##### ***Glossary:***

**51% Attack:** A type of attack on a blockchain network in which a single entity or group controls a majority of the network’s computing power, allowing them to manipulate transactions and potentially disrupt the network.

**Altcoin Season:** A period of time when alternative cryptocurrencies experience significant price increases, often due to increased investor interest and adoption.

**Altcoins:** Digital currencies excluding Bitcoin.

**Atomic Swap:** A peer-to-peer exchange of one cryptocurrency for another without the need for a centralized exchange or intermediary.

**Auction:** A process by which goods or assets are sold to the highest bidder.

**Bartering:** The exchange of goods and services without the use of money.

**Basket of Goods:** A collection of goods or services used to measure changes in the cost of living.

**Bitcoin:** A digital currency/system that allows people to send money to each other without using a bank.

**Block Explorer:** A tool used to view and explore the blockchain, allowing users to view individual blocks, transactions, and wallet addresses.

**Block Reward:** The amount of new bitcoins that are awarded to miners for adding a new block to the blockchain.

**Blockchain:** A public record of all bitcoin transactions that have taken place.

**BTC:** The unit used for bitcoins. A digital currency that can be used to make purchases or be traded.

**Capital Controls:** Restrictions on the movement of money across borders.

**Central Bank (Fed):** A government-owned institution that manages a country’s monetary policy.

**Centralization:** The concentration of power or control in a single entity.

**Centralized System:** A system in which power or control is concentrated in a single entity.

**Cold Storage:** A method of storing bitcoins offline, away from the risk of hackers or other online threats.

**Commodity Money:** Objects that have value in and of themselves and are used as a medium of exchange, such as gold or silver.

**Confirmation:** The process of a transaction being processed by the network and highly unlikely to be reversed. The method “miners” verify the authenticity of transactions with their computer hardware and software. It is recommended to wait for at least six confirmations to prevent double spending.

**Consensus Mechanism:** A method used in blockchain technology to validate transactions and ensure the integrity of the blockchain.

**Cryptocurrency Exchange:** A platform where users can buy, sell, and trade cryptocurrencies for other assets such as fiat currency or other cryptocurrencies.

**Cryptocurrency Wallet:** A software program that stores private keys and allows users to send, receive, and manage their cryptocurrency.

**Cryptography:** A branch of mathematics that helps create secure systems.

**Debasement:** The reduction in the value of a currency, often by reducing the amount of precious metal in a coin.

**Debt:** Money that is owed to someone else.

**Decentralization:** The distribution of power and control across a network rather than having a central authority.

**Decentralized Autonomous Organization (DAO):** An organization or network governed by smart contracts and run on a blockchain without a central authority or management structure.

**Decentralized Finance (DeFi):** A movement within the cryptocurrency industry to create decentralized financial products and services that operate on a blockchain.

**Decentralized System:** A system in which power or control is distributed among multiple entities.

**Digital Asset:** A digital representation of value that can be traded or used as a store of value, such as bitcoins.

**Distributed Ledger:** A database that is spread across a network of computers rather than being stored in a central location.

**Double Coincidence of Wants:** The phenomenon where two parties in a barter economy both have what the other party wants and wants what the other party has.

**Double Spend:** When a person tries to send their bitcoins to two different recipients at the same time.

**Dust Transaction:** A transaction that sends a very small amount of bitcoins that are too small to be economically viable.

**Exchange Rate:** The value of one currency in relation to another.

**FOMO:** Fear of missing out, a term used to describe the feeling of anxiety or regret that one may miss out on a profitable opportunity in the cryptocurrency market.

**FUD:** Fear, uncertainty, and doubt, a term used to describe negative rumors or information that can cause market panic or decline.

**GDP:** Gross domestic product, the total value of goods and services produced in a country in a given period of time.

**Hard Fork:** A change to the Bitcoin protocol that creates a new version of the blockchain that is not compatible with the previous version (i.e. Bitcoin Cash).

**Hardware Wallet:** A physical device used for storing private keys and managing cryptocurrency, providing enhanced security over software wallets.

**Hash Function:** A mathematical function that takes input data of any size and outputs a fixed-size string of characters, commonly used in cryptography and blockchain technology.

**Hash Rate:** A way to measure the processing power of the Bitcoin network.

**HODL:** A term used in the cryptocurrency community to describe holding onto cryptocurrency long-term rather than selling or trading it.

**Hot Wallet:** A Bitcoin wallet that is connected to the internet, allowing for easy access to bitcoins.

**Imports:** Goods and services produced in another country and sold in the domestic market.

**Inflation:** An increase in the general price level of goods and services in an economy.

**Initial Coin Offering (ICO):** A fundraising method in which a new cryptocurrency is sold to investors in exchange for a more established cryptocurrency, such as Bitcoin.

**Layer-1 Protocol:** The underlying layer of a blockchain network that handles the fundamental aspects of consensus, transaction validation, and data storage.

**Layer-2 Protocol:** A secondary layer built on top of a layer-1 blockchain network, often used to enhance scalability, speed, and functionality.

**Ledger:** A record of financial transactions.

**Lightning Network:** A layer-2 payment protocol that enables faster and cheaper bitcoin transactions by using off-chain channels for smaller transactions.

**Mediums of Exchange:** Objects or systems that are widely accepted in exchange for goods and services.

**Merkle Tree:** A tree-like data structure used in the Bitcoin blockchain to efficiently verify the integrity of large sets of data.

**Mining Pool:** A group of miners who work together to increase their chances of finding new blocks and earning bitcoins.

**Mining:** The process of using computer hardware to do mathematical calculations for the Bitcoin network to confirm transactions and increase security.

**Monetary and Fiscal Policy:** The policies of a central bank and government, respectively, that influence the money supply and interest rates in an economy.

