БОРИС ЛЕВ

КРИПТОВАЛЮТНАЯ КРИМИНАЛИСТИКА

Как проследить, вернуть и сохранить цифровые активы

Для юристов, следователей и владельцев криптоактивов

Борис Лев

Криптовалютная криминалистика

«Автор»
2026

Лев Б.

Криптовалютная криминалистика / Б. Лев — «Автор», 2026

Практическое руководство по расследованию криптовалютных хищений. Как читать блокчейн и проследить украденное, добиться заморозки средств на бирже и у эмитента стейблкоина, вернуть их через суд и защитить активы от кражи. Готовые шаблоны заявлений и запросов, чеклисты, глоссарий. Для юристов, следователей, комплаенс-специалистов и владельцев криптоактивов.

Содержание

Борис Лев
Криптовалютная криминалистика

О книге

Первое русскоязычное руководство, объединяющее техническую, юридическую и практическую стороны расследования криптовалютных преступлений — от чтения блокчейна до возврата украденных средств и защиты от физических угроз. Для юристов, следователей, compliance-специалистов и криптовладельцев.

Публичный блокчейн не забывает ничего. Когда криптовалюта «исчезает», она не исчезает — она движется по цепочке адресов, и каждый её шаг записан навсегда. Проблема криптовалютных хищений не в отсутствии доказательств, а в нехватке людей, умеющих их читать, и институтов, умеющих на них реагировать. Эта книга восполняет первое.

От природы блокчейна и механики хищений — через практику трейсинга, работу с биржами, эмитентами стейблкоинов и правоохранительными органами — к возврату средств и, наконец, к защите: цифровой, технической и физической. Теория подкреплена реальными делами и актуальной практикой, а приложения дают готовые шаблоны, чеклисты и инструменты.

ЧАСТЬ I. ФУНДАМЕНТ

Как устроен блокчейн и почему криптовалюта не анонимна

Глава 1. Природа блокчейна как публичного реестра

«Деньги исчезли». Эту фразу слышит каждый, кто работает с криптовалютными хищениями. Клиент переводит средства мошеннику, и они словно растворяются в цифровом воздухе. Но это иллюзия. В криптовалюте ничто не исчезает. Каждая монета, ушедшая с кошелька жертвы, оставляет за собой след — публичный, неизменный и доступный любому, кто умеет его читать. Проблема почти никогда не в отсутствии следа. Проблема в том, что мало кто умеет его прочитать.

Эта книга — о том, как читать этот след. Но прежде чем говорить о расследовании, нужно понять, почему след вообще существует. Ответ лежит в самой природе блокчейна.

1.1. Что такое блокчейн простыми словами

Представьте огромную бухгалтерскую книгу, лежащую на площади посреди города. В неё записываются все денежные переводы между жителями: кто, кому и сколько передал. Книга открыта — подойти и прочитать любую запись может каждый прохожий. Записи нельзя стереть или подделать: как только строчка внесена, она остаётся там навсегда, и тысячи людей уже видели её и скопировали. Если кто-то попытается подменить страницу, несоответствие мгновенно заметят все остальные, у кого есть точная копия той же книги.

Это и есть блокчейн — с той разницей, что «площадь» глобальна, а «прохожие» — тысячи компьютеров по всему миру, каждый из которых хранит полную копию книги и постоянно сверяет её с копиями соседей.

Три свойства этой книги делают её принципиально не похожей на всё, что было раньше.

Она распределённая. Не существует единственного сервера, где хранится «главная» версия. Копии реестра держат тысячи независимых участников сети. Ни один из них не может единолично изменить запись — для этого пришлось бы одновременно переписать историю у большинства участников по всему миру, что практически невозможно.

Она неизменная. Однажды подтверждённая транзакция не может быть отменена, отредактирована или удалена. В банковской системе перевод можно оспорить, заморозить, откатить. В блокчейне — нет. Запись фиксируется навсегда. Именно эта неизменность, которая делает криптовалюту привлекательной для мошенников (перевод нельзя вернуть простым звонком в банк), одновременно делает её идеальной для расследования (след нельзя стереть).

Она публичная. Здесь кроется главное недоразумение. Большинство людей уверены, что криптовалюта анонимна. На самом деле всё наоборот: публичный блокчейн прозрачнее любой банковской системы. Каждая транзакция, когда-либо совершённая в сети Bitcoin или Ethereum, видна каждому желающему — прямо сейчас, бесплатно, без единого запроса в какой-либо орган. Вы можете открыть браузер, ввести адрес чужого кошелька и увидеть всю историю его операций: когда он получал средства, сколько, от кого и куда переводил дальше.

Сравним с привычной финансовой системой. Чтобы узнать, куда ушли деньги с банковского счёта, нужен официальный запрос, судебный ордер, сотрудничество банка, и всё это касается только «своего» банка — операции в других учреждениях остаются за пределами видимости. В блокчейне вся эта информация лежит на поверхности изначально. Нет привратника, у которого нужно спрашивать разрешения. Реестр открыт по своей конструкции.

Владельцу криптоактивов. Из этого следует важный практический вывод, к которому мы ещё не раз вернёмся: всё, что вы делаете с криптовалютой, видно навсегда. Каждый ваш перевод — публичная запись. Это не повод для паранойи, но повод для осознанности, особенно когда речь пойдёт о безопасности (Часть V).

1.2. Транзакция, блок, хеш

Чтобы читать блокчейн, нужно понимать его элементарную единицу — транзакцию. Всё расследование, каким бы сложным оно ни было, в конечном счёте сводится к чтению отдельных транзакций и прослеживанию связей между ними.

Транзакция — это запись о переводе средств. Она содержит несколько ключевых элементов: адрес отправителя, адрес получателя, сумму, точное время и комиссию за проведение. Всё это фиксируется с точностью до секунды и остаётся в реестре навсегда. Ни одна деталь не может быть изменена задним числом.

У каждой транзакции есть уникальный идентификатор — **хеш транзакции** (transaction hash, или сокращённо tx hash). Это длинная строка из букв и цифр, которая служит своего рода «отпечатком пальца» операции. Двух одинаковых хешей не существует. Зная хеш, можно мгновенно найти транзакцию в реестре и увидеть все её детали. В расследовании хеш — отправная точка: с него начинается прослеживание практически любой цепочки.

Следователю. Первое, что нужно получить от заявителя, — это tx hash. Он есть в истории кошелька жертвы. Одного хеша достаточно, чтобы восстановить сумму, время, адрес получателя и начать движение по цепочке. Заявление без хеша — как заявление об угоне без номера машины.

Транзакции не висят в реестре поодиночке. Они собираются в **блоки** — группы транзакций, подтверждённых сетью примерно в одно время. Каждый новый блок содержит ссылку на предыдущий, образуя непрерывную цепочку — отсюда и название «блокчейн», цепочка блоков. Эта конструкция и обеспечивает неизменность: чтобы подделать одну старую транзакцию, пришлось бы переписать все блоки, идущие после неё, причём быстрее, чем вся остальная сеть создаёт новые. Задача, невыполнимая на практике.

Когда транзакция попадает в блок и этот блок принимается сетью, говорят, что транзакция получила **подтверждение**. С каждым следующим блоком число подтверждений растёт, и вероятность того, что операцию можно как-то обратить, стремится к нулю. Через несколько подтверждений транзакция считается окончательной — это свойство называют **финальностью**. Финальность означает простую вещь: перевод состоялся, и отменить его нельзя никаким способом.

Именно здесь проходит водораздел между криптовалютой и банковским переводом. Ошибочный или мошеннический банковский платёж можно попытаться отозвать через банк. Криптовалютный перевод после финальности необратим на уровне самой сети. Для жертвы это плохая новость: деньги ушли, и «нажать отмену» невозможно. Но для расследователя это же свойство — союзник: то, что нельзя отменить, нельзя и скрыть. Транзакция навсегда останется в реестре как улика.

1.3. Миф об анонимности

Откуда же взялось стойкое убеждение, что криптовалюта анонимна?

Отчасти виной репутация. На заре своего существования Bitcoin ассоциировался с закрытыми онлайн-площадками, где им расплачивались за нелегальные товары именно в расчёте на анонимность. Отчасти — недопонимание технологии: раз в адресе кошелька нет имени и паспорта, значит, рассуждает обыватель, владелец неизвестен. Отчасти — маркетинг самих криптопроектов, десятилетиями продававших «свободу от надзора».

Реальность устроена тоньше, и различие здесь принципиальное. Криптовалюта не анонимна. Она **псевдонимна**.

Разница между анонимностью и псевдонимностью — это разница между человеком без имени и человеком под постоянным псевдонимом. Анонимность означает, что действия невозможно связать между собой: каждое из них совершено «никем». Псевдонимность означает, что все действия совершены под одним и тем же условным именем — адресом,, но само это имя формально не привязано к личности.

Криптовалютный адрес, и есть такой псевдоним. Он не содержит вашего паспорта, но он абсолютно последователен: все операции с этого адреса видны, связаны друг с другом и образуют единую, прослеживаемую историю. Пока адрес ни с чем не связан, он остаётся «человеком под маской». Но стоит один-единственный раз раскрыть связь между адресом и реальной личностью, и маска спадает не с одной операции, а со всей истории адреса разом.

Приведём условный пример. Некто годами пользуется одним адресом, считая себя невидимым. Однажды он выводит средства на биржу, где при регистрации предъявил паспорт. С этого момента биржа знает: адрес X принадлежит гражданину Y. И теперь любая транзакция этого адреса — за все годы, вперёд и назад — потенциально ассоциируется с конкретным человеком. Одна точка контакта с реальным миром деанонимизирует всю цепочку.

Таких точек контакта в жизни любого пользователя множество: регистрация на бирже с верификацией, покупка через сервис с проверкой личности, публикация адреса в соцсети для приёма донатов, упоминание на форуме. Псевдоним держится ровно до первой утечки, а утечка почти всегда происходит, потому что рано или поздно криптовалюту нужно превратить в обычные деньги, а это делается через регулируемые точки, требующие идентификации.

Юристу. Именно на этом строится большинство успешных дел. Расследователь не «взламывает» блокчейн — он прослеживает псевдонимную цепочку до точки, где она касается идентифицируемой инфраструктуры (чаще всего биржи), и уже там, правовым путём, получает связь «адрес -> личность». Технология лишь доводит до двери; открывает её процессуальный запрос. Об этом — вся Часть IV.

Стоит оговорить и обратную сторону, чтобы не впасть в противоположную крайность. Существуют инструменты, специально созданные для усложнения прослеживания, — миксеры, мосты между сетями, приватные монеты. Они действительно затрудняют работу, и им посвящена отдельная глава (Глава 6). Но забегая вперёд: они повышают стоимость расследования, а не делают его невозможным, и почти всегда оставляют следы на стыках. Полная анонимность в точке, где криптовалюта встречается с настоящими деньгами, недостижима.

1.4. Публичность как основа криминалистики

Соберём сказанное воедино и посмотрим, что оно означает для того, кто расследует хищение.

