

# Learn the basics of blockchains and Ethereum (miners and validators, gas, cryptocurrencies and NFTs, block explorer, networks, etc.)

Updated 7 months ago

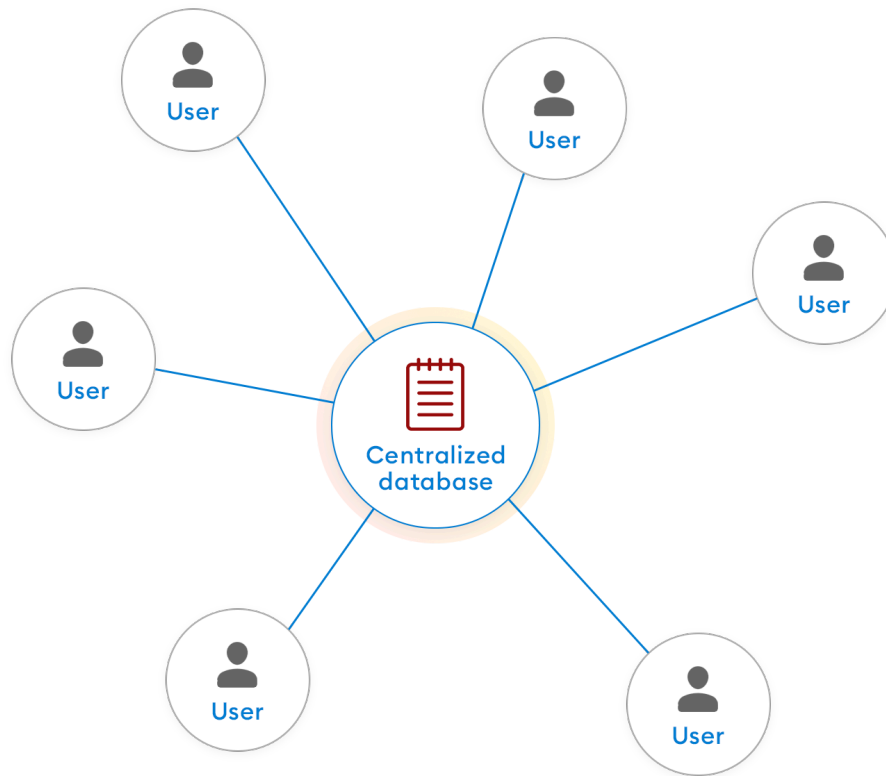
## New to crypto and web3?

Head to [MetaMask Learn](#) for a straightforward learning experience designed specifically for newcomers to web3. It's completely free, available in multiple languages, and includes useful tools such as simulations to help you find your feet with MetaMask.

## What is a blockchain?

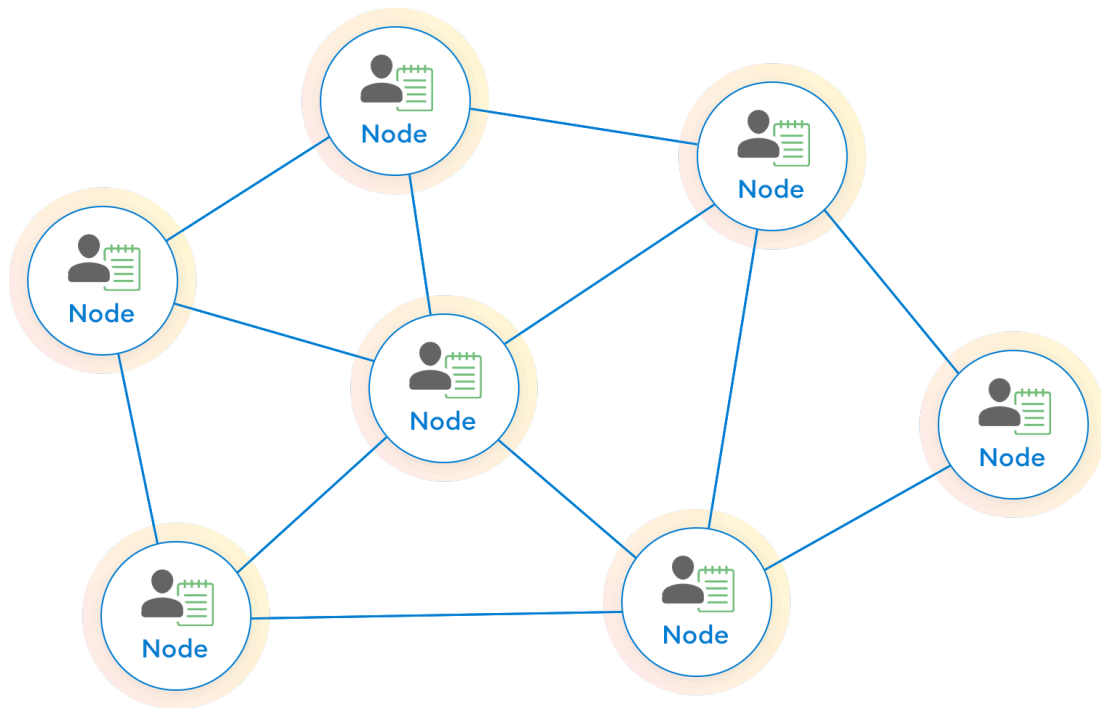
**A blockchain is a type of *distributed ledger technology*. Let's break that down.**

