Introduction to Cryptocurrency - The Basics

What Is Cryptocurrency?

A digital or virtual asset, operating on decentralized blockchain technology, employing cryptography to ensure secure transactions.

Asset - A resource with economic value

Decentralized - No single point of control or authority

Blockchain - A network of decentralized, digital, unchangeable ledgers, linked through cryptography.

Cryptography - The process of securing data and communication using mathematical algorithms to ensure security.

What is a blockchain & how does a blockchain work?

Blockchain technology is the underlying infrastructure that enables the operation of cryptocurrencies. Here's how it works:

Decentralized Ledger: A blockchain is a decentralized, distributed public ledger that records all transactions across a network of computers (nodes). Each participant in the network has a copy of the entire ledger.

Blocks: Transactions are grouped into blocks. Each block contains a list of transactions, a timestamp, and a reference (hash) to the previous block, creating a chain of blocks (hence the name "blockchain").

Cryptographic Hashing: Each block contains a cryptographic hash of the previous block. This hash is a unique digital fingerprint of the data in the previous block. It ensures the integrity of the blockchain by linking each block to the previous one.

Consensus Mechanism: To add a new block to the blockchain, the network participants must reach a consensus. Common consensus mechanisms include:

Proof of Work (PoW): Miners compete to solve complex mathematical puzzles, and the first to solve it gets to add the new block to the blockchain. This process requires significant computational power.

Proof of Stake (PoS): Validators are chosen to add new blocks based on the number of coins they hold and are willing to "stake" as collateral. This method is more energy-efficient than PoW.

Immutability: Once a block is added to the blockchain, it is extremely difficult to alter the data in that block. To change a single block, an attacker would need to change all subsequent blocks, requiring a majority of the network's computational power.

Security: The decentralized and cryptographic nature of blockchain makes it highly secure. Transactions are verified by multiple nodes, and any attempt to alter the data is easily detectable.

Transparency and Anonymity: While all transactions on the blockchain are transparent and can be viewed by anyone, the identities of the participants are typically anonymous or pseudonymous, identified only by their public keys.

How does cryptocurrency work?

Transactions:

Initiation: A transaction is initiated by a user sending cryptocurrency from their wallet to another user's wallet. Each wallet has a public key (address) and a private key.

Verification: Transactions are broadcast to the network, where nodes verify the legitimacy of the transaction using cryptographic algorithms.

Mining/Validation: Depending on the consensus mechanism (e.g Proof of Work, Proof of Stake), transactions are grouped into blocks and added to the blockchain by miners or validators.
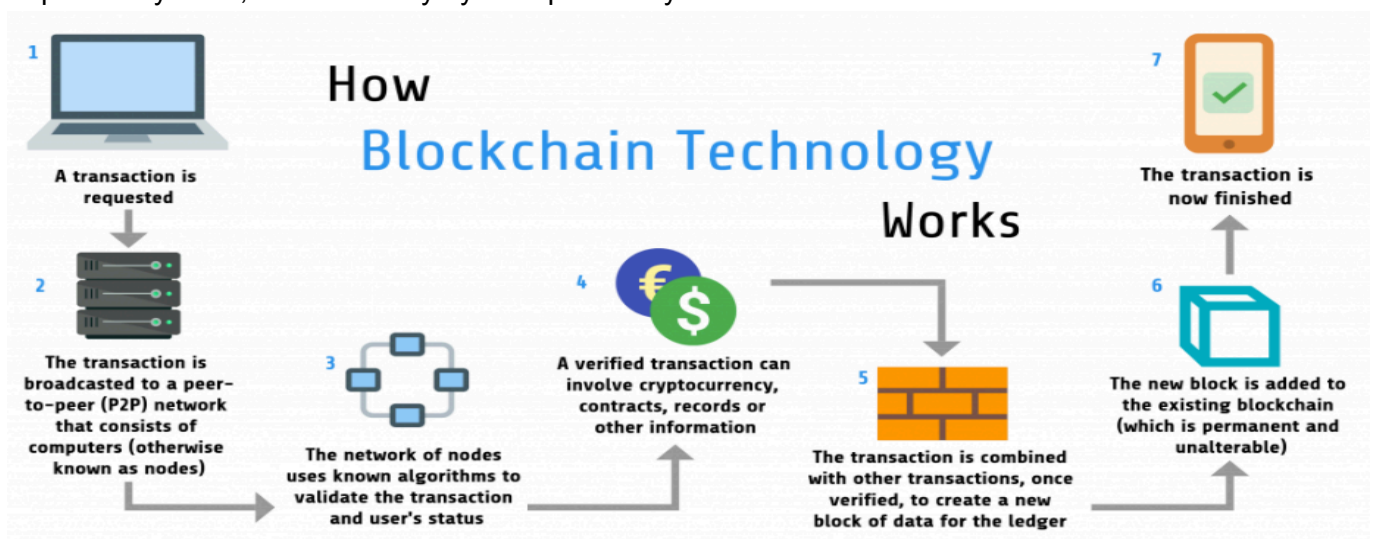
Consensus Mechanisms:

Proof of Work (PoW): Miners solve complex mathematical puzzles to add new blocks to the blockchain. This process requires significant computational power and energy.
Proof of Stake (PoS): Validators are chosen to add new blocks based on the number of coins they hold and are willing to "stake" as collateral. This method is more energy-efficient than PoW.