Каждая транзакция **верифицируема без обращения к третьим сторонам.** Чтобы подтвердить факт и детали перевода, не нужен запрос в банк, не нужно ждать ответа оператора, не нужно ничьё разрешение. Достаточно открыть публичный реестр и убедиться самому. Доказательство уже существует и доступно — его нужно лишь правильно зафиксировать (как это делается процессуально корректно, разбирается в Главе 15).

Данные доступны **в реальном времени, бесплатно и навсегда.** В тот момент, когда мошенник переводит похищенное дальше по цепочке, эта операция уже видна расследователю. Не через недели, которые уходят на межбанковские запросы, а немедленно. Это меняет саму динамику: в криптовалютном расследовании можно наблюдать за движением средств почти вживую и реагировать, пока окно возможностей открыто.

Наконец, криптовалюта в этом смысле **прозрачнее и наличных, и банковских переводов.** Наличные не оставляют следа вовсе. Банковский перевод оставляет след, но закрытый — доступный только банку и по запросу. Криптовалютный перевод оставляет след открытый, полный и вечный. Парадокс в том, что инструмент, который многие считают идеальным для сокрытия денег, на деле оказался одним из самых прозрачных инструментов в истории финансов.

Отсюда — центральная мысль всей этой книги, которую стоит сформулировать прямо.

Когда в криптовалюте «пропадают» деньги, они не пропадают. Они движутся. Они переходят с адреса на адрес, дробятся, сходятся вновь, но каждый их шаг записан в открытом реестре. Задача расследователя — не найти исчезнувшее, а прочитать то, что и так лежит на виду. Средства почти всегда можно проследить до точки, где они входят в регулируемую инфраструктуру,, и именно там начинается возможность их заморозить и вернуть.

Проблема криптовалютных хищений — не в отсутствии доказательств. Доказательства публичны, неизменны и исчерпывающи. Проблема — в отсутствии людей, умеющих их читать, и институтов, умеющих на них реагировать. Восполнить первое — цель этой книги.

Что дальше

Мы установили фундамент: блокчейн — публичный, неизменный реестр, криптовалюта псевдонимна, а не анонимна, и след хищения всегда существует. Но чтобы понять, как именно происходят хищения и где проходят границы возврата, нужно разобраться в следующем вопросе: что вообще означает «владеть» криптовалютой?

Ответ не так очевиден, как кажется. В криптовалюте владение — это не запись в чьём-то реестре собственности, а контроль над секретным ключом. Кто контролирует ключ, тот владеет средствами; кто узнал ключ, тот их получил. На этом простом факте держится и природа хищений, и пределы того, что можно вернуть. Ему посвящена следующая глава.

Ключевые понятия главы: блокчейн, распределённый реестр, транзакция, блок, хеш транзакции (tx hash), подтверждение, финальность, псевдонимность, точка деанонимизации.

Глава 2. Кошельки, адреса и ключи

В обычном мире владение деньгами подтверждается записью: банк ведёт счёт, на котором значится ваше имя и сумма. Вы владеете деньгами, потому что банк признаёт вас их владельцем. В криптовалюте нет банка и нет реестра собственности. Здесь владение — это не запись о вас, а знание секрета. Кто знает секрет, тот владеет средствами. Кто узнал ваш секрет — тот получил ваши средства, и никакой банк не восстановит справедливость. Понять природу этого секрета — значит понять и как происходят хищения, и почему одни из них поправимы, а другие — нет.

2.1. Приватный ключ, публичный ключ, адрес

В основе любого криптовалютного кошелька лежат три связанные сущности: приватный ключ, публичный ключ и адрес. Разобраться в их взаимоотношении необходимо, потому что почти каждое хищение — это, по сути, история о том, как посторонний завладел тем, чем владеть не должен.

Приватный ключ — это и есть тот самый секрет. Технически он представляет собой очень большое случайное число, но для наших целей важнее его функция: приватный ключ позволяет распоряжаться средствами. Тот, кто им обладает, может подписать транзакцию, то есть отдать сети распоряжение перевести средства. Подпись, созданная приватным ключом, математически доказывает сети, что распоряжение исходит от законного владельца, при этом сам ключ никому не раскрывается. Уместна аналогия с собственноручной подписью, которую невозможно подделать: вы ставите её под документом, и все убеждаются в подлинности, но повторить её не может никто.

Из приватного ключа математически выводится **публичный ключ**, а из публичного — **адрес**. Эта цепочка односторонняя: зная приватный ключ, легко получить публичный ключ и адрес, но проделать обратный путь — вычислить приватный ключ, зная лишь адрес, — практически невозможно. На этой односторонности держится вся безопасность криптовалюты.

Адрес — это то, что вы сообщаете другим, чтобы получить перевод. Аналогия проста: адрес — как номер счёта, который можно давать кому угодно, а приватный ключ — как подпись и доступ к счёту, которые нельзя отдавать никому. Опубликовать адрес безопасно; опубликовать приватный ключ — значит подарить все средства первому, кто его увидит.

Здесь кроется важное следствие, которое стоит усвоить сразу. Поскольку приватный ключ нельзя восстановить, зная адрес, его нельзя и «сбросить», как забытый пароль от почты. Если приватный ключ утерян — доступ к средствам утрачен навсегда, и никто в мире не поможет. Если приватный ключ украден — средства украдены вместе с ним, потому что для сети вор с ключом неотличим от владельца. Сеть не знает, кто «настоящий» хозяин. Она знает лишь, что распоряжение подписано верным ключом,, и исполняет его.

Следователю. Это объясняет, почему криптовалютное хищение так отличается от банковского мошенничества. Когда вор получил приватный ключ (через фишинг, вредоносную программу или физическое принуждение), перевод средств выглядит для сети абсолютно законным. Нет «несанкционированной операции», которую можно оспорить у оператора. Операция санкционирована — просто не тем человеком. Именно поэтому центр тяжести расследования смещается на прослеживание уже ушедших средств, а не на отмену перевода.

2.2. Seed-фраза

На практике пользователи почти никогда не имеют дела с приватным ключом напрямую — он слишком длинный и неудобный. Вместо этого современные кошельки используют **seed-фразу** (её также называют мнемонической, или восстановительной, фразой) — последовательность из двенадцати или двадцати четырёх обычных слов.

Эта фраза — не просто пароль. Из неё математически выводятся все приватные ключи кошелька, а значит, и доступ ко всем средствам на всех адресах, которые этот кошелёк создаёт. Seed-фраза — это корень всего дерева. Тот, кто знает вашу seed-фразу, обладает полным и безоговорочным контролем над вашими активами: он может восстановить ваш кошелёк на любом устройстве в любой точке мира и вывести всё.

Из этого вытекает единственное, но абсолютное правило, которое проходит красной нитью через всю книгу: **seed-фразу не должен видеть никто, кроме вас, и вводить её нужно только при восстановлении собственного кошелька.** Ни один настоящий сервис, биржа, кошелёк или служба поддержки никогда не попросит вашу seed-фразу. Любая такая просьба — без единого исключения — есть попытка хищения. Мы будем возвращаться к этому правилу в разных контекстах, потому что колоссальная доля всех хищений сводится именно к тому, что жертву тем или иным способом убедили раскрыть seed-фразу.

Владельцу. Запомните формулировку и относитесь к ней как к аксиоме: **просьба назвать seed-фразу = мошенничество.** Не бывает «проверки безопасности», «восстановления через поддержку» или «верификации кошелька», требующих ввести эти двенадцать слов на чужом сайте или сообщить их человеку. Как только вы усвоите это правило намертво, вы становитесь неуязвимы для целого класса атак, разбираемых в Главе 7.

Понимание роли seed-фразы объясняет и то, почему она — главная цель не только онлайн-мошенников, но и тех, кто идёт на физическое насилие. Завладеть seed-фразой — значит завладеть всем сразу. Этой стороне вопроса, где цифровая угроза перерастает в физическую, посвящена Глава 23.

2.3. Типы кошельков

Слово «кошелёк» в криптовалюте означает не хранилище денег, а хранилище ключей. Средства всегда «лежат» в блокчейне; кошелёк лишь хранит ключи, дающие право ими распоряжаться. Кошельки различаются по тому, где и как эти ключи хранятся, и от этого напрямую зависит уровень риска.

Горячие и холодные. Горячий кошелёк — тот, что подключён к интернету: приложение на телефоне, расширение в браузере, веб-сервис. Он удобен для повседневных операций, но именно из-за постоянного подключения уязвим для удалённых атак — вредоносных программ, фишинга, компрометации устройства. Холодный кошелёк хранит ключи офлайн, вне досягаемости сетевых атак. Он менее удобен, но несравнимо безопаснее для хранения значимых сумм.

Программные, аппаратные, бумажные. Программный кошелёк — приложение или расширение; ключи хранятся на устройстве, которое, как правило, подключено к сети. Аппаратный кошелёк (Ledger, Trezor, Keystone и подобные) — специальное физическое устройство, где ключи изолированы и никогда не покидают его: даже подписывая транзакцию, устройство не раскрывает ключ подключённому компьютеру. Это делает аппаратные кошельки стандартом для безопасного хранения. Бумажный кошелёк — ключ или seed-фраза, записанные на физическом носителе и хранящиеся вне любых устройств; надёжен против цифровых атак, но уязвим к пожару, воде, утере и подсматриванию.

Кастодиальные и некастодиальные. Это различие — одно из важнейших в криптовалюте, и его недопонимание стоило людям целых состояний. В некастодиальном кошельке ключи храните вы сами: вы, и только вы, контролируете средства. В кастодиальном кошельке ключи хранит за вас третья сторона — чаще всего биржа. Формально на счёте биржи «ваши» средства, но фактически ключами распоряжается биржа. Вы владеете не самими монетами, а обещанием биржи выдать их по требованию.

Отсюда — известная в отрасли формула: **«Не твои ключи — не твои монеты»** (not your keys, not your coins). Пока средства лежат на бирже, вы зависите от её платёжеспособности, честности и работоспособности. Если биржа рухнет, будет взломана, заморозит вывод или окажется мошеннической, вы можете потерять всё, не совершив ни единой ошибки. История криптовалют знает не один крах крупной биржи, унёсший средства сотен тысяч людей, чьи ключи хранились «в надёжном месте».

Каждый тип кошелька — это точка на шкале между удобством и безопасностью. Горячий кастодиальный кошелёк на бирже удобен для торговли, но сопряжён с максимальной зависимостью от третьей стороны. Холодный аппаратный некастодиальный кошелёк максимально безопасен, но требует дисциплины в обращении. Разумная стратегия, к которой мы вернёмся в Части V, — не выбирать одно, а разделять: держать оперативные суммы в удобных кошельках, а основные активы — в безопасных.

Юристу. Различие кастодиального и некастодиального хранения имеет прямые правовые последствия. Если средства украдены с некастодиального кошелька через компрометацию ключа, ответчиком выступает похититель, а точкой воздействия — биржа, куда средства в итоге поступят. Если же средства «пропали» на кастодиальной бирже (крах, заморозка, отказ в выводе), природа спора иная — это претензия к самой бирже, и она разбирается в Главе 20. Первый вопрос в любом деле: чьи ключи контролировали средства в момент утраты.

