Market Talks
EDUCATION CENTER

CRYPTO · BEGINNER · LESSON 10 OF 15

Sending and Receiving Safely: Networks, Addresses and Memo Tags

What every field on a withdrawal screen means, why the network must match on both sides, when you need a memo or tag, and how to protect yourself from look-alike addresses

10 min read 8 quiz questions with answer key

CRYPTO · BEGINNER · LESSON 10 OF 15

Sending and Receiving Safely: Networks, Addresses and Memo Tags

IN ONE SENTENCE

A crypto transfer cannot be reversed, so every withdrawal depends on getting four things right: the coin, the network, the address and, when required, the memo or tag.

There is no undo button

A bank transfer sent to the wrong account can sometimes be recalled. A blockchain transaction cannot. Once it is confirmed, nobody, not the network, not your wallet and usually not the exchange, can reverse it. That is the same property that makes crypto resistant to censorship, and it means every detail has to be right before you press send.

The good news is that almost all costly mistakes come from a handful of fields on one screen. This lesson goes through them one by one.

Anatomy of a withdrawal

Whether you withdraw from an exchange or send from your own wallet, you fill in the same kinds of fields:

- **Coin:** what you are sending, such as USDT.
- **Network:** which blockchain the transfer will use, such as Tron (TRC-20) or Ethereum (ERC-20).
- **Address:** where it goes. It must be an address on that same network.
- **Memo or tag:** an extra number or text, needed only for some coins and some receivers.
- **Amount:** how much to send.
- **Fee:** the network or withdrawal fee, which is taken from the amount or added to it.

Before confirming, most exchanges show a summary of what will arrive. Reading that summary slowly is the single most useful habit in this lesson.

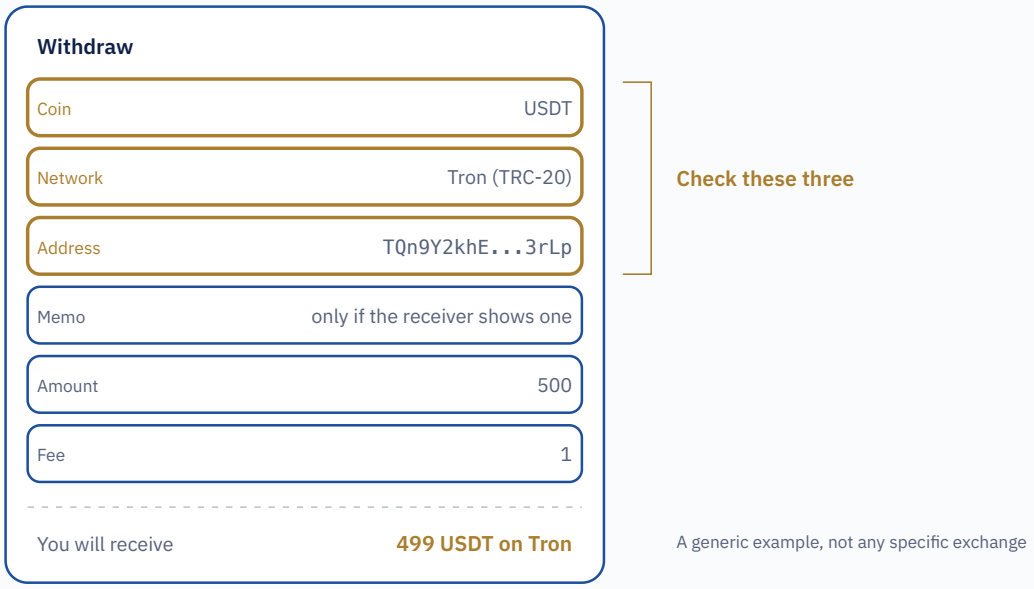


Figure 1. A generic withdrawal screen. The coin, the network and the address are the three fields where mistakes cost the most.

The network must match on both sides

Lesson 5 showed that USDT exists as separate tokens on Tron, Ethereum, BNB Chain, Solana and others. When you send, the network you choose must be a network the receiver supports for that coin, and the address must belong to that network.

Always start from the receiver's side. On the receiving exchange or wallet, choose the coin, then the network, and copy the deposit address it gives you. Then, on the sending side, choose exactly the same network.

What happens if they do not match?

- If the address format is different, for example a Tron address on the Ethereum network, the app will usually refuse the transfer. That is the lucky case.
- If both networks use the same **0x** address format, such as Ethereum and BNB Chain, the transfer goes through, but to a network the receiver may not watch. Funds sent to your own wallet can often be found by adding that network to the wallet. Funds sent to an exchange may need a recovery request, which can take weeks, cost a fee, or be refused.

