21 Keys to Bitcoin and Blockchain

Master the essentials of Bitcoin and blockchain.

BTC

October 2025 V1.0

Contents

51% Attack

A 51% attack occurs when a single entity or group controls over 50% of a blockchain's computing power or stake, allowing them to manipulate the network's transaction ledger.

A 51% attack, also known as a majority attack, is a potential vulnerability in blockchain networks. By controlling more than half of the network's computational power (in Proof of Work, PoW) or staked digital assets (in Proof of Stake, PoS), an attacker can influence the blockchain's consensus process. This enables them to double-spend digital assets, reverse confirmed transactions, or prevent new transactions from being validated, undermining the network's integrity.

In a PoW system like Bitcoin, an attacker would need to amass over 50% of the network's hash rate, which is extremely costly given Bitcoin's total hash rate of approximately 1000 EH/s (exahashes per second) as of 2025. For context, renting enough mining power for a 51% attack on Bitcoin could cost millions of dollars per hour, making it economically impractical for large networks. Smaller PoW blockchains, like Ethereum Classic, have been targeted successfully, with attacks in 2019 and 2020 causing losses of millions due to double-spending.

In PoS systems, an attacker would need to own or control over 50% of the staked assets, which is also costly but feasible if stake distribution is centralized.

While a 51% attack can disrupt a blockchain, it doesn't allow full control, such as stealing assets from other wallets. The risk is mitigated by network size, decentralization, and economic incentives, but smaller or less secure networks remain vulnerable.

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.

Coinbase Transaction

Coinbase refers to a leading U.S.-based digital asset exchange, the coinbase transaction that creates new digital assets in a blockchain block, and the block reward that incentivizes miners with new assets and transaction fees.

A coinbase transaction is the first transaction in a blockchain block, unique for creating new digital assets without prior inputs. It rewards miners with a block subsidy (newly minted coins) and aggregated transaction fees. In Bitcoin, as of 2025, the subsidy is 3.125 BTC per block (post-April 2024 halving).

Block reward, embedded in the coinbase transaction, incentivizes miners in proof-of-work blockchains like Bitcoin by combining the block subsidy and transaction fees. Fees, which spiked to over 100 BTC during 2021 peaks, are increasingly vital as subsidies decline, supporting network security and influencing scalability solutions like layer-2 networks.

Coinbase Inc., founded in 2012 by Brian Armstrong, is a prominent digital asset exchange and custody service, serving over 100 million verified users globally as of 2025. It supports trading over 250 digital assets, including Bitcoin and Ethereum, offering features like staking, institutional custody, and advanced trading tools. Coinbase is publicly listed on NASDAQ (COIN) since April 2021. Base Chain, a Ethereum Layer 2, is also also supported by Coinbase.

Consensus Algorithm

A consensus algorithm is a mechanism used by a blockchain network to achieve agreement among nodes on the validity and order of transactions in a decentralized system.

A consensus algorithm is a set of rules and processes that enables distributed nodes in a blockchain network to agree on a single, shared version of the transaction ledger, ensuring trust and security without a central authority. These algorithms address challenges like double-spending, network faults, and malicious actors, maintaining the integrity and consistency of the blockchain. They are critical for validating transactions and adding new blocks to the chain.

Primary consensus algorithms include Proof of Work (PoW) and Proof of Stake (PoS). In PoW, used by Bitcoin, nodes (miners) solve complex cryptographic puzzles to validate blocks, with Bitcoin's network requiring significant computational power, consuming approximately 140 TWh annually as of recent estimates.

PoS, used by Ethereum since its 2022 upgrade, selects validators based on staked digital assets, reducing energy consumption by over 99% compared to PoW.

Other algorithms, like Delegated Proof of Stake (DPoS) or Practical Byzantine Fault Tolerance (PBFT), optimize for speed or fault tolerance, with DPoS (used by EOS) achieving faster transaction finality by delegating validation to elected nodes.

DLT

Distributed Ledger Technology - a decentralized digital system for recording transactions across multiple computers, ensuring security and immutability.

Distributed Ledger Technology (DLT) is a decentralized digital system for recording transactions across multiple computers (nodes) in a network, ensuring security, transparency, and immutability without a central authority. Unlike traditional databases, DLT distributes data across participants, with consensus mechanisms like proof-of-work or proof-of-stake validating updates. Blockchain, a type of DLT, organizes data into cryptographically linked blocks, as seen in Bitcoin and Ethereum.

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.

Hash

A fixed-length string generated by a cryptographic function to uniquely represent data in the Bitcoin blockchain.

In the context of Bitcoin, a hash is the output of a cryptographic hash function, typically SHA-256, which transforms input data of any size into a fixed-length string of 256 bits. This process is deterministic, meaning the same input always produces the same hash, but it is computationally infeasible to reverse-engineer the original data or find two different inputs with the same hash (collision resistance).

