Market Talks
ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР

КРИПТОВАЛЮТА · НАЧАЛЬНЫЙ · УРОК 14 ИЗ 15

Мошенничество, rug pull и тревожные признаки

Как устроены самые распространённые схемы криптомошенничества, от rug pull и памп и дампа до поддельных инвестиционных платформ, самозванцев и дрейнеров кошельков, и какие тревожные признаки у них общие

11 мин чтения Вопросов в тесте: 8, с ответами

КРИПТОВАЛЮТА · НАЧАЛЬНЫЙ · УРОК 14 ИЗ 15

Мошенничество, rug pull и тревожные признаки

СУТЬ В ОДНОМ ПРЕДЛОЖЕНИИ

Криптовалютные мошенники каждый год забирают миллиарды долларов. Большинство схем следует небольшому числу шаблонов, и когда вы умеете узнавать эти шаблоны, тревожные признаки замечать гораздо легче.

Почему мошенничество занимает в криптовалютах так много места

Криптовалютные транзакции быстрые, глобальные и необратимые. Нет банка, куда можно позвонить и попросить вернуть деньги, и нет центральной службы, которая могла бы заморозить платёж, уже ушедший из вашего кошелька. Те же свойства, которые делают криптовалюты полезными, делают их привлекательными и для мошенников.

Цифры большие. По оценке Chainalysis, компании, которая занимается анализом блокчейнов, в 2025 году мошенники забрали в криптовалюте **более $17 млрд**, и это рекорд. Только в США Центр приёма жалоб на интернет-преступления при FBI (IC3) получил в 2025 году жалобы, связанные с криптовалютой, с заявленными потерями около **$11,4 млрд**, на 22% больше, чем годом ранее. Около $7,2 млрд из этой суммы пришлось на поддельные инвестиционные схемы.

Мошенничество также становится всё профессиональнее. По данным Chainalysis, в 2025 году число схем, в которых мошенники выдают себя за других, выросло более чем на 1400%, а средняя сумма одного платежа увеличилась примерно с $782 до примерно $2764. Многие группы теперь используют ИИ, чтобы писать сообщения, переводить переписку и создавать поддельные видео.



Рисунок 1. В 2025 году криптомошенничество достигло рекордного уровня. Цифры основаны на оценках Chainalysis и жалобах, поданных в FBI.

Rug pull и ханипоты

Rug pull (дословно «выдернуть ковёр») происходит, когда люди, стоящие за токеном или проектом, внезапно забирают деньги и исчезают, словно выдёргивая ковёр из-под ног покупателей. Чаще всего это случается с новыми токенами на децентрализованных биржах, где любой может за несколько минут создать токен и торговый пул (уроки 7 и 9).

Распространённые варианты:

- **Вывод ликвидности:** создатели забирают средства из торгового пула. Когда в пуле не остаётся ничего, на что можно обменять токен, его цена обрушивается почти до нуля.
- **Сброс командой:** создатели держат большую долю предложения и продают её на рынке всю сразу.
- **Ханипот (honeypot):** смарт-контракт токена написан так, что покупать можно, а продавать нельзя. График цены идёт только вверх, потому что продать не может никто, кроме создателей.



Рисунок 2. Упрощённая схема rug pull с токеном Squid Game. Пока цена росла, держатели не могли продать, а затем создатели опустошили пул.

ПРИМЕР: ТОКЕН SQUID GAME, 2021 ГОД

В конце 2021 года на децентрализованной бирже PancakeSwap появился неофициальный токен Squid Game, названный в честь популярного сериала «Игра в кальмара». За несколько дней его цена выросла на десятки тысяч процентов и 1 ноября 2021 года превысила **$2850**. Вскоре покупатели обнаружили, что не могут его продать. Затем создатели продали свои токены и опустошили пул, и за считаные минуты цена упала примерно до **$0,002**. Создатели ушли примерно с $3,38 млн. Авторы сериала не имели к этому никакого отношения.

