Market Talks
EDUCATION CENTER

BLOCKCHAIN · BEGINNER · LESSON 10 OF 13

Custody: Exchange Account or Your Own Wallet

Who really holds your coins, what history says about both choices, and how most traders split the difference

5 min read 6 quiz questions with answer key

BLOCKCHAIN · BEGINNER · LESSON 10 OF 13

Custody: Exchange Account or Your Own Wallet

IN ONE SENTENCE

Keeping crypto on an exchange means the exchange holds the keys and you hold a promise. Keeping it in your own wallet means you hold the keys and all the responsibility. Each choice protects you from different risks.

Two ways to hold the same bitcoin

Custody simply means who holds the private keys. There are two basic models:

- **Custodial.** An exchange or another company holds the keys. You sign in with a password, and your balance is a number in the company's own database, as we saw in Lesson 5. When you withdraw, the company signs the transaction for you.
- **Self-custody.** You hold the keys, usually in a wallet backed up with a seed phrase from Lesson 9. Nobody can move your coins or stop you from moving them, but nobody can rescue you if you lose the keys either.

On the blockchain, there is no such thing as "your account" at an exchange. The exchange's addresses hold everyone's coins together, and its database records how much of that pile belongs to each customer.

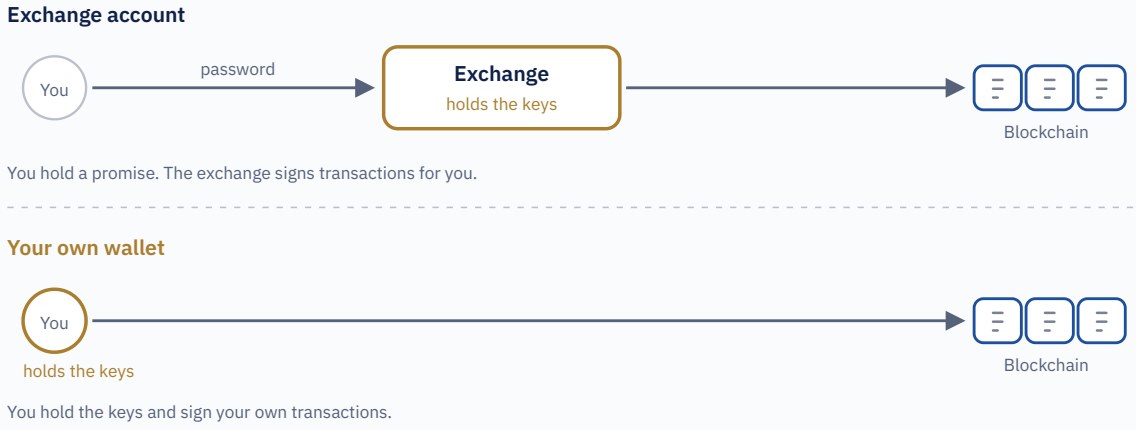


Figure 1. With an exchange account, the company holds the keys and you reach the blockchain through it. With your own wallet, you hold the keys and deal with the blockchain directly.

ANALOGY: THE COAT CHECK

At a busy event, you hand your coat to the coat check and get a numbered ticket. It is convenient, and usually your coat comes back. But for the evening, you hold a ticket, not a coat. If the cloakroom is robbed, closes early, or has quietly lent coats to someone else, your ticket is only as good as the people behind the counter. Keeping your coat on is less comfortable, but nobody else can lose it.

What history says about exchanges

Most exchanges never fail. But when large ones have, customers have waited years and often lost a large share of their money:

Exchange	What happened	What customers faced
Mt. Gox (2014)	The largest bitcoin exchange of its time lost about 850,000 BTC to theft and mismanagement	Repayments of what was left only began in July 2024, ten years later
QuadrigaCX (2019)	The founder died, and the cold wallets he alone controlled turned out to be mostly empty	About 76,000 users were owed around C$215 million
FTX (2022)	Customer money had been used by a sister trading firm, and withdrawals stopped within days	Billions in customer funds were missing, and the founder was later convicted of fraud

In each case, the screens showed normal balances right up until the end. A balance on an exchange is a claim on the company, not proof that the coins are there.

The risks of holding it yourself

Self-custody removes the company from the picture, but it hands every job to you. The most common ways people lose coins on their own are:

- **Losing the backup.** A lost seed phrase and a broken device mean the coins are locked forever. Researchers at Chainalysis estimated in 2017 that between about 2.8 and 3.8 million bitcoins were already lost this way, roughly a fifth of all coins mined at the time.
- **Leaking the backup.** A seed phrase typed into a fake site or app hands everything to a thief, as Lesson 9 showed.
- **Sending mistakes.** A wrong address or network cannot be reversed, as Lesson 8 showed.

There is no help desk and no password reset. That is the price of having no company that can fail or freeze you.