Traditionally, a digital database is kept in a specialized computer called a server. This server would be accessed by people who are granted permission to do so; it could be made public, or private, or somewhere in between, but everyone is accessing that same database—it's ***centralized***.

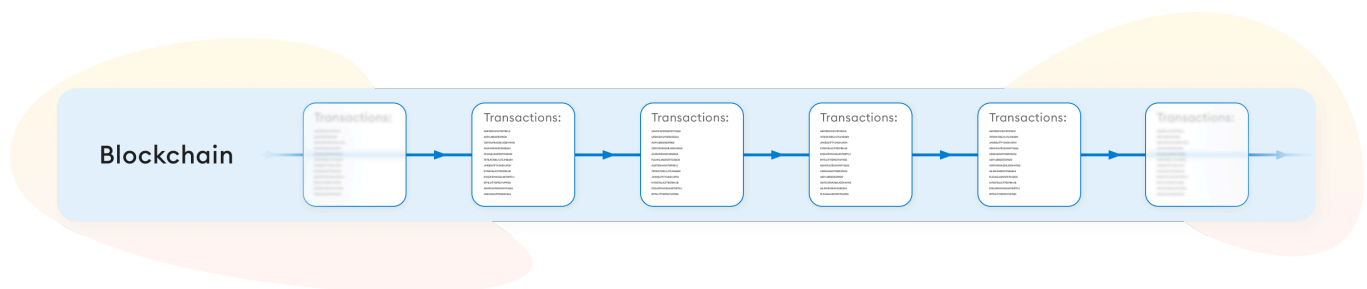


What's more, it's probably controlled by a certain set of people, and at the end of the day, we have to trust that the data is being kept safe and is accurate (and not being used for purposes that go against our own interests!). The downside to this is, of course, what if someone isn't acting in good faith? What if someone hacks the database and changes things, or steals information for their own purposes (or sells it as part of their business model)?

A blockchain—and in particular, a **public blockchain**—is, at its core, a different kind of database. The word *ledger* is used to describe it. Like a ledger, a blockchain is very good at keeping track of assets coming and going, but it can store lots of different kinds of information. However, rather than having this ledger all in one computer (centralized), it's synced across a number of different computers known as **nodes**: it's **decentralized** or, as it's often called, **distributed**.



All of those nodes are constantly syncing information between each other about transactions on the ledger: assets moving from one *address*, or account, on the network to another. These transactions are checked against the ledger's history to ensure that they're valid. Once enough nodes have verified a new transaction, it gets confirmed and becomes *final*. After a certain amount of time, or every certain number of transactions, the network will bundle up all those finalized transactions and seal them, using cryptographic software tools, into a **block**. This block is identified with a *hash* produced by those cryptographic tools: this encrypts details about the block into a long hexadecimal number. The next block will use the previous block's hash as a starting point, and so the entire history of the ledger, and therefore of the network, is linked together in a *chain of blocks* containing *transactions*: **the blockchain**.



