Market Talks
EDUCATION CENTER

BLOCKCHAIN · BEGINNER · LESSON 8 OF 13

Keys, Addresses and Wallets

What really proves you own a bitcoin, what you share to get paid, and what a wallet actually holds

6 min read 6 quiz questions with answer key

BLOCKCHAIN · BEGINNER · LESSON 8 OF 13

Keys, Addresses and Wallets

IN ONE SENTENCE

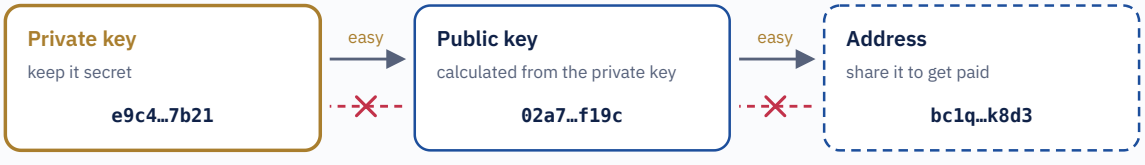
Owning bitcoin means holding a private key, a secret number that lets you sign payments. From it come a public key and an address you can share. A wallet does not hold coins at all: it holds keys and uses them to sign.

One secret, two things you can share

In Lesson 5 we saw that the blockchain holds no names, only addresses. So how does the network know a coin is yours? The answer is a set of three linked pieces:

- **Private key.** A secret number, chosen at random from a range so large that it has 78 digits, the same scale as the hashes in Lesson 6. Whoever knows it can spend the coins linked to it.
- **Public key.** A number calculated from the private key with a special kind of math. It can be shown to anyone.
- **Address.** A shorter code made by hashing the public key, plus a built-in check that catches typing mistakes. This is what you give people so they can pay you.

Each step goes one way only. Turning a private key into a public key, and a public key into an address, takes a computer a fraction of a second. Going backwards is practically impossible. That is why you can publish your address anywhere without putting your coins at risk.



Each arrow takes a fraction of a second. Going back the other way is practically impossible.

Figure 1. The private key creates the public key, which creates the address. Each step works only in one direction, so sharing your address never reveals your private key.

Spending means signing

To spend bitcoin, your wallet builds a transaction and adds a **digital signature** made with your private key. Every node can check that signature using your public key and confirm that it was made

by the matching private key, without ever seeing the private key itself.

The signature is also tied to the exact details of that one transaction. If anyone changes the amount or the destination by even one character, the signature stops matching and every node rejects it. That is why nobody can intercept your payment on its way through the network and redirect it.

This is the big shift from banking. A bank decides whether you may spend by checking who you are. Bitcoin only checks whether the signature is valid. No name, no password reset, no customer service, just math.

ANALOGY: THE MAILBOX WITH A SLOT

Think of an address as a mailbox with a slot in the front. Anyone who knows where it is can drop a letter in, and the whole street can see how many letters arrive. But only the person with the key can open the box and take letters out. Lose the key and the letters stay locked inside forever. Copy the key and someone else can empty the box.

What Bitcoin addresses look like

Bitcoin has changed its address format a few times. All of them still work, and you can tell them apart by their first characters:

Starts with	Type	Introduced
1	Legacy, the original format	2009
3	Script address, often used for shared or multi-signature wallets	2012
bc1q	Native SegWit, smaller transactions and lower fees	2017
bc1p	Taproot, the newest format, with more privacy and flexibility	2021

Other blockchains use their own styles. Ethereum addresses, for example, start with *0x* followed by 40 characters. You cannot swap a Bitcoin address for an Ethereum one, even when the same app shows both.

A good wallet creates a new address each time you ask to receive. All of them belong to the same wallet, and old ones keep working. Using fresh addresses makes it harder for strangers to link all your payments together.

What a wallet really holds

Despite the name, a wallet never holds coins. The coins exist only as entries on the blockchain. A **wallet** is a tool that stores your keys, reads the blockchain to show your balance, creates transactions and signs them.

Wallets come in two broad groups:

- **Hot wallets** keep keys on a device connected to the internet, such as a phone app or a desktop program. They are convenient for everyday use, but the keys are exposed to anything that can attack that device.
- **Cold wallets** keep keys offline. A **hardware wallet** is a small device that stores the keys inside and signs transactions without ever revealing them to your computer. It is slower to use but far harder to hack.

If your coins sit on an exchange, the exchange holds the keys, not you. Lesson 10 compares the two choices, and Lesson 9 covers the backup that protects all your keys at once.

