



**101 Blockchains**



# Ethereum

101 Blockchains Flashcards

Get familiar with common Ethereum terms with the Ethereum flashcards, and broaden your knowledge as an Ethereum developer.

## 1. Ethereum

Ethereum is an open-source blockchain platform that helps developers write smart contracts. It is also the ideal choice for developing and deploying decentralized applications or dApps. Ethereum uses its native token, Ether, as payments for miners, transaction fees, and other network services. The Ethereum Virtual Machine, or EVM, on Ethereum is capable of running on the Ethereum network, alongside enabling any individual to run any blockchain application with ease.

## 2. 51% Attack

51% attack refers to the specific type of attack on a decentralized network, in which a particular group gets control over the majority of nodes in the network, or 51% of computational power. This new model of attack can help them in carrying out fraud transactions through reversal of transactions. In addition, it can also be responsible for double-spending of ether as well as other tokens.

## 3. Computational Infeasibility

Computational infeasibility refers to a process that can take unreasonably long durations of time. This is particularly applicable in the case of anyone who might be looking for the execution of a task immediately. Computational infeasibility is quite important for cryptography in Ethereum. Mostly, around 280 computational steps, could be easily considered as the lower bound for facilitating computational infeasibility. It can promote the immutability aspect of blockchain.

## 4. Encryption

Encryption refers to the process through which a specific document or plaintext combines with a shorter string of data, referred to as a key. The outcome of the encryption process is known as ciphertext. It is possible to decrypt the ciphertext again to obtain the original plaintext. However, the key is important to unlocking the ciphertext. Individuals without the key would find it computationally difficult to decrypt an encrypted message.

## 5. Public Key Encryption

Public key encryption is one of the most common encryption techniques. It involves the process of generating two keys simultaneously. The two keys are referred to as private keys and public keys. One of the keys helps in encrypting the documents, while the other helps in decrypting the message. As the name suggests, individuals could publish their public keys openly, and maintain their private keys in secrecy for public-key encryption.

## 6. Account

An account in the case of Ethereum refers to the object which contains address, nonce, balance, as well as optional storage and code. In other words, an Ethereum account refers to the entity that has ETH or Ether balance and could transmit transactions on Ethereum. The accounts in Ethereum could be controlled by users with private keys. On the other hand, users could also deploy Ethereum accounts as smart contracts.

## 7. Address

Address is the representation of the EOA (Externally Owned Account) or contract, which could receive or send transactions on the blockchain. The EOA, or contract in this case, could serve as the destination address or the source address on the blockchain. The more accurate description of the address on Ethereum refers to the 160 bits on the extreme right side of a Keccak hash that's related to an ECDSA public key.

## 8. Beacon Chain

The Beacon Chain refers to an Eth2 upgrade that also serves as coordinator in the case of the Ethereum network. The Beacon Chain is quite significant for introducing proof-of-stake, as well as validators to the Ethereum landscape. Over the course of time, it will be melded with the mainnet. It helps in conducting or coordinating the massively wide network of stakers and shards. Beacon chain could not handle smart contracts.

## 9. Shard

A shard or shard chain is the proof-of-stake chain under the coordination of the Beacon Chain, along with the security of validators that enable Ethereum scalability. According to the Eth2 shard chain upgrade, it would include the addition of 64 shards to the network. Shard chains can provide better transaction throughput for Ethereum through the facility of additional data to layer 2 solutions such as ZK-rollups and optimistic rollups.

## 10. Rollups

Rollups are basically a specific variant of layer 2 scaling solutions for batching multiple transactions and submitting them to the Ethereum main chain during a specific transaction. Rollups help in reducing the costs of gas alongside improving transaction throughput. The two distinct types of rollups include zero-knowledge rollups and optimistic rollups. Both types of rollups use unique security approaches for ensuring access to desired scalability improvement that boosts capacity.

## 11. Gas

Gas is a fundamental requirement for different operations on the Ethereum network. It is basically the virtual fuel implemented in Ethereum for executing smart contracts. The Ethereum Virtual Machine, or EVM, employs a special accounting mechanism for monitoring the consumption of gas. In addition, EVM also works productively to impose restrictions on the consumption of different computing resources. Gas is just like the fuel you need to operate on the Ethereum blockchain.

