Quick Glossary

This quick glossary contains many of the terms used in relation to Ethereum. These terms are used throughout the book, so bookmark this for quick reference.

Account

An object containing an address, balance, nonce, and optional storage and code. An account can be a contract account or an externally owned account (EOA).

Address

Most generally, this represents an EOA or contract that can receive (destination address) or send (source address) transactions on the blockchain. More specifically, it is the rightmost 160 bits of a Keccak hash of an ECDSA public key.

Assert

In Solidity, assert(false) compiles to 0xfe, an invalid opcode, which uses up all remaining gas and reverts all changes. When an assert() statement fails, something very wrong and unexpected is happening, and you will need to fix your code. You should use assert() to avoid conditions that should never, ever occur.

Big-endian

A positional number representation where the most significant digit is first. The opposite of little-endian, where the least significant digit is first.

BIPs

Bitcoin Improvement Proposals. A set of proposals that members of the Bitcoin community have submitted to improve Bitcoin. For example, BIP-21 is a proposal to improve the Bitcoin uniform resource identifier (URI) scheme.

Block

A collection of required information (a block header) about the comprised transactions, and a set of other block headers known as ommers. Blocks are added to the Ethereum network by miners.

Blockchain

In Ethereum, a sequence of blocks validated by the proof-of-work system, each linking to its predecessor all the way to the genesis block. This varies from the Bitcoin protocol in that it does not have a block size limit; it instead uses varying gas limits.

Bytecode

An abstract instruction set designed for efficient execution by a software interpreter or a virtual machine. Unlike human-readable source code, bytecode is expressed in numeric format.

Byzantium fork

The first of two hard forks for the Metropolis development stage. It included EIP-649: Metropolis Difficulty Bomb Delay and Block Reward Reduction, where the Ice Age (see below) was delayed by 1 year and the block reward was reduced from 5 to 3 ether.

Compiling

Converting code written in a high-level programming language (e.g., Solidity) into a lower-level language (e.g., EVM bytecode).

Consensus

When numerous nodes—usually most nodes on the network—all have the same blocks in their locally validated best blockchain. Not to be confused with consensus rules.

Consensus rules

The block validation rules that full nodes follow to stay in consensus with other nodes. Not to be confused with consensus.

Constantinople fork

The second part of the Metropolis stage, originally planned for mid-2018. Expected to include a switch to a hybrid proof-of-work/proof-of-stake consensus algorithm, among other changes.

Contract account

An account containing code that executes whenever it receives a transaction from another account (EOA or contract).

Contract creation transaction

A special transaction, with the "zero address" as the recipient, that is used to register a contract and record it on the Ethereum blockchain (see "zero address").

DAO

Decentralized Autonomous Organization. A company or other organization that operates without hierarchical management. Also may refer to a contract named "The DAO" launched on April 30, 2016, which was then hacked in June 2016; this ultimately motivated a hard fork (codenamed DAO) at block #1,192,000, which reversed the hacked DAO contract and caused Ethereum and Ethereum Classic to split into two competing systems.

DApp

Decentralized application. At a minimum, it is a smart contract and a web user interface. More broadly, a DApp is a web application that is built on top of open, decentralized, peer-to-peer infrastructure services. In addition, many DApps include decentralized storage and/or a message protocol and platform.

Deed

Non-fungible token (NFT) standard introduced by the ERC721 proposal. Unlike ERC20 tokens, deeds prove ownership and are not interchangeable, though they are not recognized as legal documents in any jurisdiction—at least not currently (see also "NFT").

Difficulty

A network-wide setting that controls how much computation is required to produce a proof of work.

Digital signature

A short string of data a user produces for a document using a private key such that anyone with

the corresponding public key, the signature, and the document can verify that (1) the document was "signed" by the owner of that particular private key, and (2) the document was not changed after it was signed.

ECDSA

Elliptic Curve Digital Signature Algorithm. A cryptographic algorithm used by Ethereum to ensure that funds can only be spent by their owners.

