# **Bitcoin Halving: A Scheduled Scarcity Event**

***“Total circulation will be 21,000,000 coins. It’ll be distributed to network nodes when they make blocks, with the amount cut in half every 4 years. first 4 years: 10,500,000 coins next 4 years: 5,250,000 coins next 4 years: 2,625,000 coins next 4 years: 1,312,500 coins etc…”***

***-Satoshi Nakamoto***

The Bitcoin halving is a pivotal event programmed into the Bitcoin protocol that cuts the block reward for miners in half, roughly every four years. This mechanism directly impacts the rate at which new bitcoins enter circulation, influencing supply and potentially, price.

**Mechanics of the Halving:**

* **Total Supply Cap:** Bitcoin's core code dictates a finite supply of 21 million bitcoins. Once all are mined, no more can be created.
* **Block Rewards:** Miners compete to solve complex mathematical puzzles to verify transactions and secure the network. As a reward, they receive a set amount of bitcoins for each block mined.
* **Halving Schedule:** The block reward is automatically halved every 210,000 blocks, which roughly translates to four years. The first halving occurred in November 2012, followed by subsequent halvings in 2016 and 2020.
* **The Next Halving:** The next halving is projected for April 2024, bringing the block reward down from 6.25 bitcoins to 3.125 bitcoins.

**Impact of the Halving:**

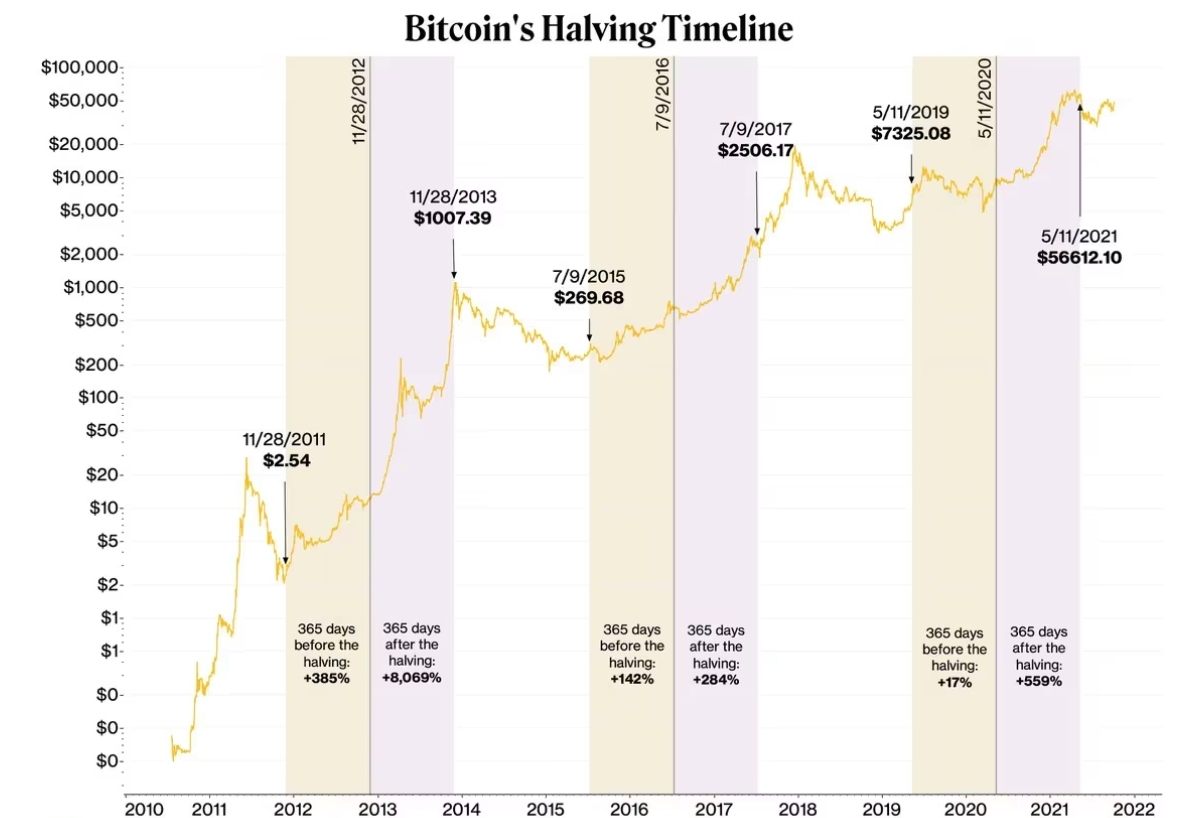
* **Reduced Supply:** The primary purpose of the halving is to control inflation by progressively decreasing the number of new bitcoins entering the market.
* **Potential Price Appreciation:** In theory, with a diminished supply and constant or increasing demand, the price of existing bitcoins could rise. However, this is not guaranteed and depends on various market factors.
* **Mining Profitability:** The halving affects miner profitability. While the block reward halves, mining difficulty typically adjusts to maintain network security. This can lead to increased competition among miners, potentially impacting profit margins.

