Market Talks
ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 8 ИЗ 13

Ключи, адреса и кошельки

Что на самом деле доказывает владение биткоином, чем вы делитесь, чтобы получить оплату, и что на самом деле хранит кошелёк

6 мин чтения Вопросов в тесте: 6, с ответами

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 8 ИЗ 13

Ключи, адреса и кошельки

СУТЬ В ОДНОМ ПРЕДЛОЖЕНИИ

Владеть биткоином значит держать закрытый ключ, секретное число, которое позволяет подписывать платежи. Из него получаются открытый ключ и адрес, которыми можно делиться. Кошелёк вообще не хранит монеты: он хранит ключи и подписывает ими.

Один секрет и две вещи, которыми можно делиться

В уроке 5 мы видели, что в блокчейне нет имён, только адреса. Как же сеть узнаёт, что монета ваша? Ответ кроется в трёх связанных частях:

- **Закрытый ключ.** Секретное число, выбранное случайно из диапазона настолько огромного, что в нём 78 цифр, того же масштаба, что и хеши из урока 6. Тот, кто его знает, может тратить связанные с ним монеты.
- **Открытый ключ.** Число, вычисленное из закрытого ключа с помощью особой математики. Его можно показывать кому угодно.
- **Адрес.** Более короткий код, полученный хешированием открытого ключа, со встроенной проверкой, которая ловит опечатки. Именно его вы даёте людям, чтобы они могли вам заплатить.

Каждый шаг работает только в одну сторону. Превратить закрытый ключ в открытый, а открытый в адрес компьютер может за долю секунды. Пройти обратно практически невозможно. Поэтому свой адрес можно публиковать где угодно, не подвергая монеты риску.



Рисунок 1. Закрытый ключ создаёт открытый ключ, а тот создаёт адрес. Каждый шаг работает только в одну сторону, поэтому, делясь адресом, вы никогда не раскрываете закрытый ключ.

Тратить значит подписывать

Чтобы потратить биткоин, кошелёк собирает транзакцию и добавляет к ней **цифровую подпись**, сделанную вашим закрытым ключом. Любой узел может проверить эту подпись с помощью вашего открытого ключа и убедиться, что её создал соответствующий закрытый ключ, ни разу не увидев сам закрытый ключ.

Подпись также привязана к точным деталям именно этой транзакции. Если кто-то изменит сумму или получателя хотя бы на один символ, подпись перестанет совпадать, и каждый узел её отклонит. Поэтому никто не может перехватить ваш платёж по дороге через сеть и перенаправить его.

В этом большое отличие от банков. Банк решает, можно ли вам тратить, проверяя, кто вы. Биткоин проверяет только, действительна ли подпись. Ни имени, ни сброса пароля, ни службы поддержки, только математика.

АНАЛОГИЯ: ПОЧТОВЫЙ ЯЩИК С ПРОРЕЗЬЮ

Представьте адрес как почтовый ящик с прорезью спереди. Любой, кто знает, где он стоит, может опустить письмо, и вся улица видит, сколько писем приходит. Но открыть ящик и достать письма может только тот, у кого есть ключ. Потеряйте ключ, и письма останутся запертыми навсегда. Если кто-то скопирует ключ, он сможет опустошить ящик.

Как выглядят адреса биткоина

Биткоин несколько раз менял формат адресов. Все они до сих пор работают, и различить их можно по первым символам:

Начинается с	Тип	Появился
1	Legacy, исходный формат	2009
3	Скриптовый адрес, часто для совместных или мультиподписных кошельков	2012
bc1q	Native SegWit, транзакции меньше, комиссии ниже	2017
bc1p	Taproot, новейший формат, больше приватности и гибкости	2021

У других блокчейнов свои форматы. Адреса Ethereum, например, начинаются с *0x*, за которым следуют 40 символов. Адрес биткоина нельзя заменить адресом Ethereum, даже если оба показывает одно и то же приложение.