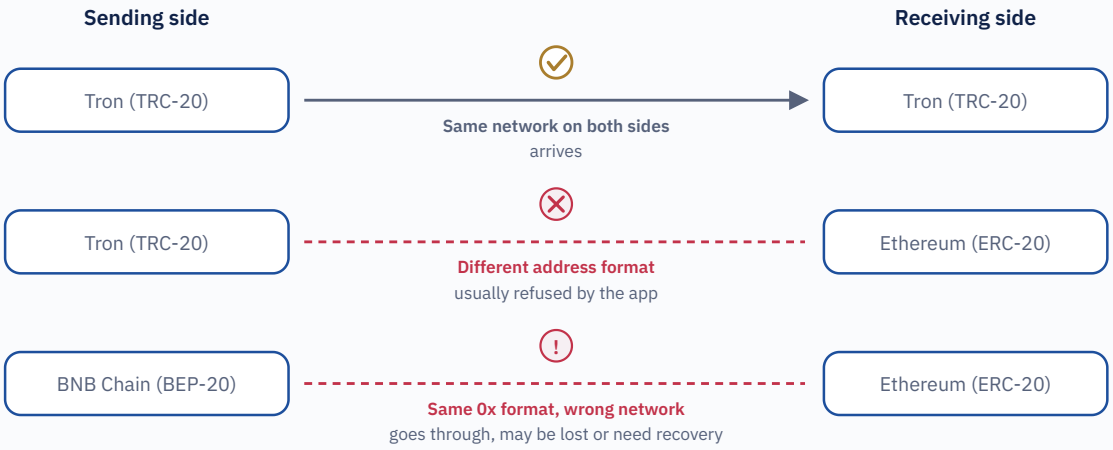


Figure 2. The network must match on both sides. A different address format is usually refused, but networks that share the 0x format accept the transfer, which can strand the funds.

Memos and tags

For some coins, exchanges use one shared deposit address for many customers. To know which customer a deposit belongs to, they add a short number or text called a **memo**, **tag** or **destination tag**. Common examples are XRP, which uses a destination tag, and Stellar (XLM), TON and Cosmos (ATOM), which use a memo or comment.

If the receiving exchange shows a memo or tag with the address, you **must** copy it into the memo field when sending. Without it, the coins arrive at the exchange's shared address but nobody can tell they are yours. Recovering them usually means contacting support with proof, and it is not guaranteed.

When you send to your own personal wallet, a memo is usually not needed, because the address belongs only to you.

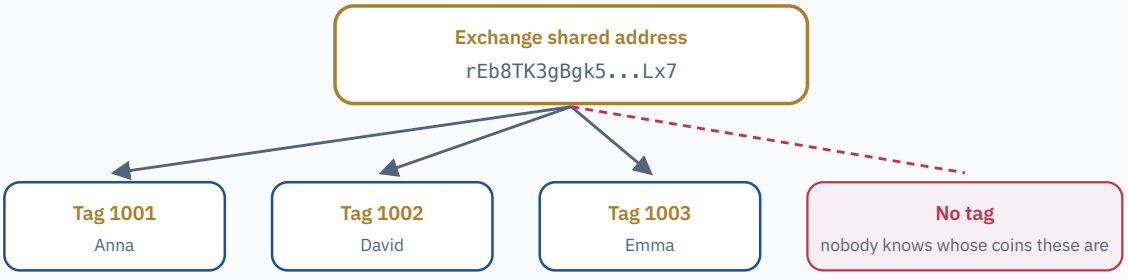


Figure 3. Exchanges often give many customers the same address for coins such as XRP, and use a tag to tell them apart. A deposit without its tag cannot be matched to anyone.

Protecting the address

Crypto addresses are long and impossible to remember, which attackers exploit in two main ways:

- **Address poisoning:** the attacker creates an address whose first and last characters match one you use, then sends you a tiny or fake transaction so it appears in your history. Later, you copy the wrong one from your history by mistake. In May 2024 a trader lost 1,155 WBTC, worth about $68 million, this way after copying an address that matched the start and end of the real one. The attacker later returned the funds after negotiations, which is extremely rare.
- **Clipboard malware:** malicious software on a computer or phone that swaps a copied address for the attacker's address at the moment you paste.

Simple habits protect against both: copy addresses from the receiver's deposit page, not from your transaction history; never type addresses by hand; after pasting, check characters at the start, the middle and the end; and use an exchange's **address whitelist** or your wallet's address book for addresses you send to often.