**Uncertainties and Considerations:**

* **Market Volatility:** The halving is a highly anticipated event, often leading to increased market volatility around the date.
* **Long-Term Impact:** The long-term effects of repeated halvings on price and network security are still being observed and debated.
* **Alternative Cryptocurrencies:** The halving's impact might be mitigated by the emergence of new cryptocurrencies with different supply models.

**Conclusion**

The Bitcoin halving is a significant event designed to maintain scarcity and potentially influence price appreciation. While its long-term effects remain under scrutiny, it is a core principle underlying Bitcoin's economic model, making it a crucial concept for investors and those interested in the cryptocurrency's future.

*Source: Coin Metrics(CoinDesk)*

# **The Technical Architecture of Bitcoin: A Distributed Ledger**

Bitcoin, the world's first and most popular cryptocurrency, functions on a robust technical architecture designed for security, transparency, and decentralization. This report explores the key components that underpin the Bitcoin network.

* **Blockchain: The Foundation of Trust**
  + At the heart of Bitcoin lies the blockchain, a distributed public ledger that records all transactions ever made on the network. Each transaction is grouped into a block, containing information like sender, receiver, and amount transferred.
  + Blocks are chained together chronologically, with each block referencing the hash (a unique cryptographic fingerprint) of the previous block. This creates an immutable record, making it virtually impossible to tamper with past transactions.
  + Copies of the entire blockchain are distributed across a vast network of computers called nodes. This distribution ensures the network's resilience and prevents any single entity from controlling the ledger.
* **Nodes: The Network Guardians**
  + There are two main types of nodes in the Bitcoin network:
    - **Full Nodes:** These nodes download and store a complete copy of the blockchain. They independently verify all transactions, ensuring the network's integrity.
    - **Light Nodes:** These nodes download only a subset of the blockchain data for faster performance. They rely on full nodes to verify transaction validity.
  + The high number of nodes globally distributed contributes to the network's security. Modifying the blockchain would require altering copies on a majority of nodes, a near-impossible feat.
* **Mining: Securing the Network and Creating New Bitcoins**
  + Miners, though not mentioned in the Bitcoin white paper, play a crucial role in the Bitcoin network. They utilize powerful computers to solve complex mathematical puzzles called *proof of work (PoW).*
  + The first miner to solve a block puzzle gets to add the block to the blockchain and receive a reward in the form of newly minted bitcoins.
  + This PoW mechanism serves two purposes:
    - **Securing the Network:** The difficulty of the puzzles adjusts automatically to maintain a desired block creation rate. Solving these puzzles requires significant computational power, making it disincentivized to attempt fraudulent transactions that would require altering the blockchain.
    - **Creating New Bitcoins:** The block reward is how new bitcoins enter circulation. This reward halves roughly every four years (halving event) to maintain a finite supply of 21 million bitcoins.
* **Transactions: Sending and Receiving Bitcoins**
  + Bitcoin transactions involve transferring ownership of bitcoins from one user to another. Users broadcast their transactions to the network.
  + Miners include verified transactions in the blocks they mine. Once a block is added to the blockchain, the transaction is considered complete and irreversible.
  + Transactions are secured by cryptography. Users hold private keys that allow them to spend their bitcoins, while public keys act as their addresses on the network.