In Bitcoin, hashes are critical for securing transactions, blocks, and the blockchain's integrity. For example, a transaction's hash (TxID) uniquely identifies it, like “1a2b3c4d…” for a transfer of 0.5 BTC, and is used in Merkle trees to summarize multiple transactions in a block.

Hashes underpin Bitcoin's proof-of-work (PoW) mechanism, where miners compete to find a block hash meeting a difficulty target (e.g., a hash with 20 leading zeros as of 2025, requiring ~10^21 computations per block).

The block hash, computed from the block header (including the previous block's hash, Merkle root, timestamp, nonce, and difficulty), links blocks chronologically, ensuring immutability; altering any transaction would change all subsequent block hashes, requiring enormous computational power to rewrite. However, quantum computing advancements, like Google's 2025 Willow chip with 105 qubits, raise theoretical concerns about SHA-256's long-term collision resistance.

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.

Mnemonic and Private Key

A mnemonic is a human-readable phrase used to generate and recover cryptographic keys, while a private key is a secret number authorizing Bitcoin transactions.

A mnemonic (or mnemonic phrase, seed phrase) is a 12-24 word sequence, standardized by BIP-39 (Bitcoin Improvement Proposal 39), that serves as a user-friendly backup for generating a cryptographic seed, which derives private keys for Bitcoin wallets. The mnemonic, typically drawn from a 2,048-word list (e.g., “apple book cat…”), encodes 128-256 bits of entropy plus a checksum. This seed is then used to generate a master private key, from which multiple private keys and Bitcoin addresses are derived via a deterministic path (e.g., m/44'/0'/0'/0/0 for a SegWit address).

A private key is a 256-bit random number that authorizes spending Bitcoin by signing transactions via the Elliptic Curve Digital Signature Algorithm (ECDSA). Private keys are derived from the seed through a hierarchical structure, allowing a single mnemonic to manage millions of keys for different addresses (e.g., bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq).

The mnemonic-to-seed-to-private-key process ensures security and portability: a mnemonic is easier to back up than raw keys, and BIP standards guarantee interoperability. However, users must store mnemonics securely (e.g., offline on metal plates), as 2025 blockchain analytics show 1-2% of stolen funds trace to compromised phrases.

Node and Client

Client are a software that enable participation in the Bitcoin network, where a node validates and relays blockchain data.

In the Bitcoin digital asset ecosystem, a "node" refers to any device running client software that connects to the peer-to-peer network to validate transactions and blocks against consensus rules, contributing to decentralization and security. As of 2025, over 20,000 reachable Bitcoin nodes are operational worldwide, with Bitcoin Core dominating at approximately 97% market share, followed by alternatives like Bitcoin Knots at 2-3%.

A "client," the software powering nodes, comes in thick (full-featured) and thin (lightweight) variants. Bitcoin Core client functions as both a full node and wallet, enabling users to send/receive digital assets.

The distinction blurs in practice: all nodes run clients, but not all clients operate as full nodes; for instance, SPV clients connect outbound to 8-10 full nodes without inbound relays, limiting their decentralizing impact. In 2025, institutional adoption via providers like Crypto APIs' Node-as-a-Service has surged, offering dedicated RPC nodes with low-latency access to validated data, absorbing costs for businesses while individuals use affordable hardware like Raspberry Pi 5 setups under $200. This setup ensures the network's integrity, as nodes collectively store replicas of the 19.92 million BTC circulating supply, verifying against attacks like double-spends.

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.

Quantum Resistance

Cryptographic designs protecting blockchains from quantum computer attacks on public keys.

Quantum resistance refers to cryptographic algorithms designed to secure blockchain networks against potential attacks from quantum computers, which could break traditional encryption methods like RSA or ECDSA.

Quantum computers leverage algorithms such as Shor's, which can factor large numbers and solve discrete logarithm problems in polynomial time on sufficiently powerful machines (e.g., 1 million-qubit systems projected by 2030), threatening the security of public keys used in blockchains like Bitcoin and Ethereum.

To counter this, quantum-resistant algorithms like lattice-based CRYSTALS-Kyber or hash-based signatures (XMSS) are implemented. For instance, the Quantum Resistant Ledger (QRL) uses XMSS, supporting up to 1,000 signatures per key, securing its $100 million total value locked (TVL) as of 2025. In 2024, the National Institute of Standards and Technology (NIST) standardized post-quantum cryptography (PQC) algorithms, including CRYSTALS-Dilithium for digital signatures, which Ethereum is integrating into upgrades like BLS12-381 curves to resist Grover's algorithm, a quantum method that halves the security of symmetric cryptography.

