

# **Ethereum Overview**

### What is Ethereum?



Ethereum is a futuristic, open-source blockchain network for Decentralized Applications (DApps), powered by smart contracts and combined with digital native currency Ether (ETH). On Ethereum, code can be written to monitor digital value transfer, depending on programmable conditions.

Ethereum was designed to build on the primary role of Bitcoin as a centralized Peer-to-Peer (P2P) currency. It is achieved by introducing a network capable enough to implement smart contracts and more complex systems, such as DApps and DAOs."

| Asset                | Ether (ETH)   |
|----------------------|---|
| Inception of Network | July 30, 2015   |
| Price (USD)          | \$264.14  |
| Market Cap (USD)     | \$29.5 Billion  |
| Average Block Time   | Approx. 13 Seconds  |
| Market Segment       | Digital Currency Smart Contracts General-Purpose Platform |

# Bitcoin Vs Ethereum



| Basis of<br>Comparison | Bitcoin                                     | Ethereum  |
|------------------------|---|---|
| Ticker                 | втс   | ETH   |
| Founder                | Satoshi Nakamoto (Unknown)                  | Vitalik Buterin & Team  |
| Smallest Unit          | 1 Satoshi = 0.00000001 BTC                  | 1 Wei = 0.000000000000000001 ETH                                  |
| Max Supply             | 21,000,000                                  | No Fixed Supply   |
| Block Reward           | 6.25 BTC<br>(Halving after 2,10,000 Blocks) | 2 ETH   |
| Miners Fees            | Collects Transaction Fees                   | Collects Gas Fees   |
| Consensus Algorithm    | POW   | POW (Will be shifted to POS soon)                                 |
| Purpose                | Be a Global Decentralized<br>Payment System | Be a Decentralized supercomputer to power DApps around the world. |

## Proof-of-Work Vs Proof-of-Stake



### **Proof of Work**



Mining capacity depends on computational power



Miners receive block rewards to solve a cryptographic puzzle



Hackers would need to have a computer powerful than 51% of the network to add a malicious block, leading to 51& attack

### **Proof of Stake**

Validating capacity depends on the stake in the network



Validators do not receive a block reward, instead they collect transaction fees as reward



Hackers would need to own 51% off all the cryptocurrency on the network, which is practically impossible and therefore, making 51% attacks impossible



# Ethereum Virtual Machine (EVM)



The Ethereum Virtual Machine (EVM) is an efficient, virtualized computing stack embedded within every full Ethereum node which is responsible for executing bytecode contract. Contracts are usually written in high-level languages, such as Solidity, and then compiled into EVM bytecode.

Each node in the Ethereum network executes an instance on Ethereum Virtual Machine (EVM) that allows them to agree on the same instruction. The EVM is Turing complete, which means they can execute every logical step of the computational process.

Ethereum Virtual Machine is successfully implemented in different programming languages like C++, Java, JavaScript, Python, Ruby, and several others.

Dr. Gavin Wood developed the EVM in 2014 and outlined the theoretical version in the original Ethereum yellow paper, which is similar to the whitepaper.

### What is Ether?



Ether is the alternative to the traditional payment issue — a digital asset-bearer such as a bond or other security. Just like cash, it does not require the processing or approval of transactions by third parties. This can be used as fuel for the applications on the open Ethereum network, according to ethereum.org.

This gives the nodes the opportunity to verify blocks on the Ethereum network containing the smart contract code. Each time a block is validated, it generates 2 Ethers and assigns them to the successful node.

Maximum Ether supply isn't capped like total bitcoin supply.



### Wei Vs Ether



Wei is the smallest Ether denomination, the coin used on the Ethereum network for crypto-currency.

1 Ether = 1,000,000,000,000,000 Wei (1018)

Wei is named after Wei Dai, an activist in cryptography, considered in promoting the popular use of powerful cryptography and privacy-oriented technology.

| Unit              | Wei Value | Wei                       |
|-------------------|-----------|---------------------------|
| Wei               | 1 wei     | 1                         |
| Kwei(babbage)     | 1e3 wei   | 1,000                     |
| Mwei(lovelace)    | 1e6 wei   | 1,000,000                 |
| Gwei(shannon)     | 1e9 wei   | 1,000,000,000             |
| Microether(szabo) | 1e12 wei  | 1,000,000,000,000         |
| Millether(finney) | 1e15 wei  | 1,000,000,000,000,000     |
| Ether             | 1e18 wei  | 1,000,000,000,000,000,000 |

# **Ethereum Mining**



Ethereum Mining is a computationally rigorous work that requires a substantial amount of time and computing power. A miner gets paid with Ether to provide solutions to difficult math problems, much like bitcoin mining.

There are three ways in which Ether can be mined:

### Pool mining

The simplest and cheapest way to get started is by pool mining. All the people who mine in a single pool agree to the term that they're going to share rewards with others if one of them finds the correct answer to the puzzle.

### Mining alone

Mining by itself might sound like a great idea. You don't have the rewards to share. Mining by itself is only profitable if you have a lot of money at your disposal.

#### Cloud mining

If you use cloud mining, you pay someone else to mine for you. In this type of mining you hire other people's mining time, and in exchange, they give you all the rewards they mine.

### **Smart Contract**



A smart contract is a self-execution contract whereby the terms of the settlement between buyer and seller are translated directly into the code. The code and the contracts it comprises operate through a network of distributed, decentralized blockchains. The code governs the execution of the contract.



A contract between the parties is written as code and published into the blockchain. Individuals involved are anonymous, but the contract is visible in a public ledger.



A triggering event like an expiration date or strike price is hit, and the contract executed itself according to the coded terms.



Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions.

# Transaction, Gas & Fees



#### • Transaction:

Transactions are signed messages produced, distributed, and registered on the Ethereum blockchain, by an externally owned account.

To be legitimate, every transaction needs to go through a method of authentication known as mining.

#### Gas:

Gas is the method used to calculate the fees needed for a particular computation.

Gas price is the amount of Ether that the customer is willing to pay on each gas unit.

#### Transaction Fee:

Transaction Fee = Gas price X Gas limit