2.4. Как теряется и похищается доступ

Теперь, когда механика ключей ясна, соберём воедино способы, которыми люди утрачивают контроль над средствами. Эта карта угроз — своего рода оглавление к Главе 7, где каждая схема разбирается подробно; здесь же важно увидеть, как все они сводятся к одному: к получению злоумышленником контроля над ключом или к перенаправлению средств.

Утечка seed-фразы. Самый прямой путь. Жертву обманом побуждают ввести seed-фразу на поддельном сайте (фишинг), либо вредоносная программа считывает её с устройства, либо человека вынуждают назвать её под давлением. Во всех случаях результат одинаков и необратим: злоумышленник получает полный контроль и выводит средства. Напомним ещё раз — ни один законный сервис seed-фразу не запрашивает, поэтому любой запрос заведомо враждебен.

Компрометация устройства. Вредоносное программное обеспечение, попавшее на телефон или компьютер через поддельное приложение, заражённый файл или вредоносное расширение браузера, способно похитить ключи, перехватить seed-фразу или незаметно подменить действия пользователя. Особенно коварна подмена адреса в буфере обмена: пользователь копирует адрес получателя, а вредонос подставляет вместо него адрес злоумышленника, и перевод уходит не туда. Человек в момент операции ничего не замечает.

Подмена адреса. Даже без заражения устройства средства можно увести, заставив жертву отправить их не на тот адрес. Приём под названием «отравление адреса» (address poisoning) эксплуатирует привычку копировать адрес из истории операций: злоумышленник заранее «загрязняет» историю адресом-двойником, внешне похожим на настоящий. К этому классу относится и упомянутая подмена через буфер обмена. Общий принцип: похититель не крадёт ключ, а обманывает жертву относительно того, куда идут средства.

Кастодиальный риск. Здесь ключ не похищается вовсе — он изначально не у пользователя. Средства теряются из-за краха биржи, её взлома, заморозки вывода или мошенничества оператора. Это не «взлом» в техническом смысле, а реализация того самого риска доверия, о котором говорит формула «не твои ключи — не твои монеты».

Все эти пути объединяет общая логика. В криптовалюте невозможно «взломать блокчейн» — реестр надёжно защищён математикой. Атакуют не блокчейн, а человека и его окружение: его доверчивость, его устройство, его привычки, его зависимость от посредников. Понимание этого разворачивает всю стратегию защиты (Часть V): бессмысленно укреплять то, что и так неприступно, — нужно защищать слабое звено, а слабое звено — почти всегда сам пользователь.

И то же понимание задаёт границы возврата, что критически важно осознать честно. Если приватный ключ или seed-фраза скомпрометированы, средства уходят необратимо на уровне блокчейна — «откатить» перевод нельзя. Единственная надежда на возврат появляется дальше по цепочке: когда похищенные средства достигают регулируемой точки — биржи или эмитента стейблкоина, — где их можно проследить, заморозить и, возможно, вернуть правовым путём. Вся Часть IV — об этом окне возможностей. Но само окно существует лишь потому, что похититель, завладев средствами, вынужден их куда-то двигать,, а каждое движение, как мы установили в Главе 1, публично и вечно.

Что дальше

Мы разобрались, что владение криптовалютой есть контроль над ключом и что хищение — это, по сути, утрата такого контроля тем или иным способом. Но до сих пор мы говорили о криптовалюте вообще, будто это единая система. На деле это не так. Существуют десятки различных сетей, устроенных по-разному, и то, в какой именно сети произошла операция, определяет, как её читать, каким инструментом прослеживать и где искать след.

Прежде чем расследовать, нужно определить сеть. Ошибка здесь означает поиск в неверном реестре и потерю драгоценного времени. Тому, чем различаются основные сети и почему это принципиально для расследования, посвящена следующая глава.

Ключевые понятия главы: приватный ключ, публичный ключ, адрес, seed-фраза (мнемоническая фраза), горячий и холодный кошелёк, аппаратный кошелёк, кастодиальное и некастодиальное хранение, «не твои ключи — не твои монеты», компрометация устройства, отравление адреса, кастодиальный риск.

Глава 3. Сети и их особенности

«Криптовалюта» — слово в единственном числе, и оно вводит в заблуждение. За ним скрывается не одна система, а десятки самостоятельных сетей, устроенных по-разному, живущих по разным правилам и требующих разных инструментов для чтения. Для расследователя первый и обязательный шаг — определить, в какой именно сети произошла операция. Ошибка на этом шаге означает, что вы ищете след в чужом реестре, где его нет и быть не может,, и теряете время, которого при хищении почти нет. Эта глава — о том, чем различаются основные сети и почему различие принципиально.

3.1. Bitcoin и модель UTXO

Bitcoin — первая и старейшая криптовалюта, и её внутреннее устройство заметно отличается от большинства пришедших следом. Понять его логику важно не ради истории, а потому, что на этой логике строятся специфические приёмы прослеживания.

В привычном представлении у счёта есть баланс — единое число, которое растёт при поступлениях и уменьшается при тратах. В Bitcoin такого «баланса» в буквальном смысле не существует. Вместо него сеть оперирует **непотраченными выходами транзакций** — по-английски Unspent Transaction Outputs, сокращённо UTXO. Разберём это на понятной аналогии.

Представьте, что все ваши деньги — это не сумма на счёте, а набор отдельных купюр в кармане. Каждая купюра имеет свой номинал и получена в результате какого-то конкретного платежа. Когда вы хотите что-то купить, вы не «списываете сумму со счёта» — вы достаёте одну или несколько купюр. Если точной суммы нет, вы отдаёте купюру большего номинала и получаете сдачу — новую купюру. Именно так работает Bitcoin. Каждый UTXO — это «купюра», полученная в прошлой транзакции и ещё не потраченная. Когда владелец совершает перевод, он «тратит» один или несколько своих UTXO целиком, а разница возвращается ему в виде нового UTXO — сдачи.

Отсюда важное практическое следствие: одна транзакция в Bitcoin может иметь несколько входов и несколько выходов. Несколько «купюр» на входе объединяются, чтобы набрать нужную сумму; на выходе появляются платёж получателю и сдача отправителю. Для читающего реестр это и сложность, и возможность.

Возможность заключается в приёме, который называется **кластеризацией по общим входам**. Логика проста: если в одной транзакции несколько UTXO тратятся вместе, значит, отправитель контролировал приватные ключи ко всем этим «купюрам» одновременно. Следовательно, соответствующие адреса с высокой вероятностью принадлежат одному владельцу. Прослеживая, какие адреса регулярно «скидываются» в общие транзакции, аналитик группирует их в кластеры, стоящие за одним лицом или сервисом. Это один из фундаментальных методов анализа Bitcoin, к которому мы вернёмся в Главе 12.

Следователю. В Bitcoin не ищите «баланс адреса» как единое движение. Читайте транзакции как наборы входов и выходов, обращайте внимание на сдачу (часто это выход, возвращающийся на адрес, связанный с отправителем) и используйте общие входы как указание на принадлежность адресов одному владельцу.

Bitcoin остаётся главной сетью для крупных переводов стоимости и по-прежнему фигурирует в значительной части серьёзных дел. Но большинство современного криптомошенничества, особенно с использованием стейблкоинов, происходит в сетях иного типа — устроенных вокруг понятия счёта.

3.2. Ethereum и account-based модель

Ethereum ввёл принципиально иную модель — **основанную на счетах** (account-based). Здесь всё устроено привычнее: у каждого адреса есть баланс — единое число, которое увеличивается при поступлениях и уменьшается при тратах, ровно как на банковском счёте. Нет «купюр», нет UTXO, нет сдачи. Есть счёт и его состояние.

Эта модель проще для чтения: чтобы понять положение адреса, достаточно посмотреть его текущий баланс и историю операций, каждая из которых прямо изменяет этот баланс. Но подлинное значение Ethereum не в удобстве учёта, а в другом его свойстве.

Ethereum — не просто платёжная сеть, а платформа для **смарт-контрактов**. Смарт-контракт — это программа, живущая в блокчейне и исполняющаяся автоматически при заданных условиях. Проще говоря, наряду с обычными адресами-«счетами», которыми управляют люди с помощью ключей, в Ethereum существуют адреса-программы, которые действуют по заложенному в них коду. На этой возможности выросла вся индустрия децентрализованных приложений: биржи без оператора (DEX), протоколы кредитования, и — что особенно важно для нашей темы — токены.

Именно смарт-контракты делают Ethereum и родственные ему сети основной средой для выпуска токенов, включая стейблкоины. А стейблкоины, как мы увидим, — центральный элемент и криптомошенничества, и его расследования. Поэтому большая часть практической работы современного крипторасследователя проходит именно в среде account-based сетей.

Владельцу. Различие между переводом «монеты сети» и переводом токена — не техническая тонкость, а вещь, с которой вы столкнётесь на практике и которую эксплуатируют мошенники. К этому мы вернёмся в разделе 3.5; пока запомните, что «отправить USDT» и «отправить ETH» — технически разные операции, хотя внешне и похожи.

3.3. EVM-совместимые сети

Успех Ethereum породил целое семейство сетей, построенных на той же технической основе. В их сердце — **виртуальная машина Ethereum** (Ethereum Virtual Machine, EVM), среда, в которой исполняются смарт-контракты. Сети, использующие EVM, называют **EVM-совместимыми**, и к ним относятся многие из наиболее активных сегодня: Arbitrum, Base, Polygon, BNB Smart Chain (BSC) и другие.

Практическое значение совместимости огромно, и его нужно ясно осознать. Все EVM-сети используют один и тот же формат адресов — тот, что начинается с символов «0x». Это означает, что один и тот же адрес существует одновременно во всех этих сетях. Адрес, на который вам пришли средства в сети Ethereum, технически «существует» и в Arbitrum, и в Polygon, и в BSC — это буквально одна и та же строка.

Отсюда следует правило, критически важное для расследования: **обнаружив адрес, проверять его нужно в каждой сети по отдельности.** Средства могли прийти на этот адрес в одной сети, а уйти — в другой. Если аналитик смотрит только Ethereum, он не увидит операций, произошедших в BSC с тем же адресом, и решит, что след оборвался, тогда как в действительности он просто перешёл в другую сеть. Это одна из самых распространённых ошибок начинающих, и мы ещё вернёмся к ней в главе о методологии.

Следователю. Один «0x»-адрес — множество сетей. Прежде чем заключить, что средства «застыли» или «исчезли», проверьте адрес в основных EVM-сетях. Мультичейн-инструменты (о них в Главе 10) делают это автоматически, но и вручную через разные эксплореры проверка обязательна.

Различаются EVM-сети между собой в основном скоростью, стоимостью операций и составом сервисов. Для мошенника выбор сети часто диктуется дешевизной переводов: чем ниже комиссия, тем дешевле дробить и гонять средства по длинным цепочкам. Это подводит нас к сети, которая по этой самой причине стала доминирующей в криптомошенничестве, — к TRON.

