C

Cryptocurrency: How It Works, Wallet Security, and Scam Prevention

Learn how cryptocurrency, blockchains, keys, and wallets work; compare custody options; protect a seed phrase; and recognize or respond to crypto scams.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 How cryptocurrency works
02 Coins, tokens, and stablecoins
03 Custodial vs self-custody wallets
04 How to secure a cryptocurrency wallet
05 Common cryptocurrency scams
06 Checks before sending cryptocurrency
07 What to do after cryptocurrency theft or a scam
08 Frequently asked questions
09 References

Cryptocurrency is a digital asset transferred on a blockchain or another distributed ledger. Instead of a bank updating a private account database, a network validates transactions according to the rules of that cryptocurrency. Bitcoin is the best-known example, but cryptocurrencies differ widely in purpose, governance, privacy, fees, and risk.

Owning cryptocurrency does not mean coins are stored inside a wallet app. The ledger records which addresses control funds; the wallet manages the private keys needed to authorize a transfer. Whoever controls the private key or recovery seed can usually move the assets.

01 How cryptocurrency works

1. A wallet creates or imports cryptographic keys.
2. The public address can be shared to receive funds.
3. The private key signs a transaction authorizing a transfer.
4. Network participants validate the transaction under the protocol's consensus rules.
5. The confirmed transaction becomes part of the ledger history.

Blockchains do not make every claim attached to a coin true. A transaction can be genuine while the investment, website, token, or person requesting it is fraudulent. Technical confirmation only shows that the network accepted the transfer.

02 Coins, tokens, and stablecoins

Term	Meaning	Important risk
Coin	Native asset of its own blockchain, such as bitcoin on Bitcoin	Price, protocol, custody, and transaction risk
Token	Asset created through a smart contract on an existing network	Malicious contracts, fake copies, and issuer risk

Term	Meaning	Important risk
Stablecoin	Token designed to track a currency or other reference asset	The peg, reserves, issuer, or redemption can fail
NFT	Token representing a unique ledger entry	Ownership of a token may not grant copyright or guarantee the linked content remains available

Names and logos are easy to copy. Verify the exact network and contract address through an authoritative project source before receiving or swapping a token.

03 Custodial vs self-custody wallets

Wallet model	Who controls the key?	Main tradeoff
Custodial exchange account	The provider	Password recovery may be available, but access depends on the company, account security, and withdrawals
Software self-custody wallet	The user	Direct control, but malware or a stolen seed can drain the wallet
Hardware wallet	The user, with signing isolated in a device	Reduces online key exposure, but supply-chain, phishing, backup, and approval-screen risks remain
Multi-signature wallet	Several keys under a defined policy	Can reduce single-key failure but requires careful recovery planning

A recovery or seed phrase, commonly 12 to 24 words, can recreate a self-custody wallet. It is not an ordinary password. Entering it into a fake support page, browser extension, airdrop site, or "verification" form gives an attacker control of the assets.

04 How to secure a cryptocurrency wallet

- Never share a private key or seed phrase. Legitimate support staff do not need it.

- Store offline backups where theft, fire, water, and accidental disposal are considered.
- Use a unique password and phishing-resistant MFA on custodial accounts.
- Download wallet software from the verified publisher and check the exact domain.
- Keep the operating system, browser, wallet, and hardware-wallet firmware current.
- Read the destination address and amount on the trusted signing screen, not only on the computer.
- Send a small test transaction before a large transfer when the workflow permits.
- Do not approve an unexplained smart-contract allowance or wallet connection.
- Avoid keeping seed phrases in cloud notes, screenshots, email drafts, or chat history.

Clipboard-stealing malware can replace a copied address with an attacker's address. Compare the full destination, not merely the first and last characters. Address-poisoning scams deliberately create look-alike entries in transaction history.

05 Common cryptocurrency scams

- **Guaranteed-return investments:** a fake platform displays profits but demands more deposits, taxes, or fees before withdrawal.
- **Impersonation:** a caller or message pretends to be an exchange, government agency, employer, celebrity, or family member.
- **Wallet recovery:** someone offers to recover stolen assets, then requests a seed phrase or advance cryptocurrency payment.
- **Giveaways and airdrops:** the victim is asked to send funds first or connect a wallet to a malicious contract.
- **Romance and relationship scams:** trust is built over time before the victim is directed to a fraudulent investment site.
- **Fake apps and extensions:** a cloned wallet steals credentials, seeds, or transaction approvals.
- **Mining and liquidity schemes:** screenshots and dashboards simulate earnings while deposits go to the operator.

Pressure, secrecy, guaranteed profit, a demand to pay only in cryptocurrency, and instructions to move money "for protection" are strong warning signs. A balance displayed on a website is not proof that real assets exist or can be withdrawn.

06 Checks before sending cryptocurrency

1. Confirm why the payment is required and independently verify the recipient.
2. Search the company or person's name with terms such as scam, review, complaint, or fraud.
3. Verify the destination network; sending to an incompatible network can permanently lose access.
4. Check the address on a second trusted channel and on the signing device.
5. Understand fees, confirmations, token approvals, and whether the transaction can be reversed. Most cannot.
6. Stop if anyone asks for remote access, a seed phrase, or an additional payment to release existing funds.

07 What to do after cryptocurrency theft or a scam

1. **Stop sending money.** Additional tax, recovery, or unlock payments are usually part of the same fraud.
2. **Preserve evidence.** Save wallet addresses, transaction hashes, websites, messages, account names, dates, and payment records.
3. **Protect remaining assets.** If a seed or private key was exposed, create a new wallet on a clean device and move unaffected assets carefully.
4. **Revoke malicious approvals.** Use the blockchain's trusted explorer or wallet tools, and verify every contract.
5. **Contact the exchange promptly.** A regulated service may be able to flag an account, though blockchain transfers are not guaranteed to be recoverable.
6. **Secure accounts and devices.** Change passwords, revoke sessions, scan for infostealers, and replace compromised MFA methods.

7. **Report the crime.** Use the appropriate police, financial regulator, consumer-protection, and exchange reporting channels in your country.

Be cautious of unsolicited recovery agents. The FBI and consumer agencies warn that recovery offers can be a second scam targeting people who already lost money.

08 Frequently asked questions

Is cryptocurrency anonymous?

Not necessarily. Many blockchains are public and transactions can be traced between addresses. Connecting an address to an exchange account, purchase, IP record, or public post may identify its owner.

Can a cryptocurrency transaction be canceled?

Usually not after it is confirmed. A recipient may voluntarily return funds, and an exchange may act before withdrawal, but there is no universal chargeback mechanism.

Does a hardware wallet make crypto completely safe?

No. It can keep keys away from an infected computer, but it cannot prevent you from approving a fraudulent transaction, exposing the recovery phrase, or buying a tampered device.

09 References

- FTC: What to know about cryptocurrency and scams
- FBI: Wallet-draining airdrop scams
- IC3: Cryptocurrency investment scam warning

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com