Market Talks
EDUCATION CENTER

BLOCKCHAIN · BEGINNER · LESSON 11 OF 13

A Transaction's Journey

What happens between pressing Send and the coins arriving, and why it sometimes takes longer than you expect

6 min read 6 quiz questions with answer key

BLOCKCHAIN · BEGINNER · LESSON 11 OF 13

A Transaction's Journey

IN ONE SENTENCE

A crypto transaction is built and signed in your wallet, passed from node to node, held in a waiting area, picked up by a miner or validator, and then buried under new blocks. The fee you pay decides how soon it leaves the queue.

Step 1: your wallet builds and signs it

When you press Send, nothing reaches the blockchain yet. First your wallet puts together a small message that says three things: which coins are being spent, where they go, and how much you are offering as a fee.

In Bitcoin, your balance is not one number. It is a set of separate pieces of coin you received earlier, called **unspent outputs**. To send 0.3 BTC from a piece worth 0.5 BTC, the wallet spends the whole piece: 0.3 goes to the receiver, a small amount goes to the fee, and the rest comes back to an address of yours as **change**. Ethereum works more like a bank balance, but the idea of signing is the same.

Finally the wallet signs the message with your private key, as we saw in Lesson 8. The signature proves the owner approved this exact payment. Change one digit afterwards and the signature no longer fits.

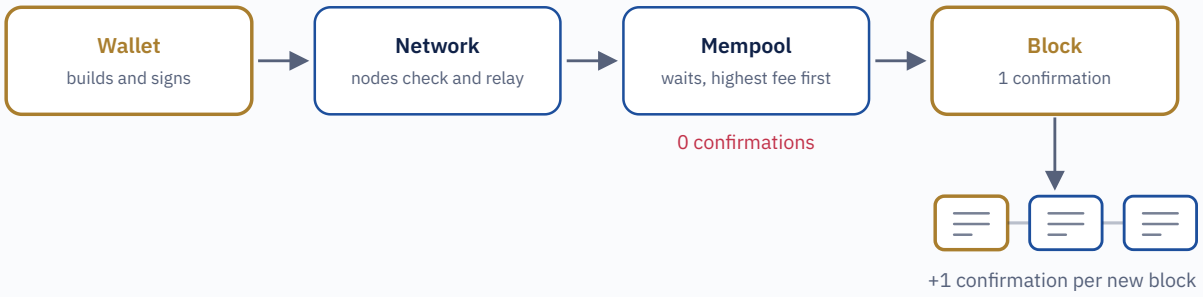


Figure 1. A transaction is signed in the wallet, checked and relayed by nodes, waits in the mempool, and gets its first confirmation once a miner includes it in a block. Each later block adds one more.

EXAMPLE: WHERE 0.5 BTC GOES

You hold one piece worth 0.5 BTC and want to send 0.3 BTC to a friend. Your wallet writes a transaction with two outputs: 0.3 BTC to your friend and 0.1999 BTC back to your own change address. The missing 0.0001 BTC is not written anywhere as an output. Whatever is left over is the fee, and the miner who includes the transaction collects it.

Step 2: broadcast and the waiting room

The signed transaction is handed to a node, which checks it: are the signatures valid, do the coins exist, have they already been spent? If everything passes, the node passes it on to its peers, and within seconds it has spread across the network, as Lesson 7 showed.

Each node keeps the valid transactions it has heard about in a holding area called the **mempool**, short for memory pool. There is no single mempool. Every node has its own, so their contents differ slightly. While your transaction sits there it has **zero confirmations**: the network knows about it, but it is not on the blockchain yet and could in rare cases still be replaced.

Step 3: fees decide who goes first

A Bitcoin block arrives about every ten minutes and has limited room. When more transactions are waiting than one block can hold, miners fill it with the ones that pay the most for the space they take. Bitcoin fees are therefore quoted as a rate, in **satoshis per virtual byte** (sat/vB), not as a percentage of the amount. Sending $10 or $10 million costs the same if the transactions are the same size.

Network condition	What usually happens
Quiet mempool	Even a low fee gets into the next block or two
Busy mempool	Low-fee transactions wait, sometimes for hours or days
Sudden rush	Fees can jump many times over within an hour

The rush can be extreme. On 20 April 2024, the block that cut Bitcoin's mining reward in half, block 840,000, collected more than 37 BTC in fees, worth about $2.4 million at the time, because many users competed to get into that historic block.

ANALOGY: THE LAST FERRY OF THE EVENING

A small ferry leaves every ten minutes with a fixed number of seats. On a quiet night everyone gets on. On a holiday weekend the queue is long, and the crew lets aboard whoever offers the highest ticket price per seat. If you offered the minimum, you are still in the queue when the next boat arrives, and the one after that.

Step 4: confirmations and settlement

When a miner includes your transaction in a block that the network accepts, it has **one confirmation**. Every block added on top adds one more. Each extra block makes reversing the payment harder, because an attacker would have to redo all of those blocks, as Lesson 6 explained.

Confirmations (Bitcoin)	Typical meaning
0	Seen by the network, not yet in a block
1	In a block, fine for small everyday amounts
Several	What exchanges usually wait for before crediting a deposit, depending on the platform
6	A long-standing rule of thumb for large amounts, about one hour

Other networks have their own rhythm. Ethereum adds a block every 12 seconds and treats a block as final after about 13 minutes, when it can no longer be reversed without destroying a huge amount of staked ETH.