3.4. TRON и доминирование в USDT-переводах

TRON — отдельная сеть, не входящая в семейство EVM, но крайне важная для практики, потому что именно через неё проходит огромная доля мошеннических переводов в стейблкоине USDT.

Причина этого доминирования прозаична — деньги. Переводы в сети TRON обходятся очень дёшево, значительно дешевле, чем в основной сети Ethereum. Для того, кто перемещает похищенные средства, дробит их на части и прогоняет через десятки адресов, стоимость каждой операции имеет прямое значение. Низкая комиссия TRON делает эту сеть удобной для отмывания: можно совершать множество переводов, почти не теряя на издержках. В результате TRON стал, по сути, сетью по умолчанию для USDT-операций в теневой части рынка, и подавляющее большинство дел, связанных с хищением стейблкоинов, так или иначе выходит на TRON.

Практически это означает, что расследователь обязан уверенно работать с TRON и его эксплорером — Tronscan. Формат адресов здесь иной, чем в EVM-сетях: адреса TRON начинаются с символа «T». Логика чтения транзакций близка к account-based модели: у адреса есть баланс, операции его изменяют. Но инфраструктура, метки, инструменты — свои, и переносить навыки из Ethereum нужно с поправкой на специфику сети.

Юристу. Если клиент сообщает, что перевёл или потерял USDT, первый уточняющий вопрос — в какой сети. Чаще всего ответом будет TRON, реже Ethereum или BSC. От этого зависит выбор эксплорера, набор инструментов и даже адресат запросов. Универсального «USDT» не существует — есть USDT в конкретной сети, и путать их нельзя.

3.5. Токены и стандарты

Мы несколько раз упомянули различие между «монетой сети» и «токеном». Пришло время разобрать его до конца, потому что на этом различии основаны и практика чтения транзакций, и целый ряд мошеннических приёмов.

У каждой сети есть своя **собственная монета**: у Ethereum это ETH, у TRON — TRX, у BSC — BNB. Эта монета встроена в саму сеть и используется, в частности, для оплаты комиссий за операции. **Токен** — это нечто иное. Токен не встроен в сеть на базовом уровне; он существует как смарт-контракт, «живущий» поверх сети. USDT, USDC и тысячи других — это токены, выпущенные контрактами на базовых сетях.

Различие имеет прямые практические последствия. Перевод собственной монеты сети — простая операция, прямо меняющая баланс. Перевод токена — это, с технической точки зрения, вызов смарт-контракта токена, который ведёт свой внутренний учёт того, кому сколько принадлежит. Поэтому в блокчейн-эксплорере переводы токенов часто отображаются в отдельном разделе (обычно он называется Token Transfers), а не вместе с «обычными» транзакциями. Аналитик, который смотрит только основную вкладку транзакций и не заглядывает в раздел токенов, рискует не увидеть именно те переводы, которые его интересуют. Это ещё одна типичная ошибка, о которой пойдёт речь в главах о чтении реестра.

Чтобы токены разных проектов могли единообразно работать с кошельками и сервисами, введены **стандарты**. В сети Ethereum это стандарт ERC-20, в TRON — TRC-20, в BSC — BEP-20. Все они описывают, по сути, одинаковый набор правил поведения токена, но в своей сети. Именно поэтому USDT существует в нескольких «версиях» — как токен ERC-20 в Ethereum, как TRC-20 в TRON, как BEP-20 в BSC. Это один и тот же по назначению стейблкоин, но технически — разные токены в разных сетях, и переводы между ними напрямую невозможны без специальных мостов (о них в Главе 6).

Есть и ещё одна деталь, которую стоит запомнить, потому что она порождает отдельный тип мошенничества. Комиссия за перевод токена платится не в самом токене, а в собственной монете сети. Чтобы отправить USDT в сети Ethereum, нужен ETH на комиссию; чтобы отправить USDT в TRON, нужен TRX. Пользователь, у которого на кошельке есть только токены, но нет монеты сети на комиссию, не сможет совершить перевод. Это техническое обстоятельство мошенники обыгрывают в схемах, где жертву заманивают на «кошелёк с USDT», доступа к которому она в реальности получить не может,, но об этом подробнее в Главе 7.

Владельцу. Практический вывод: всегда проверяйте не только сумму и адрес, но и то, какой именно токен и в какой сети вы отправляете или получаете. Токен-двойник с тем же названием, но иным контрактом, или перевод в неожиданной сети — распространённый приём обмана, который мы разберём в разделе о подмене сумм и токенов.

Что дальше

Мы установили, что «криптовалюта» — это множество различных сетей, и что определение сети есть обязательный первый шаг любого расследования. Bitcoin с его моделью «купюр»-UTXO, Ethereum и родственные ему account-based сети со смарт-контрактами, семейство EVM с общим форматом адресов, TRON как царство дешёвых USDT-переводов, токены и их стандарты — вот карта местности, по которой предстоит вести поиск.

Среди всех активов один класс требует отдельного, пристального внимания — стейблкоины. Они одновременно являются главным инструментом криптомошенников и главной надеждой на возврат средств, потому что, в отличие от Bitcoin или Ethereum, имеют централизованного эмитента, способного заморозить средства прямо на уровне контракта. Этой двойственной природе стейблкоинов и той уникальной точке воздействия, которую они открывают, посвящена следующая, завершающая Часть I глава.

Ключевые понятия главы: UTXO (непотраченный выход), кластеризация по общим входам, account-based модель, смарт-контракт, EVM, EVM-совместимые сети, формат адреса (0x, T), собственная монета сети, токен, стандарты ERC-20 / TRC-20 / BEP-20, комиссия в монете сети.

Глава 4. Стейблкоины и их эмитенты

Среди всех криптовалютных активов есть один класс, который заслуживает отдельной главы, — стейблкоины. Причина в их двойственной природе. С одной стороны, стейблкоины стали главным инструментом криптомошенников: именно в них чаще всего похищают, отмывают и выводят средства. С другой — они же дают жертве и следствию уникальную, недоступную для других криптовалют возможность: их можно заморозить прямо на месте, одним действием эмитента, пока похититель не успел вывести их дальше. Понять устройство стейблкоинов — значит понять и где сосредоточена угроза, и где открывается главный шанс на возврат.

4.1. Что такое стейблкоин

Обычные криптовалюты — Bitcoin, Ethereum — известны своей волатильностью: их цена относительно доллара может измениться на десятки процентов за считанные дни. Для спекуляции это привлекательно, но для расчётов и хранения — неудобно. Никто не хочет, чтобы сумма, отложенная на сделку, за ночь подешевела на четверть. Ответом на эту проблему стали **стейблкоины** — криптовалюты, чья стоимость привязана к стабильному активу, чаще всего к доллару США, в соотношении один к одному.

Идея проста: один стейблкоин всегда стоит примерно один доллар. Это сочетает удобство криптовалюты — мгновенные глобальные переводы без банков — со стабильностью привычной валюты. Именно поэтому стейблкоины стали, по сути, «рабочими деньгами» криптовалютного мира: в них торгуют, в них хранят, в них рассчитываются.

Существует несколько крупнейших стейблкоинов, и различие между ними имеет прямое практическое значение для расследования. **USDT** (Tether) — крупнейший и наиболее распространённый, особенно в сером и теневом обороте. **USDC** (Circle) — второй по величине, с репутацией более регулируемого и консервативного. Существуют и другие модели, включая обеспеченные и так называемые алгоритмические стейблкоины, но для наших целей ключевое различие лежит не в механизме привязки, а в том, кто и как контролирует токен, — об этом следующий раздел.

Важно сразу зафиксировать факт, определяющий всю практику: подавляющее большинство криптомошеннических операций и схем отмывания проходит именно через стейблкоины, и прежде всего через USDT. Причина понятна — мошеннику, как и любому участнику рынка, нужна стабильная стоимость: похищенное удобнее держать и перемещать в активе, который не обесценится за время вывода. Поэтому, говоря о расследовании криптохищений на практике, мы чаще всего говорим о движении стейблкоинов.

Следователю. В большинстве современных дел предметом хищения оказывается именно USDT, чаще всего в сети TRON (по причинам, разобранным в Главе 3). Это определяет и инструменты, и — что важнее — саму возможность заморозки, которой у «классических» криптовалют нет.

4.2. Централизованные эмитенты

Здесь кроется свойство стейблкоинов, которое отличает их от Bitcoin и Ethereum радикально и делает столь значимыми для возврата средств.

Bitcoin и Ethereum децентрализованы: у них нет владельца, нет компании, нет никого, кто мог бы вмешаться в чужую транзакцию или заблокировать чей-то адрес. В этом их идеология и их сила. Но крупнейшие стейблкоины устроены иначе. За USDT стоит компания Tether, за USDC — компания Circle. Это **централизованные эмитенты**: конкретные организации, которые выпускают токен, поддерживают его привязку к доллару и — что критически важно — сохраняют административный контроль над смарт-контрактом токена.

Что означает этот контроль на практике? Смарт-контракт стейблкоина устроен так, что эмитент может внести любой адрес в «чёрный список» (blacklist) и тем самым заморозить находящиеся на нём средства. Замороженные токены остаются на адресе, но становятся неподвижными: их владелец не может ни перевести их, ни продать, ни как-либо использовать. Фактически эмитент способен одним действием обездвижить средства на любом адресе в сети.

Для Bitcoin или Ethereum такое немыслимо — там просто нет субъекта, обладающего подобной властью. Для стейблкоина это встроенная функция. И именно она превращает стейблкоин из «слабого места» жертвы в её главную надежду: если похищенные средства находятся в USDT на идентифицированном адресе, их можно заморозить.

Подходы двух крупнейших эмитентов при этом заметно различаются, и это различие стоит понимать. Tether занимает проактивную позицию: он замораживает адреса не только по формальным судебным решениям, но и по запросам правоохранительных органов, а иногда и на основании собственного анализа рисков, до завершения формальных процедур. Circle придерживается более консервативного подхода, замораживая средства преимущественно тогда, когда к этому обязывают судебный ордер, санкционные списки или прямое предписание регулятора. Насколько велика эта разница, показывает ончейн-исследование за период с 2023 по 2025 год. За три года первый эмитент заблокировал 7 268 адресов и обездвижил порядка 3,3 миллиарда долларов; второй за тот же период — 372 адреса и 109 миллионов. Разрыв примерно тридцатикратный и по числу адресов, и по сумме. Показательно и распределение по сетям: у первого больше половины заблокированного приходится на TRON, у второго — почти всё на Ethereum, что отражает разную клиентскую географию.

Стоит учитывать и регуляторное измерение, которое в последние годы стало значимым. В Европейском союзе к эмитентам стейблкоинов предъявляются самостоятельные требования: формирование достаточного ликвидного резерва в соотношении один к одному, надзор со стороны европейского банковского регулятора и присутствие эмитента в Союзе как условие выпуска (подробнее — Глава 18). В США с 2025 года действует федеральный закон о платёжных стейблкоинах: он устанавливает резервное обеспечение один к одному и режим, приближенный к банковскому, включая обязанности по противодействию отмыванию (Глава 18). Регуляторный статус конкретного стейблкоина в конкретной юрисдикции влияет на то, где им можно оперировать легально, — и, соответственно, на то, где искать точки воздействия.

