21 Keys to Bitcoin and Digital Assets

Master the essentials of Bitcoin and digital asset investment.

BTC

October 2025 V1.0

Contents

Bitcoin (BTC)

The first and most valuable decentralized digital currency, created by Satoshi Nakamoto in 2009.

Bitcoin (abbreviation: BTC; sign: ₿) is the first decentralized cryptocurrency or digital asset, invented in 2008 by an unknown entity under the pseudonym Satoshi Nakamoto and launched in 2009 as open-source software. It operates on a peer-to-peer network where computers (nodes) maintain a public distributed ledger called a blockchain to record transactions without central oversight.

Bitcoin enables encrypted, peer-to-peer transactions without needing a central bank or third-party involvement, making it a digital currency for secure, direct value transfer worldwide. Its value has grown significantly since inception, from fractions of a penny in 2010 to over $110,000 in 2025, driven by adoption as a store of value and medium of exchange. Demand from retail investors, traditional financial institutions, and institutional investors seeking portfolio diversification and inflation hedge has driven this growth.

Spot Bitcoin ETFs, approved by the U.S. SEC in January 2024, are exchange-traded funds that directly hold Bitcoin, tracking its spot price in real-time. They provide investors with regulated exposure to Bitcoin without direct ownership, with major players like BlackRock's IBIT and Grayscale's GBTC managing billions in assets, enhancing accessibility and liquidity.

Bitcoin Core

Bitcoin Core is the primary software client for running a Bitcoin full node, validating transactions, and contributing to the network's proof-of-work consensus.

Bitcoin Core is the reference implementation of the Bitcoin protocol, a free and open-source software developed by a global community of contributors, initially released by Satoshi Nakamoto in 2009 as Bitcoin-Qt. It serves as the backbone for running a full Bitcoin node, enabling users to validate transactions, enforce consensus rules, and maintain a complete copy of the bitcoin blockchain.

Bitcoin Core supports the network's decentralization, with ~15,000 reachable nodes worldwide verifying the ~860,000 blocks and ~19.75 million BTC in circulation.

The software handles critical functions like transaction verification, block propagation, and mining coordination for Proof of Work, ensuring Bitcoin's security within its ~1000 EH/s hash rate network. It also includes a wallet for managing Bitcoin transactions, supporting features like SegWit and Taproot.

Bitcoin Core evolves slowly to prioritize stability, with version 27.0 released in 2024 introducing improved privacy and performance feature.

Bitcoin Block Reward

The amount of newly created Bitcoin awarded to miners for successfully adding a new block to the blockchain.

The block reward in Bitcoin is the incentive given to miners for validating transactions and adding a new block to the Bitcoin blockchain. It consists of newly minted Bitcoin, created as part of the protocol's issuance mechanism. The block reward is the only way new Bitcoins are introduced into circulation, following Bitcoin's controlled supply schedule.

As of 2025, the current block reward is 3.125 BTC, following the most recent halving event in April 2024. This reward halves approximately every four years (every 210,000 blocks) as part of Bitcoin's monetary policy to cap the total supply at 21 million BTC. The reward was 50 BTC at Bitcoin's launch in 2009, reduced to 25 BTC in 2012, 12.5 BTC in 2016, 6.25 BTC in 2020, and 3.125 BTC in 2024.

The block reward incentivizes miners to secure the network through computational work (proof-of-work). Miners also earn transaction fees, which are becoming increasingly significant as the block reward decreases over time. As the reward continues to halve, miners will rely more on transaction fees, potentially impacting network economics and miner participation in the future.

Bitcoin Standard

The Bitcoin Standard refers to a proposed monetary system where Bitcoin serves as the primary global reserve currency, replacing fiat currencies and traditional stores of value like gold.

The Bitcoin Standard is a concept popularized by economist Saifedean Ammous in his 2018 book, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. It envisions Bitcoin as a global monetary standard due to its decentralized, scarce, and censorship-resistant properties, akin to the historical gold standard where currencies were backed by gold.