**Conclusion**

The technical architecture of Bitcoin is a masterpiece of cryptography, distributed computing, and game theory. By combining these elements, it creates a secure, transparent, and decentralized system for digital currency. As Bitcoin continues to evolve, its underlying architecture will remain a cornerstone of its success.

# **Decentralized Exchanges: Democratizing Cryptocurrency Trading**

Decentralized Exchanges (DEXs) are a revolutionary innovation within the cryptocurrency ecosystem, aiming to empower users and foster a more transparent decentralized financial(De-Fi) landscape. Unlike traditional Centralized Exchanges (CEXs) controlled by a single entity, DEXs operate on a peer-to-peer (P2P) model, eliminating the need for intermediaries. This report delves into the workings, advantages, and a popular example of a DEX.

**Decentralized Exchange Operations:**

* **Smart Contracts:** DEXs leverage smart contracts, self-executing code stored on a blockchain. These contracts define the rules for trading, ensuring secure and transparent transactions without human intervention.
* **Order Matching Mechanisms:** DEXs employ various order matching mechanisms. Popular models include Automated Market Makers (AMMs) which utilize liquidity pools (funds locked by users) and algorithms to determine prices based on supply and demand.
* **Liquidity Provision:** Liquidity is crucial for smooth trading. On DEXs, users can become liquidity providers by depositing crypto assets into liquidity pools, earning fees for facilitating trades.

**Advantages of DEXs:**

* **Self-Custody:** DEXs grant users complete control over their crypto assets, as funds remain in their wallets throughout the trading process.
* **Transparency:** All transactions are recorded on a public blockchain, fostering trust and immutability.
* **Anonymity:** DEXs require no KYC, so transactions remain anonymous and don't require sharing of confidential information.
* **Accessibility:** DEXs generally offer permissionless access, meaning users can trade without extensive KYC (Know Your Customer) procedures.
* **Resistance to Censorship:** The decentralized nature makes DEXs resistant to control by a single entity, promoting financial inclusion.

**Downsides of DEXs:**

* **Limited Liquidity:** Compared to CEXs, DEXs often face lower liquidity, particularly for less popular tokens. This can lead to higher slippage (difference between expected and actual price) for traders.
* **Order Book vs. AMM:** Order matching can be less efficient on DEXs. While some DEXs utilize order books similar to CEXs, others rely on Automated Market Makers (AMMs) which can introduce complexities.
* **User Interface and Functionality:** DEXs may have less intuitive interfaces and may lack advanced features commonly found on CEXs, such as margin trading or stop-loss orders.
* **Constant need of Hot Storage Device:** To trade on DEX, the user must have their wallet connected to the internet either physically through PCs or through extensions like *Metamask*.