## 12. Ethereum Virtual Machine

Ethereum Virtual Machine, or EVM, is the stack-based virtual machine that executes bytecode. The execution model is a significant element in Ethereum for specifying the approaches for modification in system state with a specific set of bytecode instructions. In addition, the execution model also considers a small tuple of environmental data for executing bytecode. A formal model for a virtual state machine helps in specifying the instructions and tuple.

## 13. Ethash

Ethash is a renowned proof-of-work for Ethereum 1.0, and the proof-of-work protocol implies that miners have to go through a process of trial and error to find the nonce for a specific block. Generally, blocks having a valid nonce are only eligible for addition to the chain. Miners should find the numeric solution for the Ethash algorithm and ensure that their solution fulfills a difficult target set for the whole network.

## 14. Staking

Beacon Chain introduces proof-of-stake in the case of Ethereum as a new approach for maintaining the security of Ethereum. It is basically aimed for the general good, ensuring that the Ethereum landscape becomes stronger and helping users earn more ETH during the process. The process of staking basically involves placing your ETH as stakes for activating validator software. Users could process transactions alongside creating new blocks in their validator role.

## 15. Compiling

The conversion of code scripted in a high-level programming language such as Solidity into a lower-level language such as EVM bytecode is known as compiling. Compilation of a smart contract is necessary to ensure that your web app, as well as the Ethereum Virtual Machine, has the capability to understand it. The compiler would also generate an Application Binary Interface, or ABI, needed for understanding contracts and calling contract functions.

## 16. Decentralized Exchange

Decentralized Exchange or DEX is basically another type of decentralized application which enables users to swap tokens with their peers on the decentralized network. Users could require Ether for using a Decentralized Exchange, primarily for paying the transaction fees. However, DEXs don't have any geographical limitations like in the case of centralized exchanges. Therefore, Decentralized Exchanges encourage almost any individual to participate. As open marketplaces, they connect sellers and buyers directly.

## 17. Miner

Miner is the network node that is responsible for finding a valid proof-of-work for new blocks, achieved through consistent pass hashing. Miners in an Ethereum network basically point out to the computers running Ethereum by directing computation power and time for processing transactions, and producing blocks. Miners are important for Ethereum as they ensure agreement on the order of transactions. The process of mining generally involves solving computationally tough puzzles.

## 18. Network

With reference to the Ethereum network, a network could be considered as a peer-to-peer network involved in propagation of transactions alongside blocks to each Ethereum node. Networks are generally the unique Ethereum environments you could access for different use cases involving developing, testing, and starting production. An Ethereum account could function seamlessly throughout different networks. In addition, users must be aware of network availability for testing purposes in Ethereum environments.

## 19. Mainnet

Mainnet is the basic public Ethereum production blockchain. Public networks are easily accessible to any individual in the world with a simple internet connection. Any individual could read the transactions on a public blockchain and create their own transactions and validate them accordingly. Consensus among peers is essential for validating the agreements on transactions followed by the state of the network. Mainnet is the platform for execution of actual-value ETH transactions.

## 20. Testnets

Public testnets are also important networks in the functioning of Ethereum alongside the mainnet. Testnets basically refer to the networks leveraged by protocol developers, or smart contract developers, for testing protocol upgrades. In addition, they also play a crucial role in testing potential smart contracts before deployment in a production-like environment. Testnets serve as the perfect alternative to production versus staging servers, and are important for testing any contract code.

## 21. ERC-721

ERC-721 is a unique standard for non-fungible tokens or NFTs. NFTs are unique and could have different values other than a token from the same smart contract. The NFTs enjoy uniqueness on the grounds of rarity, age, and visuals. In the case of any ERC-721 contract, the pair of contract addresses and the uint256 tokenId, should be unique in all cases. ERC-721 standard can encourage the widespread adoption of NFTs.