Imagine your bank account's security relying on a traditional lock that a super-powerful quantum computer could pick in seconds, exposing your savings. Quantum resistance is like upgrading to a futuristic, unbreakable lock (e.g., a complex puzzle only solvable with unimaginable computing power). For example, when you use a DeFi wallet on Ethereum to swap tokens, quantum-resistant algorithms like Dilithium ensure your private keys remain secure,

even if a hacker with a quantum computer tries to steal your funds years later. This is similar to how a modern smartphone's fingerprint scanner protects your data compared to an old, easily bypassed PIN code.

SegWit (Segregated Witness)

SegWit (Segregated Witness) is a Bitcoin protocol upgrade that separates signature data from transaction data to increase block capacity and improve transaction malleability.

Segregated Witness, activated on Bitcoin's network in August 2017 at block height 481,824, is a soft fork upgrade designed to optimize the blockchain's scalability and security.

It restructures how transaction data is stored by separating (or "segregating") the witness data—primarily digital signatures verifying transactions—from the transaction body. This reduces the size of each transaction, allowing more transactions to fit within Bitcoin's 1 MB block size limit (effectively increasing capacity to ~1.7-2.2 MB, depending on transaction types).

SegWit addresses transaction malleability, a pre-2017 issue where third parties could alter transaction IDs without changing their content, potentially disrupting unconfirmed transactions. By moving signatures to a separate witness field, SegWit ensures transaction IDs are stable, enabling secure second-layer solutions like the Lightning Network, which supports faster, cheaper off-chain transactions. SegWit also enhances security for multisignature wallets and reduces the risk of certain attacks. Adoption faced initial resistance due to compatibility concerns, but major wallets and exchanges, like Coinbase, now default to SegWit addresses (starting with “bc1”). The upgrade remains backward-compatible, preserving Bitcoin's decentralized consensus while boosting efficiency.

Taproot

Taproot is a Bitcoin protocol upgrade that enhances privacy, efficiency, and smart contract capabilities by introducing a new transaction type and signature scheme.

Taproot is a significant soft fork upgrade to the Bitcoin network, activated in November 2021 at block height 709,632, aimed at improving transaction privacy, scalability, and flexibility.

It introduces a new output type called Pay-to-Taproot (P2TR), which combines the benefits of traditional public key-based transactions and complex scripts (like multisignature or timelocks) into a single, indistinguishable format. By leveraging Schnorr signatures and a Merkle Abstract Syntax Tree (MAST), Taproot makes complex transactions appear identical to regular ones on the blockchain, enhancing privacy. As of 2025, approximately 15-20% of Bitcoin transactions use Taproot, with adoption growing among wallets and exchanges like Coinbase.

Schnorr signatures, a key component, replace the older ECDSA signatures, allowing signature aggregation to reduce data size for multisignature transactions (e.g., cutting a 3-of-5 multisig transaction's size by ~20%). This efficiency lowers fees (Taproot transactions average ~0.00015 BTC in fees vs. ~0.0002 BTC for non-Taproot in 2025) and supports scalability solutions like the Lightning Network. MAST further optimizes smart contracts by only revealing executed script conditions, reducing blockchain bloat.

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.

Trust Compnay

Fiduciary entities that manage investment trusts holding cryptocurrencies for investors seeking regulated exposure without direct ownership.

In the context of digital assets, a trust company, such as Grayscale, is a fiduciary entity that manages investment trusts holding digital assets like Bitcoin and Ethereum for investors seeking regulated exposure without direct ownership. Grayscale, founded in 2013, operates trusts like the Grayscale Bitcoin Trust (GBTC), which holds significant Bitcoin and other vehicles for assets like ETH and SOL.

These trusts provide wealth management and investment advisory services, enabling institutional and retail investors to access digital assets through public quotations or private placements, ensuring tax-efficient strategies and asset protection. Operating under U.S. regulatory frameworks, such trust companies facilitate secure, compliant investment in the digital asset market, often acting as a bridge between traditional finance and decentralized ecosystems.

UTXO (Unspent Transaction Output)

UTXO (Unspent Transaction Output), a record of unspent Bitcoin used for on-chain analysis to track fund flows, ownership patterns, and network activity.

A UTXO (Unspent Transaction Output) is a discrete unit of Bitcoin, a digital asset, received from a transaction and available for spending, identified by a transaction ID (TxID) and output index, linked to a specific address. Each UTXO contains an amount (e.g., 0.5 BTC) and a locking script (governed by BIP-16 for P2SH or BIP-141 for SegWit), which defines spending conditions, enabling analysts to map transaction flows with precision.

In on-chain analysis, UTXOs are critical for tracing the movement, ownership, and behavior of Bitcoin across the blockchain. For on-chain analysis, UTXOs reveal spending patterns, wallet clustering, and economic activity.

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