

Plain-English glossary

Every term used on this site, defined without assuming you already know the next one. If something here is still unclear, that is our failing rather than yours - write to us and we will rewrite it.

Address

The destination a transfer goes to — a long string of letters and numbers. Like an account number, except there is no name attached and no bank to ask.

Atomic swap

A trade where both halves complete or neither does, enforced by code rather than trust. If someone describes a deal as atomic but you must send first, it is not atomic.

Blockchain

A public record of transactions that anyone can read and no single party controls. Its strength and its danger are the same thing: no one can alter it, including to help you.

Block explorer

A free website for looking up any transaction or address on a public blockchain. Use one you navigated to yourself, never a link you were sent.

Cold wallet / cold storage

Keys kept on a device that never exposes them to the internet. How serious holdings are stored.

Confirmation

A block added on top of the one containing your transaction, making reversal progressively infeasible. Not a review period — nobody is checking your intent.

Custody

Who is holding the asset. Ranges from a regulated trust company to a person with a spreadsheet. The word alone tells you nothing; the named custodian and their licence do.

DVP (delivery versus payment)

A settlement structure where both legs move together, so neither party is ever exposed. The professional answer to 'who sends first'.

Dusting

Sending a tiny amount to an address to plant something in its history — usually so a lookalike address appears there and gets copied later.

Escrow

A neutral third party holding both sides until both have arrived. Only meaningful if the escrow agent is genuinely independent and identifiable.

Gas / network fee

The fee paid to the network for processing a transaction. Paid automatically by the sender from their own wallet. Nobody can invoice you for it.

Hash (transaction ID)

The unique identifier of a transaction. Your receipt, and the thing an investigator needs first.

Honeypot

A token you can buy but cannot sell, because the contract forbids selling. The chart looks excellent until you try to exit.

Hot wallet

A wallet whose keys are on an internet-connected device. Convenient; exposed to whatever compromises that device.

KYC (know your customer)

Identity verification a regulated firm must perform. Its absence is not privacy — it means no regulator is supervising, and no record exists to subpoena later.

Liquidity pool

A shared pot of two assets that lets people trade between them automatically. Real mechanism; the phrase is heavily borrowed by frauds.

Mainnet / testnet

The real network, versus a free practice copy. A testnet transaction looks genuine and moves nothing of value.

Mixer / tumbler

A service that pools funds to break the trail. Once proceeds enter one, tracing usually ends.

OTC desk

A venue arranging large trades directly between two parties rather than on a public order book. Real ones onboard you, document the trade, and settle simultaneously or through escrow.

Private key

The secret that authorises moving funds. Whoever holds it owns the funds, with no appeal.

Seed phrase / recovery phrase

Twelve or twenty-four words that generate your private key. It is not a password to an account — it is the account. Never share it with anyone, for any reason.

Settlement

The moment a transfer becomes final. On a blockchain this is seconds to minutes, and final means final.

Smart contract

A program on the blockchain that runs automatically. It does exactly what it was written to do, including things its author intended and you did not read.

Stablecoin

A token intended to hold a fixed value, issued by a company — USDT by Tether, USDC by Circle. Because there is an issuer, there is someone who can freeze a specific address.

Token approval

Permission you grant a contract to move your tokens. Malicious approvals are how wallets are drained without the seed phrase ever being shared.

Wallet

Software or hardware holding your keys. It does not hold coins; the coins are entries on the ledger.

Disclaimer

This document is general information about how cryptocurrency systems and common frauds work. It is not legal advice, not financial advice, and not a substitute for either. Nothing in it guarantees or predicts the recovery of any funds.

BlockchainFraud.org charges a flat fee stated in advance and never a percentage of any recovery. We will never contact you unsolicited offering to recover funds, and anyone who does should be treated as a second fraud.