Юристу. Различие подходов Tether и Circle имеет тактическое значение. Средства в USDT потенциально замораживаются быстрее и по более широкому кругу оснований, включая оперативный запрос правоохранителей. Средства в USDC, как правило, требуют более формального основания. При выработке стратегии возврата это учитывается: тип стейблкоина влияет на скорость и вероятность заморозки.

4.3. Механизм заморозки

Рассмотрим, как заморозка работает технически и что она даёт на практике.

Поскольку эмитент контролирует смарт-контракт токена, он может добавить адрес в чёрный список этого контракта. С этого момента контракт отказывается исполнять любые операции перевода с данного адреса. Средства формально остаются на нём, отображаются в реестре, но не могут быть сдвинуты — они заморожены на уровне самого токена, а не на уровне кошелька или биржи. Обойти это средствами блокчейна невозможно: правило заложено в сам контракт.

Для возврата средств законным владельцам применяется дополнительный механизм, который можно описать формулой **«заморозка — сжигание — перевыпуск»**. Сначала адрес замораживается, чтобы средства не ушли. Затем, по решению компетентного органа, замороженные токены «сжигаются» — уничтожаются на заблокированном адресе. И наконец эквивалентная сумма перевыпускается на адрес, контролируемый государственным органом или уполномоченным лицом, для последующего возврата пострадавшим. Так похищенное, оказавшееся в стейблкоине, может вернуться к жертве — чего практически невозможно добиться с необратимо ушедшим Bitcoin.

Стоит подчеркнуть границу этого механизма, чтобы не создавать ложных ожиданий: заморозить можно только стейблкоин и только тот, эмитент которого обладает такой функцией. Если похищенные средства конвертированы в Bitcoin, Ethereum или другую децентрализованную валюту, замораживать нечего — субъекта, способного это сделать, не существует. Именно поэтому окно возможности существует ровно до тех пор, пока средства остаются в стейблкоине.

Есть и ещё одна практическая тонкость, которую важно знать. Замороженный адрес продолжает получать USDT: мошенник, знающий, что его адрес заблокирован, технически может и дальше собирать средства с новых жертв — пока баланс не будет уничтожен. Заморозка обездвиживает то, что на адресе есть, но сама по себе не закрывает адрес для новых поступлений. Это влияет на тактику: заморозка — не финал, а фиксация, за которой должны следовать дальнейшие процессуальные шаги.

4.4. Значение для расследования

Соберём воедино, что всё это означает для того, кто пытается вернуть похищенное.

Первое и главное: **стейблкоин на идентифицированном адресе — это реальная возможность заморозки и возврата.** Это принципиально отличает стейблкоины от прочих криптовалют. Проследив цепочку до адреса, где лежит похищенный USDT, расследователь оказывается не в тупике, а у двери, которую можно открыть — правовым путём добиться заморозки, а затем и возврата.

Второе: **окно возможности ограничено во времени.** Пока средства в стейблкоине и не выведены — шанс есть. Как только похититель конвертирует их в децентрализованную валюту или обналичит, возможность заморозки исчезает. Это придаёт всей работе характер гонки, о которой подробно пойдёт речь в главе о первых сутках после хищения (Глава 14).

Третье: **масштаб механизма реален, а не теоретичен.** Это не редкая экзотика, а работающая практика, применяемая тысячи раз. Сам эмитент приводит и более широкие оценки — о миллиардах замороженных средств, сотнях взаимодействующих ведомств и тысячах поддержанных дел. К корпоративной отчётности стоит относиться с известной осторожностью, но порядок величины подтверждается и независимыми ончейн-исследованиями. Отдельные операции достигают сотен миллионов долларов: в апреле 2026 года Tether заморозил более 344 миллионов долларов на двух адресах, действуя по информации от властей. Для жертвы это означает простую вещь: механизм существует, работает и доступен — при условии правильных и своевременных действий.

Четвёртое, о чём нельзя умолчать ради честности картины: **у механизма есть ограничения и своя цена.** Инициировать заморозку может не сам пострадавший и не его адвокат напрямую — как правило, для этого нужен запрос правоохранительного органа или судебное решение (детали — в Главе 17). Кроме того, широкие полномочия эмитента вызывают обоснованные вопросы: частная компания способна обездвижить чужие средства, и вокруг таких действий возникают споры о должной правовой процедуре. Критики указывают, что заморозка без судебного решения создаёт прецедент финансовой цензуры, поскольку решение о том, кто может распоряжаться своими активами, принимает частная компания без установленной процедуры обжалования. Эту неоднозначность мы обсудим в главе о заморозке через эмитентов; здесь достаточно зафиксировать, что инструмент мощный, но не безусловный.

Итог главы можно сформулировать так. Стейблкоины — ахиллесова пята криптопреступника. Стремясь к стабильной стоимости, он держит похищенное в активе, который единственный из всех можно заморозить по требованию. Если средства оказались в USDT на установленном адресе и с момента хищения прошло немного времени, у жертвы есть реальный, подтверждённый тысячами случаев шанс на возврат. Реализовать этот шанс — задача, которой посвящена вся четвёртая часть книги.

Что дальше

На этом завершается первая часть — фундамент. Мы установили, что блокчейн публичен и неизменен, а криптовалюта псевдонимна (Глава 1); что владение сводится к контролю над ключом, а хищение — к его утрате (Глава 2); что сетей много и определение сети есть первый шаг расследования (Глава 3); и, наконец, что стейблкоины дают уникальную точку воздействия — заморозку (Глава 4). Этого достаточно, чтобы двигаться дальше со знанием дела.

Вторая часть посвящена экосистеме и угрозам. Прежде чем учиться прослеживать средства, нужно понять карту местности: где криптоактивы входят в регулируемую инфраструктуру и выходят из неё, какими инструментами их пытаются скрыть, какими бывают мошеннические схемы и как похищенное отмывается. Начнём с ключевого узла всей этой карты — с бирж, потому что именно биржа чаще всего оказывается той точкой, где псевдонимный адрес встречается с реальной личностью. Ей посвящена следующая глава.

Ключевые понятия главы: стейблкоин, привязка к доллару, USDT (Tether), USDC (Circle), централизованный эмитент, чёрный список (blacklist), заморозка на уровне смарт-контракта, «заморозка — сжигание — перевыпуск», окно возможности, ограничения механизма заморозки.

ЧАСТЬ II. ЭКОСИСТЕМА И УГРОЗЫ

Инфраструктура криптовалют и способы мошенничества

Глава 5. Биржи: централизованные и децентрализованные

Всё расследование криптовалютного хищения, каким бы извилистым ни был путь, стремится к одной точке — к бирже. Причина в том, что блокчейн псевдонимен, но деньги рано или поздно нужно превратить в нечто, что можно потратить в реальном мире, а сделать это, минуя регулируемую инфраструктуру, почти невозможно. Биржа — то место, где псевдонимный адрес встречается с паспортом. Довести след до биржи означает получить шанс на две вещи, ради которых всё и затевается: узнать, кто стоит за адресом, и заморозить то, что он украл. Эта глава — о том, как устроены биржи и почему они оказываются ключевым узлом любого дела.

5.1. Централизованные биржи (CEX)

Централизованная биржа (по-английски centralized exchange, сокращённо CEX) — это компания-посредник, которая позволяет пользователям покупать, продавать и хранить криптовалюту, а также обменивать её на обычные деньги. Крупнейшие площадки — Binance, Coinbase, OKX, Bybit, Kraken и другие — обслуживают десятки и сотни миллионов пользователей и пропускают через себя основную часть мирового криптооборота.

Ключевое, что нужно понять об устройстве CEX, — это её роль **кастодиана**. Когда пользователь вводит средства на биржу, контроль над приватными ключами переходит к бирже. С этого момента, как мы установили в Главе 2, средствами фактически распоряжается биржа, а пользователь владеет лишь записью в её внутренней системе учёта и обещанием выдать средства по требованию. Это имеет прямое следствие для расследования, и следствие это двоякое.

С одной стороны — важнейшая деталь, которую обязан понимать каждый, кто читает блокчейн. **Внутренние переводы между пользователями одной биржи не отражаются в блокчейне.** Когда один клиент Binance переводит средства другому клиенту Binance, никакой транзакции в сети не происходит — биржа просто меняет цифры в своей внутренней базе данных. Для внешнего наблюдателя эти средства неподвижны: на блокчейне ничего не видно. Это означает, что как только средства попадают на биржу, их дальнейшее движение внутри неё становится невидимым снаружи и известно только самой бирже.

Разберём, как именно средства попадают на биржу. Для приёма депозитов биржа генерирует каждому пользователю уникальный **депозитный адрес**. Когда пользователь отправляет средства на этот адрес, происходит зачисление на его внутренний счёт. Но средства не остаются на депозитном адресе: биржа периодически «сметает» их (этот процесс называют sweeping) на свои общие кошельки, где деньги всех пользователей объединяются. Поэтому на блокчейне типичная картина такова: средства приходят на депозитный адрес и почти сразу уходят с него на горячий кошелёк биржи, смешиваясь с чужими.

Именно на депозитном адресе обрывается видимый след. Дальше цепочку продолжает не блокчейн, а внутренний учёт биржи, и доступ к нему есть только у неё.

Следователю. Это объясняет, почему в какой-то момент трейсинг «упирается» в биржу и дальше по блокчейну не идёт. Это не тупик и не ошибка — это конструктивная особенность. Прослеживание довело вас до депозитного адреса конкретной биржи; связь «депозитный адрес -> пользователь» существует, но она заперта во внутренней системе биржи. Извлечь её можно только запросом к бирже (Глава 16). На блокчейне дальше искать нечего — искать нужно у биржи.

Стоит различать два типа кошельков самой биржи. **Горячий кошелёк** содержит оперативные средства, доступные для быстрых выводов, и подключён к сети. **Холодный кошелёк** хранит основные резервы офлайн, в безопасности. Адреса горячих кошельков крупных бирж обычно известны и помечены в аналитических системах — распознав такой адрес в цепочке, аналитик понимает, что средства достигли биржи. После краха ряда крупных площадок биржи стали чаще раскрывать свои резервы (практика, известная как Proof of Reserves), что дало аналитикам дополнительные ориентиры, хотя и не полную картину обязательств.

5.2. KYC и AML на биржах

То, что делает биржу решающим звеном расследования, — это обязательная идентификация клиентов. Регулируемые биржи применяют процедуры **KYC** (know your customer, «знай своего клиента») и **AML** (anti-money laundering, противодействие отмыванию).

