Glossary

Address

A bitcoin address is the destination for a payment. It consists of a string of letters and numbers. Just as you ask others to send an email to your email address, you would ask others to send you bitcoin to one of your bitcoin addresses.

Cold Storage

Cold storage is when cryptoassets are controlled by private keys that have never been on a device that has been online.

Custodial Service

Cryptoassets are controlled by a custodian's keys, not yours. The custodian holds the assets on your behalf, showing their value in your account.

Digital Signature

A mechanism to authenticate that a transaction was ‘signed’ by the owner of that private key and that the transaction wasn’t changed after it was signed.

Hardware Wallet

A special type of bitcoin wallet which creates, stores, and manages the user’s private keys in a secure hardware device.

HD (Hierarchical Deterministic) Wallet

A type of wallet that requires only one private key to gain access to all funds held in the HD wallet. This is made possible by the HD protocol (BIP-32) which allows the creation of child keys from parent keys in a hierarchy.

Hot Storage

A wallet that is created and/or stored on a device connected regularly to the internet. Example: A software wallet on your PC or mobile device.

Hybrid Custody

When cryptoassets are locked in a way that requires more than one person or entity to agree to unlock them.

Mnemonic Phrase (see also 'Seed Phrase')

Multi-Factor Authentication or MFA (also known as 2FA)

An authentication system that requires more than one distinct authentication factor for successful authentication. This can include something you know (like a password), something you are (a biometric,) and something you own (like a security key.)

Multisignature

Multisignature (multisig) refers to requiring a minimum number (K) of keys (N) to authorize an K-of-N transaction. For example, a simple 2-of-3 multisignature scheme would require two (K) of three (N) initialization keys to be used to unlock the funds.

Passphrase

An optional additional word or phrase created as another layer of protection for the seed phrase. If implemented, a wallet cannot be recovered with the seed phrase alone, it must be accompanied by the passphrase.

PIN (Personal Identification Number)

On hardware wallets, a PIN is a number created by the user to protect the device from being accessed by others.

Private Key

The secret number that allows users to prove ownership of an asset by producing a digital signature. This number can also produce public keys, from which addresses are derived.

Public Key

A number, derived via a one-way function from a private key, which can be shared publicly and used by anyone to verify a digital signature made with the corresponding private key.

Seed Phrase (see also 'Mnemonic Phrase')

An ordered list of 12-24 words from a specific dictionary, created when you initialize a new wallet. All of these words are required to recreate (restore or recover) your wallet if it becomes lost or destroyed

Self Custody

When an individual can control their cryptoassets independently, without the cooperation of another person or entity.

TOTP (Time-based One-Time Password)

A temporary, time-limited 6-digit code created by an application to verify your identity to another application.

U2F (Universal Second Factor)

A device used as a second form of authentication to verify your identity to another device or application.

Warm Storage

A special purpose device that can interact with an internet connected device without being connected to the internet itself.