Unlike fiat currencies, which central banks can print without limit, Bitcoin has a fixed supply cap of 21 million coins, with approximately 19.75 million in circulation as of 2025, making it a deflationary asset. The standard argues that Bitcoin's predictable issuance and its resistance to manipulation could stabilize economies, reduce inflation, and limit government overspending.

Proponents highlight Bitcoin's advantages: it operates on a decentralized network secured by proof-of-work mining, requires no intermediaries, and enables peer-to-peer transactions globally. For example, Bitcoin processed $2.1 trillion in transaction volume in 2024, rivaling traditional payment networks like Visa.

Critics, however, argue that its volatility (e.g., 2021 peak of $69,000 vs. 2022 low of $16,500), slow transaction speed (~7 TPS), and energy consumption (~140 TWh annually) make it impractical as a global currency. The Bitcoin Standard remains a theoretical framework, with adoption limited to niche cases like El Salvador's 2021 legal tender law.

Bitcoin Supply Curve and Halving

The Bitcoin supply curve is a step-wise logarithmic function that schedules the issuance of 21 million total digital assets over approximately 140 years via halvings, which reduce mining rewards every 210,000 blocks to enforce scarcity.

The Bitcoin supply curve defines the predetermined rate of new digital asset issuance, starting at 50 BTC per block in 2009 and halving every 210,000 blocks (roughly four years) until the block reward reaches zero around 2140, capping the total supply at exactly 21 million BTC. This creates a predictable, diminishing issuance schedule. As of 2025, the circulating supply stands at 19.92 million BTC, with roughly 1.08 million BTC left to mine and daily new supply at 450 BTC.

Halvings enforce this curve by slashing the block reward by 50%, reducing inflation from 1.7% pre-2024 to 0.85% post-April 20, 2024 event (block 840,000), where rewards dropped from 6.25 to 3.125 BTC. Historical halvings include: November 28, 2012 (50 to 25 BTC, block 210,000); July 9, 2016 (25 to 12.5 BTC, block 420,000); and May 11, 2020 (12.5 to 6.25 BTC, block 630,000). The next halving, at block 1,050,000 around April 16-20, 2028, will cut rewards to 1.5625 BTC, halving annual issuance to 164,250 BTC and inflation to 0.42%. This mechanism mimics gold's scarcity but with mathematical precision, driving value through reduced supply amid growing demand.

Block and Block Height

A block is a collection of transactions recorded on a blockchain, and block height is the sequential number of a block in the chain, starting from the genesis block.

A block is a fundamental component of a blockchain, serving as a digital container that holds a set of verified transactions. Each block is cryptographically linked to the previous one, forming a secure, chronological chain.

It typically includes a header with metadata (like a timestamp, nonce, and previous block's hash) and a body containing the transaction data. For example, in Bitcoin, a block is created approximately every 10 minutes and can store up to 1 MB of transaction data, though this varies by blockchain.

Block height refers to the position of a block in the blockchain, counted as the number of blocks from the genesis block (the first block, at height 0). For instance, the 100th block in a blockchain has a block height of 100.

Blockchain

A decentralized digital ledger that securely records transactions across a network of computers in an immutable chain.

A blockchain is a decentralized, distributed digital ledger that records transactions with a network of computers (nodes) in a secure, transparent, and tamper-resistant manner. Each transaction is grouped into a block, cryptographically linked to the previous one, forming a chronological chain. Initially developed for Bitcoin in 2008 by Satoshi Nakamoto, blockchains use consensus algorithm like proof-of-work(PoW) or proof-of-stake(PoS) to validate data without a central authority.

Public blockchains, such as Ethereum and Solana are open, permissionless networks where anyone can participate as a node. Ethereum powers smart contracts, DeFi, NFTs, and DAOs via its Ethereum Virtual Machine (EVM); Solana offers high-speed, low-cost transactions for scalable dApps and Web3 ecosystems.

