title: Mining description: An explanation of how mining worked on Ethereum. lang: en

Proof-of-work is no longer underlying Ethereum's consensus mechanism, meaning mining has been switched off. Instead, Ethereum is secured by validators who stake ETH. You can start staking your ETH today. Read more on [The Merge](#), [proof-of-stake](#), and [staking](#). This page is for historical interest only.

Prerequisites {#prerequisites}

To better understand this page, we recommend you first read up on [transactions](#), [blocks](#) and [proof-of-work](#).

What is Ethereum mining? {#what-is-ethereum-mining}

Mining is the process of creating a block of transactions to be added to the Ethereum blockchain in Ethereum's now-deprecated proof-of-work architecture.

The word mining originates in the context of the gold analogy for cryptocurrencies. Gold or precious metals are scarce, so are digital tokens, and the only way to increase the total volume in a proof-of-work system is through mining. In proof-of-work Ethereum, the only mode of issuance was via mining. Unlike gold or precious metals however, Ethereum mining was also the way to secure the network by creating, verifying, publishing and propagating blocks in the blockchain.

Mining ether = Securing the Network

Mining is the lifeblood of any proof-of-work blockchain. Ethereum miners - computers running software - used their time and computation power to process transactions and produce blocks prior to the transition to proof-of-stake.

Why do miners exist? {#why-do-miners-exist}

In decentralized systems like Ethereum, we need to ensure that everyone agrees on the order of transactions. Miners helped this happen by solving computationally difficult puzzles to produce blocks, securing the network from attacks.

[More on proof-of-work](#)

Anyone was previously able to mine on the Ethereum network using their computer. However, not everyone could mine ether (ETH) profitably. In most cases, miners had to purchase dedicated computer hardware, and have access to inexpensive energy sources. The average computer was unlikely to earn enough block rewards to cover the associated costs of mining.

Cost of mining {#cost-of-mining}

- Potential costs of the hardware necessary to build and maintain a mining rig
- Electrical cost of powering the mining rig
- If you were mining in a pool, these pools typically charged a flat % fee of each block generated by the pool
- Potential cost of equipment to support mining rig (ventilation, energy monitoring, electrical wiring, etc.)

To further explore mining profitability, use a mining calculator, such as the one [Etherscan](#) provides.

How Ethereum transactions were mined {#how-ethereum-transactions-were-mined}

The following provides an overview of how transactions were mined in Ethereum proof-of-work. An analogous description of this process for Ethereum proof-of-stake can be found [here](#).

1. A user writes and signs a [transaction](#) request with the private key of some [account](#).
2. The user broadcasts the transaction request to the entire Ethereum network from some [node](#).
3. Upon hearing about the new transaction request, each node in the Ethereum network adds the request to their local

mempool, a list of all transaction requests they've heard about that have not yet been committed to the blockchain in a block.

4. At some point, a mining node aggregates several dozen or hundred transaction requests into a potential block, in a way that maximizes the transaction fees they earn while still staying under the block gas limit. The mining node then:

5. Verifies the validity of each transaction request (i.e. no one is trying to transfer ether out of an account they haven't produced a signature for, the request is not malformed, etc.), and then executes the code of the request, altering the state of their local copy of the EVM. The miner awards the transaction fee for each such transaction request to their own account.

6. Begins the process of producing the proof-of-work "certificate of legitimacy" for the potential block, once all transaction requests in the block have been verified and executed on the local EVM copy.

7. Eventually, a miner will finish producing a certificate for a block which includes our specific transaction request. The miner then broadcasts the completed block, which includes the certificate and a checksum of the claimed new EVM state.

8. Other nodes hear about the new block. They verify the certificate, execute all transactions on the block themselves (including the transaction originally broadcasted by our user), and verify that the checksum of their new EVM state after the execution of all transactions matches the checksum of the state claimed by the miner's block. Only then do these nodes append this block to the tail of their blockchain, and accept the new EVM state as the canonical state.

9. Each node removes all transactions in the new block from their local mempool of unfulfilled transaction requests.

10. New nodes joining the network download all blocks in sequence, including the block containing our transaction of interest. They initialize a local EVM copy (which starts as a blank-state EVM), and then go through the process of executing every transaction in every block on top of their local EVM copy, verifying state checksums at each block along the way.

Every transaction is mined (included in a new block and propagated for the first time) once, but executed and verified by every participant in the process of advancing the canonical EVM state. This highlights one of the central mantras of blockchain: **Don't trust, verify**.

Ommer (uncle) blocks {#ommer-blocks}

Block mining on proof-of-work was probabilistic, meaning sometimes two valid blocks were published simultaneously due to network latency. In this case, the protocol had to determine the longest (and therefore most "valid") chain while ensuring fairness towards miners by partially rewarding the unincluded valid block proposed. This encouraged further decentralization of the network as smaller miners, who might face greater latency, could still generate returns via ommer block rewards.

The term "ommer" is the preferred gender-neutral term for the sibling of a parent block, but this is also sometimes referred to as an "uncle". **Since Ethereum's move to proof-of-stake, ommer blocks are no longer mined** as only one proposer is elected in each slot. You can see this change by viewing the historical chart of the ommer blocks mined.

A visual demo {#a-visual-demo}

Watch Austin walk you through mining and the proof-of-work blockchain.

The mining algorithm {#mining-algorithm}

Ethereum Mainnet only ever used one mining algorithm - 'Ethash'. Ethhash was the successor to an original R&D algorithm known as 'Dagger-Hashimoto'.

More on mining algorithms.

Related topics {#related-topics}

- Gas
- EVM
- Proof-of-work