KYC — это верификация личности при регистрации и особенно при выводе средств. Уровни верификации различаются: базовый может требовать лишь электронной почты, но для сколько-нибудь значимых операций биржа запрашивает полный набор — удостоверение личности или паспорт, фотографию (нередко селфи с документом), подтверждение адреса проживания (Proof of Address, PoA), а иногда и подтверждение источника средств. Помимо этого биржа фиксирует и технические данные: IP-адреса, с которых происходили входы, использованные устройства, номер телефона, привязанные банковские карты и счета для ввода-вывода фиата.

Именно этот массив данных превращает псевдонимный адрес в конкретного человека. Депозитный адрес сам по себе — лишь строка символов. Но у биржи он связан с аккаунтом, а аккаунт — с паспортом, телефоном, IP и платёжными реквизитами. В этом и состоит смысл доведения следа до биржи: там, и только там, хранится недостающее звено между адресом и личностью.

Юристу. Перечисленный набор данных — ровно то, что запрашивается через правоохранительный запрос к бирже (детали механики — в Главе 16). Понимание того, что именно биржа собирает и хранит, позволяет заранее сформулировать, какие данные истребовать: не абстрактные «сведения о владельце», а KYC-документы, историю операций, логи входов с IP, привязанные счета и связанные аккаунты.

AML — это постоянный мониторинг операций на предмет подозрительной активности. Биржи в реальном времени оценивают риски входящих и исходящих переводов, автоматически блокируют подозрительные депозиты, формируют отчёты о подозрительных операциях для регуляторов. Действует и так называемое «правило путешествия» (Travel Rule), обязывающее площадки обмениваться данными об отправителе и получателе перевода. Порог, начиная с которого оно применяется, различается по юрисдикциям, и здесь важна деталь: в Европейском союзе соответствующий регламент о сведениях, сопровождающих переводы средств, распространяется на переводы криптоактивов **независимо от суммы** (подробнее — Глава 18). Всё это означает, что биржа не пассивный хранитель, а активный участник контроля, обязанный реагировать на признаки противоправного оборота.

Данные KYC, история операций, логи входов и переписка с поддержкой хранятся биржами длительное время в силу регуляторных требований — как правило, годами. Это важно: даже если с момента хищения прошло существенное время, данные, скорее всего, ещё существуют. Более того, их можно «зафиксировать» специальным запросом о сохранении (preservation request), пока готовится основное истребование, — об этом в Главе 16.

Было бы неверно рисовать KYC всесильным. У него есть слабое место, которое активно эксплуатируется, — **поддельные и купленные аккаунты**. Существует целая теневая индустрия «дропов» — людей, которые проходят верификацию на своё имя и продают доступ к аккаунту, а также ферм, изготавливающих аккаунты на подставных и синтетических лиц. В результате идентифицированный по KYC «владелец» может оказаться не бенефициаром, а лишь дропом, за которым стоит кто-то другой.

Следователю. Идентификация по KYC — не всегда конечная точка. Установленное лицо может быть дропом. Но это не обесценивает результат: дроп — не тупик, а новый узел расследования, зацепка, ведущая дальше (к тому, кто его нанял, к каналу вербовки, к другим аккаунтам). Об этом подробнее в главах об атрибуции и об отмывании.

5.3. Децентрализованные биржи (DEX)

Противоположность CEX — **децентрализованная биржа** (decentralized exchange, DEX). Здесь нет компании-посредника и нет кастодиана. Обмен одного токена на другой происходит напрямую через смарт-контракты, а пользователь торгует «из своего кошелька», не передавая никому свои ключи. Наиболее известные DEX — Uniswap, PancakeSwap, Curve.

Технически DEX работает на автоматических пулах ликвидности: пользователи вносят пары токенов в общий пул, а обмен совершается по формуле, заложенной в смарт-контракт, без участия человека-оператора. Для наших целей достаточно понимать, что DEX — это программа, а не организация, и у неё нет ни офиса, ни службы соответствия, ни базы клиентов.

Отсюда — принципиальное свойство: **на DEX нет KYC.** Любой адрес может подойти к смарт-контракту и совершить обмен, не предъявляя никаких документов. Никто не спрашивает, кто вы. Это делает DEX привлекательным инструментом для запутывания следа: похищенный токен можно обменять на другой, сменить актив, усложнить прослеживание.

Но здесь важно не поддаться распространённому заблуждению, будто DEX «обрывает» след, как это делает CEX. Всё наоборот. В отличие от внутреннего учёта централизованной биржи, обмены на DEX происходят на блокчейне и полностью видны. Своп на DEX не прячет транзакцию — он лишь меняет один актив на другой у всех на виду. Аналитик видит: на такой-то адрес пришёл токен A, через смарт-контракт DEX он обменян на токен B, и токен B ушёл дальше. Цепочка не рвётся — она продолжается, просто меняется актив.

И главное — **DEX не выводит в фиат.** На децентрализованной бирже можно менять одни криптоактивы на другие, но нельзя получить обычные деньги на банковский счёт. А значит, чтобы в конечном счёте обналичить похищенное, злоумышленник рано или поздно вынужден прийти на централизованную биржу с её KYC. DEX — это транзит, промежуточная станция; конечная цель вывода — всё равно CEX.

Следователю. Своп на DEX — не повод останавливать расследование. Это видимая на блокчейне операция, за которой цепочка продолжается. Следуйте за новым активом дальше — путь почти всегда в итоге приводит к централизованной точке, где возможна идентификация.

5.4. Биржи как точка воздействия

Мы подошли к тому, ради чего след и доводят до биржи. Централизованная биржа — не просто место, где обрывается блокчейн-след; это **точка воздействия**, где возможны и заморозка, и получение данных.

Как только похищенные средства поступают на биржу, их можно заморозить по соответствующему запросу. Это создаёт гонку со временем, определяющую всю логику первых действий после хищения. Мошенник стремится как можно быстрее вывести или обналичить средства; расследование стремится успеть заморозить их, пока они ещё на бирже. Счёт нередко идёт на часы: чем раньше подан корректный запрос, тем выше вероятность застать средства на месте.

Что определяет успех? Три вещи, к которым мы будем возвращаться. **Скорость** — средства на бирже не лежат вечно, и промедление стоит возможности. **Точность данных** — запрос должен содержать конкретику: хеш транзакции, депозитный адрес на бирже, сумму, время; расплывчатое «у меня украли криптовалюту» не приводит ни к чему. **Правовая основа** — биржа реагирует только на обращение, имеющее надлежащее юридическое основание, и, как правило, исходящее от правоохранительного органа, а не от жертвы или её адвоката напрямую. Все три условия и механика их соблюдения подробно разбираются в Главе 16; здесь важно зафиксировать саму связку: биржа = возможность заморозки, но возможность обусловленная.

Роль биржи в возврате не сводится к заморозке. Заморозив средства, биржа удерживает их до разрешения ситуации компетентным органом, а затем, по соответствующему решению, они могут быть возвращены пострадавшим. При этом биржа не выступает арбитром и не решает спор сама — она действует по запросу уполномоченных лиц и в рамках установленных процедур. Крупные площадки в целом заинтересованы в сотрудничестве с правоохранительными органами: репутация регулируемой и «чистой» биржи имеет для них коммерческую ценность, и масштаб такого сотрудничества сегодня весьма значителен (конкретные цифры и практика — в Главе 16).

Юристу. Стратегический вывод главы: работа адвоката в криптоделе во многом сводится к тому, чтобы довести след до конкретной биржи и подготовить основу для запроса — точную, полную, с правовым обоснованием. Биржа не откроется навстречу расплывчатому обращению, но реагирует на корректно оформленный запрос уполномоченного органа. Превратить результат трейсинга в такой запрос — ключевая компетенция, которой посвящена четвёртая часть.

Что дальше

Мы установили, что биржа — конечная цель большинства расследований: именно там псевдонимный адрес соединяется с личностью через KYC и именно там возможна заморозка. Централизованные биржи обрывают видимый след, но хранят недостающее звено; децентрализованные не прячут след вовсе и всё равно ведут к централизованной точке вывода.

Но между хищением и биржей похититель редко идёт напрямую. Чаще он пытается запутать след — прогнать средства через инструменты, специально созданные для сокрытия: миксеры, мосты между сетями, приватные монеты. Насколько эти инструменты действительно эффективны, что они скрывают, а что оставляют на виду — тема следующей главы. Разобраться в ней важно, чтобы не преувеличивать сложность там, где след на деле сохраняется, и трезво оценивать перспективы там, где он действительно теряется.

Ключевые понятия главы: централизованная биржа (CEX), кастодиан, депозитный адрес, sweeping, внутренний учёт (off-chain), горячий и холодный кошелёк биржи, KYC, AML, Travel Rule, preservation request, дроп, децентрализованная биржа (DEX), пул ликвидности, точка воздействия.

Глава 6. Инструменты сокрытия: миксеры, мосты, приватные монеты

Вокруг инструментов криптографического сокрытия сложилось два противоположных мифа. Первый — обывательский: раз существуют миксеры и «анонимные монеты», значит, отследить средства невозможно, и расследование бессмысленно. Второй — противоположный, порождённый маркетингом аналитических компаний: любой след прослеживается, любая анонимизация — иллюзия. Правда, как обычно, посередине, и эта глава — попытка занять трезвую позицию. Инструменты сокрытия действительно усложняют работу и повышают её стоимость. Но они редко делают расследование невозможным и почти всегда оставляют следы — прежде всего на стыках, где один инструмент сменяется другим, и там, где пользователь ошибается. Понять, что именно скрывает каждый инструмент, а что оставляет на виду, — значит научиться работать там, где прямой след обрывается.

6.1. Миксеры

Миксер (mixer, или tumbler) — сервис, предназначенный для разрыва связи между отправителем и получателем средств. Принцип его работы можно представить так. Множество пользователей отправляют свои средства в общий «котёл», перемешивают их, а затем каждый забирает эквивалентную сумму, но уже «чужими», перемешанными монетами, не связанными напрямую с тем, что он внёс. На выходе прямая цепочка «адрес А отправил адресу Б» разрывается: из миксера средства выходят на новый адрес, формально не связанный с адресом входа.

Различают два типа миксеров. **Кастодиальные** — где оператор принимает средства на свой контроль, перемешивает и выдаёт; такой сервис управляется людьми и сам является слабым звеном (оператора можно установить, сервис — закрыть, а его записи — истребовать). **Некастодиальные**, построенные на смарт-контрактах, действуют автоматически, без оператора-посредника. Наиболее известный пример второго типа — Tornado Cash, работающий по принципу депозитов фиксированными номиналами: пользователь вносит стандартную сумму, а позже выводит её на новый адрес, и в общей массе одинаковых депозитов конкретную связь установить трудно.

Ключевое понятие здесь — **множество анонимности** (anonymity set): круг всех, чьи средства перемешаны вместе. Чем этот круг больше, тем труднее связать конкретный вход с конкретным выходом. Если через миксер за нужный период прошли тысячи одинаковых операций, вычленить «вашу» — статистически сложно. Если же операций было мало, круг узок, и сопоставление становится реальным.