Памп и дамп

В схеме **памп и дамп** (pump and dump) группа тихо скупает небольшую монету с низкой ликвидностью, а затем громко продвигает её через посты в соцсетях, платных инфлюенсеров или чаты. Когда набегают новые покупатели, цена подскакивает. Затем организаторы продают («сбрасывают») свои монеты этим запоздалым покупателям, и цена падает обратно, часто ниже исходного уровня.

Памп и дамп работает потому, что у небольших монет очень мало ликвидности (урок 8), и даже скромный объём покупок может сильно сдвинуть цену. Внезапный поток одинаковых постов о неизвестной монете, часто с обратным отсчётом и ценовыми целями, служит типичным признаком такой схемы.

Поддельные инвестиционные платформы и «забой свиней»

Больше всего денег теряют в поддельных инвестиционных схемах. Одна из известных форм называется **«забой свиней»** (pig butchering). Так переводится китайское выражение, которым пользуются сами мошенники: они «откармливают» жертву доверием, прежде чем «забить» её.

Обычно всё начинается с безобидного на вид сообщения: SMS «не на тот номер», совпадения в приложении знакомств или нового контакта в соцсетях. Неделями мошенник выстраивает дружбу или роман. В какой-то момент он упоминает, что хорошо зарабатывает на торговле криптовалютой, и предлагает показать, как это делается.

Жертву направляют на торговый сайт или в приложение, которые выглядят профессионально, но поддельны. Баланс на экране быстро растёт, и небольшие первые выводы могут даже проходить, что укрепляет доверие. Депозиты увеличиваются. Когда жертва пытается вывести крупную сумму, платформа вдруг требует сначала заплатить «налог», «комиссию» или «депозит за разблокировку». После оплаты платформа и «друг» исчезают.

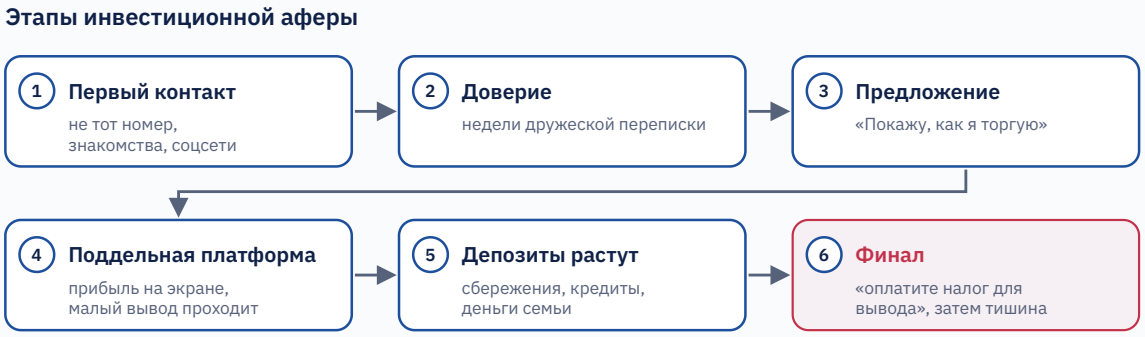


Рисунок 3. Типичные этапы схемы «забой свиней». Доверие выстраивается медленно, а потери приходят в конце.

ПРИМЕР: КАК ЭТО ВЫГЛЯДИТ ИЗНУТРИ

Лоре приходит SMS от Майкла: «Привет, Давид, в субботу гольф в силе?» Она отвечает, что он ошибся номером. Майкл извиняется, и они начинают переписываться. Через шесть недель он показывает ей скриншоты своей прибыли от торговли и помогает открыть счёт на платформе, которой пользуется сам. Её первые $1000 превращаются на экране в $1600, а вывод $200 приходит ей в кошелёк. Она вносит $25 000. Когда она просит вывести деньги, поддержка сообщает, что сначала нужно заплатить «налог» 20% с прибыли. Цифры на экране никогда не были настоящими.