Хороший кошелёк создаёт новый адрес каждый раз, когда вы хотите получить платёж. Все они принадлежат одному кошельку, и старые продолжают работать. Новые адреса мешают посторонним связать все ваши платежи между собой.

Что на самом деле хранит кошелёк

Вопреки названию, кошелёк никогда не хранит монеты. Монеты существуют только как записи в блокчейне. **Кошелёк** представляет собой инструмент, который хранит ваши ключи, читает блокчейн, чтобы показать баланс, создаёт транзакции и подписывает их.

Кошельки делятся на две большие группы:

- **Горячие кошельки** хранят ключи на устройстве, подключённом к интернету, например в приложении на телефоне или программе на компьютере. Они удобны для повседневного использования, но ключи открыты для всего, что может атаковать это устройство.
- **Холодные кошельки** хранят ключи офлайн. **Аппаратный кошелёк** представляет собой небольшое устройство, которое хранит ключи внутри и подписывает транзакции, никогда не показывая ключи компьютеру. Им пользоваться медленнее, но взломать его гораздо труднее.

Если ваши монеты лежат на бирже, ключи держит биржа, а не вы. Урок 10 сравнивает эти два варианта, а урок 9 рассказывает о резервной копии, которая защищает сразу все ваши ключи.

РЕАЛЬНЫЙ ПРИМЕР: ЖЁСТКИЙ ДИСК НА СВАЛКЕ

В 2013 году Джеймс Хауэллс, компьютерный инженер из Уэльса, случайно выбросил старый жёсткий диск с закрытым ключом к 8000 биткоинов, которые он добыл несколькими годами раньше. Диск оказался на городской свалке. Больше десяти лет он добивался разрешения раскопать её. В январе 2025 года британский суд отклонил его иск, а в марте была отклонена и его апелляция. Монеты по-прежнему в блокчейне, их видят все, но потратить не может никто.

Почему это важно трейдерам

- **Проверяйте весь адрес, каждый раз.** При мошенничестве с отравлением адреса злоумышленники отправляют крошечную транзакцию с адреса, почти неотличимого от того, которым вы пользуетесь, в надежде, что в следующий раз вы скопируете его из истории. В мае 2024 года один трейдер отправил на такой адрес 1155 обёрнутых биткоинов стоимостью около 68 млн долларов. Позже злоумышленник вернул большую часть после переговоров, что случается крайне редко.
- **Сверяйте сеть, а не только адрес.** Биржи часто поддерживают одну и ту же монету в нескольких сетях. Отправка в сети, которую принимающая сторона не поддерживает, может сделать возврат средств очень трудным или невозможным. Перед подтверждением проверьте сеть и обязательный мемо или тег, если он нужен.
- **Сначала отправьте небольшую тестовую сумму.** При крупных или первых переводах маленький тестовый платёж стоит немного комиссии, но может спасти всю сумму. Многие трейдеры также используют белые списки адресов для вывода в своих биржевых аккаунтах.

Ключевые термины

Закрытый ключ	Секретное случайное число, которое позволяет его владельцу подписывать транзакции и тратить связанные с ним монеты.
Открытый ключ	Число, вычисленное из закрытого ключа, которым можно делиться и которым проверяют подписи.
Адрес	Более короткий код, полученный из открытого ключа, которым вы делитесь, чтобы вам могли отправить монеты.
Цифровая подпись	Доказательство, созданное закрытым ключом, которое одобряет одну конкретную транзакцию и которое любой может проверить открытым ключом.
Кошелёк	Инструмент, который хранит ваши ключи, показывает баланс по данным блокчейна, создаёт и подписывает транзакции.
Аппаратный кошелёк	Небольшое устройство, которое держит закрытые ключи офлайн и подписывает транзакции, не показывая ключи компьютеру.

