BITCOIN BUTLERS

The Bitcoin Self-Custody Glossary

Every term you'll meet on the way to holding your own keys, in plain English.

Address
A string of letters and numbers that receives Bitcoin. Like an email address for money. Safe to share; it is not your private key.

Air-gapped
A device that never touches the internet. Data moves by SD card or QR codes. The gold standard for key storage.

BIP (Bitcoin Improvement Proposal)
A formal standard document. The ones you'll meet: BIP-39 (seed phrase words), BIP-32 (HD wallets), BIP-44 (account structure).

Block
A bundle of transactions added to the chain roughly every 10 minutes, each referencing the previous one.

Blockchain
The public ledger of every Bitcoin transaction ever made, copied across thousands of computers, immutable once confirmed.

Block explorer
A tool to view blockchain data: transactions, addresses, blocks. Example: mempool.space.

Change address
When you spend, the leftover returns to a fresh address in your own wallet. Like getting $5 change from a $20 bill.

Coinjoin
A privacy technique where many users combine transactions, obscuring who paid whom.

Cold storage
Keys kept fully offline. Maximum security for long-term holdings.

Confirmation
Each new block after your transaction. 1 means received; 6 means settled for practical purposes.

Custodial
Someone else holds your keys. Exchanges are custodial. Not your keys, not your coins.

Derivation path
The route a wallet uses to generate keys from your seed. Standard paths: m/84'/0'/0' for native segwit.

Dust
Amounts so small they cost more in fees to spend than they're worth.

Entropy
True randomness. Your seed must come from it. Never patterns, dates, or "clever" choices.

Fiat
Government-issued currency. "Fiat" means "by decree": it has value because the state says so.

Full node
Software that validates every Bitcoin rule and stores the whole chain (~500GB). Maximum trustlessness.

Hardware wallet / signing device
A physical device that keeps keys offline and signs transactions. Coldcard, SeedSigner, Jade, Trezor.

Hash
A one-way function turning any input into a fixed-length fingerprint. Used everywhere: addresses, blocks, mining.

HODL
A 2013 typo of "hold" that became the ethos: don't sell through volatility.

Hot wallet
A wallet connected to the internet. Convenient, less secure. Spending money, not savings.

BITCOIN BUTLERS

HTLC
Hash time-lock contract. The mechanism that makes Lightning payments all-or-nothing across multiple hops.

Inbound liquidity
On Lightning: your capacity to receive. You can only receive what your channel partner holds on their side.

KYC
Know Your Customer. Identity checks at regulated exchanges, permanently linking your name to your coins.

Lightning Network
Bitcoin's fast, cheap payment layer built on payment channels. Great for spending; needs more attention than on-chain.

Mempool
The waiting room for unconfirmed transactions. Higher fee, earlier confirmation.

Multisig
Requiring multiple keys to spend. 2-of-3 means any two of three keys. Removes the single point of failure.

Node
A computer running Bitcoin software, validating rules or routing Lightning payments.

Non-custodial
You hold the keys. Nobody can freeze, seize, or "pause withdrawals" on your funds.

On-chain
Recorded directly on the Bitcoin blockchain, as opposed to Lightning.

Passphrase ("25th word")
An optional extra word that creates an entirely different wallet from the same seed. Powerful; lose it and the funds are gone.

Private key
The secret that controls your Bitcoin. Anyone holding it holds your money. Never share, never digitize.

Proof of work
The computational race miners run to add blocks. It makes rewriting history prohibitively expensive.

Public key
Derived from the private key, used to build addresses. Safe to share.

Sat (satoshi)
The smallest Bitcoin unit. 1 BTC = 100,000,000 sats.

Seed phrase
12 or 24 words that regenerate every key in your wallet. The master backup. Guard it absolutely.

SegWit
2017 upgrade improving efficiency. Addresses starting "bc1q".

Self-custody
Holding your own keys. You control your Bitcoin. Nobody else.

Shamir's Secret Sharing
Math that splits a secret into shares where any k-of-n reconstruct it and fewer reveal nothing. Used by codex32 and SLIP-39.

Taproot
2021 upgrade enabling more private, flexible scripts. Addresses starting "bc1p".

UTXO
An unspent "coin." Your balance is the sum of your UTXOs; spending consumes some and creates new ones.

Wallet
Software or hardware that manages keys and builds transactions. The Bitcoin itself lives on the blockchain.

Watchtower
A service that watches your Lightning channels for cheating while you're offline.

xpub
An extended public key that can derive all your addresses. Share carefully: it reveals your full transaction history.

Words are the first step. The second is doing it. Free interactive guides at **bitcoinbutlers.com/content**, or book a Butler and do it live: **bitcoinbutlers.com/butlers**