Самозванцы, поддельная поддержка и мошенничество с «возвратом средств»

Многие схемы строятся на том, что мошенник выдаёт себя за того, кому вы доверяете:

- **Поддельная поддержка:** после того как вы задаёте вопрос на открытом форуме или в групповом чате, кто-то пишет вам в личные сообщения, представляясь службой поддержки биржи или кошелька. Настоящие службы поддержки не начинают личную переписку и никогда не просят сид-фразу или пароль.
- **Поддельные обращения от биржи или госорганов:** в звонке, письме или SMS сообщают, что вашему счёту грозит опасность и нужно срочно перевести средства на «безопасный» кошелёк.
- **Поддельные знаменитости и раздачи:** на видео или в посте известный человек обещает вернуть в двойном размере любую отправленную ему криптовалюту. Созданные с помощью ИИ дипфейки (deepfake) теперь делают такие ролики убедительными. Ни одна настоящая раздача так не работает.
- **Мошенничество с «возвратом средств»:** после того как человек теряет деньги, «эксперт по возврату» или поддельная юридическая фирма предлагает вернуть их за предоплату.

Мишенью становятся люди, которых уже однажды обманули.

Дрейнеры кошельков, разрешения и поддельные эйрдропы

Некоторым схемам не нужно, чтобы вы что-либо отправляли. Вместо этого они обманом заставляют вас дать вредоносному смарт-контракту разрешение перемещать ваши токены.

Когда вы пользуетесь приложением DeFi, кошелёк часто просит **одобрить** (approve) контракт, чтобы тот мог тратить определённый токен от вашего имени (урок 12). Поддельный сайт, который часто рекламируют как бесплатный **эйрдроп**, минт или получение награды, просит подключить кошелёк и подписать запрос. На самом деле вы подписываете разрешение, иногда на неограниченную сумму, и оно позволяет контракту мошенника забрать ваши токены. Такой инструмент называют **дрейнером кошелька** (wallet drainer).

К другим распространённым уловкам относятся поддельные приложения-кошельки и расширения для браузера, которые крадут сид-фразу, пока вы её вводите, адреса сайтов, похожие на настоящие, и отравление адреса (урок 10). Тот, у кого есть ваша **сид-фраза**, полностью контролирует ваш кошелёк, как говорилось в уроке 9 курса «Блокчейн». Старые разрешения остаются активными, пока их не отзовут, а такие инструменты, как Revoke.cash, и некоторые обозреватели блоков показывают, какие разрешения выдал кошелёк.



Рисунок 4. Дрейнер кошелька не просит отправить средства. Он просит подписать разрешение, которое позволяет ему их забрать.

Тревожные признаки, общие для большинства схем

Истории меняются, но тревожные признаки повторяются:

- **Гарантированная или очень высокая доходность**, например «2% в день» или «без риска».
- **Спешка и давление:** действуйте сейчас, предложение заканчивается сегодня вечером, ваш счёт закроют.
- **Просьбы сообщить сид-фразу или приватный ключ**, под любым предлогом.
- **Непрошеный контакт**, который постепенно переходит к инвестициям.

- **Малоизвестная платформа**, которую советует новый онлайн-друг, или приложение, найденное не через официальные источники.
- **Вывод средств, для которого сначала нужно заплатить комиссию.**
- **«Отправьте криптовалюту и получите вдвое больше».**
- **Токены, которые нельзя продать**, анонимная команда, владеющая большей частью предложения, или незаблокированная ликвидность.

Один тревожный признак ещё не доказывает мошенничество, но несколько сразу служат серьёзным предупреждением.

