Securing the Network – Incentive

Table of Content

1. Significance of Incentives in Securing Network

- **Decentralization and Security:**

In a decentralized network, there's no single point of control, ensuring that no single entity can manipulate the system. The incentive system is crucial in motivating participants (miners) to maintain and secure this decentralized network.

- **Proof of Work (PoW) and Incentives:**

Bitcoin's security relies on the Proof of Work consensus mechanism. Miners compete to solve complex mathematical problems to validate transactions and add them to the blockchain.

The incentive for miners is the reward for solving these problems. This reward is in the form of newly minted bitcoins and transaction fees from the included transactions.

By investing computational power (electricity and hardware costs) into solving these problems, miners are incentivized to act honestly and compete fairly to earn rewards.

- **Game Theory and Self-Interest:**

Satoshi Nakamoto's brilliance lies in aligning individual self-interest with the network's best interest through economic incentives.

Miners, acting in their own self-interest to earn rewards, collectively contribute to the security of the network. The more miners participating, the more secure the network becomes against attacks.

- **Incentive Alignment and Security:**

The system's security is based on the assumption that most miners are honest. Incentives ensure that it's more profitable for miners to follow the rules (validating transactions honestly) than to attempt attacks.

Any attempt to subvert the network's rules requires an immense amount of computational power, making it economically unfeasible to execute an attack.

- **Long-Term Sustainability and Halving:**

  The Whitepaper addresses the long-term sustainability of the incentive system by introducing the concept of halving the block rewards.

  The block reward halves approximately every four years, reducing the number of new bitcoins entering circulation. This scarcity model is designed to mimic the limited supply of a valuable resource, encouraging value retention.

- **Trustless System and Security:**

  The incentive structure, coupled with cryptographic principles, ensures a trustless system where participants don't need to trust each other. They only need to trust the mathematical principles governing the system.

  This trustless nature, enabled by incentives, contributes to the overall security and reliability of the Bitcoin network.

Incentives in Bitcoin

Incentive Structure

Satoshi Nakamoto introduces a reward system for miners who participate in validating transactions, contributing to the formation of new blocks in the blockchain. Here is how you can earn incentives by participating in network:

- **Incentive for Transaction Validation:**
  Miners play a crucial role in verifying and validating transactions on the Bitcoin network. They gather unconfirmed transactions into blocks and compete to solve complex mathematical puzzles, a process known as mining.
  As miners solve these puzzles and successfully add a block to the blockchain, they are rewarded for their efforts.

- **Block Rewards:**
  The primary incentive for miners is the block reward, which is a predefined amount of newly minted bitcoins assigned to the miner who successfully mines a block.
  In the early days of Bitcoin, this reward started at 50 bitcoins per block. However, the system is designed to halve this reward approximately every four years through a process called "halving."

- **Transaction Fees:**
  In addition to block rewards, miners also receive transaction fees. When users initiate transactions, they can include a fee to incentivize miners to prioritize their transactions. These fees supplement the block reward and serve as an additional incentive for miners.

2. Bitcoins Reward Mechanism

a. Block Reward and Halving Events:

A block reward is a portion of newly minted digital tokens assigned to a user who helps to verify transactions on a blockchain protocol. The users who verify transactions are collectively known miners.

Protocols need to provide incentives for distributed volunteer users to discover new blocks in order to secure the network and ensure it continues to operate. Because no central administrator watches over bitcoin (BTC) and all other cryptocurrencies, block rewards serve as the primary financial incentive for people to participate in the network.

As mentioned, block rewards also serve as the exclusive issuance system for releasing newly minted coins into circulation. These are given to each successful validator that discovers (miner) or proposes (staker) new blocks. Sometimes, these rewards are fixed, meaning the same number of tokens are given as block rewards every time, while others gradually decrease the number of coins given as block rewards over time.

Bitcoin goes through a ‘‘halving‘’ roughly every four years, or 210,000 blocks. This means the block reward given to miners systematically halves over its lifespan. Since the last halving in May 2020, successful miners have been receiving 6.25 BTC for each block discovered, which usually takes approximately 10 minutes.

Bitcoin’s block rewards have halved three times since the protocol launched in 2009 and will continue to halve until the total number of coins in circulation reaches the maximum supply of 21 million coins. After that, no more block rewards and no more new coins will enter circulation.

Halving Impact

In terms of the halving’s broader implications, a lower reward for mining Bitcoin will reduce the amount of money miners may make by adding new transactions to the blockchain. Miner rewards determine the flow of new Bitcoin into circulation.

As a result, halving these payments reduces the influx of new Bitcoin — bringing demand and supply economics into play. While supply drops, demand fluctuates and the price changes.

Bitcoin's inflation rate is also reduced due to the halving event. In crypto, inflation relates to new coins being introduced to the circulating supply. However, Bitcoin is designed to be deflationary, and the halving plays a crucial role in its design.