EIP

Ethereum Improvement Proposal. A design document providing information to the Ethereum community, describing a proposed new feature or its processes or environment. For more information, see https://github.com/ethereum/EIPs (see also "ERC").

ENS

Ethereum Name Service. For more information, see https://github.com/ethereum/ens/.

Entropy

In the context of cryptography, lack of predictability or level of randomness. When generating secret information, such as private keys, algorithms usually rely on a source of high entropy to ensure the output is unpredictable.

EOA

Externally Owned Account. An account created by or for human users of the Ethereum network.

ERC

Ethereum Request for Comments. A label given to some EIPs that attempt to define a specific standard of Ethereum usage.

Ethash

A proof-of-work algorithm for Ethereum 1.0. For more information, see https://github.com/ethereum/wiki/wiki/Ethash.

Ether

The native cryptocurrency used by the Ethereum ecosystem, which covers gas costs when executing smart contracts. Its symbol is Ξ, the Greek uppercase Xi character.

Event

Allows the use of EVM logging facilities. DApps can listen for events and use them to trigger JavaScript callbacks in the user interface. For more information, see http://solidity.readthedocs.io/en/develop/contracts.html#events.

EVM

Ethereum Virtual Machine. A stack-based virtual machine that executes bytecode. In Ethereum, the execution model specifies how the system state is altered given a series of bytecode instructions and a small tuple of environmental data. This is specified through a formal model of a virtual state machine.

EVM assembly language

A human-readable form of EVM bytecode.

Fallback function

A default function called in the absence of data or a declared function name.

Faucet

A service that dispenses funds in the form of free test ether that can be used on a testnet.

Finney

A denomination of ether. 1 finney = 10^{15} wei, 10^{3} finney = 1 ether.

Fork

A change in protocol causing the creation of an alternative chain, or a temporal divergence in two potential block paths during mining.

Frontier

The initial test development stage of Ethereum, which lasted from July 2015 to March 2016.

Ganache

A personal Ethereum blockchain that you can use to run tests, execute commands, and inspect state while controlling how the chain operates.

Gas

A virtual fuel used in Ethereum to execute smart contracts. The EVM uses an accounting mechanism to measure the consumption of gas and limit the consumption of computing resources (see "Turing complete").

Gas limit

The maximum amount of gas a transaction or block may consume.

Gavin Wood

A British programmer who is the cofounder and former CTO of Ethereum. In August 2014 he proposed Solidity, a contract-oriented programming language for writing smart contracts.

Genesis block

The first block in a blockchain, used to initialize a particular network and its cryptocurrency.

Geth

Go Ethereum. One of the most prominent implementations of the Ethereum protocol, written in Go.

Hard fork

A permanent divergence in the blockchain; also known as a hard-forking change. One commonly occurs when nonupgraded nodes can’t validate blocks created by upgraded nodes that follow newer consensus rules. Not to be confused with a fork, soft fork, software fork, or Git fork.

Hash

A fixed-length fingerprint of variable-size input, produced by a hash function.

HD wallet

A wallet using the hierarchical deterministic (HD) key creation and transfer protocol (BIP-32).

HD wallet seed

A value used to generate the master private key and master chain code for an HD wallet. The wallet seed can be represented by mnemonic words, making it easier for humans to copy, back up, and restore private keys.

Homestead

The second development stage of Ethereum, launched in March 2016 at block #1,150,000.

ICAP

Inter-exchange Client Address Protocol. An Ethereum address encoding that is partly compatible with the International Bank Account Number (IBAN) encoding, offering a versatile, checksummed, and interoperable encoding for Ethereum addresses. ICAP addresses use a new IBAN pseudo-country code: XE, standing for "eXtended Ethereum," as used in nonjurisdictional currencies (e.g., XBT, XRP, XCP).

Ice Age

A hard fork of Ethereum at block #200,000 to introduce an exponential difficulty increase (aka Difficulty Bomb), motivating a transition to proof of stake.