When a transaction gets stuck

If you set the fee too low during a busy period, your transaction can wait in mempools for a long time. Nothing is lost: the coins have not left. Very old transactions are eventually dropped from most mempools, and the coins simply stay where they were. Two common fixes exist:

- **Replace-by-fee (RBF).** Your wallet sends a new version of the same payment with a higher fee, which replaces the old one.
- **Child pays for parent (CPFP).** The receiver, or you through your change, spends the stuck coins in a new transaction with a high fee, so a miner has a reason to include both together.

Whatever the fix, you can follow the whole journey yourself. Every transaction has an ID, the **txid**, which you can paste into a block explorer to see whether it is waiting, confirmed, and how deep it is buried.

Why this matters for traders

- **Deposits are not instant.** An exchange credits your bitcoin only after its required number of confirmations. If you plan to trade a fast move, the coins need to be on the exchange before the move, not on their way.
- **Fees rise when markets move.** Sharp price swings send many people to the blockchain at once, and fees jump with them. Check the current fee rate before sending, and avoid choosing the lowest setting when timing matters.
- **Keep the txid.** If a deposit or withdrawal seems late, the txid tells you exactly where it is. It is also the first thing exchange support will ask for.

Key terms

Mempool	The holding area where each node keeps valid transactions that are waiting to be included in a block.
Transaction fee	What the sender pays to have a transaction included. In Bitcoin it is whatever is left after the outputs are subtracted from the inputs.
sat/vB	Satoshis per virtual byte, the rate used to compare Bitcoin fees. One satoshi is one hundred-millionth of a bitcoin.
Confirmation	One block on the chain that contains or comes after your transaction. More confirmations mean a payment that is harder to reverse.
Change output	The part of a spent coin that the wallet sends back to the sender's own address.
Transaction ID (txid)	The unique code that identifies a transaction and lets you look it up in a block explorer.

Key takeaways

1. A transaction is built and signed in your wallet before anything is sent to the network.
2. Nodes check it, pass it on, and hold it in their mempools, where it has zero confirmations.
3. Block space is limited, so miners pick the transactions paying the highest fee rate, not the largest amount.

4. Each block added after yours is one more confirmation, and exchanges wait for a set number before crediting you.
5. A stuck transaction can be sped up with replace-by-fee or child pays for parent, and tracked with its txid.

Test yourself

Circle one answer for each question. The answer key with explanations is on the next page. You can also take this quiz online at markettalks.info and see your score instantly.

1. Where is a transaction signed?

- A By the first node that receives it
- B In the sender's wallet, before it is sent
- C By the miner who includes it in a block
- D By the receiver's wallet when it arrives

2. You spend a 0.5 BTC coin to send 0.3 BTC. What happens to the rest?

- A It is lost forever
- B It stays locked until the next halving
- C Most comes back to you as change, and the small remainder is the fee
- D The receiver keeps it as a tip

3. What is the mempool?

- A Each node's holding area for valid transactions waiting for a block
- B A single global server run by Bitcoin's developers
- C A wallet that stores coins for exchanges
- D The part of a block where fees are recorded

4. Two Bitcoin transactions are the same size. One sends $10, the other $10 million. Which needs a higher fee to be included quickly?

A. The $10 million one, because fees are a percentage
B. Neither, they need the same fee rate
C. The $10 one, because small payments are delayed
D. Fees are fixed by the exchange, not the network

5. Your transaction is in a block, and two more blocks have been added after it. How many confirmations does it have?

A. One
B. Two
C. Three
D. Six

6. Your low-fee transaction has been waiting for hours during a busy period. What is a standard fix?

A. Send the same coins again to a new address
B. Contact the miners and ask them to include it
C. Restore your wallet from the seed phrase
D. Use replace-by-fee to send a new version with a higher fee

Answer key

1 B

In the sender's wallet, before it is sent

The wallet signs with the private key before broadcasting. Nodes and miners only check the signature, they cannot create it.

2 C

Most comes back to you as change, and the small remainder is the fee

Bitcoin spends whole coins. The wallet sends the difference back to your own change address and leaves a little unassigned as the fee.

3 A

Each node's holding area for valid transactions waiting for a block

Every node keeps its own mempool, so there is no single one. It holds transactions that are valid but not yet in a block.

4 B

Neither, they need the same fee rate

Miners compare fees per virtual byte of space. The amount being sent does not matter, only the size of the transaction.

5 C

Three

The block that contains it counts as the first confirmation, and each block after it adds one more, so one plus two makes three.

6 D

Use replace-by-fee to send a new version with a higher fee

Replace-by-fee swaps the waiting transaction for a version with a higher fee. Child pays for parent is the other common option.

SOURCES

- Bitcoin Developer Guide, Transactions: https://developer.bitcoin.org/devguide/transactions.html
- Cointelegraph, Bitcoin users spend a record $2.4M in fees on the halving block: https://cointelegraph.com/news/bitcoin-halving-users-spend-record-millions-block-space-runes-rare-satoshis
- ethereum.org, Proof-of-stake and finality: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
- Bitcoin Optech, Replace-by-fee: https://bitcoinops.org/en/topics/replace-by-fee/

Market Talks

CONTINUE LEARNING

Up next: Lesson 12 Public, Private and Consortium Blockchains

This lesson is part of the free Blockchain track at the MARKET TALKS Education Center: Beginner, Intermediate and Advanced lessons, each with a quiz and a downloadable PDF.

Education Center
Lessons from first principles to advanced topics

Markets Analysis
Technical and fundamental analysis on major markets

Reports
Bitcoin, Gold, Silver, SPX and more

markettalks.info

Telegram @MARKET_TALKS

For education only. Nothing in this document is financial advice. © 2026 MARKET TALKS. You are welcome to share this PDF unchanged.