

Чей ключ, тот и распоряжается: кошельки, биржи и DEX

Человек потерял токен, не потеряв сид-фразу и не ошибившись с адресом: он просто подписал разрешение. Разбираем, что такое ключ, чем биржа отличается от кошелька и чем вы платите за удобство одного и свободу другого.

Три вывода урока

1. **Чей ключ, тот и распоряжается.** Поэтому вывод на бирже это просьба, а в своём кошельке это действие.
2. **Биржа даёт скорость, стакан и поддержку за риск контрагента.** Кошелёк даёт полный контроль за необратимость, газ и то, что помочь вам некому.
3. **На бирже вас подводит чужое решение, в кошельке ваше собственное.** Блокировка и приостановка вывода против подписи, которую вы не прочитали.

1. Ключ и сид-фраза

Монета это запись в реестре: адрес и количество (урок 1). Изменить запись может тот, у кого ключ. Ключ это право подписать перевод с адреса. Сеть не спрашивает, кто вы, чей аккаунт и на кого он оформлен. Она проверяет одно: подпись сходится с адресом, значит перевод исполнен.

Кошелёк монет не хранит, хранить их негде: они в реестре. Кошелёк хранит ключ, и больше ничего.

Сид-фраза это 12 или 24 слова, которые показывают при создании кошелька. Это не пароль. Из этих слов считаются все ваши ключи и все адреса во всех сетях. Пароль можно сменить, сид-фразу нельзя. Кто её увидел, тот получил кошелёк целиком, а ваш доступ при этом не пропадёт: вы даже не заметите, что кошелёк уже не только ваш.

2. Два вида кошельков

	Некастодиальный	Кастодиальный
У кого ключ	у вас	у кого-то другого, чаще у биржи
Примеры	приложение в телефоне, расширение в браузере, аппаратный кошелёк	счёт на бирже
Вывод	действие: подписываете вы	просьба: подписывает биржа
Если ошиблись	никто не поможет, «забыли пароль» нет	иногда поддержка может исправить

Аппаратный кошелёк это отдельное устройство, которое подписывает внутри себя и ключ наружу не отдаёт.

На бирже баланс это строчка в базе, сделка это правка двух строк (урок 2). Теперь видно почему: ключ у биржи, и ей незачем идти в сеть, чтобы переписать собственную таблицу. Запрос на вывод подаёте вы, а транзакцию подписывает биржа.

3. Биржа: что даёт и чем вы платите

Биржа даёт стакан в одном месте, мгновенные сделки, мгновенные переводы между спотом и фьючерсами, плечо и поддержку. Для арбитража главное: обе ноги в одном интерфейсе и закрываются за секунды.

Платите вы одним: **риском контрагента**. У него три формы.

1. **Не отдаст вообще.** Банкротство, вывод средств основателями, взлом: Mt.Gox, FTX. Клиентам FTX деньги в итоге вернули, но в долларах, по цене на день банкротства. Биткоин с того дня вырос в разы. Доллары вернулись, монеты нет.
2. **Не отдаст сейчас.** Вывод монеты приостановлен: техработы, проблема в сети, перегрузка. Деньги целы, но связка стоит, а спред уходит. Поэтому в уроке 8 это был пункт чек-листа.
3. **Не отдаст вам.** Биржи проверяют происхождение входящих монет. Монета с плохой историей может заморозить счёт целиком, даже если вы её не покупали, а вам её просто прислали.

Доказательство резервов показывает, что активы у биржи есть. Сколько она должна, не показывает. Это снимок, а не проверка, как аттестация у стейблкоинов (урок 6).

4. DEX: сделка прямо в блокчейне

Децентрализованная биржа это не компания, а программа в блокчейне, смарт-контракт. Вы туда ничего не заводите, вы подключаете кошелёк. Сайт видит ваш адрес, но распоряжаться ничем не может. Монеты остаются у вас до секунды сделки.

Сделка это транзакция, которую подписываете вы сами. Сеть её исполняет, монеты меняются местами в тот же момент. Нет депозита, вывода, регистрации и лимитов. Вывод здесь действие, а не просьба.