Security: The decentralized nature of blockchain, combined with cryptographic hashing, makes it highly secure. Altering a single block would require changing all subsequent blocks, which is practically impossible without controlling a majority of the network's computational power.

Wallets: Users store their cryptocurrencies in digital wallets, which can be software-based (online, mobile, desktop) or hardware-based (physical devices). Wallets hold the private keys needed to authorize transactions.

Transparency and Anonymity: While all transactions on a blockchain are transparent and can be viewed by anyone, the identities of the participants are typically anonymous or pseudonymous, identified only by their public keys.

How **Blockchain Technology** Works

1. A transaction is requested

2. The transaction is broadcasted to a peer-to-peer (P2P) network that consists of computers (otherwise known as nodes)

3. The network of nodes uses known algorithms to validate the transaction and user's status

4. A verified transaction can involve cryptocurrency, contracts, records or other information

5. The transaction is combined with other transactions, once verified, to create a new block of data for the ledger

6. The new block is added to the existing blockchain (which is permanent and unalterable)

7. The transaction is now finished

Types of cryptocurrency

Payment Coins:
General Purpose currency, which has its own dedicated blockchain that supports only itself. Generally has a limited amount of currency which makes them deflanary. As time passes they become less available therefore increasing in value.

Examples: Bitcoin (BTC), Litecoin (LTC), Ripple (XRP)

Stable Coins:
Designed as a "stable" store of value. These currencies are pegged to the value of stable assets and can be exchanged for one or more traditional fiat currencies such as USD or Euros.

Examples: Tether (USDT), USD Coin (USDC) Dai (DAI)

Privacy Coins:
Privacy coins are a type of cryptocurrency designed to enhance the privacy and anonymity of transactions. Unlike most cryptocurrencies, where transaction details are recorded on a public ledger, privacy coins employ various techniques to obscure the details of the sender, receiver, and transaction amounts

Examples: Monero (XMR), Zcash (ZEC), Dash (DASH)

Utility Tokens
A utility token is a type of cryptocurrency token that is designed to provide access to a specific product or service within a blockchain-based platform. Unlike cryptocurrencies such as Bitcoin, which function primarily as a medium of exchange or store of value, utility tokens have a specific use case within the ecosystem of a particular project.They are an asset that runs on top of another blockchain.

Examples:

DeFi/Finance Tokens: Tokens used within the decentralized finance ecosystem to facilitate various financial services without traditional intermediaries. Uniswap (UNI)

Utility Tokens: Tokens that provide access to a product or service within a specific blockchain platform. Binance Coin (BNB)

Non-Fungible Tokens (NFTs): Unique digital assets representing ownership of a specific item or piece of content, such as digital art, music, or virtual real estate.

Governance Tokens: Tokens that give holders the right to vote on decisions and changes within a blockchain project or decentralized autonomous organization. Yearn Finance (YIFI)

Media Tokens: Media tokens are a specific type of cryptocurrency used within the media and entertainment industries to facilitate transactions, incentivize content creation, and engage audiences. Basic Attention Token (BAT)

Central Bank Digital Currencies: Central Bank Digital Currencies are digital forms of a country's fiat currency issued and regulated by the central bank. They represent a new form of digital money that complements traditional banknotes and coins.

Example: China's Digital Yuan (DCEP)

Types of cryptocurrency wallets

Hot Wallets: Hot wallets are cryptocurrency wallets that are connected to the internet and are used for frequent transactions and easy access to cryptocurrencies.

Cold Storage: Cold storage refers to the practice of keeping cryptocurrencies offline in a secure manner, away from internet-connected devices, thereby minimizing the risk of unauthorized access, hacking, and theft.

(Cold) Hardware Wallets: Physical devices designed to securely store cryptocurrencies offline, offering robust protection against hacking and malware.

(Hot) Software Wallets: Applications or programs installed on computers or mobile devices to manage cryptocurrencies.

Examples: Exodus, Electrum, MyEtherWallet.

