Glossary

Ð

Ð, D with stroke, is used in Old English, Middle English, Icelandic, and Faroese to stand for an uppercase letter “Eth”. It is used in words like ÐEV or Ðapp (decentralized application), where the Ð is the Norse letter “eth”. The uppercase eth (Ð) is also used to symbolize the cryptocurrency Dogecoin.

decentralized application (= dapp)

Service that operates without a central trusted party. An application that enables direct interaction/agreements/communication between end users and/or resources without a middleman. See Dapps.

DAO

decentralized autonomous organization DAO is type of contract on the blockchain (or a suite of contracts) that is supposed to codify, enforce or automate the workings of an organization including governance, fund-raising, operations, spending and expansion.

identity

A set of cryptographically verifiable interactions that have the property that they were all created by the same person.

digital identity

The set of cryptographically verifiable transactions signed by the same public key define the digital identity's behavior. In many real world scenarios (voting) it is desireable that digital identities coincide with real world identities. Ensuring this without violence is an unsolved problem.

unique identity

A set of cryptographically verifiable interactions that have the property that they were all created by the same person, with the added constraint that one person cannot have multiple unique identities.

reputation

The property of an identity that other entities believe that identity to be either (1) competent at some specific task, or (2) trustworthy in some context, i.e., not likely to betray others even if short-term profitable.

escrow

If two mutually-untrusting entities are engaged in commerce, they may wish to pass funds through a mutually trusted third party and instruct that party to send the funds to the payee only when evidence of product delivery has been shown. This reduces the risk of the payer or payee committing fraud. Both this construction and the third party is called escrow.

deposit

Digital property placed into a contract involving another party such that if certain conditions are not satisfied that property is automatically forfeited and either credited to a counterparty as insurance against the conditions, or destroyed (= burnt = equally distributed) or donated to some charitable funds.

web of trust

The idea that if A highly rates B, and B highly rates C, then A is likely to trust C. Complicated and powerful mechanisms for determining the reliability of specific individuals in specific concepts can theoretically be gathered from this principle.

incentive compatibility

A protocol is incentive-compatible if everyone is better off "following the rules" than attempting to cheat, at least unless a very large number of people agree to cheat together at the same time (collusion).

collusion

In an incentivized protocol scenario, when a number of participants *play together* (conspire) to game the rules to their own benefit.

token system

A fungible virtual good that can be traded. More formally, a token system is a database mapping addresses to numbers with the property that the primary allowed operation is a transfer of N tokens from A to B, with the conditions that N is non-negative, N is not greater than A's current balance, and a document authorizing the transfer is digitally signed by A. Secondary "issuance" and "consumption" operations may also exist, transaction fees may also be collected, and simultaneous multi-transfers with many parties may be possible. Typical use cases include currencies, cryptographic tokens inside of networks, company shares and digital gift cards.

block

A block is a package of data that contains zero or more transactions, the hash of the previous block ("parent"), and optionally other data. The total set of blocks, with every block except for the initial "genesis block" containing the hash of its parent, is called the blockchain and contains the entire transaction history of a network. Note that some blockchain-based cryptocurrencies use the word "ledger" instead of blockchain; the two are roughly equivalent, although in systems that use the term "ledger" each block generally contains a full copy of the current state (e.g. currency balances, partially fulfilled contracts, registrations) of every account allowing users to discard outdated historical data.

dapp

Đapp Stands for "decentralized application". Some say it is pronounced Ethapp due to the use of the uppercase eth letter Đ.

address

An Ethereum address represents an account. For EOA, the address is derived as the last 20 bytes of the public key controlling the account, e.g., `cd2a3d9f938e13cd947ec05abc7fe734df8dd826`. This is a hexadecimal format (base 16 notation), which is often indicated explicitly by appending `0x` to the address. Web3.js and console functions accept addresses with or without this prefix but for transparency we encourage their use. Since each byte of the address is represented by 2 hex characters, a prefixed address is 42 characters long. Several apps and APIs are also meant to implement the new checksum-enabled address scheme introduced in the Mist Ethereum wallet as of version 0.5.0.

hexadecimal

Common representation format for byte sequencing. Its advantage is that values are represented in a compact format using two characters per byte (the characters `[0-9][a-f]`).

ether

Ether is the name of the currency used within Ethereum. It is used to pay for computations within the EVM. Ambiguously, ether is also the name of a unit in the system;

EOA

Externally Owned Account. An account controlled by a private key. If you own the private key associated with the EOA you have the ability to send ether and messages from it. Contract accounts also have an address, see Accounts. EOAs and contract accounts may be combined into a single account type during Serenity.

gas

Name for the *cryptofuel* that is consumed when code is executed by the EVM. The gas is paid for execution fee for every operation made on an Ethereum blockchain.

gas limit

Gas limit can apply to both individual transactions, see transaction gas limit and to blocks, *block-gas-limit*. For individual transactions, the gas limit represents the maximum amount of gas you indicate you are willing to pay for a contract execution transaction. It is meant to protect users from getting their ether depleted when trying to execute buggy or malicious contracts. The block gas limit represents the maximum cumulative gas used for all the transactions in a block. With the launch of Homestead, the block gas limit floor will increase from 3,141,592 gas to 4,712,388 gas (~50% increase).

gas price

Price in ether of one unit of gas specified in a transaction. With the launch of Homestead, the default gas price reduces from 50 shannon to 20 shannon (~60% reduction).

transaction

The signed data package that stores a message to be sent from an externally owned account. Simply put, a transaction describes a transfer of information from an EOA to another EOA or a contract account.

message

A data transfer mechanism contracts use to communicate with other contracts. Messages can also be described as virtual objects that are never serialized and exist only in the Ethereum execution environment.