# What is Ethereum?

**Ethereum** is a public blockchain network with a vast vision. Ethereum's designers realized that if you built a public blockchain network, you could do a lot more than just track digital currency: you could run a **global public computer**, always available and open to the world. And that's what Ethereum is: it's a global network that is capable of running programs on the **Ethereum Virtual Machine**, or **EVM**. Programs are written for the EVM in a language called **Solidity**, and the network uses a cryptocurrency, called **ether** (or **ETH**, pronounced "eeth") to compensate the people that maintain the network—and also as a token of value for transactions carried out on the network.

## So, how do you coordinate all that?

As mentioned previously, an essential function of a blockchain network is coordinating the process of agreement between all the nodes in the network regarding whether a transaction is valid or not. The agreement is referred to as *consensus*, and the process by which it occurs is called a **consensus mechanism**, or *consensus protocol*. Two different consensus mechanisms are relevant for Ethereum, the first being **Proof of Work (PoW)** and the second **Proof of Stake (PoS)**. PoW was replaced by PoS on Ethereum mainnet in 2022.

In both mechanisms, computers are provided to do the work of verifying the validity of the transactions, and agreeing on them.

## What are miners? And is a validator the same thing?

Under **PoW consensus**, actors known as '**miners**' carry the responsibility of verifying the transactions, creating the blocks, and maintaining the chain. In exchange, these miners are given a reward (in ETH) each time their node is the first to finalize, or mine, a new block; this also incentivizes miners having good-quality equipment and connection speeds, which in turn helps the network.

However, there exists the possibility for enough miners to band together—at least 51% of the network—and subvert control of the network to their own ends, rewriting the transaction history, stealing tokens, etc. In order to prevent this and other security problems, the mining is made intentionally difficult, that is, computationally complex

(often called "expensive") in order to make it virtually impossible for any rogue actor(s) to carry out a so-called '51% attack'.

This design—made to keep the network safe—has side effects, in particular environmental and real-world economic ones; the economic model on the blockchain is also inefficient. The constant incentive to mine blocks faster means that miners have a real motivation to buy new computers, even specialized ones that do nothing other than mine on blockchains. And big, powerful computers use a lot of electricity, and generate a lot of heat. This environmentally-unfriendly, inefficient arms race is difficult to justify, on a number of points.

Enter **PoS consensus**: instead of miners, **validators** are the actors ensuring transaction validity and network integrity. In place of costly number-crunching as a security measure, each validator must have **staked** 32 ETH; that is, deposited it in a **smart contract**, a kind of computer program that lives on the Ethereum blockchain, with the promise that they will operate their validator according to the rules. If they act in bad faith, or try to subvert or attack the network, or just don't maintain enough connectivity, their staked currency will be **slashed**, or taken from them. If they do what they're supposed to do, maintain connectivity and confirm transactions, they will be rewarded with ETH, the same as miners. For more on PoS, see [here](#).

## PoS vs. PoW: which does Ethereum use?

Ethereum currently uses PoS, which means the mainnet (i.e. the current single blockchain in use) relies on special nodes called validators to create and confirm the validity of blocks, and also to secure the ongoing integrity of the network. Ethereum switched from PoW to PoS on September 15, 2022, representing a reduction in a 99% reduction in energy expenditure.

## What is gas, and why do I have to use it?

*Gas* is the unit of measure for how much computational work is required to process transactions and smart contracts on the Ethereum Virtual Machine (EVM). More complex smart contracts, and code, will require more gas to execute, in the same way that a bigger, more powerful car takes more gas to run.

Calculating gas used to be very complicated, but as of the implementation of Ethereum Improvement Protocol (EIP) 1559 on August 4, 2021, it was greatly simplified.

Essentially, you pay a **base fee** for every unit of gas, which is **burned**, or disappears, upon successful completion of the transaction. On top of the base fee, you add a **priority fee**, again per unit of gas, the value of which depends on how quickly you want the transaction to go through.