(Hot) Mobile Wallets: Wallet applications specifically designed for mobile devices, offering portability and ease of use.
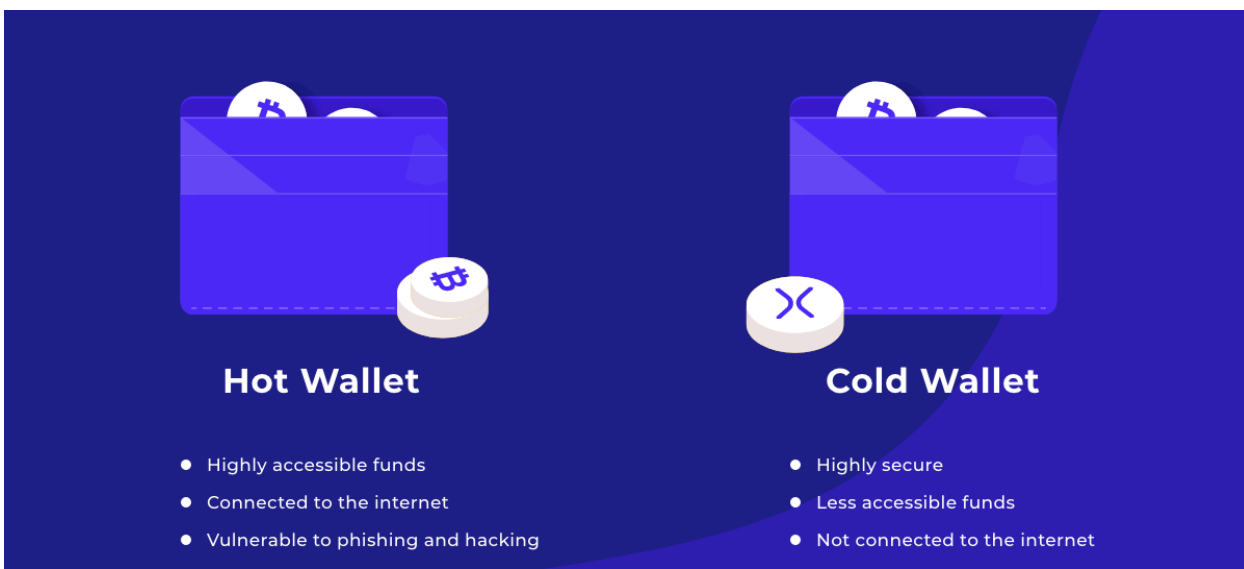
Examples: Trust Wallet, Coinomi, Atomic Wallet.

(Hot) Desktop Wallets: Software wallets installed on desktop computers, providing control over private keys and transactions.

Examples: Electrum (supports both desktop and mobile), Exodus.

(Hot) Online/Web Wallets: Web-based wallets accessible via internet browsers, hosted by third-party service providers.

Examples: Coinbase Wallet, Binance Wallet.

(Cold) Paper Wallets:Physical documents or prints containing public and private keys, usually generated offline.

Hot Wallet

- Highly accessible funds
- Connected to the internet
- Vulnerable to phishing and hacking

Cold Wallet

- Highly secure
- Less accessible funds
- Not connected to the internet

How to obtain cryptocurrency

Choose a Cryptocurrency Exchange: Select a reputable cryptocurrency exchange platform that supports the cryptocurrency you want to buy. Popular options include Coinbase, Binance, Kraken, and Independant Reserve.

Create an Account: Sign up for an account on your chosen cryptocurrency exchange. Provide necessary information for identity verification.

Deposit Funds: Deposit fiat currency (like USD, AUD, etc.) or other cryptocurrencies into your exchange account. This is usually done via bank transfer, credit/debit card, or cryptocurrency transfer from another wallet.

Place an Order: Navigate to the spot trading section of the exchange and choose the cryptocurrency you want to buy. Specify the amount you wish to purchase or the amount of fiat currency you want to spend. Review the order details and confirm the purchase.

How cryptocurrency can make you $$$

Holding & Staking

Description: Cryptocurrency holding refers to the act of acquiring digital currencies and retaining them over time. Emphasizing a long-term investment approach to withstand market volatility and price fluctuations.

Staking: Staking cryptocurrency assets for a set period of time to help support the operation of a blockchain. The primary advantage of staking is earning additional cryptocurrency, with generous interest rates.

Benefits: Holding & Staking is a longer term strategy. The main benefit of Holding & Staking is the low risk and low volatility nature of the market. It allows long term accumulation of assets, while providing stability and predictability.

Risks: Low

Cryptocurrency Trading

Description: Spot trading is where cryptocurrencies are exchanged in real-time, with transactions settled instantly at the prevailing market prices. Traders aim to buy low and sell high, reacting to real-time market fluctuations

Margin trading refers to a trading strategy that combines elements of spot trading and margin trading. In this approach, traders can leverage their existing assets to borrow additional funds, thereby increasing their trading capital and potential profits.

Futures trading involves trading futures contracts tied to the price movements of cryptocurrencies. Cryptocurrency futures are derivative contracts allowing investors to speculate on future cryptocurrency prices without owning the actual assets

Benefits: Spot, Futures & Margin Trading is typically used for short-term speculation or attempting to quickly profit from market inefficiencies. One of the main benefits of margin trading is the ability to trade with leverage, which increases the potential returns on a trade. Traders borrow funds to purchase cryptocurrencies, they can potentially profit from price movements that are larger than their initial investment amount.

Risk: Moderate - High