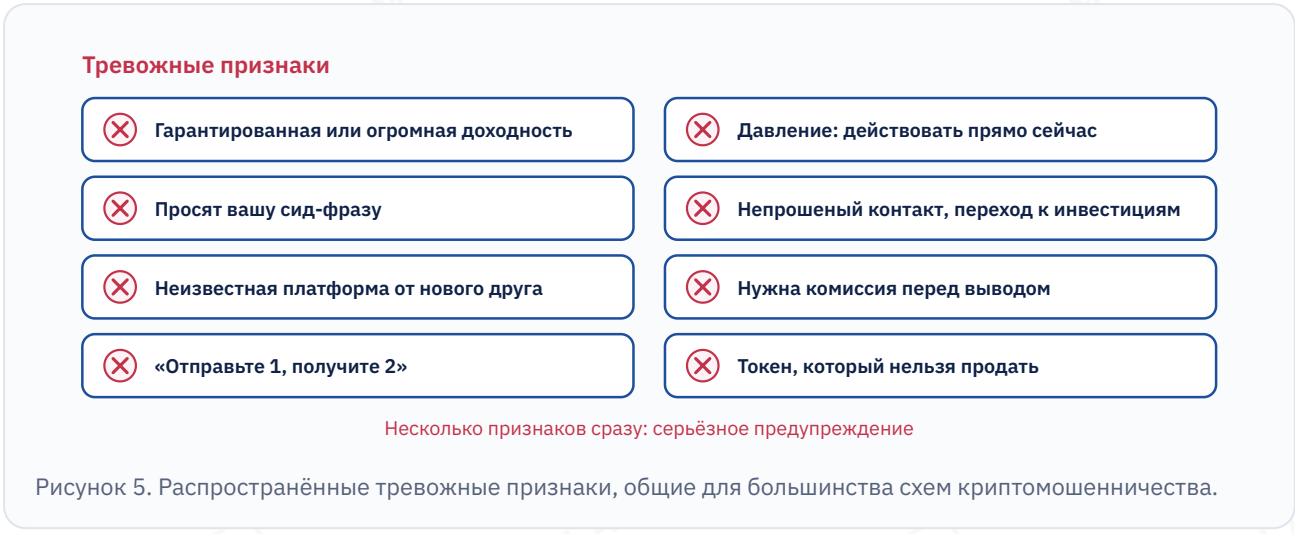


Рисунок 5. Распространённые тревожные признаки, общие для большинства схем криптомошенничества.

Что происходит после мошенничества

Поскольку переводы в блокчейне окончательны, деньги, отправленные мошеннику, возвращаются очень редко. Иногда, если средства быстро попадают на регулируемую биржу, она может их заморозить, а эмитенты стейблкоинов, такие как Tether и Circle, в ряде случаев замораживали украденные средства.

Шаги, которые описывают такие органы, как FBI, включают заявление о мошенничестве в полицию, а в США также в IC3; сообщение бирже или платформе, через которую шли средства; сохранение записей, таких как хеши транзакций, адреса кошельков, сообщения и ссылки на сайты; и отзыв всех выданных разрешений кошелька. Многие также переводят оставшиеся средства на новый кошелёк с новой сид-фразой, если считают, что старая могла быть раскрыта.

Органы власти также предупреждают, что с людьми, сообщившими о потере, потом часто связываются мошенники, предлагающие «возврат средств», и за первой потерей может последовать вторая.

Почему это важно для трейдеров

- **Быстрый рост привлекает мошенников.** Именно новые токены с огромным дневным ростом становятся местом для rug pull, ханипотов и схем памп и дамп. Проверка того, можно ли продать токен, кто держит предложение и заблокирована ли ликвидность, входит в базовое исследование, которое проводят многие трейдеры.
- **Предложения «копируйте мои сделки».** Группы, обещающие закрытые торговые подсказки или управление счётом в обмен на депозиты, часто служат входом на поддельные платформы.
- **Разрешения накапливаются.** У активных пользователей DeFi со временем может собраться много старых разрешений на токены. Каждое из них становится возможным риском, если контракт когда-нибудь будет скомпрометирован.
- **Те же привычки безопасности защищают торговые счета.** Аккаунты на биржах тоже под прицелом: фишинговые письма, поддельные страницы входа и подмена SIM-карты нацелены на захват аккаунтов и вывод средств. Урок 15 рассказывает о базовых мерах защиты, которые предлагают биржи.