Не все DEX устроены как пулы: есть такие, что выглядят как биржа, со стаканом, перпами и плечом. Но и там распоряжается ваш ключ, а не счёт компании.

Пул: цену двигает ваша сделка

Чаще всего на DEX вы торгуете не против человека, а против **пула**. Пул это две монеты, которые кто-то сложил в контракт, а цена берётся из их соотношения. Покупая, вы доливаете в пул одну монету и забираете другую, соотношение сдвигается, и цена уходит против вас. Чем больше сумма относительно пула, тем хуже ваша цена.

Пример на классическом пуле (формула $x \cdot y = k$), ETH по 2 000 \$:

Пул	Сделка	Доля сделки в пуле	Что в пуле после сделки
2 000 000 \$ (1 000 000 USDT + 500 ETH)	20 000 \$	1 %	1 020 000 USDT + 490,2 ETH
2 000 000 \$	200 000 \$	10 %	1 200 000 USDT + 416,7 ETH
100 000 \$ (50 000 USDT + 25 ETH)	20 000 \$	20 %	70 000 USDT + 17,9 ETH

Те же 20 000 \$ в маленьком пуле занимают 20 % и двигают его сильнее, чем 200 000 \$ большой. Это то же проскальзывание, что в уроке 3, только считается не по стакану, а по размеру пула. В уроке 8 мы смотрели глубину стакана, а не общий объём. На DEX правило то же: смотрите **размер пула**. На маленьком пуле от красивой цифры спреда не остаётся ничего.

Посчитать на своих цифрах: калькулятор проскальзывания в пуле, он под этим уроком.

Газ

За транзакцию платите газ, и только **нативной монетой сети**:

Сеть	Газ платят в
Ethereum	ETH
BNB Chain	BNB
Solana	SOL

Без газа кошелёк не может ничего, даже если на нём миллион в USDT. И газ списывается, даже когда транзакция не прошла.

Сэндвич-атака

В большинстве сетей транзакция сначала попадает в общую очередь и только потом в блок, поэтому её видно до того, как она исполнена. Этим живут боты. Вы разрешили проскальзывание, скажем, 3 %. Бот покупает перед вами, двигает цену ровно на эти 3 % и продаёт сразу после вас. Вы оказываетесь зажаты между двумя его сделками, поэтому это называют **сэндвич-атакой**. Ваш допуск это его заработок. Допуск ставят минимальный, какой проходит.

5. Кошелёк: чем вы платите за свободу

- Всё необратимо.** Отправили не на тот адрес, не в ту сеть, подтвердили не то: кнопки отмены нет, жаловаться некому. Сеть сделала ровно то, что вы подписали.
- Кошельки выносят не взломом, а подписью.** Чтобы обменник мог продать ваш токен, вы даёте контракту разрешение этим токеном распоряжаться. По умолчанию часто без ограничения суммы и срока. Это нормальная механика, на ней работает весь обмен. Но точно так же выглядит разрешение, которое просит поддельный сайт. Подписали, и ваш токен может забрать кто угодно и когда угодно, уже без вас. Перевода вы при этом не делали, вы просто дали право.

3. **Подпись без газа тоже бывает разрешением.** «Бесплатно» и «безопасно» здесь не одно и то же.
4. **Аппаратный кошелёк защищает ключ, но не от вашей подписи.** Ключ физически не выходит наружу, но кнопку подтверждения вы нажмёте сами.
5. **Название монеты не значит ничего.** Выпустить токен с любым именем может кто угодно, это стоит копейки. Монету ищут по адресу контракта из официального источника, а не по названию в поиске.

«Без ограничения суммы» это умолчание, а не закон. В окне кошелька перед подписью сумму разрешения можно выставить вручную. А уже выданное право можно отозвать в любой момент.