In contrast, private blockchains restrict access to authorized participants, often used by enterprises for internal processes with enhanced privacy and control (e.g., Hyperledger Fabric). Consortium blockchains, a hybrid model, are governed by a group of organizations, balancing decentralization with restricted access for use cases like supply chain or banking (e.g., R3 Corda).

As of 2025, public blockchains process trillions in transactions annually, driving global adoption in finance, gaming, and digital ownership, while private and consortium chains cater to specialized, permissioned applications.

BTC ETF

Exchange-traded funds that provide direct exposure to Bitcoin's spot price, approved by the SEC in January 2024.

Spot Bitcoin ETF, or BTC ETF, is an investment vehicle traded on major U.S. stock exchanges like the NYSE and Nasdaq that hold actual Bitcoin in custody, tracking its spot price through professional custodians such as Coinbase. Approved by the U.S. Securities and Exchange Commission (SEC) on January 10, 2024, following a Grayscale lawsuit victory, they launched on January 11, 2024, enabling institutional and retail investors to access Bitcoin without managing private keys or wallets. As of 2025, 11 spot BTC ETF are active, with BlackRock's iShares Bitcoin Trust (IBIT) leading at $86 billion in assets under management (AUM), holding approximately 625,000 BTC.

These BTC ETFs have driven significant institutional inflows, totaling over $14.8 billion year-to-date through 2025, reducing Bitcoin's circulating supply by about 6.62% of its market cap. On September 12, 2025, BTC ETF recorded $642 million in net inflows, led by Fidelity's FBTC with $315 million, contributing to a broader crypto market cap exceeding $4.11 trillion. Overall U.S. spot BTC-ETF AUM reached $219 billion by early 2025, with in-kind creations/redemptions approved in August 2025 to enhance efficiency.

Key products include Grayscale Bitcoin Trust (GBTC) at 1.5% expense ratio, ARK 21Shares Bitcoin ETF (ARKB) at 0.21%, and VanEck Bitcoin Trust (HODL) at 0.25%, with promotional waivers like IBIT's 0.12% until January 2025 for the first $5 billion.

Cryptocurrency

Digital currencies and assets secured by cryptography and operating on decentralized blockchain networks without central authority.

A cryptocurrency is a digital or virtual form of currency that uses cryptography for security and operates on a decentralized ledger (blockchain) to record transactions, without reliance on central banks or intermediaries. It functions as a peer-to-peer electronic cash system, enabling secure, verifiable transfers of value. Bitcoin, launched in 2009, was the first, followed by over 25,000 others, often classified as commodities, securities, or currencies depending on jurisdiction. Cryptocurrencies like ETH, USDT and USDC are used for payments, investments, and powering decentralized applications.

Decentralization

Decentralization is the distribution of control, authority, and operations across a network of nodes in a blockchain, eliminating the need for a central authority.

Decentralization in the context of blockchain refers to a system where no single entity or intermediary, such as a bank or government, controls the network's operations, data, or transaction validation. Instead, these responsibilities are distributed among independent nodes (computers) that collectively maintain the blockchain's integrity through consensus algorithms like Proof of Work or Proof of Stake.

This structure enhances security, censorship resistance, and trustlessness, as no central point of failure exists. For example, Bitcoin's network, as of 2025, is maintained by approximately 15,000 reachable nodes globally, with a hash rate of ~1000 EH/s, ensuring no single party can alter the ledger without majority consensus.

Decentralization varies in degree across blockchains. Bitcoin is highly decentralized due to its widespread node distribution and miner diversity (no single mining pool exceeds 27% of hash rate). Ethereum, with ~6,000 nodes and a shift to Proof of Stake in 2022, is also decentralized but faces concerns over validator concentration, as top staking pools control ~30% of staked ETH.