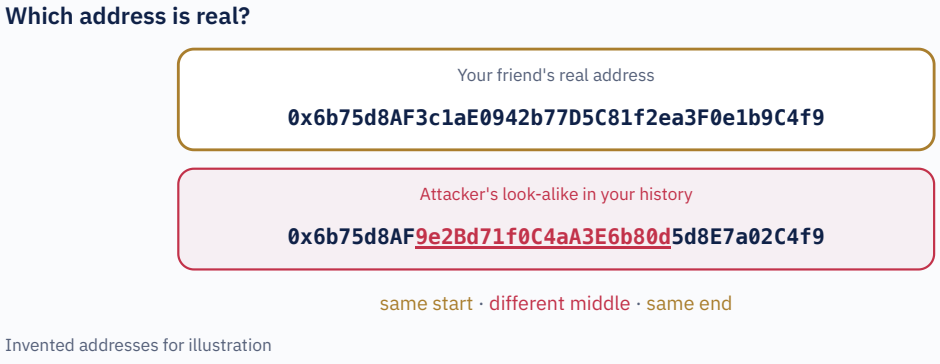


Figure 4. Address poisoning: the attacker's address matches the start and end of the real one, so only the middle reveals it. The addresses are invented.

Test first, then track

For a first transfer to a new address, many experienced users send a small **test transaction** first, wait until it arrives, and only then send the rest. The extra fee is usually small compared with the cost of a mistake.

After sending, you get a **transaction hash** or TxID: a unique code that identifies your transfer. Pasting it into a block explorer for that network, such as Etherscan for Ethereum or Tronscan for Tron, shows whether the transfer is confirmed and where it went. Exchanges credit deposits only after a set number of **confirmations**, so a transfer can show as complete on the blockchain a few minutes before it appears in your account.

If something does go wrong, act quickly: keep the transaction hash, contact the receiving platform's official support through its website or app, and ignore anyone who messages you offering to recover funds. Those offers are almost always a second scam.

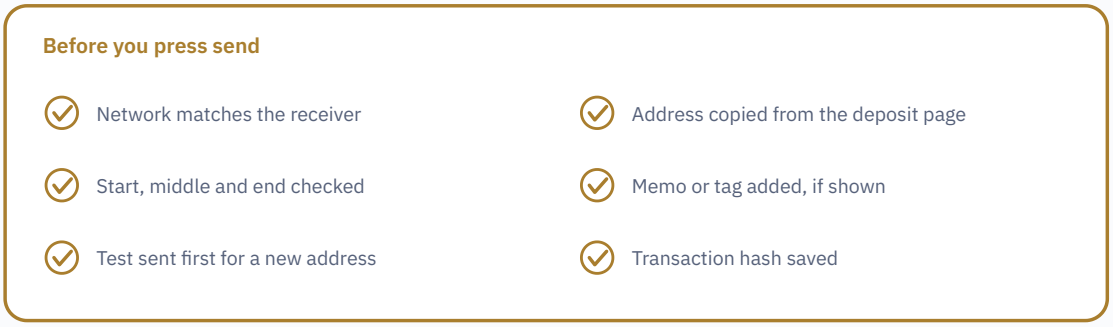


Figure 5. A short checklist for every transfer.

Why this matters for traders

- **Moving funds is part of trading.** Traders move money between exchanges and wallets often, sometimes in a hurry. Most costly transfer mistakes happen under time pressure.
- **Network choice changes speed and cost.** USDT on Tron or Solana usually arrives in minutes for a low fee. The same transfer on Ethereum can cost more, and bitcoin can need an hour or more of confirmations.
- **Exchanges sometimes pause a network.** During upgrades or congestion, deposits or withdrawals on one network can be suspended. Checking the network status before sending avoids funds stuck in transit.
- **Whitelists add a safety layer.** Many exchanges let you restrict withdrawals to saved addresses, which helps if an account is ever compromised.

Key terms

Withdrawal network	The blockchain chosen to carry a transfer. It must be supported by the receiver for that coin.
Deposit address	The address a receiver gives you for a specific coin on a specific network.
Memo, tag, destination tag	An extra code that tells an exchange which customer a deposit to a shared address belongs to.

Address poisoning	A scam that plants a look-alike address in your transaction history, hoping you copy it by mistake.
Clipboard malware	Malicious software that replaces a copied crypto address with the attacker's address.
Test transaction	A small transfer sent first to confirm that the address and network are correct.
Transaction hash (TxID)	A unique code that identifies a transaction and can be looked up in a block explorer.
Address whitelist	An exchange setting that allows withdrawals only to addresses you have saved in advance.