IDE

Integrated Development Environment. A user interface that typically combines a code editor, compiler, runtime, and debugger.

Immutable deployed code problem

Once a contract's (or library's) code is deployed, it becomes immutable. Standard software development practices rely on being able to fix possible bugs and add new features, so this represents a challenge for smart contract development.

Internal transaction (also "message")

A transaction sent from a contract account to another contract account or an EOA.

IPFS

InterPlanetary File System. A protocol, network, and open source project designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed filesystem.

KDF

Key Derivation Function. Also known as a "password stretching algorithm," it is used by keystore formats to protect against brute-force, dictionary, and rainbow table attacks on passphrase encryption, by repeatedly hashing the passphrase.

Keccak-256

Cryptographic hash function used in Ethereum. Keccak-256 was standardized as SHA-3.

Keystore file

A JSON-encoded file that contains a single (randomly generated) private key, encrypted by a passphrase for extra security.

LevelDB

An open source on-disk key–value store, implemented as a lightweight, single-purpose library, with bindings to many platforms.

Library

A special type of contract that has no payable functions, no fallback function, and no data storage. Therefore, it cannot receive or hold ether, or store data. A library serves as previously deployed code that other contracts can call for read-only computation.

Lightweight client

An Ethereum client that does not store a local copy of the blockchain, or validate blocks and transactions. It offers the functions of a wallet and can create and broadcast transactions.

Merkle Patricia Tree

A data structure used in Ethereum to efficiently store key–value pairs.

Message

An internal transaction that is never serialized and only sent within the EVM.

Message call

The act of passing a message from one account to another. If the destination account is associated with EVM code, then the VM will be started with the state of that object and the message acted upon.

METoken

Mastering Ethereum Token. An ERC20 token used for demonstration in this book.

Metropolis

The third development stage of Ethereum, launched in October 2017.

Miner

A network node that finds valid proof of work for new blocks, by repeated hashing.

Mist

The first Ethereum-enabled browser, built by the Ethereum Foundation. It contains a browser-based wallet that was the first implementation of the ERC20 token standard (Fabian Vogelsteller, author of ERC20, was also the main developer of Mist). Mist was also the first wallet to introduce the camelCase checksum (EIP-55; see [EIP55]). Mist runs a full node and offers a full DApp browser with support for Swarm-based storage and ENS addresses.

Network

Referring to the Ethereum network, a peer-to-peer network that propagates transactions and blocks to every Ethereum node (network participant).

NFT

A non-fungible token (also known as a "deed"). This is a token standard introduced by the ERC721 proposal. NFTs can be tracked and traded, but each token is unique and distinct; they are not interchangeable like ERC20 tokens. NFTs can represent ownership of digital or physical assets.

Node

A software client that participates in the network.

Nonce

In cryptography, a value that can only be used once. There are two types of nonce used in Ethereum: an account nonce is a transaction counter in each account, which is used to prevent replay attacks; a proof-of-work nonce is the random value in a block that was used to satisfy the proof of work.

Ommer

A child block of an ancestor that is not itself an ancestor. When a miner finds a valid block, another miner may have published a competing block which is added to the tip of the blockchain. Unlike with Bitcoin, orphaned blocks in Ethereum can be included by newer blocks as ommers and receive a partial block reward. 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."

Parity

One of the most prominent interoperable implementations of the Ethereum client software.

Private key

See “secret key.”

Proof of stake (PoS)

A method by which a cryptocurrency blockchain protocol aims to achieve distributed consensus. PoS asks users to prove ownership of a certain amount of cryptocurrency (their "stake" in the network) in order to be able to participate in the validation of transactions.

Proof of work (PoW)

A piece of data (the proof) that requires significant computation to find. In Ethereum, miners must find a numeric solution to the Ethash algorithm that meets a network-wide difficulty target.

Public key

A number, derived via a one-way function from a private key, which can be shared publicly and used by anyone to verify a digital signature made with the corresponding private key.

