Market Talks

ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 11 ИЗ 13

Путь транзакции

Что происходит между нажатием кнопки «Отправить» и поступлением монет, и почему иногда это занимает больше времени, чем вы ожидаете

6 мин чтения Вопросов в тесте: 6, с ответами

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 11 ИЗ 13

Путь транзакции

СУТЬ В ОДНОМ ПРЕДЛОЖЕНИИ

Криптотранзакция собирается и подписывается в вашем кошельке, передаётся от узла к узлу, ждёт в зоне ожидания, попадает в блок к майнеру или валидатору, а затем оказывается погребённой под новыми блоками. От комиссии, которую вы платите, зависит, как быстро она покинет очередь.

Шаг 1: кошелёк собирает и подписывает транзакцию

Когда вы нажимаете «Отправить», в блокчейн пока ничего не попадает. Сначала кошелёк составляет небольшое сообщение, в котором сказано три вещи: какие монеты тратятся, куда они идут и какую комиссию вы предлагаете.

В биткоине ваш баланс не является одним числом. Он представляет собой набор отдельных кусочков монет, которые вы получили раньше. Они называются **непотраченными выходами**. Чтобы отправить 0,3 BTC из кусочка стоимостью 0,5 BTC, кошелёк тратит его целиком: 0,3 уходит получателю, небольшая сумма идёт на комиссию, а остаток возвращается на ваш же адрес как **сдача**. Ethereum устроен скорее как банковский баланс, но принцип подписи там тот же.

В конце кошелёк подписывает сообщение вашим закрытым ключом, как мы видели в уроке 8. Подпись доказывает, что владелец одобрил именно этот платёж. Если потом изменить хотя бы одну цифру, подпись перестанет подходить.



Рисунок 1. Транзакция подписывается в кошельке, проверяется и передаётся узлами, ждёт в мемпуле и получает первое подтверждение, когда майнер включает её в блок. Каждый следующий блок добавляет ещё одно.

ПРИМЕР: КУДА УХОДЯТ 0,5 BTC

У вас есть один кусочек стоимостью 0,5 BTC, и вы хотите отправить другу 0,3 BTC. Кошелёк составляет транзакцию с двумя выходами: 0,3 BTC другу и 0,1999 BTC обратно на ваш адрес для сдачи. Недостающие 0,0001 BTC нигде не записаны как выход. Всё, что остаётся сверх выходов, и есть комиссия, и её забирает майнер, который включит транзакцию в блок.

Шаг 2: рассылка и зал ожидания

Подписанная транзакция передаётся узлу, и он её проверяет: верны ли подписи, существуют ли монеты, не потрачены ли они уже? Если всё в порядке, узел передаёт её своим пирам, и за несколько секунд она расходится по сети, как показал урок 7.

Каждый узел держит известные ему действительные транзакции в зоне ожидания, которая называется **мемпулом** (memory pool, «пул памяти»). Единого мемпула не существует. У каждого узла свой, поэтому их содержимое немного различается. Пока ваша транзакция находится там, у неё **ноль подтверждений**: сеть о ней знает, но в блокчейне её ещё нет, и в редких случаях её ещё можно заменить.

Шаг 3: комиссия решает, кто пройдёт первым

Блок биткоина появляется примерно раз в десять минут, и места в нём ограничено. Когда ожидающих транзакций больше, чем помещается в один блок, майнеры заполняют его теми, кто платит больше всего за занимаемое место. Поэтому комиссии в биткоине указываются как ставка, в **сатоши за виртуальный байт** (sat/vB), а не как процент от суммы. Отправка 10 долларов и 10 миллионов долларов стоит одинаково, если транзакции одного размера.

Состояние сети	Что обычно происходит
Спокойный мемпул	Даже с низкой комиссией транзакция попадает в ближайший блок или следующий за ним
Загруженный мемпул	Транзакции с низкой комиссией ждут, иногда часами или днями
Внезапный наплыв	Комиссии могут вырасти в несколько раз за час

Наплыв бывает экстремальным. 20 апреля 2024 года блок 840 000, тот самый, который вдвое сократил награду за майнинг биткоина, собрал более 37 BTC комиссий, около 2,4 миллиона долларов по тогдашнему курсу, потому что множество пользователей соревновались за место в этом историческом блоке.