Decentralization reduces risks of censorship (e.g., governments blocking transactions) and data breaches, but it can lead to slower transaction speeds (Bitcoin: ~7 TPS; Ethereum: ~30 TPS) compared to centralized systems like Visa (~24,000 TPS). Challenges include potential 51% attacks on smaller networks and regulatory hurdles, as seen in debates over Ethereum's staking centralization in 2025.

Digital Asset

Electronically stored items of value that can be owned, transferred, or traded, typically secured by blockchain technology for immutability and transparency.

A digital asset is a broad term often used synonymously with cryptocurrency, which can be owned, transferred, or traded, typically secured by blockchain technology to ensure immutability and transparency. It better reflects the diverse nature of these assets, including Bitcoin and Ethereum, stablecoins, and tokenized real-world assets (RWAs) such as real estate, commodities, or U.S. Treasury bonds.

In the U.S., the term "digital asset" is widely adopted in policy and regulatory frameworks, notably by the IRS for tax purposes (defining cryptocurrencies as property) and the SEC for securities regulation, emphasizing their role in financial markets.

Digital Asset Treasuries (DAT), such as Strategy (MSTR) and BitMine Immersion (BMNR), strategically hold digital assets as core reserves to drive shareholder value, leveraging their liquidity and global accessibility.

Digital Asset Treasury (DAT)

Public companies that strategically accumulate digital assets(primarily BTC or ETH) as core treasury reserves to drive shareholder value and provide digital asset market exposure.

Digital Asset Treasury (DAT or DATCO), refers to public companies that strategically accumulate digital assets (primarily BTC or ETH) as core treasury reserves to drive shareholder value and provide amplified exposure to digital asset markets. These firms, like Strategy (formerly MicroStrategy), hold over $100 billion in assets collectively as of 2025.

DATs act as ETF alternatives in restricted markets, enabling capital efficiency through equity issuance and debt for acquisitions. In 2025, over $15 billion has been raised for DAT strategies.

Don't Trust, Verify

"Don't Trust, Verify" is a core principle in blockchain technology, emphasizing that users should independently validate transactions and data on the network rather than relying on intermediaries.

"Don't Trust, Verify" encapsulates the trustless nature of blockchain systems, where participants can confirm the integrity of transactions, blocks, and the entire ledger without depending on a central authority.

In blockchains like Bitcoin, this is achieved through transparent, open-source protocols and decentralized Proof-of-Work consensus mechanisms. Anyone can run a full node to verify transactions against the blockchain's rules, ensuring no need to trust third parties like banks or payment processors.

This principle empowers users to audit the network themselves, enhancing security and reducing risks of fraud or manipulation. For example, a Bitcoin user can verify a transaction's inclusion in a block by checking its Merkle tree path.

The ethos contrasts with centralized systems, where users must trust entities like banks, and has driven adoption in censorship-resistant applications, such as remittances in regions with unstable financial systems.

Grayscale

One of the world's largest digital asset investment platforms, offering regulated products for digital assets exposure including trusts and ETFs of Bitcoin and Ethereum.

Grayscale Investments is one of the world's largest digital asset-focused investment platform, founded in 2013, offering regulated products for exposure to cryptocurrencies like Bitcoin and Ethereum.

It manages trusts such as the Grayscale Bitcoin Trust (GBTC), which holds over 3% of Bitcoin's supply (about 643,572 BTC in 2022), and has expanded to ETFs and thematic funds. Grayscale enables institutional and retail access through private placements, public quotes, and ETFs. In 2024, it launched spot Bitcoin and Ethereum ETFs following SEC approvals.

Immutability

Immutability refers to the property of a blockchain, like Bitcoin, where once data is recorded in a block and added to the chain, it cannot be altered or deleted without consensus from the network.

In the context of Bitcoin, immutability ensures that the transaction ledger, stored across ~15,000 reachable nodes as of 2025, remains permanent and tamper-resistant. Once a transaction is included in a block and confirmed (typically after six confirmations, or ~60 minutes), altering it requires rewriting the block and all subsequent blocks, which is computationally infeasible due to Bitcoin's Proof of Work (PoW) mechanism. With a network hash rate of ~1000 EH/s, changing a single block would demand an attacker control over 50% of this power, costing millions of dollars per hour and requiring impractical coordination.