Важно ясно понимать, **что миксер скрывает, а что — нет.** Он скрывает прямую связь между конкретным адресом-отправителем и конкретным адресом-получателем. Но он не скрывает сам факт использования миксера — напротив, обращение к известному миксеру прекрасно видно на блокчейне и само по себе служит сигналом, «красным флагом», привлекающим внимание. Не скрывает он и время операций, и номиналы. А это оставляет пространство для анализа.

Методы работы с миксерами существуют, и они опираются именно на то, что миксер оставляет на виду. **Тайминг-анализ** сопоставляет моменты депозитов и выводов: если вскоре после внесения средств на близкую сумму происходит вывод, между ними можно предположить связь. **Анализ номиналов и сдачи** отслеживает нестандартные суммы, выделяющиеся из общей массы. И, что чаще всего решает дело, — **ошибки пользователя**: вывод на адрес, уже связанный с ним прежними операциями; повторное использование адресов; касание KYC-инфраструктуры до или после микширования. Множество деанонимизаций миксеров произошло не потому, что взломали сам миксер, а потому, что пользователь где-то нарушил гигиену и оставил зацепку.

Отдельно стоит сказать о **правовом статусе миксеров**, потому что он важен и при этом переменчив. Миксеры не раз попадали под санкции, что имело прямые последствия: биржи начинали отклонять средства, прошедшие через них, а само их использование меняло юридическую оценку операции. Но статус этот нестабилен. Показательна история Tornado Cash: внесённый в санкционный список в 2022 году, он был исключён из него в марте 2025 года после того, как суд счёл, что неизменяемые смарт-контракты не являются «собственностью», подпадающей под санкционные полномочия; при этом уголовное преследование отдельных разработчиков продолжилось. Этот пример — не столько справка о конкретном сервисе, сколько иллюстрация принципа: регуляторный статус инструментов сокрытия подвижен, и при работе с делом его нужно проверять на актуальность, а не полагаться на вчерашнее знание.

Юристу. Из подвижности статуса следует практическое правило: санкционный и правовой статус конкретного миксера необходимо устанавливать на дату событий и на текущую дату

отдельно. То, что было под санкциями в момент операции, могло быть исключено из списка позже, и наоборот. Это влияет и на квалификацию, и на позицию биржи, и на стратегию.

6.2. Кросс-чейн мосты

Мост (bridge) — механизм переноса стоимости из одной сети в другую, например из Ethereum в BSC. Поскольку напрямую токен одной сети не может существовать в другой, мост использует схему, которую упрощённо описывают как «заблокировать и выпустить»: средства блокируются в исходной сети, а их эквивалент выпускается в сети назначения (нередко в виде так называемого «обёрнутого» токена). Обратная операция высвобождает исходные средства.

Для похитителя мост привлекателен тем, что смена сети сбивает линейное прослеживание. Аналитик, работавший в одном эксплорере, обнаруживает, что след «исчез» — средства ушли в мост, — и, если не знает, что делать дальше, может ошибочно счесть цепочку оборванной. На деле она продолжается в другой сети.

Именно поэтому важно понимать, **как отслеживать переходы через мост.** Мост по своей природе фиксирует обе стороны операции: депозит в исходной сети и выпуск в сети назначения. Эти две стороны можно сопоставить — по времени, по сумме, по адресам контрактов моста. Аналитик переключается в сеть назначения и ищет соответствующий выпуск средств, восстанавливая разорванную было цепочку. Мост, задуманный как средство запутывания, сам оказывается точкой корреляции, потому что вынужден оставить след с обеих сторон.

Сложности, разумеется, есть. Похититель может использовать несколько мостов подряд, прогонять средства через агрегаторы, дробить суммы при переходе, вносить временные задержки. Каждый такой приём добавляет работы. Но каждый же оставляет новый стык — новую точку сопоставления. Инструменты с поддержкой межсетевого анализа (о них в Главе 10) во многом автоматизируют эту работу, но принцип остаётся прежним: мост не разрывает след, а переносит его в другую сеть, где его нужно подхватить.

Следователю. Если след «оборвался» на адресе контракта, похожего на мост, — это сигнал не к остановке, а к переключению сети. Зафиксируйте время и сумму депозита в мост и ищите соответствующий выпуск в предполагаемой сети назначения. Переход через мост — не конец цепочки, а её изгиб.

6.3. Приватные монеты

Отдельный класс инструментов — **приватные монеты**, спроектированные так, чтобы скрывать детали транзакций на уровне самого протокола. Наиболее значимый пример — **Monero (XMR)**. В отличие от Bitcoin, где все переводы публичны, Monero с помощью специальных криптографических приёмов (кольцевых подписей, скрытых адресов, конфиденциальных сумм) прячет отправителя, получателя и сумму. Здесь нужно быть честным: прямое прослеживание Monero по блокчейну в общем случае несостоятельно. Это не тот случай, где след «трудно, но можно» проследить, — сама конструкция сети лишает наблюдателя данных, на которых строится трейсинг.

Другой пример — **Zcash (ZEC)**, где приватность опциональна: транзакции могут быть «прозрачными» или «экранированными». На практике опциональная приватность часто не используется в полной мере, что оставляет больше возможностей для анализа, чем в случае Monero.

Значит ли это, что перевод в приватную монету — гарантированный тупик? Нет, и причина в **точках входа и выхода.** Приватная монета где-то покупается и где-то продаётся — как правило, на бирже с KYC или через обменник. Схема «получил Bitcoin -> обменял на Monero -> позже обменял обратно» непрозрачна в середине, но оставляет следы на концах: видно, как средства ушли в конвертацию, и видно, как эквивалент появился на выходе. Атаковать нужно не саму монету, а эти точки конвертации. К тому же многие биржи под давлением регуляторов прекращают работу с приватными монетами, сужая круг мест, где их можно легально обменять,, а значит, сужая и точки выхода, за которыми можно наблюдать.

Следователю. С приватными монетами бессмысленно бороться «в лоб» на уровне их блокчейна. Работайте с концами: где средства вошли в приватную монету и где вышли обратно в прослеживаемый актив. Именно точки конвертации, а не сама монета, — уязвимое место схемы.

6.4. Пределы анонимизации

Сведём наблюдения в общую картину. Главный принцип таков: **ни один инструмент сокрытия не обеспечивает полной анонимности в точке, где криптовалюта встречается с фиатом.** Анонимность не бинарна — это не «есть» или «нет», а вопрос стоимости и вероятности. Инструменты сокрытия повышают цену расследования: требуют больше времени, больше данных, более дорогих инструментов. Но чтобы в конечном счёте воспользоваться похищенным, его нужно обналичить, а обналичивание происходит через регулируемые точки, требующие идентификации. Там анонимность и заканчивается.

Решающим фактором чаще всего оказывается **человеческий фактор.** Повторное использование адресов, связь с KYC-аккаунтом до или после сокрытия, раскрытие себя в соцсетях, на форумах, в переписке, спешка при выводе — всё это оставляет зацепки, сводящие на нет самую изощрённую техническую анонимизацию. История расследований показывает, что большинство успешных деанонимизаций опирается не на «взлом» инструмента сокрытия, а на ошибку того, кто им пользовался.

Комбинация инструментов — миксер, затем мост, затем приватная монета — на первый взгляд кажется непреодолимой. Но каждый слой добавляет **стык**, а каждый стык — потенциальную точку корреляции. Чем сложнее схема, тем больше в ней переходов, на каждом из которых можно ошибиться и оставить след.

При этом честность требует признать и обратное: **иногда след действительно теряется.** Профессионально исполненная схема с безупречной операционной гигиеной — без повторов, без касаний KYC, с грамотным использованием Monero и достаточным множеством анонимности — может оказаться нераскрываемой доступными средствами. Отрицать это — значит вводить в заблуждение. Но такие случаи скорее исключение: большинство мошенников не обладают ни дисциплиной, ни терпением для безупречной гигиены, и именно на их ошибках строится большинство успешных дел. Практический вывод один: наличие в цепочке инструментов сокрытия — не повод отказываться от расследования, а повод сменить метод.

Юристу. В коммуникации с клиентом важна калиброванная честность. Присутствие миксера или приватной монеты в цепочке снижает вероятность и повышает стоимость возврата, но само по себе не означает провала. Правильная формулировка — не «всё пропало» и не «мы всё вернём», а трезвая оценка: что именно скрыто, где сохраняются зацепки и каковы реалистичные перспективы.

Что дальше

Мы разобрали инструменты, которыми похититель пытается разорвать след, и убедились, что они — препятствие, а не стена. Но чтобы понимать, против чего вообще ведётся расследование, нужно вернуться к истоку: к тому, как средства оказываются похищенными. Инструменты сокрытия применяются уже к добыче; сама же добыча берётся из мошеннических схем.

Следующая глава — систематический разбор способов криптомошенничества. Это самая объёмная глава второй части и один из практических центров всей книги: классификатор схем с признаками каждой, к которому читатель будет возвращаться и для профилактики, и для того, чтобы квалифицировать конкретный инцидент. Ведь прежде чем прослеживать похищенное, нужно понять, как именно его похитили.

Ключевые понятия главы: миксер (кастодиальный и некастодиальный), множество анонимности (anonymity set), тайминг-анализ, кросс-чейн мост, «заблокировать и выпустить», обёрнутый токен, точка корреляции, приватные монеты (Monero, Zcash), точки конвертации, пределы анонимизации, человеческий фактор.

Глава 7. Анатомия криптомошенничества

Это самая большая глава книги, и не случайно. Прежде чем прослеживать похищенное, нужно понять, как именно его похищают,, а способов этих множество, и каждый имеет свою логику, свои признаки и свою уязвимую точку. Здесь важно сразу зафиксировать главное наблюдение, которое определяет всё: подавляющее большинство криптовалютных хищений эксплуатирует не технику, а человека. По разным оценкам, около двух третей всех инцидентов основаны на социальной инженерии, то есть на обмане, манипуляции и злоупотреблении доверием, а не на взломе кода. Блокчейн, как мы знаем, взломать практически невозможно. Взламывают пользователя. Поэтому эта глава — одновременно и справочник для расследователя, позволяющий квалифицировать инцидент, и практическое руководство по защите. Знание схемы — лучшая профилактика: распознанная вовремя, почти любая из них рассыпается.

Схемы сгруппированы по логике, а не по алфавиту: сначала обман через отношения, затем технический обман, затем обман в момент сделки, затем атаки на инфраструктуру доступа и, наконец, отдельный класс — охота на тех, кто уже пострадал.

7.1. Схемы социальной инженерии

Это самый разрушительный по объёму потерь класс. Он не требует технических навыков — только терпения, психологии и умения втираться в доверие. Жертва здесь не «взломана»; она добровольно, своими руками отдаёт средства, будучи уверенной, что поступает разумно.

Pig butchering («разделка свиньи»)

Название схемы — жаргонное и циничное: жертву сначала «откармливают» доверием и мнимой прибылью, а затем «забивают», забирая всё. Это самая масштабная схема современности, и понимать её механику нужно детально, потому что именно с ней чаще всего сталкивается расследователь.