## 22. Difficulty

Difficulty is one of the basic terms that you would come across in Ethereum. It is basically the reference to a network-wide setting that helps in controlling the computation power required for production of proof-of-work. In addition, difficulty is also associated with difficulty bomb in Ethereum. The difficulty bomb points out a predefined exponential growth in configuration of proof-of-work difficulty. Difficulty bomb encourages the shift to proof-of-stake, thereby reducing forking.

## 23. Ethereum Improvement Proposal

Ethereum Improvement Proposal, or EIP, is a design document that offers information to the Ethereum community with a detailed description of proposed new features or the associated processes and environment. EIPs are basically the standards with specifications for potential new features or processes that could be included in Ethereum. EIPs include technical specifications for proposed changes alongside serving as the 'source of truth' for the Ethereum community and supporting upgrades and standards.

## 24. Ether

The fundamental cryptocurrency of the Ethereum ecosystem, Ether, or ETH, is mandatory to compensate for gas costs during the execution of transactions. Ether is the foundation element of Ethereum and is important for sending ETH or using an Ethereum application. Users have to pay the transaction fee as an incentive to miners for their work in processing and verifying the user's transactions. Ether can be used for different applications seamlessly.

## 25. Event

Event is a unique feature in Ethereum that helps you to communicate with your smart contract from the front end, as well as other subscribing applications. When mining a transaction, smart contracts could emit events alongside writing logs to the blockchain which could be subject to processing by the frontend. Events are also important for the use of EVM logging facilities. Decentralized apps could use events for triggering callbacks.

## 26. Functions

Functions are important components of smart contracts and crucial for their functionality. In the basic sense, functions could receive information or configure information in accordance with incoming transactions. The two common types of function calls in Ethereum smart contracts include internal and external function calls. Internal function calls don't result in an EVM call, while external functional calls create an EVM call. Functions could also be private or public accordingly.

## 27. Fraud Proof

Fraud Proof is a unique security model meant for specific layer 2 solutions. It is applicable in case of solutions where transactions are bundled up in batches before submission to Ethereum for increased speed. Even if they are assumed as valid transactions, any suspicion of fraud could be a good cause to challenge the transactions. Running fraud-proof helps in finding out whether a fraud has actually taken place.

## 28. HD Wallet

HD Wallet in Ethereum is a wallet that leverages the hierarchical deterministic (HD) protocol for creation and transformation of keys. It depends on the HD wallet seed, the value that helps in generating the master private key, alongside the master chain code. The wallet seed offers the flexibility for representation in the form of mnemonic words. Therefore, it ensures ease of copying, backup, and restoring private keys.

## 29. Inter-Exchange Client Address Protocol (ICAP)

ICAP is the Ethereum address encoding that supports partial compatibility with the International Bank Account Number or IBAN encoding. As a result, it can present a versatile, interoperable, and checksummed encoding for Ethereum addresses. Interestingly, ICAP addresses depend on a new IBAN pseudo-country code, XE. The meaning of the code implies that it is 'extended Ethereum.' The pseudo-country code is the same as you can find in non-jurisdictional currency examples.



# 101 Blockchains

**101 Blockchains is the world's leading research-based platform built for Enterprise Blockchain Professionals, with a thriving community of over 25,000 professionals.**

**101 Blockchains offers world-class training courses and industry-recognized certification programs that are helping professionals all over the world upgrade their skills and accelerate their career growth.**

**Check out our collection of [101 Blockchains Flashcards](#). Gain further knowledge about blockchain technology with in-depth [guides and blogs](#). Find world-class [professional training courses](#).**

*101 Blockchains Ltd © 2021. All rights reserved. This document may not be distributed, transmitted or reproduced in any form or by any means without 101 Blockchains' prior written permission. While the information contained in this document has been obtained from sources believed to be reliable, 101 Blockchains disclaims all warranties as to the completeness or accuracy. Although 101 Blockchains research may address business, financial, investment and legal issues, 101 Blockchains does not provide any business, financial, legal or investment advice and this document should not be construed or used as such. 101 Blockchains shall not be responsible for any loss sustained by any person who relies on this publication.*