Ключевые термины

Rug pull	Ситуация, когда создатели проекта внезапно забирают деньги, например выводят ликвидность или сбрасывают свои токены, и токен почти полностью обесценивается.
Ханипот (honeypot)	Токен, смарт-контракт которого позволяет покупать, но блокирует продажу для всех, кроме создателей.
Памп и дамп	Схема, в которой организаторы покупают небольшую монету, раздувают ажиотаж, чтобы поднять цену, а затем продают её запоздалым покупателям.
«Забой свиней» (pig butchering)	Долгая схема, в которой мошенник неделями выстраивает доверие, а затем убеждает жертву вносить крупные суммы на поддельную инвестиционную платформу.
Фишинг	Поддельные сообщения, письма или сайты, которые копируют настоящий сервис, чтобы выманить у людей пароли, коды или сид-фразы.

Дрейнер кошелька	Вредоносный код на поддельном сайте, который обманом заставляет пользователей подписывать разрешения или транзакции, переводящие их токены мошеннику.
Разрешение на токен	Подписанное вами разрешение, которое позволяет смарт-контракту тратить определённый токен из вашего кошелька, до заданной суммы или без ограничений.
Дипфейк	Поддельное видео или аудио, обычно созданное с помощью ИИ, в котором реальный человек говорит то, чего никогда не говорил.
Мошенничество с «возвратом средств»	Повторная схема, нацеленная на людей, которые уже потеряли деньги: им обещают вернуть их за предоплату.

Главное

1. Криптовалютные платежи быстрые и окончательные, и это делает их привлекательными для мошенников. По оценке Chainalysis, в 2025 году потери от мошенничества превысили $17 млрд.
2. Rug pull, ханипоты и схемы памп и дамп чаще всего встречаются у новых небольших токенов. Токен Squid Game за считаные минуты упал с уровня выше $2850 почти до нуля.
3. Больше всего потерь приносят поддельные инвестиционные платформы, к которым жертву часто приводит долгая онлайн-дружба. Поддельные балансы и небольшие первые выводы создают доверие.
4. Самозванцы выдают себя за поддержку, биржи, чиновников и знаменитостей. Настоящая поддержка никогда не просит сид-фразу.
5. Дрейнеры кошельков используют подписанные разрешения, а не просят отправить средства. Старые разрешения действуют, пока их не отзовут.
6. Самые частые тревожные признаки: гарантированная доходность, спешка, просьбы сообщить сид-фразу и комиссии за вывод.

Проверьте себя

Обведите один ответ на каждый вопрос. Ответы с пояснениями находятся на следующей странице. Пройти этот тест можно и онлайн на markettalks.info, сразу узнав свой результат.

1. Чем криптовалютные платежи привлекательны для мошенников?

A Они всегда анонимны и невидимы
B Они быстрые, глобальные и необратимые
C Биржи гарантируют мошенникам прибыль
D Их можно отправлять только ночью

2. Что такое токен-ханипот?

A Токен, обеспеченный настоящим мёдом
B Токен с высокими наградами за стейкинг
C Токен, контракт которого позволяет покупать, но не продавать
D Стейблкоин, привязанный к золоту

3. Что произошло с токеном Squid Game в ноябре 2021 года?

A Его разместили на всех крупных биржах
B Создатели опустошили пул, и цена упала с уровня выше $2850 примерно до $0,002
C Авторы сериала выкупили всё предложение
D Он стал стейблкоином

4. Кто обычно теряет деньги в схеме памп и дамп?

A Организаторы, которые купили первыми
B Запоздалые покупатели, пришедшие на волне ажиотажа
C Валидаторы блокчейна
D Никто, это без риска

5. Почему в схеме «забой свиней» небольшие первые выводы часто проходят?

A Потому что платформа настоящая
B Чтобы создать доверие перед крупными депозитами
C Из-за правил блокчейна
D Потому что этого требует банк

6. Человек в личных сообщениях называет себя службой поддержки вашего кошелька и просит сид-фразу, чтобы решить проблему. Что это?