Here are some essential details for dealing with gas in **MetaMask**:

## The gas limit

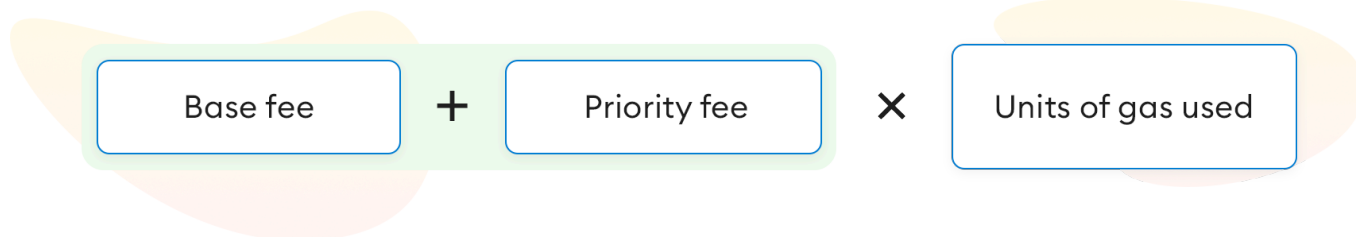
The *gas limit* is the **maximum number of units of gas you are willing to pay for** in order to carry out a transaction or EVM operation. A standard transaction sending ETH normally costs **21,000 gas**.

## The max priority fee

The *max priority fee*, also referred to as the "miner tip", goes to the miner or validator, and incentivizes them to prioritize your transaction. Most often, the value you put in for "max priority fee" will be the amount you pay.

## The max fee

The max fee is the total, global amount paid for your transaction. It is calculated as: **(base fee + priority fee) x units of gas used**. The difference between max fee per gas and base fee + max priority fee per gas is "refunded" to the user.



Want to know more about gas? Start [here](#).

## Tokens

Aside from ether, the *native currency* of the Ethereum network, there are two main types of tokens that get used on Ethereum: [ERC-20](#), which are "fungible" tokens and correspond to what people call "**cryptocurrencies**", and [ERC-721](#) and [ERC-1155](#), the "non-fungible tokens", the origin of the acronym [NFT](#).

The difference between the two is, of course, highly technical, but it boils down to the difference in the name. ERC-20 tokens are designed specifically to be fully interchangeable and liquid, the way a traditional fiat currency is. Like a dollar, for example, every single ERC-20 token of the same type has the exact same value: this is what "fungible" means.

ERC-721 and ERC-1155 tokens, on the other hand, are specifically designed to be unique and non-replicable, but of course can be transferred between parties, [often for significant value](#). ERC-721 is the *OG* NFT standard on Ethereum, and provides a blueprint for "minting" (creating) one-off, distinct NFTs. ERC-1155 came a little later, and standardizes a way for minting multiple NFTs (and indeed fungible tokens) simultaneously.