АНАЛОГИЯ: ПОСЛЕДНИЙ ВЕЧЕРНИЙ ПАРОМ

Небольшой паром отходит каждые десять минут, и мест в нём фиксированное количество. Тихим вечером садятся все. В праздничные выходные очередь длинная, и команда пускает на борт тех, кто предлагает самую высокую цену за место. Если вы предложили минимум, вы всё ещё стоите в очереди, когда приходит следующий паром, и тот, что за ним.

Шаг 4: подтверждения и окончательный расчёт

Когда майнер включает вашу транзакцию в блок, который принимает сеть, у неё появляется **одно подтверждение**. Каждый блок, добавленный сверху, прибавляет ещё одно. С каждым новым блоком отменить платёж всё труднее, потому что атакующему пришлось бы заново создать все эти блоки, как объяснялось в уроке 6.

Подтверждения (биткоин)	Обычное значение
0	Сеть видит транзакцию, но в блоке её ещё нет
1	Транзакция в блоке, этого достаточно для небольших повседневных сумм
Несколько	Столько обычно ждут биржи, прежде чем зачислить депозит, в зависимости от платформы
6	Давнее практическое правило для крупных сумм, около часа

У других сетей свой ритм. Ethereum добавляет блок каждые 12 секунд и считает блок окончательным примерно через 13 минут, когда его уже нельзя отменить, не уничтожив огромное количество застейканного ETH.

Когда транзакция застревает

Если в загруженный период вы поставили слишком низкую комиссию, транзакция может долго ждать в мемпулах. Ничего не теряется: монеты никуда не ушли. Очень старые транзакции в итоге удаляются из большинства мемпулов, и монеты просто остаются там, где были. Есть два распространённых способа решения:

- **Replace-by-fee (RBF, замена с повышением комиссии).** Кошелёк отправляет новую версию того же платежа с более высокой комиссией, и она заменяет старую.
- **Child pays for parent (CPFP, «ребёнок платит за родителя»).** Получатель или вы сами через сдачу тратите застрявшие монеты в новой транзакции с высокой комиссией, и у

майнера появляется причина включить обе транзакции вместе.

Какой бы способ вы ни выбрали, весь путь можно отследить самостоятельно. У каждой транзакции есть идентификатор, **txid**, который можно вставить в обозреватель блоков и увидеть, ждёт ли она, подтверждена ли и насколько глубоко погребена.

Почему это важно трейдерам

- **Депозиты не мгновенны.** Биржа зачисляет ваш биткоин только после нужного ей числа подтверждений. Если вы рассчитываете торговать на быстром движении, монеты должны быть на бирже до движения, а не в пути.
- **Комиссии растут, когда рынок движется.** Резкие колебания цены одновременно приводят в блокчейн множество людей, и комиссии взлетают вместе с ними. Проверяйте текущую ставку комиссии перед отправкой и не выбирайте самую низкую настройку, когда важно время.
- **Сохраняйте txid.** Если депозит или вывод задерживается, txid точно покажет, где он находится. Это также первое, что спросит служба поддержки биржи.

Ключевые термины

Мемпул	Зона ожидания, где каждый узел держит действительные транзакции, ожидающие включения в блок.
Комиссия за транзакцию	То, что платит отправитель, чтобы транзакцию включили в блок. В биткоине это всё, что остаётся после вычитания выходов из входов.
sat/vB	Сатоши за виртуальный байт, ставка, по которой сравнивают комиссии в биткоине. Один сатоши равен одной стомиллионной биткоина.
Подтверждение	Один блок в цепочке, который содержит вашу транзакцию или идёт после неё. Чем больше подтверждений, тем труднее отменить платёж.
Выход для сдачи	Часть потраченной монеты, которую кошелёк отправляет обратно на собственный адрес отправителя.
Идентификатор транзакции (txid)	Уникальный код, который обозначает транзакцию и позволяет найти её в обозревателе блоков.