**Money Supply:** The total amount of money in circulation in an economy.

**Multi-Signature (Multisig) Wallet:** A wallet that requires multiple signatures or approvals before a transaction can be executed, providing additional security and control.

**Multi-Signature:** A security feature that requires more than one private key to authorize a bitcoin transaction.

**Network:** A group of interconnected entities.

**Node Network:** A network of connected computers or devices that support and maintain the Bitcoin network.

**Node:** A computer or device that is connected to the Bitcoin network and participates in the verification and transmission of transactions.

**Non-Fungible Token (NFT):** A type of digital asset that represents a unique or one-of-a-kind item, often used to represent art, collectibles, or other unique objects.

**Nonce:** A random number added to a block header to create a hash that meets the difficulty target.

**Orphan Block:** A block not included in the main chain of the blockchain due to being invalidated by a longer competing chain.

**Paper Wallet:** A printed copy of a user's private and public keys used for storing and managing cryptocurrency offline.

**Peer-to-Peer (P2P):** A decentralized network in which participants interact directly with each other rather than through a central authority.

**Peg:** A fixed exchange rate between two currencies where one is pegged to the value of another.

**Private Blockchain:** A blockchain controlled by a single organization rather than being decentralized.

**Private Key:** A secret piece of data that proves a person's right to spend bitcoin from a specific wallet through a cryptographic signature.

**Proof-of-Stake (PoS):** A consensus mechanism used in some blockchain networks that requires users to hold a certain amount of cryptocurrency to participate in the validation of transactions.

**Proof-of-Work:** A consensus mechanism that requires users to perform a certain amount of computational work to participate in the network.

**Public Blockchain:** A blockchain open to anyone to participate in and verify transactions, making it decentralized.

**Public Key:** A unique identifier used for receiving bitcoins derived from a user's private key through a mathematical process.

**Public Key/Bitcoin Address:** A public password/number used to receive bitcoins.

**Public Ledger:** A decentralized database that keeps a public record of all transactions on the Bitcoin network.

**Purchasing Power:** The ability of money to buy goods and services.

**Recovery Phrase/Seed Keyword:** A series of 12, 18, or 24 words that can be used to generate multiple pairs of private and public keys. These can be used to restore a Bitcoin wallet.

**Reserve Ratio:** The proportion of deposits that a bank must hold as reserves.

**Restrictive Banking:** Restrictions or limitations on banking services or access to banking services.

**Satoshi Nakamoto:** The pseudonym used by the anonymous creator(s) of Bitcoin.

**Satoshi:** The smallest unit of Bitcoin, equal to 1/100,000,000 of a bitcoin. It is named after the creator of Bitcoin, Satoshi Nakamoto.

**Satoshis per Byte (sat/b):** A unit used to measure the amount of bitcoin transaction fee paid per byte of transaction data.

**SegWit (Segregated Witness):** A Bitcoin protocol upgrade that changes the way data is stored on the blockchain, allowing for increased capacity and lower transaction fees.

**Sidechain:** A blockchain connected to another blockchain, allowing for the transfer of assets or information between the two chains.

**Signature:** A mathematical mechanism that allows someone to prove ownership.

**Smart Contract:** A self-executing contract with the terms of the agreement written into code.

**Soft Fork:** A change to the Bitcoin protocol that is backward-compatible with older versions of the software.

**Stablecoin:** A type of cryptocurrency designed to maintain a stable value often by being pegged to a fiat currency or other asset.

**Supply and Demand:** The economic principle that the price of goods or services is determined by the interaction of the quantity of the goods or services supplied and the quantity demanded.

**Time Value of Money:** The principle that money is worth more in the present than in the future.

**Token:** A unit of value created on a blockchain often used to represent a specific asset or utility within a particular ecosystem.

**Tokenization:** The process of creating a digital representation of an asset or asset class on a blockchain, allowing for fractional ownership and transferability.

**Trading Pair:** A set of two currencies or assets that can be traded against each other on a cryptocurrency exchange.

**Transaction Fee:** A small amount of bitcoins paid by the sender of a transaction, incentivizing miners to include the transaction in a block and add it to the blockchain.

**Transaction ID:** A string of numbers and letters that shows the details of a bitcoin transfer (such as the amount sent, the addresses of the sender and recipient, and the date of the transfer) on the Bitcoin blockchain.

**Transaction:** The transfer of bitcoins from one address to another on the Bitcoin network.

**Trustless:** A system or transaction that does not require trust in any third party or intermediary. instead relying on the security and transparency of the underlying technology.

**Two-Factor Authentication (2FA):** A security measure that requires two methods of authentication, typically a password and a separate code or device, to access an account or complete a transaction.

**Unbanked:** Individuals or communities without access to traditional banking services.

**Unit of Account:** A standard unit of measurement used to express the value of goods and services.

**Volatility:** The degree of variation in the price of an asset over time.

**Wallet Address:** A unique identifier used to send and receive bitcoins on the Bitcoin network, typically represented as a string of letters and numbers.

**Wallet Backup:** A copy of the private keys and recovery phrase/seed keywords of a Bitcoin wallet, which can be used to restore access to the wallet in case the original is lost or stolen.

**Wallet:** A virtual container for bitcoins similar to a physical wallet that contains private key(s) that allow you to spend the bitcoins allocated to it in the blockchain.

**Whale:** An individual or organization that holds a significant amount of cryptocurrency, capable of influencing market prices through large trades.

**White Hat Hacker:** An ethical hacker who uses their skills to identify and fix vulnerabilities in computer systems and networks.

**Whitepaper:** A report that explains the problem and solution that a blockchain project or cryptocurrency is trying to address.

**XBT and BTC:** Abbreviations for bitcoin.