Key takeaways

1. Confirmed crypto transfers cannot be reversed, so the details must be right before sending.
2. A withdrawal needs the right coin, network, address and, when required, memo or tag.
3. Start from the receiver: pick the coin and network there, copy the deposit address, then choose the same network when sending.
4. If the receiver shows a memo or tag, it must be included, or the funds may not be credited.
5. Address poisoning and clipboard malware target careless copying. Copy from the deposit page, never from history, and check start, middle and end.
6. A small test transaction, a transaction hash and a block explorer let you confirm a transfer step by step.

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. Why do details matter so much when sending crypto?

A Fees are very high

B Confirmed transactions cannot be reversed

C Exchanges check every transfer by hand

D Addresses expire after one use

2. What is the safest order of steps when moving USDT to another exchange?

A Pick any network on the sending side, then find an address

B On the receiving side, choose the coin and network and copy the deposit address, then choose the same network when sending

C Type the address from memory

D Use the address from your last transaction

3. You send BEP-20 USDT to your Ethereum wallet address. Why might the transfer still go through?

A USDT works on every network automatically

B BNB Chain and Ethereum use the same 0x address format

C The exchange converts it for you

D It will not go through in any case

4. When is a memo or destination tag required?

A For every bitcoin transfer

B When the receiving exchange shows one with its deposit address, for coins such as XRP, XLM or TON

C Only for transfers above $10,000

D Never, it is optional

5. What happens if you leave out a required memo?

- A The transfer is automatically refunded
- B The coins arrive at the exchange but cannot be matched to your account without contacting support
- C The coins are destroyed
- D Nothing, memos are only for information

6. How does address poisoning work?

- A It infects the blockchain with a virus
- B It plants a look-alike address with the same start and end in your history so you copy it by mistake
- C It changes your private key
- D It raises network fees

7. Where is the safest place to copy a receiving address from?

- A Your transaction history
- B A message from a stranger
- C The receiver's own deposit page or your saved address book
- D A screenshot from social media

8. What can you do with a transaction hash?

- A Reverse the transaction
- B Look it up in a block explorer to see whether the transfer is confirmed and where it went
- C Change the receiving address
- D Get the fee refunded

Answer key

1 B

Confirmed transactions cannot be reversed

Once confirmed, a blockchain transfer is final. Nobody can recall it for you.

2 B

On the receiving side, choose the coin and network and copy the deposit address, then choose the same network when sending

Starting from the receiver guarantees the network is one it supports, and the address belongs to that network.

3 B

BNB Chain and Ethereum use the same 0x address format

The same 0x address exists on both networks. In your own wallet you can often see it by adding BNB Chain; at an exchange, recovery may be slow or refused.

4 B

When the receiving exchange shows one with its deposit address, for coins such as XRP, XLM or TON

Exchanges use one shared address for many customers on these coins. The memo tells them the deposit is yours.

5 B

The coins arrive at the exchange but cannot be matched to your account without contacting support

The funds reach the shared address but nobody knows they are yours. Recovery through support is possible in some cases, not guaranteed.

6 B

It plants a look-alike address with the same start and end in your history so you copy it by mistake

Attackers copy the first and last characters of an address you use. In May 2024 a trader lost about $68 million this way.

7 C

The receiver's own deposit page or your saved address book

Copying from history is exactly what address poisoning exploits. Use the official deposit page or a saved, verified address.

8 B

Look it up in a block explorer to see whether the transfer is confirmed and where it went

The hash identifies your transfer. A block explorer for that network shows its status and confirmations.

SOURCES

- CoinDesk, Exploiter steals $68M worth of crypto through address poisoning: https://www.coindesk.com/business/2024/05/03/exploiter-steals-68m-worth-of-crypto-through-address-poisoning

- Cointelegraph, WBTC address poisoner returns funds after negotiations: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations
- Stablecoin Insider, USDT Q2 2026 report (USDT by network): https://stablecoininsider.org/usdt-q2-2026-report-supply-regulation-and-the-two-tier-market/

Market Talks

CONTINUE LEARNING

Up next: Lesson 11 Spot vs Derivatives: A First Look at Futures, Perpetuals and Leverage

This lesson is part of the Crypto course at the MARKET TALKS Education Center. Beginner lessons are free, each with a quiz and a downloadable PDF. Intermediate and Advanced lessons are for members.

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.