заседании телефон предоставляется. Судья листает экран. Приложений бирж нет. Но в галерее — скриншот от 14 марта 2021 года: тёмный интерфейс, зелёные цифры, надпись «BTC/USDT», баланс «1,247 BTC». Внизу — логотип биржи «Bybit».

Адвокат фиксирует скриншот в протоколе заседания. Просит суд приобщить к делу. Сергей бледнеет. Говорит: «Это старый скриншот, я тогда только пробовал, там было мало, потом всё продал».

Но у адвоката уже есть: название биржи (Bybit), дата, примерный объём (1,247 BTC на март 2021 — это около 70 000 долларов по курсу того периода). Это отправная точка для запроса на биржу и для ончейн-анализа, если удастся получить адрес.

Следующий шаг: запрос на Bybit с требованием предоставить данные аккаунта, зарегистрированного на Сергея К. Биржа зарегистрирована на Сейшелах. Ответит ли? Не факт. Но это уже задача главы 16 — исполнение за рубежом. А пока: холодный старт преодолён. Адрес ещё не получен, но направление задано.

* * *

Вместо заключения

Оффлайн-разведка — это детективная работа в рамках процессуального закона. Вы не хакер. Вы не сыщик. Вы юрист, который знает, где искать, как запросить и как зафиксировать. Банковские выписки, устройства, переписка, свидетели, цифровой след — каждый из этих каналов может дать ту самую ниточку, за которую потянет ончейн-аналитик.

В следующей главе мы соберём все нитки дела Елены и Сергея воедино и пройдем весь путь от подозрения до доказанного факта. А затем перейдем к главному: как противник прячет активы через структуры. Там, где обычный поиск бессилен, начинается настоящая работа.

* * *

Примечания

Гражданский процессуальный кодекс РФ: ст. 57 (истребование доказательств), ст. 58 (осмотр), ст. 64–66 (обеспечение доказательств), ст. 69 (свидетели), ст. 139–140 (обеспечительные меры).

Арбитражный процессуальный кодекс РФ: ст. 66 (истребование), ст. 72 (обеспечение), ст. 78 (осмотр), ст. 88 (свидетели), ст. 91–92 (обеспечительные меры).

Основы законодательства РФ о нотариате: ст. 102–103 (обеспечение доказательств).

Федеральный закон от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)»: ст. 20.3, 213.9 (полномочия финансового управляющего). 4.1. Федеральный закон от 04.08.2026 № 282-ФЗ: ст. 14–18 (участники рынка и их обязанности), положения о реестре Банка России и об отказе кредитных организаций в переводах в пользу лиц, не включённых в реестр (применяются с 01.07.2027). 4.2. Обязанность физических лиц — резидентов информировать налоговые органы об операциях с цифровыми валютами в зарубежных информационных системах вводится со 02.05.2027; порядок и формы уведомления подлежат установлению подзаконными актами — сверять на дату направления запроса.

Уголовно-процессуальный кодекс РФ: ст. 182–183 (обыск, выемка), ст. 186 (контроль и запись переговоров).

Федеральный закон «Об адвокатской деятельности и адвокатуре в РФ»: ст. 6.1 (адвокатский запрос).

Специальных методических рекомендаций по назначению экспертиз в отношении цифровых данных не издавалось. Применяются общие акты: Методические рекомендации по производству судебных экспертиз в государственных судебно-экспертных учреждениях системы Минюста России (приказ Минюста России от 20.12.2002 № 346) и Инструкция по организации производства судебных экспертиз (приказ Минюста России от 28.12.2023 № 404). Исследование устройств проводится в рамках компьютерно-технической экспертизы; отдельного рода экспертизы для криптоактивов в Перечне родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России (утв. приказом Минюста России от 20.04.2023), не выделено.

* * *

Глава 4. Сквозной кейс № 1: от подозрения к доказанному факту

* * *

Елена К. пришла к адвокату Морозовой в сентябре. На столе лежали: свидетельство о браке, свидетельство о рождении двух детей, выписка из ЕГРН на квартиру (приобретена до брака), ПТС на Toyota Camry. И одно предложение: «Он точно что-то купил. Я видела. Но доказать не могу». Через четыре месяца работы у адвоката Морозовой на столе лежали: банковские выписки за три года, протокол осмотра телефона с зафиксированным скриншотом, показания двух свидетелей, нотариально заверенная переписка из семейного чата, частичный ответ биржи и заключение ончейн-аналитика на двенадцать страниц. Из «он точно что-то купил» дело превратилось в «ответчик владел 1,247 BTC и 14,8 ETH на общую сумму около 9,2 миллиона рублей на дату раздела». Это не финал. Но это фундамент, на котором строится иск.

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.