How most people split it

For many people the answer is not one or the other. A common approach is to treat the exchange like a wallet in your pocket and self-custody like a safe at home:

	Exchange account	Your own wallet
Who holds the keys	The exchange	You
If you forget your password	Customer support can usually restore access	Only your seed phrase can
If the company fails	Your coins may be frozen or lost	Nothing changes
Best suited to	Active trading and amounts you are about to use	Long-term holdings and savings
Main risk	The company: hacks, fraud, freezes, collapse	You: lost backups, scams, mistakes

If you do keep funds on an exchange, prefer large, regulated platforms with a long track record, turn on every security feature they offer, and check whether they publish regular proof of reserves. Remember that proof of reserves shows assets the exchange holds at a moment in time, but not always everything it owes.

Why this matters for traders

- **Futures and margin need custody.** To trade perpetual contracts, your collateral has to sit on the exchange. Keep there what your positions need, not your whole net worth, and move profits you do not need for trading into your own wallet regularly.
- **Watch for warning signs.** Slow or paused withdrawals, sudden changes to withdrawal limits, and large flows of coins leaving an exchange on-chain have often come before trouble. In early November 2022, FTX withdrawals slowed and stopped within days. Acting on the first signs is easier than acting on the last.
- **Self-custody has a cost in speed.** Moving coins from your wallet to an exchange takes time and network fees, and in a fast market minutes matter. Plan how much you keep on each side before volatility arrives, not during it.

Key terms

Custody	Control of the private keys, and therefore of the coins they unlock.
Custodial	A setup where a company holds the keys for you, such as an exchange account.
Self-custody	Holding your own keys in a wallet you control, usually backed up with a seed phrase.
Counterparty risk	The risk that a company holding your assets fails, freezes them, or does not give them back.
Proof of reserves	A published check showing the assets an exchange holds at a point in time, which may not show everything it owes.
Not your keys, not your coins	A common saying: if someone else holds the keys, you hold only their promise to give the coins back.

Key takeaways

1. Custody means who holds the keys. On an exchange the company holds them, and in self-custody you do.
2. An exchange balance is a number in the company's database and a claim on that company, not coins in your control.
3. Mt. Gox, QuadrigaCX and FTX show that exchange failures can freeze customer funds for years or lose them entirely.
4. Self-custody removes company risk but adds personal risk: lost backups, leaked seed phrases and sending mistakes.
5. Many people keep trading funds on a reputable exchange and long-term holdings in their own wallet.

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 does custody mean in crypto?

A. Who holds the private keys
B. Which exchange has the lowest fees
C. How long you plan to hold a coin
D. Which country regulates a coin

2. You have 1 BTC in your exchange account. What do you actually hold?

A. A private key stored in your name
B. A claim on the exchange, recorded in its database
C. Coins in a personal address that only you control
D. A hardware wallet kept by the exchange

3. What was a key reason QuadrigaCX customers could not get their money back?

A. Bitcoin's network stopped working
B. The customers lost their seed phrases
C. The founder alone controlled the wallets, and they were mostly empty when he died
D. A government seized all exchanges in Canada

4. Which risk does self-custody remove?

A. The risk of losing your seed phrase
B. The risk of sending to a wrong address
C. The risk of phishing
D. The risk of an exchange freezing or losing your coins

5. What is a common way to split funds between the two models?

A. Everything on the exchange for convenience
B. Trading funds on a reputable exchange, long-term holdings in your own wallet
C. Everything in self-custody, including futures collateral
D. Spread evenly across as many exchanges as possible

6. What can proof of reserves fail to show?

A Which coins the exchange holds

B The exchange's wallet addresses

C Everything the exchange owes to customers and lenders

D The date the check was made

Answer key

1 A

Who holds the private keys

Whoever holds the private keys controls the coins. Custody is simply the question of who that is.

2 B

A claim on the exchange, recorded in its database

The exchange holds the keys to shared addresses. Your balance is its record of how much it owes you.

3 C

The founder alone controlled the wallets, and they were mostly empty when he died

With one person controlling the keys and the funds misused, there was no way to recover most of the money after his death.

4 D

The risk of an exchange freezing or losing your coins

With your own keys, no company can freeze, lend out or lose your coins. The risks that remain are your own mistakes and scams.

5 B

Trading funds on a reputable exchange, long-term holdings in your own wallet

Trading needs funds on the exchange, while savings are safer from company risk in your own wallet. Each side does what it is good at.

6 C

Everything the exchange owes to customers and lenders

Proof of reserves shows assets at a moment in time. Without a full picture of liabilities, it cannot prove the exchange can pay everyone back.

SOURCES

- The Block, Mt. Gox to distribute bitcoin repayments from July 2024: https://www.theblock.co/post/301448/mt-gox-to-distribute-9-billion-of-bitcoin-bitcoin-cash-repayments-from-beginning-of-july
- Crowdfund Insider, QuadrigaCX trustee report: 76,000 users owed $215 million: https://www.crowdfundinsider.com/2019/05/147401-quadrigacx-trustees-final-report-finds-not-much-left-for-76-000-exchange-users-who-lost-215-million/
- Wikipedia, Bankruptcy of FTX: https://en.wikipedia.org/wiki/Bankruptcy_of_FTX
- Cointelegraph, up to four million bitcoins may be gone forever (Chainalysis estimate): https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

CONTINUE LEARNING

Up next: Lesson 11 A Transaction's Journey

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.