

# Digital Asset Glossary

TERM	DEFINITION
Bitcoin / BTC	A decentralized digital monetary network and asset that allows value to be stored and transferred without a central authority such as a bank or government. Ownership is determined by control of the private keys associated with a wallet. BTC is the ticker symbol used for pricing and trading bitcoin.
Blockchain	A decentralized digital ledger that records transactions in linked blocks, each referencing the previous one to create a tamper-resistant history.
Block	A batch of validated transactions added to the blockchain roughly every 10 minutes in Bitcoin.
Scarcity (21 Million Cap)	Bitcoin's protocol permanently limits supply to 21 million coins, creating a predictable and transparent insurance schedule that cannot be changed by policy decision.
Satoshi	The smallest unit of bitcoin. One bitcoin equals 100,000,000 satoshis, enabling very small or granular transactions.
Bearer Asset	An asset where control equal ownership rather than formal registration in a name. In digital assets, whoever controls the private keys effectively controls the asset.
Public and Private Keys	<p>Cryptographic keys that determine asset ownership and authorization. The private key is a secret code used to sign transactions and access assets.</p> <p>The public key (or derived address) is shared so others can send funds or verify ownership. Losing the private key usually means losing access to the assets permanently.</p>
Bitcoin Address	A destination identifier used to receive bitcoin, similar to a digital account number, generated by wallet software.
Bitcoin Wallet	Software or hardware that manages the cryptographic keys controlling bitcoin holdings. Wallets display balances, generate new addresses, and authorize transactions.

TERM	DEFINITION
Seed Phrase	A list of words that backs up a wallet’s key material. It allows users to recover funds if a device is lost, destroyed, or replaced.
Self-Custody vs. Custodial	<p>In self-custody, the asset owner directly controls the private keys controlling bitcoin holdings.</p> <p>In custodial arrangements, a third part—such as an exchange or qualified custodian—holds the keys on behalf of the client.</p>
Qualified Custodian	A regulated financial institution, such as a trust company, legally permitted to hold and safeguard client assets. Qualified custodians maintain segregation of assets and adhere to high standards of reporting, governance, and security,
Asset Segregation	The practice of holding client assets separately from a custodian’s own assets to ensure clear ownership and reduce counterparty risk.
Cold Storage vs. Hot Wallet	<p>Cold storage keeps private keys offline (e.g., hardware devices or paper backups) to minimize cyber risk, typically for long-term asset holding.</p> <p>A hot wallet keeps keys on an internet-connected device or service for ease of access and frequent transactions.</p>
Proof of Work and Mining	The consensus mechanism securing Bitcoin. Miners perform computational work to add new blocks, validating transactions and preventing double-spending without a central authority.
Bitcoin Halving	A programmed event every four years that reduces the number of new bitcoins created per block by 50%, gradually slowing new supply and reinforcing Bitcoin’s scarcity.
On-Chain vs. Off-Chain (Lightning)	<p>On-chain transactions occur directly on the Bitcoin blockchain and settle transparently on the base layer.</p> <p>Off-chain transactions, such as those on the Lightning Network, occur on secondary layers for faster and cheaper settlement, periodically reconciling back to the main chain.</p>
Altcoin and Stablecoin	<p>An altcoin is any cryptocurrency other than bitcoin, often with different design goals or trade-offs.</p> <p>A stablecoin is a crypto asset designed to maintain a stable value by tracking a reference asset—usually a fiat currency such as the U.S. dollar—through reserves or collateralization</p>