

Mining & Proof of Work 🪓



Mining 

Mining Key Points

1. Mining is the process of creating a block of transactions to be added to the **Ethereum blockchain**
2. Peers in the mining process are called “**miners**”
 - a. To network
 - b. Miners provide processing power to network in exchange for chance to get rewarded
3. Mining is just an automated software that people run
 - a. There is no human element to mining except setup + maintenance



Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



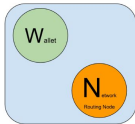
Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.



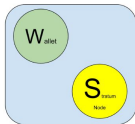
Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.



Mining Nodes

Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.



Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

Mining has *TWO* main functions:

1. **Enforcement of consensus rules** (very important!)
 - a. No double-spending, block size, check all txs
2. **Currency issuance** (not that important!)
 - a. Incentive to those who contribute security to the system

Mining Algorithm

- **Q: When a miner “mines” a block, what does the miner actually do?**
- A: Mining software continuously hashes a block (containing txs) until a hash is found that meets a target difficulty

<https://emn178.github.io/online-tools/sha256.html>

1. Take current block's block header
2. Append a nonce, starting at nonce = 0
3. Hash data from #1 and #2
4. Check hash versus target (provided by protocol)
5. If hash < target, puzzle is solved! Get rewarded.
6. Else, restart process from step #2, but increment nonce



1. **Mining and Proof of Work:**

In a Proof of Work (PoW) consensus mechanism, miners compete to solve a mathematical puzzle based on a given set of data. This data includes the hash of the previous block, the transactions in the current block, and a timestamp. The puzzle is essentially finding a specific input (called a nonce) that, when combined with the data, produces a hash output that meets certain criteria. The criteria are defined by the target difficulty level set by the network.

2. **Target Difficulty and Leading Zeros:**

The target difficulty level is a value that determines how "hard" it is to find a valid nonce that produces a hash below the target value. The target value is inversely proportional to the target difficulty level. The higher the target difficulty level, the lower the target value, and vice versa. The hash output is represented as a hexadecimal number, which means it contains characters from 0 to 9 and A to F. However, from a binary perspective, a hexadecimal digit corresponds to 4 bits. When we say "more leading zeros," it means that the hash output, when converted to binary, starts with more zeros. For example, let's say the target difficulty requires a hash output that starts with 5 leading zeros. In binary, this means the output should start with "00000," which translates to "0000," "0000," "0000," and "0000" in hexadecimal.

3. **Difficulty Adjustment:**

The target difficulty level is adjusted periodically to ensure that new blocks are mined at a consistent rate, usually around every 10 minutes in the case of Bitcoin. The target difficulty level is adjusted every 2016 blocks (approximately every two weeks) by using a formula that compares the actual time taken to mine the last 2016 blocks with the expected time of 10 minutes per block. If miners are finding blocks too quickly, the target difficulty increases, making it harder to find a valid nonce. Conversely, if blocks are being mined too slowly, the target difficulty decreases, making it easier to find a valid nonce.

4. **Mining Process:**

Miners start by selecting a nonce and combining it with the block's data. They then hash this combined data using a cryptographic hash function (e.g., SHA-256 in the case of Bitcoin). The resulting hash output is compared to the target value. If the hash output is below the target value, the miner has found a valid proof of work.

5. **Proof of Work Validity:**

When a miner finds a valid nonce that produces a hash below the target value, they broadcast this solution to the network. Other participants can easily verify the validity of the solution by checking that the hash output meets the target difficulty criteria. This serves as a proof that the miner has performed a certain amount of computational work to find the solution. Once a valid solution is verified and accepted by a majority of nodes, it becomes part of the blockchain and cannot be reversed or modified. The miner who found the solution receives a reward in cryptocurrency (e.g., bitcoin) and transaction fees.

The smaller the target value, the smaller number of possible combinations can satisfy the condition, because the target value sets a limit on how large the hash output can be. The hash output is a hexadecimal number that represents the result of applying a cryptographic function (such as SHA-256) to the block header, which contains information such as the previous block's hash, the transactions in the current block, and a random number called nonce. The nonce is what miners change to try different hash outputs until they find one that is below or equal to the target value.