Механика разворачивается по этапам. **Контакт.** Мошенник выходит на жертву через мессенджер, социальную сеть, приложение для знакомств, а иногда — с якобы «случайно ошибшегося номером» сообщения. Первый контакт всегда выглядит невинно и никогда не касается денег. **Сближение.** В течение недель, а порой и месяцев выстраиваются отношения — дружеские или романтические. Мошенник вникает в жизнь жертвы, проявляет заботу, создаёт ощущение близости и доверия. Это стадия «откорма»: чем прочнее связь, тем крупнее будущая добыча. **Введение темы инвестиций.** Как бы невзначай мошенник упоминает, что зарабатывает на криптовалюте — через «проверенную платформу», «инсайдерскую стратегию», «арбитраж». Он не уговаривает; он делится успехом, показывает скриншоты прибыли, вызывает интерес и лёгкую зависть. **Первая инвестиция.** Жертва вносит небольшую сумму на указанную платформу, и видит, как баланс растёт. Здесь ключевой элемент: платформа поддельная, а «рост» — нарисованные цифры на экране, не имеющие отношения к реальным средствам. Жертве даже позволяют вывести небольшую сумму на раннем этапе — это снимает подозрения и укрепляет доверие. **Наращивание.** Убедившись, что всё «работает», жертва вкладывает больше — часто все сбережения, кредиты, заёмные средства. Мошенник поощряет и подталкивает. **Забой.** Когда вложено достаточно, попытка вывести средства наталкивается на препятствия: «налог на вывод», «комиссия за разблокировку», «верификация», требующая доплат. Каждая доплата — новая потеря. В какой-то момент связь обрывается, платформа исчезает, а с ней и деньги, которых, по сути, никогда и не было на «счёте».

За этой схемой нередко стоит целая индустрия — организованные центры с сотнями операторов, работающих по скриптам, причём часть операторов сами являются жертвами принудительного труда. Это не одиночка за ноутбуком, а конвейер.

Красные флаги, позволяющие распознать pig butchering до потери средств: незнакомец пишет первым и проявляет несоразмерный интерес; разговор довольно быстро сворачивает к теме заработка на крипте; демонстрируются скриншоты прибыли; предлагается платформа, о которой нет независимой информации, с нереалистичной доходностью; собеседник избегает живого видеообщения и личных встреч.

Владельцу. Универсальное правило против pig butchering: инвестиционный совет от человека, с которым вы познакомились онлайн и никогда не видели вживую, — это по умолчанию мошенничество, каким бы тёплым ни было общение. Настоящие отношения не начинаются с приглашения вложиться в крипту.

Romance scam

Близкая родственница pig butchering, где рычагом выступает не столько «инвестиционная возможность», сколько эмоциональная привязанность как таковая. Механика похожа —

долгое выстраивание романтических отношений на расстоянии,, но развязка может быть иной: не вложение в платформу, а прямые просьбы о деньгах под предлогом внезапной беды, срочной поездки, медицинских расходов, замороженного «наследства». Общее с pig butchering — терпеливая игра вдолгую и эксплуатация доверия; отличие — акцент на чувствах, а не на жадности.

Фейковые инвестиционные платформы и «доходные боты»

Обособленный вариант, где отношения могут отсутствовать вовсе, а приманкой служит сама «возможность»: сайт или приложение, обещающее гарантированную доходность — «10% в день», «безрисковый AI-бот», «арбитражный алгоритм». Механика та же нарисованная прибыль и та же стена «комиссий» при выводе. Ключевой маркер — обещание гарантированной или неправдоподобно высокой доходности, которой в реальном мире инвестиций не существует.

Психология жертвы

Стоит развеять вредный миф, будто на такие схемы попадаются только наивные. Напротив, жертвами часто становятся образованные, осторожные, финансово грамотные люди. Работают универсальные психологические механизмы: постепенность (каждый следующий шаг лишь чуть больше предыдущего), доверие (выстроенное неделями), эффект невозвратных затрат (вложив много, трудно признать потерю и остановиться), искусственный дефицит времени. Понимание этих рычагов — часть защиты: уязвимость не в глупости, а в нормальной человеческой психологии, которой мошенник управляет.

7.2. Технический обман

Здесь эксплуатируется уже не столько доверие к человеку, сколько доверие к интерфейсу, бренду, привычному действию. Жертва обманывается не отношениями, а видимостью легитимности.

Фишинг

Классика, не теряющая эффективности. **Механика.** Создаётся поддельный сайт, визуально неотличимый от настоящего — биржи, кошелька, популярного сервиса. Ссылка на него доставляется по электронной почте, в мессенджере, через рекламу в поисковике (так что «первая ссылка» в выдаче ведёт на подделку), иногда через взломанные аккаунты знакомых. Жертва, полагая, что вошла на настоящий сайт, вводит учётные данные, пароль или — самое губительное — seed-фразу, либо подключает кошелёк и подписывает вредоносную транзакцию. Результат: контроль над средствами переходит к мошеннику.

Красные флаги: адрес сайта (URL) отличается на один-два символа от настоящего; сообщение содержит «срочное» предупреждение о безопасности, требующее немедленных действий; запрашивается ввод seed-фразы (напомним из Главы 2 — законный сервис не делает этого никогда); предлагается подтвердить транзакцию, которую вы не инициировали.

Deepfake и имперсонация

Технология сделала эту схему массовой. **Механика.** С помощью искусственного интеллекта создаётся поддельное видео с узнаваемой публичной фигурой — известным предпринимателем, основателем биржи, — которая якобы анонсирует «раздачу криптовалюты» или новый «проект». Видео распространяется через видеоплатформы, соцсети, мессенджеры. Схема эксплуатирует авторитет и вечную приманку «удвоения»: жертве предлагается отправить криптовалюту на «адрес раздачи», чтобы получить вдвое больше. Разумеется, отправленное просто исчезает.

Красные флаги: любое предложение по формуле «отправь X — получи 2X» (оно не работает никогда); видео со знаменитостью, рекламирующей незнакомый проект; ссылки в комментариях под популярными роликами; искусственная срочность («осталось 5 минут»).

Фейковый airdrop и токены-ловушки

Схема, эксплуатирующая механику токенов, разобранную в Главе 3. **Механика.** В кошельке жертвы «сам собой» появляется незнакомый токен — якобы бесплатная раздача (airdrop). Любопытство побуждает разобраться, и здесь расставлены ловушки. При попытке продать токен на децентрализованной бирже или перейти на «сайт проекта» жертва либо подписывает транзакцию с разрешением (approve) на неограниченное списание своих настоящих токенов, либо попадает на фишинговую страницу, запрашивающую подключение кошелька и seed-фразу. Существуют и токены-«ловушки» (honeypot), которые технически невозможно продать: купить можно, а продать — нет.

Красные флаги: в кошельке появились токены, которых вы не покупали; токен невозможно продать обычным способом; название токена содержит адрес сайта или призыв «перейти и активировать».

Владельцу. С незнакомыми токенами, возникшими в кошельке ниоткуда, единственно верное действие — не делать ничего. Не пытаться продать, перевести, «активировать». Игнорировать. Любое взаимодействие — вход в ловушку.

Компрометация устройства

Здесь атакуют не психологию, а сам аппарат жертвы. **Механика.** Вредоносное программное обеспечение проникает на телефон или компьютер — через поддельное приложение (в том числе внешне похожее на настоящий кошелёк), заражённый файл, вредоносное расширение браузера. Дальше возможны варианты: программа считывает seed-фразу или ключи с устройства; получает удалённый доступ; или, что особенно коварно, подменяет адрес получателя в буфере обмена — жертва копирует правильный адрес, а вставляется адрес мошенника. Человек в момент операции не замечает подмены.

Красные флаги: приложение кошелька скачано не из официального источника; расширение браузера запрашивает избыточные разрешения; вставленный из буфера адрес отличается от скопированного (всегда сверять!); в истории кошелька появляются операции, которых вы не совершали.

7.3. Обман при транзакциях

Этот класс схем нацелен на момент самого перевода. Здесь мошенник не крадёт ключ и не строит отношений — он обманывает жертву относительно того, куда, сколько и в каком виде уходят средства. Часто цель — не единичный крупный «улов», а те, кто регулярно совершает переводы: фрилансеры, торговцы, участники P2P-обмена.

Address poisoning (отравление адреса)

Одна из самых коварных схем, эксплуатирующая привычку копировать адрес из истории операций. **Механика.** Мошенник с помощью специальных программ генерирует адрес-«двойник», у которого совпадают первые и последние символы с адресом реального контрагента жертвы (кошельки обычно показывают адрес сокращённо — начало и конец,, и на глаз двойник неотличим). Затем на адрес жертвы отправляется микроскопическая транзакция (dust) с этого двойника — чтобы он попал в историю операций. Расчёт прост: когда жертва в следующий раз захочет отправить средства своему контрагенту, она скопирует адрес из недавней истории, и скопирует двойник. Средства уйдут мошеннику. Известны случаи потери огромных сумм именно так — из-за одного скопированного не того адреса.

Красные флаги: в истории появляются входящие микротранзакции от незнакомых адресов; адрес в истории похож на нужный, но отличается в середине; операция на ничтожную сумму, которую вы не инициировали.

Защита прямая: никогда не копировать адрес из истории транзакций; пользоваться адресной книгой или сохранёнными контактами; перед крупным переводом сверять адрес целиком, все символы, а не только начало и конец.

Подмена суммы (decimal scam)

Тонкая схема, играющая на невнимательности и на различии в записи чисел. **Механика.** Стороны договариваются о платеже — скажем, 3 500 USDT. Мошенник отправляет сумму, которая на скриншоте выглядит как «4.500 USDT», но в действительности означает четыре доллара пятьдесят центов, а не четыре тысячи пятьсот: разница спрятана в десятичном разделителе (точка против запятой, «4.500» против «4,500»). Затем мошенник заявляет, что переплатил по ошибке, и просит вернуть «лишнюю тысячу». Присылает скриншот перевода. Если у жертвы на кошельке крупный баланс и она не всматривается в точную сумму, она может не заметить, что реально пришло $4.50, а не $4 500,, и отправить «возврат» в 1 000 настоящих долларов.

Вариации усиливают обман: перевод в поддельном токене с тем же тикером, что и настоящий USDT (внешне «пришли USDT», а на деле — ничего не стоящий двойник); или перевод в другой, дешёвой сети на минимальную сумму, тогда как «возврат» просят в основной.

Красные флаги: контрагент торопит с подтверждением получения; просит вернуть «лишнее» немедленно, без паузы; сумма в блокчейн-эксплорере не совпадает с показанной на скриншоте; перевод пришёл в неожиданной сети или в токене-двойнике.

Защита: всегда проверять фактически поступившую сумму в блокчейн-эксплорере, а не по скриншоту и не по всплывающему уведомлению; смотреть точную сумму, название токена и сеть; при любой просьбе «вернуть» — не спешить и перепроверить.

Фейковый комплаенс при P2P-обмене

Конец ознакомительного фрагмента.