Receipt

Data returned by an Ethereum client to represent the result of a particular transaction,

including a hash of the transaction, its block number, the amount of gas used, and, in case of deployment of a smart contract, the address of the contract.

Re-entrancy attack

An attack that consists of an attacker contract calling a victim contract function in such a way that during execution the victim calls the attacker contract again, recursively. This can result, for example, in the theft of funds by skipping parts of the victim contract that update balances or count withdrawal amounts.

Reward

An amount of ether included in each new block as a reward by the network to the miner who found the proof-of-work solution.

RLP

Recursive Length Prefix. An encoding standard designed by the Ethereum developers to encode and serialize objects (data structures) of arbitrary complexity and length.

Satoshi Nakamoto

The name used by the person or people who designed Bitcoin, created its original reference implementation, and were the first to solve the double-spend problem for digital currency. Their real identity remains unknown.

Secret key (aka private key)

The secret number that allows Ethereum users to prove ownership of an account or contracts, by producing a digital signature (see “public key,” “address,” “ECDSA”).

Serenity

The fourth and final development stage of Ethereum. Serenity does not yet have a planned release date.

Serpent

A procedural (imperative) smart contract programming language with syntax similar to Python.

SHA

Secure Hash Algorithm. A family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST).

Singleton

A computer programming term that describes an object of which only a single instance can exist.

Smart contract

A program that executes on the Ethereum computing infrastructure.

Solidity

A procedural (imperative) programming language with syntax that is similar to JavaScript, C++, or Java. The most popular and most frequently used language for Ethereum smart contracts. Created by Dr. Gavin Wood (coauthor of this book).

Solidity inline assembly

EVM assembly language in a Solidity program. Solidity's support for inline assembly makes it easier to write certain operations.

Spurious Dragon

A hard fork of the Ethereum blockchain, which occurred at block #2,675,000 to address more denial-of-service attack vectors and clear state (see also "Tangerine Whistle"). Also, a replay attack protection mechanism.

Swarm

A decentralized (P2P) storage network, used along with Web3 and Whisper to build DApps.

Szabo

A denomination of ether. 1 szabo = 10^{12} wei, 10^{6} szabo = 1 ether.

Tangerine Whistle

A hard fork of the Ethereum blockchain, which occurred at block #2,463,000 to change the gas calculation for certain I/O-intensive operations and to clear the accumulated state from a denial-of-service attack, which exploited the low gas cost of those operations.

Testnet

Short for "test network," a network used to simulate the behavior of the main Ethereum network.

Transaction

Data committed to the Ethereum Blockchain signed by an originating account, targeting a specific address. The transaction contains metadata such as the gas limit for that transaction.

Truffle

One of the most commonly used Ethereum development frameworks.

Turing complete

A concept named after English mathematician and computer scientist Alan Turing: a system of data-manipulation rules (such as a computer's instruction set, a programming language, or a cellular automaton) is said to be "Turing complete" or "computationally universal" if it can be used to simulate any Turing machine.

Vitalik Buterin

A Russian–Canadian programmer and writer primarily known as the cofounder of Ethereum and of *Bitcoin Magazine*.

Vyper

A high-level programming language, similar to Serpent, with Python-like syntax. Intended to get closer to a pure functional language. Created by Vitalik Buterin.

Wallet

Software that holds secret keys. Used to access and control Ethereum accounts and interact with smart contracts. Keys need not be stored in a wallet, and can instead be retrieved from offline

storage (e.g., a memory card or paper) for improved security. Despite the name, wallets never store the actual coins or tokens.

Web3

The third version of the web. First proposed by Dr. Gavin Wood, Web3 represents a new vision and focus for web applications: from centrally owned and managed applications, to applications built on decentralized protocols.

Wei

The smallest denomination of ether. 10^{18} wei = 1 ether.

Whisper

A decentralized (P2P) messaging service. It is used along with Web3 and Swarm to build DApps.

Zero address

A special Ethereum address, composed entirely of zeros, that is specified as the destination address of a contract creation transaction.