To illustrate this with an example, let's say the target value is 0000FFFF, which means that any hash output that starts with 0000 and has any combination of digits after that is valid. The hexadecimal digits are 0 to 9 and A to F, so there are 16 possible values for each digit. Therefore, there are 16^4 possible combinations for the first four digits of the hash output, and 16^{28} possible combinations for the remaining 28 digits. The total number of possible combinations that satisfy the condition is $16^4 * 16^{28} = 16^{32}$.



Now, let's say the target value is smaller, such as 00000FFF. This means that any hash output that starts with 00000 and has any combination of digits after that is valid. The number of possible combinations for the first five digits of the hash output is 16^5 , and the number of possible combinations for the remaining 27 digits is 16^{27} . The total number of possible combinations that satisfy the condition is $16^5 * 16^{27} = 16^{32} / 16 = 16^{31}$.

As you can see, by reducing the target value by one hexadecimal digit, we have reduced the number of possible combinations by a factor of 16. This makes it harder to find a valid hash output, because there are fewer options to choose from. The smaller the target value, the more leading zeros are required in the hash output, and the more computational power and luck are needed to find a valid nonce.

Proof of Work

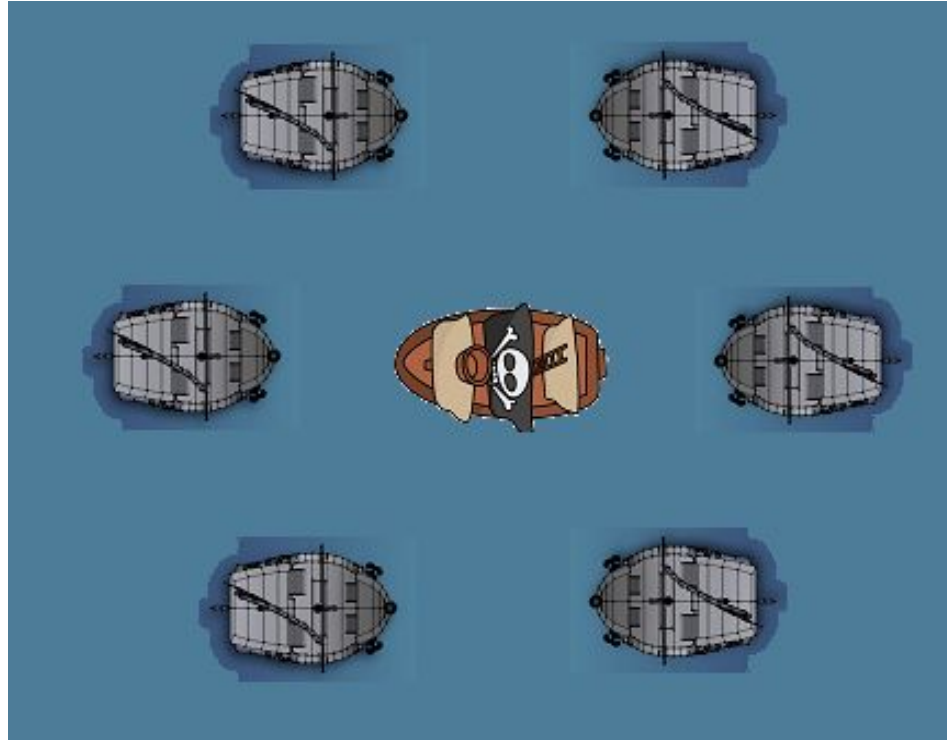


Proof of Work

- A **consensus mechanism** is how decentralized networks like Bitcoin and Ethereum decide what blocks/txs are considered “valid” and who gets to add new blocks to the chain
- **Proof-of-work** and proof-of-stake are two different types of consensus mechanisms
 - Bitcoin uses proof-of-work consensus while Ethereum will transition from PoW to PoS consensus
- In PoW, in order to add a block and receive a reward, a miner must present some type of proof that they spent significant resources securing the network
 - **The proof of work is the solution to the mining process**
-  Repeatedly hashing until we find a hash lower than the target difficulty
 - Miners **compete** to find a valid proof of work every 10 minutes
-  Solves the **Byzantine Generals' Problem**
 - What chain is the “main chain”?

The Byzantine Generals' Problem

- Problem?
 - Coordination in a decentralized environment
- Solution?
 - **Proof of Work Consensus**
- Game Theory
 - Losing Strategy = Traitor Wins
 - Winning Strategy = Consensus



[See Satoshi's write-up on BGP](#)