Bitcoin's inflation rate was 50% in 2011, plummeting to 12% after the 2012 halving and 4–5% in 2016. Currently, Bitcoin has a 1.74% inflation rate. In simple terms, after each halving, the value of Bitcoin increases. Every halving event has historically resulted in a bull run for Bitcoin. The price rises as supply decreases, causing demand to rise. This upward tendency, however, is usually not immediate.

Because of the high cost of electricity used to power the computers that solve the mathematical puzzles, the price of BTC would have to rise significantly for miners to receive half as many coins. Miners will find it challenging to stay competitive if the price does not rise in tandem with the decline in reward.

Miners will need to be as efficient as possible; therefore, a new technology that can generate more hashes per second while consuming less energy and lowering overheads will be in demand.

Furthermore, as countries get involved in Bitcoin, their economies may affect the price. More importantly, the price of Bitcoin is likely to rise due to the increased visibility it is now receiving. The volume of transactions will only increase as more stores, small businesses and institutions start using Bitcoin.

b. Transaction Fees:

A Bitcoin transaction fee is what a user pays to miners to get their transaction included in the blockchain. The more a user pays, the higher the chance their transaction will be picked up immediately as there is only a limited amount of space in each block.

Bitcoin transaction fees are an important income stream for miners alongside the block subsidy. Users who pay transaction fees are contributing to the security of the bitcoin network.

Once a miner has validated a new block, they receive the transaction fees and block subsidy associated with that block. The sum of the transaction fees and block subsidy is the block reward.

With each Bitcoin halving, the block subsidy drops and miners earn less, so transaction fees play a significant role to keep the network secure in the long term.

How are Transaction Fees Determined?

Transaction fees on Bitcoin are mostly determined by two factors:

The "size," or data volume of the transaction.

Users' demand for block space. The faster a user wants their transaction confirmed, the more fees they will be willing to pay (generally).

A block can contain a maximum of 4 MB of data, so there is a limit to how many transactions can be processed in one block. A larger transaction will take up more block data. Thus, larger transactions typically pay higher fees on a per-byte basis.

If you are sending a transaction with the help of a Bitcoin wallet, the wallet should display an option for you to select your fee rate. This fee rate will be calculated in satoshis per unit of data your transaction will consume on the blockchain, abbreviated as sats/vByte. The total fee paid by your transaction will then be this rate multiplied by the size of your transaction.

Historically, transaction fees average between $0.50 - $2.50. But as you can see in the graph below, during periods of high demand for block space, transaction fees have a tendency to spike.

If you wish to have your transaction confirmed immediately, your optimal fee rate may vary depending on the above factors. Best practice in determining an optimal fee rate is to consult your preferred block explorer, like mempool.space. Be aware that fee estimation algorithms are fallible in certain instances; if you need your transaction confirmed ASAP, better to err on the side of caution, and pay a higher fee.

Mathematically, transaction fees are the difference between the amount of bitcoin sent and the amount received.

Conceptually, transaction fees are a reflection of the speed with which a user wants their transaction validated on the blockchain.

Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

c. Economic Model Driving Miners:

- **Self-Interest and Competition:**
  Bitcoin's design is influenced by game theory principles, where individual actors (miners) are rational and act in their own self-interest to maximize their gains.
  Miners compete to add new blocks to the blockchain by solving complex cryptographic puzzles through a process known as mining. This competition is intense, as only one miner can successfully mine a block at a time.

- **Profit Motive:**
  Miners are economically incentivized to act honestly and follow the established consensus rules of the network.
  By adhering to the rules and successfully mining a block, miners are rewarded with block rewards (newly minted bitcoins) and transaction fees from included transactions. Attempting to manipulate the network or engage in malicious activities (such as attempting double spending or invalid transactions) goes against the rules and the protocol. Such actions risk losing the rewards and fees that miners could otherwise claim.

- **Rational Decision Making:**
  Miners weigh the costs of investing in computational power (electricity costs, hardware expenses) against the potential rewards they could earn by participating in the network.

Rational miners choose the path that maximizes their profits. This means dedicating resources to secure the network and validate transactions in accordance with the rules to claim rewards.

- **Network Security and Trust:**
  The economic incentives align with the network's security. Honest participation in mining not only earns rewards but also contributes to the overall security and trust in the network.
  Consistently following the consensus rules and behaving honestly establishes trust among users. Miners, acting in their economic self-interest, collectively uphold the integrity of the network.

- **Economic Rationality vs. Malicious Actions:**
  Any attempt to manipulate the network or break the rules is economically irrational for miners. Such actions would risk losing the rewards and fees they could otherwise claim by following the rules.
  The collective economic rationality of miners reinforces a shared consensus on the rules of the network. Consensus among miners serves as a safeguard against malicious actors, as any attempt to deviate from the rules would be rejected by the network.