Главное

1. Транзакция собирается и подписывается в вашем кошельке ещё до того, как что-либо отправлено в сеть.
2. Узлы проверяют её, передают дальше и держат в своих мемпулах, где у неё ноль подтверждений.
3. Место в блоке ограничено, поэтому майнеры выбирают транзакции с самой высокой ставкой комиссии, а не с самой большой суммой.
4. Каждый блок после вашего означает ещё одно подтверждение, а биржи ждут определённого их числа, прежде чем зачислить средства.
5. Застрявшую транзакцию можно ускорить с помощью replace-by-fee или child pays for parent и отследить по её txid.

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. Где подписывается транзакция?

- A Первым узлом, который её получает
- B В кошельке отправителя, до отправки
- C Майнером, который включает её в блок
- D Кошельком получателя, когда она приходит

2. Вы тратите монету в 0,5 BTC, чтобы отправить 0,3 BTC. Что происходит с остатком?

- A Он теряется навсегда
- B Он заблокирован до следующего халвинга
- C Большая часть возвращается вам как сдача, а небольшой остаток и есть комиссия
- D Получатель оставляет его себе в качестве чаевых

3. Что такое мемпул?

A Зона ожидания каждого узла для действительных транзакций, ожидающих блока

B Единый глобальный сервер, которым управляют разработчики биткоина

C Кошелёк, в котором хранятся монеты бирж

D Часть блока, где записываются комиссии

4. Две транзакции биткоина одинакового размера. Одна отправляет 10 долларов, другая 10 миллионов. Какой нужна более высокая комиссия, чтобы быстро попасть в блок?

A Той, что на 10 миллионов, потому что комиссия считается в процентах

B Ни одной, им нужна одинаковая ставка комиссии

C Той, что на 10 долларов, потому что мелкие платежи задерживаются

D Комиссии устанавливает биржа, а не сеть

5. Ваша транзакция в блоке, и после него добавлено ещё два блока. Сколько у неё подтверждений?

A Одно

B Два

C Три

D Шесть

6. Ваша транзакция с низкой комиссией ждёт уже несколько часов в загруженный период. Какое решение является стандартным?

A Отправить те же монеты ещё раз на новый адрес

B Связаться с майнерами и попросить включить её

C Восстановить кошелёк из сид-фразы

D Использовать replace-by-fee и отправить новую версию с более высокой комиссией

Ответы

1 B

В кошельке отправителя, до отправки

Кошелёк подписывает её закрытым ключом перед рассылкой. Узлы и майнеры только проверяют подпись, создать её они не могут.

2 C

Большая часть возвращается вам как сдача, а небольшой остаток и есть комиссия

Биткоин тратит монеты целиком. Кошелёк отправляет разницу на ваш адрес для сдачи и оставляет немного нераспределённым в качестве комиссии.

3 A

Зона ожидания каждого узла для действительных транзакций, ожидающих блока

У каждого узла свой мемпул, поэтому единого не существует. В нём хранятся транзакции, которые действительны, но ещё не попали в блок.

4 B

Ни одной, им нужна одинаковая ставка комиссии

Майнеры сравнивают комиссии за виртуальный байт места. Отправляемая сумма не важна, важен только размер транзакции.

5 C

Три

Блок, в котором она находится, считается первым подтверждением, и каждый следующий блок добавляет ещё одно, то есть один плюс два дают три.

6 D

Использовать replace-by-fee и отправить новую версию с более высокой комиссией

Replace-by-fee заменяет ожидающую транзакцию версией с более высокой комиссией. Другой распространённый вариант представляет собой child pays for parent.

ИСТОЧНИКИ

- Bitcoin Developer Guide, транзакции: https://developer.bitcoin.org/devguide/transactions.html
- Cointelegraph, пользователи биткоина потратили рекордные 2,4 млн долларов на комиссии в блоке халвинга: https://cointelegraph.com/news/bitcoin-halving-users-spend-record-millions-block-space-runes-rare-satoshis
- ethereum.org, доказательство доли и окончательность: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
- Bitcoin Optech, Replace-by-fee: https://bitcoinops.org/en/topics/replace-by-fee/

Market Talks

ПРОДОЛЖАЙТЕ ОБУЧЕНИЕ

Далее: урок 12 Публичные, частные и консорциумные блокчейны

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.