A REAL EXAMPLE: THE HARD DRIVE IN THE LANDFILL

In 2013, James Howells, a computer engineer in Wales, accidentally threw away an old hard drive holding the private key to 8,000 bitcoins he had mined years earlier. The drive ended up in a city landfill. He spent more than a decade asking to dig it up. In January 2025, a UK court dismissed his case, and his appeal was rejected that March. The coins are still on the blockchain, visible to everyone and spendable by no one.

Why this matters for traders

- **Check the whole address, every time.** In an address poisoning scam, attackers send a tiny transaction from an address that looks almost like one you use, hoping you copy it from your history next time. In May 2024, one trader sent 1,155 wrapped bitcoin, worth about $68 million, to such an address. The attacker later returned most of it after negotiations, a very rare outcome.
- **Match the network, not just the address.** Exchanges often support the same coin on several networks. Sending on a network the receiving side does not support can make funds very hard or impossible to recover. Check the network and any required memo or tag before you confirm.
- **Send a small test first.** For large or first-time transfers, a small test payment costs a little in fees and can save the whole amount. Many traders also use withdrawal address whitelists on their exchange accounts.

Key terms

Private key	A secret random number that lets its holder sign transactions and spend the coins linked to it.
Public key	A number calculated from the private key that can be shared and used to check signatures.
Address	A shorter code made from the public key, which you share so others can send you coins.
Digital signature	Proof made with a private key that approves one exact transaction, which anyone can check with the public key.
Wallet	A tool that stores your keys, shows your balance from the blockchain, and creates and signs transactions.
Hardware wallet	A small device that keeps private keys offline and signs transactions without exposing the keys to a computer.

Key takeaways

1. Owning bitcoin means controlling a private key. Whoever has the key can spend the coins.

2. A public key and an address are calculated from the private key, and neither can be turned back into it.
3. Spending requires a digital signature tied to the exact transaction, which every node can check without seeing the private key.
4. Bitcoin addresses start with 1, 3, bc1q or bc1p depending on their type, and a wallet can create a fresh address for every payment.
5. Wallets hold keys, not coins. Hot wallets are convenient, while cold wallets keep keys offline and much safer.

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. What gives someone the power to spend bitcoin?

- A Knowing the address
- B Holding the private key
- C Having an account at an exchange
- D Knowing the transaction ID

2. Why is it safe to share your address publicly?

- A Because addresses expire after one use
- B Because the network hides the address from others
- C Because nobody can work backwards from the address to the private key
- D Because addresses are encrypted

3. What happens if someone changes the amount in a signed transaction?

- A The signature no longer matches, so nodes reject it
- B The transaction goes through with the new amount
- C The signature updates automatically
- D The miner decides which amount to use

4. What does a crypto wallet actually store?

A Your coins
B A copy of the whole blockchain
C Your bank details
D Your keys

5. A Bitcoin address starts with bc1q. What type is it?

A Legacy
B Native SegWit
C Ethereum
D Taproot

6. What is the main advantage of a hardware wallet?

A It makes transactions faster
B It removes all fees
C It keeps private keys offline and signs without exposing them
D It lets you recover coins sent to the wrong address

Answer key

1 B

Holding the private key

The private key is what signs payments. Anyone who has it can spend the coins, which is why it must stay secret.

2 C

Because nobody can work backwards from the address to the private key

Each step from private key to public key to address is one-way. Others can send to your address, but they cannot use it to find your private key.

3 A

The signature no longer matches, so nodes reject it

A signature is tied to the exact details of one transaction. Any change, even one character, makes it invalid.

4 D

Your keys

Coins exist only on the blockchain. The wallet stores your keys, reads your balance from the chain and signs your transactions.

5 B

Native SegWit

Addresses starting with bc1q are native SegWit, introduced in 2017. Taproot addresses start with bc1p, and legacy ones with 1.

6 C

It keeps private keys offline and signs without exposing them

A hardware wallet stores keys inside the device and only sends out signed transactions, so malware on your computer cannot read the keys.

SOURCES

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- Wikipedia, Bitcoin buried in Newport landfill: https://en.wikipedia.org/wiki/Bitcoin_buried_in_Newport_landfill
- Cointelegraph, Trader loses $68 million in address poisoning scam (May 2024): https://cointelegraph.com/news/trader-loses-68-million-address-poisoning-scam
- Cointelegraph, Address poisoner returns funds after negotiations: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations

Market Talks

CONTINUE LEARNING

Up next: Lesson 9 Seed Phrases and Backups

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.