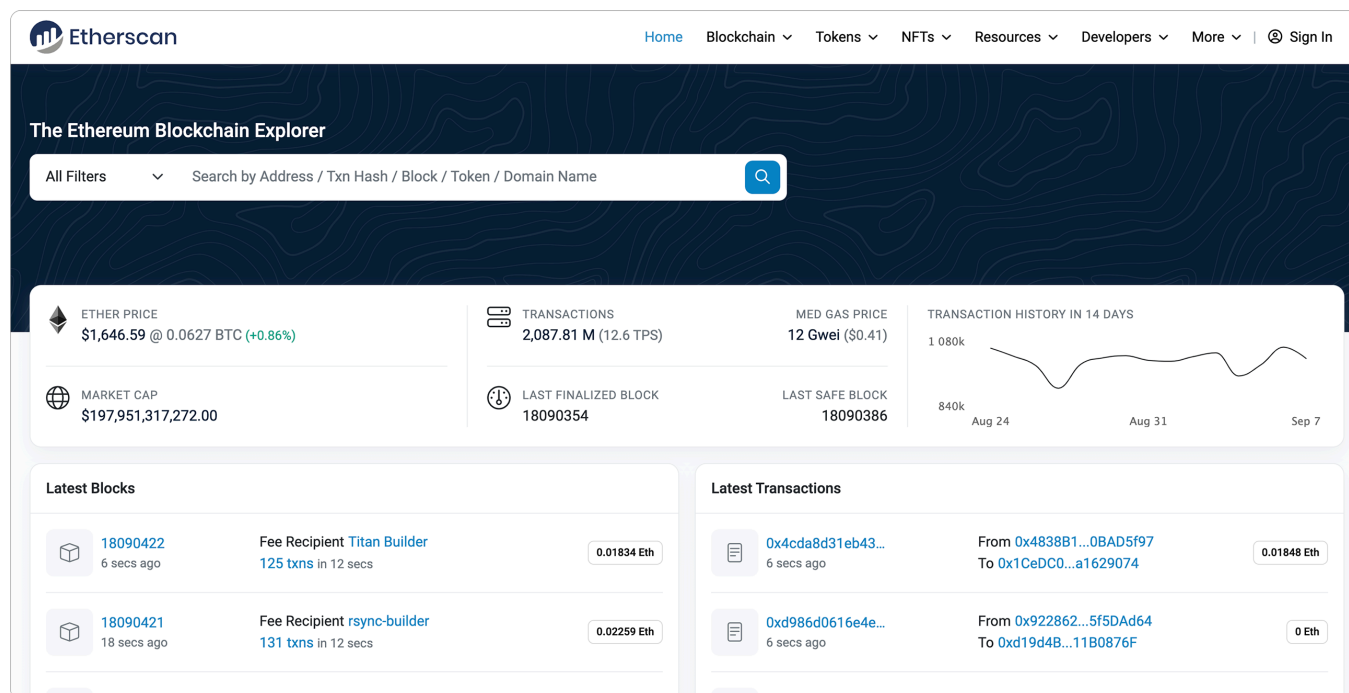
## How do I access Ethereum?

Because a blockchain network is a separate network, different and distinct from traditional Internet connections, specific software is necessary to access the network and show the data being recorded on the blockchain. This is possible through an Ethereum *client*, which is standalone software, often command-line interface only, and is the tool of choice for many developers. Additionally, the Ethereum community has developed a number of resources that allow connections between the traditional Internet and the Ethereum network.

The backbone of these efforts has been [MetaMask](#), a trailblazing browser plugin and mobile app that provides users with a custodial (user-controlled and owned) Ethereum wallet and access to *dapps*, or decentralized apps, that allow you to interact with the Ethereum blockchain.

## What is a block explorer?

When you want to go deeper and see details of individual transactions or take a bird's eye view of the Ethereum network, a block explorer is required. A block explorer is a website that provides an interface to navigate and examine the information contained on the network. Prominent examples include [Etherscan](#) and [Ethplorer](#), and other networks related to Ethereum ("EVM-compatible") have their own variants.



## Ethereum mainnet, testnets, sidechains and the rest

As you venture forth into the decentralized web, or **Web3** as it's often called, you will learn that Ethereum is, in fact, not just one network. The Ethereum blockchain and the EVM live and operate on the *Ethereum mainnet*, and there exist a number of *testnets* for Ethereum that are exactly what they sound like, sandboxed versions of the mainnet where ETH has no real value except to test out applications.

That's just the beginning, though; there are many Ethereum-compatible *sidechains* that have been developed, offering users the option to carry out transactions on a separate blockchain, in that chain's native currency, in order to avoid the sometimes-costly EVM and Ethereum mainnet transaction fees. Some of these chains are designed specifically for a use case, such as a video game or DeFi; others are general-purpose "scaling networks", called Layer 2s or L2s, for the purpose of increasing the volume and capacity of Ethereum.

Users often end up with tokens and NFTs on these sidechains that they can bring back onto Ethereum mainnet through [bridges](#); the NFTs can be kept, displayed, sold on marketplaces; the tokens can be swapped for others, redeemed for ETH, staked, borrowed, lent, used in other dapps, transferred to other sidechains and used in videogames, or [videogame-investment engine hybrids](#), or, well... the future is still being written.