Bitcoin's immutability stems from its cryptographic structure: each block contains a hash of the previous block, creating a chain where any modification would invalidate all subsequent hashes. For example, a transaction in block 850,000, part of Bitcoin's ~860,000-block chain in 2025, is secured by the cumulative work of miners expending ~140 TWh annually. This makes historical transactions, like the 50 BTC coinbase transaction in the 2009 genesis block, effectively unchangeable.

Mining and Miner

Mining is the process of validating transactions and adding new blocks to a blockchain by solving computational puzzles, and a miner is who performs this task to earn rewards.

In blockchain networks, particularly those using Proof of Work (PoW) like Bitcoin, mining is the process by which nodes validate transactions and secure the network by solving complex cryptographic puzzles. Miners compete to find a nonce that, when hashed with a block's data, produces a hash meeting specific criteria (e.g., a target number of leading zeros in Bitcoin).

Successful miners add a new block to the blockchain, including a coinbase transaction that rewards them with newly minted digital assets and transaction fees. Bitcoin mining, for instance, occurs approximately every 10 minutes, with the network's hash rate at around 1000 EH/s (exahashes per second) as of 2025, consuming roughly 140 TWh annually, comparable to a mid-sized country's energy use. Mining ensures network security and decentralization but is criticized for its high energy consumption and environmental impact.

A miner is an individual, group, or entity operating specialized hardware (e.g., ASICs for Bitcoin) or software to perform mining. Miners contribute computational power to validate transactions and maintain the blockchain's integrity. In Bitcoin, miners receive a block reward, currently 3.125 BTC per block (post-2024 halving) plus variable transaction fees (e.g., ~0.244 BTC in recent blocks). Miners often join mining pools, like Foundry USA or AntPool, which control 27% and 18% of Bitcoin's hash rate respectively in 2025, to share resources and stabilize earnings. Miners are crucial to PoW blockchains but face challenges from declining block subsidies and regulatory pressures on energy use.

Proof of Work

Proof of Work (PoW) is a consensus algorithm where nodes (miners) solve complex cryptographic puzzles to validate transactions and add new blocks to a blockchain.

Proof of Work is a decentralized consensus mechanism used by blockchains like Bitcoin to secure the network and ensure transaction validity. Miners compete to solve computationally intensive mathematical problems, typically involving finding a nonce that, when hashed with the block's data, produces a hash meeting specific criteria (e.g., starting with a certain number of zeros). The first miner to solve the puzzle broadcasts the solution, and if validated by other nodes, their block is added to the blockchain, earning them a reward in digital assets (e.g., 3.125 BTC per block as of Bitcoin's 2024 halving).

This process, called mining, requires significant computational power and energy. For instance, Bitcoin's network consumes approximately 140 TWh annually as of 2025, equivalent to the energy use of a mid-sized country. PoW's strength lies in its security, as altering a block requires re-mining all subsequent blocks, which is computationally infeasible. However, it faces criticism for its energy intensity and limited scalability, with Bitcoin processing around 7 transactions per second compared to faster alternatives like Proof of Stake systems.

S2F (Stock-to-Flow)

A model that measures Bitcoin's scarcity by comparing its existing supply (stock) to its annual issuance rate (flow), often used to predict price trends.

The Stock-to-Flow (S2F) model quantifies Bitcoin's scarcity by dividing its total circulating supply (stock) by the annual amount of new Bitcoin issued through mining (flow).

As of 2025, Bitcoin's circulating supply is approximately 19.92 million BTC, with an annual flow of about 164,250 BTC (post-2024 halving at 3.125 BTC per block, assuming 144 blocks daily). This yields an S2F ratio of roughly 121.3 (19.92 million ÷ 164,250), meaning it would take 121.3 years to produce the current stock at the current issuance rate. Higher S2F ratios indicate greater scarcity, akin to precious metals like gold (S2F ~60).