Главное

1. Владеть биткоином значит контролировать закрытый ключ. У кого ключ, тот и может тратить монеты.
2. Открытый ключ и адрес вычисляются из закрытого ключа, и ни один из них нельзя превратить обратно.
3. Чтобы потратить монеты, нужна цифровая подпись, привязанная к точной транзакции, которую любой узел проверяет, не видя закрытого ключа.
4. Адреса биткоина начинаются с 1, 3, bc1q или bc1p в зависимости от типа, и кошелёк может создавать новый адрес для каждого платежа.
5. Кошельки хранят ключи, а не монеты. Горячие кошельки удобны, а холодные держат ключи офлайн и гораздо безопаснее.

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. Что даёт возможность тратить биткоин?

- A Знание адреса
- B Владение закрытым ключом
- C Аккаунт на бирже
- D Знание идентификатора транзакции

2. Почему адресом можно спокойно делиться публично?

- A Потому что адреса действуют только один раз
- B Потому что сеть скрывает адрес от других
- C Потому что по адресу никто не может вычислить закрытый ключ
- D Потому что адреса зашифрованы

3. Что произойдёт, если кто-то изменит сумму в подписанной транзакции?

A Подпись перестанет совпадать, и узлы её отклонят
B Транзакция пройдёт с новой суммой
C Подпись обновится автоматически
D Майнер сам решит, какую сумму использовать

4. Что на самом деле хранит криптокошелёк?

A Ваши монеты
B Копию всего блокчейна
C Ваши банковские реквизиты
D Ваши ключи

5. Адрес биткоина начинается с bc1q. Какого он типа?

A Legacy
B Native SegWit
C Ethereum
D Taproot

6. В чём главное преимущество аппаратного кошелька?

A Транзакции проходят быстрее
B Он убирает все комиссии
C Он держит закрытые ключи офлайн и подписывает, не раскрывая их
D Он позволяет вернуть монеты, отправленные не на тот адрес

Ответы

1 B

Владение закрытым ключом

Платежи подписывает закрытый ключ. Любой, у кого он есть, может тратить монеты, поэтому его нужно держать в секрете.

2 C

Потому что по адресу никто не может вычислить закрытый ключ

Каждый шаг от закрытого ключа к открытому и к адресу работает только в одну сторону. Другие могут отправлять на ваш адрес, но не могут найти по нему закрытый ключ.

3 A

Подпись перестанет совпадать, и узлы её отклонят

Подпись привязана к точным деталям одной транзакции. Любое изменение, даже одного символа, делает её недействительной.

4 D

Ваши ключи

Монеты существуют только в блокчейне. Кошелёк хранит ваши ключи, читает баланс из цепочки и подписывает транзакции.

5 B

Native SegWit

Адреса, начинающиеся с bc1q, относятся к Native SegWit и появились в 2017 году. Адреса Taproot начинаются с bc1p, а Legacy с 1.

6 C

Он держит закрытые ключи офлайн и подписывает, не раскрывая их

Аппаратный кошелёк хранит ключи внутри устройства и отдаёт наружу только подписанные транзакции, поэтому вредоносная программа на компьютере не может прочитать ключи.

ИСТОЧНИКИ

- Сатоси Накамото, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- Википедия, биткоины на свалке в Ньюпорте: https://en.wikipedia.org/wiki/Bitcoin_buried_in_Newport_landfill
- Cointelegraph, трейдер потерял 68 млн долларов из-за отравления адреса (май 2024): https://cointelegraph.com/news/trader-loses-68-million-address-poisoning-scam
- Cointelegraph, злоумышленник вернул средства после переговоров: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations

Market Talks

ПРОДОЛЖАЙТЕ ОБУЧЕНИЕ

Далее: урок 9
Сид-фразы и резервные копии

Этот урок входит в бесплатный курс «Блокчейн» Образовательного центра MARKET TALKS: уроки начального, среднего и продвинутого уровней, в каждом из которых есть тест и PDF для скачивания.

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.