A Обычная процедура поддержки
B Обязательная проверка безопасности
C Типичная схема с самозванцем
D Обновление программы

7. Как дрейнер кошелька обычно забирает токены?

A Подбирает ваш пароль
B Добивается, чтобы вы подписали разрешение или транзакцию на поддельном сайте
C Взламывает весь блокчейн
D Меняет цену токена

8. Какой из этих признаков часто указывает на мошенничество?

A Платформа требует комиссию, прежде чем вы сможете вывести средства
B Токен можно продать в любой момент
C Известная биржа с публичными аудитами
D Цена, которая движется и вверх, и вниз

Ответы

1 B

Они быстрые, глобальные и необратимые

Подтверждённый перевод не может отменить ни банк, ни платёжная компания, а средства за минуты пересекают границы.

2 C

Токен, контракт которого позволяет покупать, но не продавать

Контракт блокирует продажу для обычных держателей, поэтому цена лишь кажется растущей, пока создатели не выведут деньги.

3 B

Создатели опустошили пул, и цена упала с уровня выше $2850 примерно до $0,002

Покупатели не могли продать токен, затем создатели продали свои токены и забрали ликвидность, и цена рухнула за минуты.

4 B

Запоздалые покупатели, пришедшие на волне ажиотажа

Организаторы покупают рано и продают тем, кто приходит после рекламы, и у тех на руках остаётся дешевеющая монета.

5 B

Чтобы создать доверие перед крупными депозитами

Когда небольшую сумму позволяют вывести, поддельная платформа выглядит настоящей, и жертва чувствует себя спокойно, внося гораздо больше.

6 C

Типичная схема с самозванцем

Тот, у кого есть ваша сид-фраза, контролирует ваш кошелёк. Настоящая поддержка никогда её не просит.

7 B

Добивается, чтобы вы подписали разрешение или транзакцию на поддельном сайте

Пользователь подписывает разрешение, часто под видом получения эйрдропа, и оно позволяет контракту мошенника перемещать токены.

8 A

Платформа требует комиссию, прежде чем вы сможете вывести средства

Требование заплатить налог, комиссию или депозит до вывода средств служит классическим признаком поддельной платформы.

ИСТОЧНИКИ

- Decrypt, ИИ и самозванцы довели потери от криптомошенничества до рекордных $17 млрд в 2025 году (Chainalysis): https://decrypt.co/354624/ai-impersonation-drove-crypto-scam-losses-record-17-billion-2025-chainalysis
- Yahoo Finance, FBI сообщает о росте потерь от криптомошенничества на 22% в 2025 году: https://finance.yahoo.com/markets/crypto/articles/fbi-reports-22-rise-crypto-191510401.html

- Cointelegraph, мошенническая криптовалюта по мотивам «Игры в кальмара» рухнула: цена упала с $2800 до нуля: https://cointelegraph.com/news/game-over-squid-game-inspired-crypto-scam-collapses-as-price-crashes-from-2-8k-to-zero
- Cointelegraph, пользователи не могут продать токен Squid Game: https://cointelegraph.com/news/users-not-able-to-sell-squid-game-token-clocking-45-000-gains

Market Talks

ПРОДОЛЖАЙТЕ ОБУЧЕНИЕ

Далее: урок 15 С чего на самом деле начать: биржи, KYC и кошельки

Этот урок входит в курс «Криптовалюта» Образовательного центра MARKET TALKS. Уроки начального уровня бесплатны, в каждом есть тест и PDF для скачивания. Уроки среднего и продвинутого уровней доступны участникам.

Образовательный центр
Уроки от базовых принципов до продвинутых тем

Анализ рынков
Технический и фундаментальный анализ ключевых рынков

Отчёты
Биткоин, золото, серебро, SPX и другое

markettalks.info

Telegram @MARKET_TALKS

Только в образовательных целях. Ничто в этом документе не является финансовой рекомендацией. © 2026 MARKET TALKS. Вы можете свободно делиться этим PDF без изменений.