6. Где это встречается в арбитраже

Связка	Где ноги	Риски
Биржа — биржа	обе в чужом кастодиале	быстро и удобно, но зависит от того, что обе биржи работают и вывод открыт
Биржа — DEX	одна на бирже, вторая под вашим ключом	закрытого вывода и блокировки нет, зато газ, время блока, цена пула и боты в очереди

Связку биржа — DEX разберём в практическом треке.

Про капитал: в уроке 8 мы решали, на каких биржах держать деньги. Вопрос шире: сколько держать на биржах вообще. На бирже рабочая сумма, та, которой торгуете. Остальное под своим ключом. Биржа рабочий инструмент, а не сейф.

Чек-лист

1. Сид-фраза на бумаге и не рядом с телефоном. Не в заметках, не в фотографиях, не в облаке.
2. Два кошелька: рабочий с небольшой суммой, который подписывает на сайтах, и хранилище, которое не подписывает нигде.
3. Нативная монета на газ заведена до первой сделки. Без неё нельзя даже забрать свои монеты.
4. Разрешения, выданные контрактам, проверять и отзываться всё, чем больше не пользуетесь. Десять минут, которые закрывают самую частую причину потери кошелька.

Термины

- **Ключ (приватный ключ):** право подписать перевод с адреса. Кто держит ключ, тот распоряжается монетами.
- **Сид-фраза:** 12 или 24 слова, из которых считаются все ключи и адреса кошелька. Сменить нельзя.

- **Некастодиальный кошелёк:** кошелёк, ключ от которого у вас.
- **Кастодиальный кошелёк:** кошелёк, ключ от которого у кого-то другого, чаще у биржи.
- **Риск контрагента:** риск, что сторона, которая держит ваши деньги, не отдаст их вообще, сейчас или вам.
- **Доказательство резервов:** отчёт биржи о том, какие активы у неё есть. Обязательства в нём не видны.
- **DEX:** децентрализованная биржа, программа в блокчейне. Сделку подписываете вы сами.
- **Пул ликвидности:** две монеты в контракте DEX. Цена берётся из их соотношения.
- **Проскальзывание:** разница между ценой до сделки и средней ценой, по которой сделка исполнилась.
- **Газ:** плата сети за транзакцию, в нативной монете сети.
- **Допуск проскальзывания:** насколько цена может уйти от ожидаемой, чтобы транзакция всё равно исполнилась.
- **Сэндвич-атака:** бот покупает перед вашей сделкой и продаёт сразу после неё, забирая разницу в пределах вашего допуска.
- **Разрешение (approve):** право, которое вы даёте контракту распоряжаться вашим токеном.
- **Адрес контракта:** уникальный адрес токена в сети. По нему, а не по названию, отличают настоящую монету от подделки.

Проверь себя

Почему вывод с биржи это просьба, а не действие?

Ключ у биржи. Запрос подаёте вы, а транзакцию подписывает она и может не подписать.

Кошелёк хранит монеты?

Нет. Монеты это записи в реестре. Кошелёк хранит ключ.

Клиентам FTX вернули деньги. Почему они всё равно потеряли?

Вернули доллары по цене на день банкротства. Монеты с того дня выросли в разы.

Одна и та же сделка на 20 000 \$ в пуле на 2 млн и в пуле на 100 тысяч. Где цена хуже?

В маленьком: там сделка занимает 20 % пула, а не 1 %, и сдвигает соотношение монет сильнее.

На кошельке миллион в USDT и ноль нативной монеты. Что можно сделать?

Ничего: ни перевода, ни обмена, ни вывода. Газ платят только нативной монетой сети.

Зачем ставить минимальный допуск проскальзывания?

Допуск это заработок бота в сэндвич-атаке. Чем он больше, тем больше бот может забрать.

Аппаратный кошелёк спасёт от поддельного сайта?

Нет. Он защищает ключ от кражи, но разрешение вы подпишете сами.

Следующие уроки: три ролика с записью экрана. Как начать на бирже, как начать в кошельке и мосты: как перевести монету из одной сети в другую и не потерять по дороге.

Материал носит образовательный характер и не является инвестиционной рекомендацией.
Любые решения о сделках вы принимаете самостоятельно и на свой риск.