**How do DEXs work?**

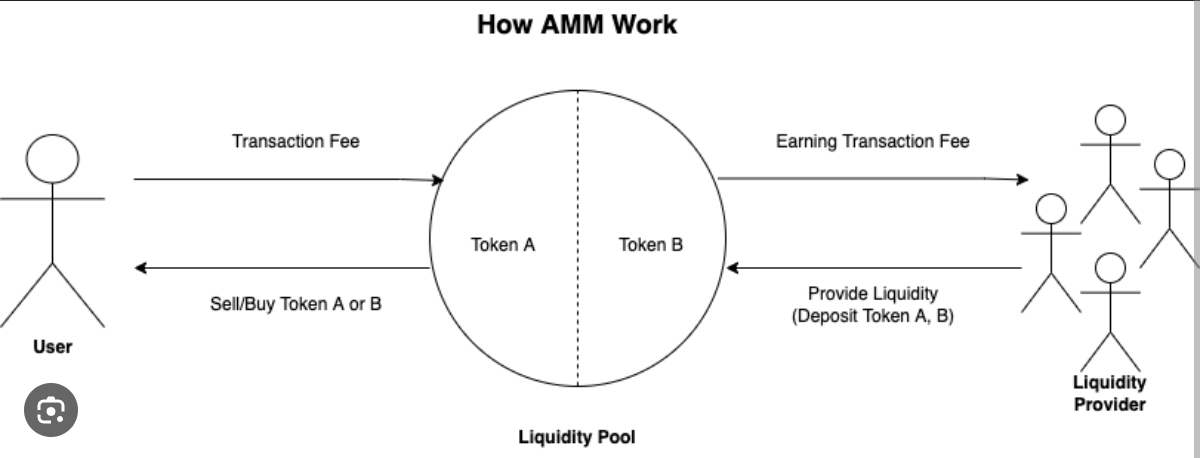
1. **Order Book Method**

* **Traditional Approach:** Order books resemble those found on centralized exchanges. Users submit orders specifying the price they are willing to buy (bid) or sell (ask) a particular token for, along with the desired quantity.
* **Matching Orders:** The DEX's core function is to efficiently match these buy and sell orders. Orders with the highest bid price are matched with the lowest ask price, prioritizing trades with the most favorable terms for both parties.
* **Transparency:** Order books provide a clear picture of market depth, displaying the total buy and sell orders at various price levels. This allows users to gauge market sentiment and assess potential slippage (difference between expected and actual price).
* **Limitations:** Order book DEXs can suffer from limited liquidity for less popular tokens. This can lead to wider bid-ask spreads (difference between buy and sell price) and higher slippage for traders.

1. **AMM(Automated Market Makers)**

* **Algorithmic Price Discovery:** AMMs utilize smart contracts to automate price discovery and facilitate trades between cryptocurrencies like *Ethereum* with *basic attention tokens*. They rely on liquidity pools, which are smart contract-managed reserves of tokens deposited by users.
* **Constant Product Market Maker Formula:** Many AMMs employ a constant product formula. This formula dictates that the price of a token within the pool is determined by preserving the ratio(usually 50:50) of its reserves compared to the other token in the pool. As one token is bought from the pool, its price increases due to a decrease in its reserve relative to the other token.
* **Transaction fee and Liquidity providers:** Transaction fees are a small amount of cryptocurrency paid by users on a DEX to cover the cost of processing their trades. These fees are typically distributed among *liquidity providers*.Liquidity providers deposit their crypto assets into liquidity pools on a DEX, essentially acting as market makers. They earn a portion of the transaction fees as a reward for contributing to the smooth functioning of the DEX by ensuring there are enough assets available for trading.
* **Benefits:** AMMs address liquidity deficiencies by allowing anyone to contribute to the pool. This fosters a more inclusive trading environment, particularly for new or less popular tokens.
* **Impermanent Loss:** A crucial concept for liquidity providers in AMMs is impermanent loss. This occurs when the price of a deposited token fluctuates significantly between the time it's deposited and withdrawn. PWhile fees can offset this loss, it's a risk to consider.

**Example:** Uniswap: A leading DEX utilizing the AMM model is Uniswap. Users can swap tokens directly from their wallets by interacting with liquidity pools on Uniswap. This platform offers a user-friendly interface and vast token support, making it a popular choice for traders.



**Choosing the Right Method:**

The choice between order book and AMM methods depends on individual needs and risk tolerance.

* **Order Book:** For users who prioritize transparency and market depth, order book DEXs might be preferable. However, they should be prepared for potentially lower liquidity for certain tokens.
* **AMM:** For users seeking to trade less popular tokens or who value ease of access, AMM-based DEXs offer a compelling alternative. However, they need to be aware of the potential for impermanent loss when providing liquidity.

**Popular DEX Examples:**

Uniswap, SushiSwap, PancakeSwap, Curve DEX etc.



1. **Uniswap**

Uniswap, a leading DEX built on the Ethereum blockchain, utilizes an AMM model. Users can swap tokens directly from their wallets through liquidity pools, with prices determined by an algorithm based on the pool's asset ratios. Uniswap offers a user-friendly interface and supports a vast array of tokens, making it a popular choice for traders.

**Conclusion**

Decentralized exchanges represent a significant advancement in cryptocurrency trading. By empowering users and prioritizing transparency, DEXs are shaping a more democratic and secure financial future. As the technology matures and adoption grows, DEXs are poised to play a vital role in the evolution of the cryptocurrency landscape.