Introduced by pseudonymous analyst PlanB in 2019, the S2F model correlates Bitcoin's price with its increasing scarcity, driven by halvings that reduce flow every four years. The model predicts significant price increases post-halving due to reduced supply growth; for instance, Bitcoin's price surged to $120,000 by July 2025, aligning with S2F projections of $100,000–$150,000 post-2024 halving.

However, critics argue S2F oversimplifies market dynamics, ignoring demand fluctuations, regulatory impacts, or macroeconomic factors. Despite this, its historical accuracy—predicting peaks like $69,000 in 2021—has made it influential, though not definitive, in digital asset analysis.

Stablecoin

Stablecoin is designed to maintain stable value by pegging to fiat currencies, commodities, or algorithms to minimize volatility.

A stablecoin is designed to maintain a stable value by pegging to assets like fiat currency (e.g., USD) or commodities(e.g., gold), to minimize volatility for payments, decentralized finance (DeFi), and cross-border transfers. Stablecoin types include fiat-backed (e.g., USDT and USDC, supported by reserves), crypto-backed (over-collateralized), and algorithmic.

In 2025, in the U.S., the GENIUS Act (Guiding Effective Non-Fiat Innovation and Utility for Stablecoins) was passed to establish a tailored regulatory framework for stablecoins. It emphasizing consumer protection, reserve transparency, and financial stability to foster innovation while mitigating risks like de-pegging.

Transfer Bitcoin and Transaction

A Bitcoin transaction is a digitally signed transfer of digital assets (BTC) between addresses on the bitcoin blockchain.

A Bitcoin transaction is the process of transferring Bitcoin (BTC) from one wallet address to another, recorded immutably on the Bitcoin blockchain. Transactions are created by a sender's wallet, which uses a private key to sign a data structure specifying inputs (unspent transaction outputs, or UTXOs, from prior transactions), outputs (recipient addresses and amounts), and a fee for miners.

For example, sending 0.1 BTC to an address like "bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq" requires a transaction ID (TxID), a 64-character hash (e.g., "1a2b3c4d…"), to track it. Each transaction, typically 200-500 bytes, is broadcast to the network, validated by nodes (requiring ~600 GB for a full blockchain copy), and confirmed in a block every ~10 minutes.

To transfer Bitcoin, a user inputs the recipient's address, amount, and fee in their wallet. The wallet selects UTXOs to cover the amount, signs the transaction with the private key, and broadcasts it to nodes. Miners prioritize transactions with higher fees. Transactions achieve finality after 6 confirmations (~1 hour), though 1 confirmation often suffices for low-value transfers.

Wallet and Address

A Bitcoin wallet is software or hardware that manages private keys to access digital assets, while an address is a public identifier for receiving Bitcoin payments.

A Bitcoin wallet is a software application or hardware device that stores and manages private keys, public keys, and Bitcoin addresses to enable users to send, receive, and track digital assets on the Bitcoin blockchain. Private keys, typically 256-bit random numbers, cryptographically secure access to Bitcoin funds, while public keys (derived via ECDSA) generate addresses. Together, wallets and addresses enable secure, pseudonymous Bitcoin transactions.

Bitcoin Wallets come in types: software wallets (e.g., Electrum, BlueWallet) run on devices like phones or computers, requiring 5-50 MB for lightweight clients or 600+ GB for full nodes like Bitcoin Core; hardware wallets (e.g., Ledger Nano X, Trezor Model T) store keys offline for enhanced security, costing $70-$150 as of 2025; and paper wallets, printed key pairs, now largely obsolete due to risks of loss or theft. Wallets do not store Bitcoin itself but enable signing transactions, with 90% of users opting for custodial wallets (e.g., Coinbase) versus non-custodial ones for self-sovereignty.

BTC

October 2025 V1.0