Web3

The exact definition of the Web3 paradigm is still taking form, but it generally refers to the phenomenon of increased connectedness between all kinds of devices, decentralization of services and applications, semantic storage of information online and application of artificial intelligence to the web.

DAO

See Decentralized Autonomous Organization.

epoch

Epoch is the interval between each regeneration of the DAG used as seed by the PoW algorithm Ethash. The epoch in specified as 30000 blocks.

elliptic curve (cryptography)

Refers to an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. See elliptic curve cryptography.

wallet

A wallet, in the most generic sense, refers to anything that can store ether or any other crypto token. In the crypto space in general, the term wallet is used to mean anything from a single private/public key pair (like a single paper wallet) all the way to applications that manage multiple key pairs, like the Mist Ethereum wallet.

contract

A persistent piece of code on the Ethereum blockchain that encompasses a set of data and executable functions. These functions execute when Ethereum transactions are made to them with certain input parameters. Based on the input parameters, the functions will execute and interact with data within and outside of the contract.

suicide

See self-destruct. `selfdestruct` acts as an alias to the deprecated `suicide` terminology in accordance with EIP 6 - Renaming SUICIDE OPCODE.

selfdestruct

A global variable in the Solidity language that allows you to "destroy the current contract, sending its funds to the given address". `selfdestruct` acts as an alias to the deprecated `suicide` terminology in accordance with EIP 6 - Renaming SUICIDE OPCODE. It frees up space on the blockchain and prevents future execution of the contract. The contract's address will still persist, but ether sent to it will be lost forever. The possibility to kill a contract has to be implemented by the contract creator him/herself using the Solidity `selfdestruct` function.

transaction fee

Also known as gas cost, it is the amount of ether that the miners will charge for the execution of your transaction.

mining

The process of verifying transactions and contract execution on the Ethereum blockchain in exchange for a reward in ether with the mining of every block.

mining pool

The pooling of resources by miners, who share their processing power over a network, to split the reward equally, according to the amount of work they contributed to solving a block.

mining reward

The amount of cryptographic tokens (in this case ether) that is given to the miner who mined a new block.

state

Refers to a snapshot of all balances and data at a particular point in time on the blockchain, normally referring to the condition at a particular block.

blockchain

An ever-extending series of data blocks that grows as new transactions are confirmed as part of a new block. Each new block is chained to the existing blockchain by a cryptographic proof-of-work.

peer

Other computers on the network also running an Ethereum node (Geth) with an exact copy of the blockchain that you have.

signing

Producing a piece of data from the data to be signed using your private key, to prove that the data originates from you.

discovery (peer)

The process of 'gossiping' with other nodes in the network to find out the state of other nodes on the network.

gas price oracle

A helper function of the Geth client that tries to find an appropriate default gas price when sending transactions.

light client
: A client program that allows users in low-capacity environments to still be able to execute and check the execution of transactions without needing to run a full Ethereum node (Geth).

etherbase
: It is the default name of the account on your node that acts as your primary account. If you do mining, mining rewards will be credited to this account.

coinbase
: Coinbase is analogous to etherbase, but is a more generic term for all cryptocurrency platforms.

balance
: The amount of cryptocurrency (in this case) belonging to an account.

solidity
: Solidity is a high-level language whose syntax is similar to that of JavaScript and it is designed to compile to code for the Ethereum Virtual Machine.

serpent
: Serpent is a high-level language whose syntax is similar to that of Python and it is designed to compile to code for the Ethereum Virtual Machine.

EVM
: Ethereum Virtual Machine, the decentralized computing platform which forms the core of the Ethereum platform.

virtual machine
: In computing, it refers to an emulation of a particular computer system.

peer to peer network
: A network of computers that are collectively able to perform functionalities normally only possible with centralized, server-based services.

decentralization
: The concept of moving the control and execution of computational processes away from a central entity.

distributed hash table
: A distributed hash table (DHT) is a class of a decentralized distributed system that provides a lookup service similar to a hash table: (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key.

NAT
: Network address translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

nonce

Number Used Once or Number Once. A nonce, in information technology, is a number generated for a specific use, such as session authentication. Typically, a nonce is some value that varies with time, although a very large random number is sometimes used. In general usage, nonce means “for the immediate occasion” or “for now.” In the case of Blockchain Proof of Work scenarios, the hash value, found by a Miner, matching the network’s Difficulty thus proving the Block Validity is called Nonce as well.

proof-of-work

Often seen in its abbreviated form “PoW”, it refers to a mathematical value that can act as the proof of having solved a resource and time consuming computational problem.

proof-of-stake

An alternative method of mining blocks that require miners to demonstrate their possession of a certain amount of the currency of the network in question. This works on the principle that miners will be disincentivized to try to undermine a network in which they have a stake. PoS is less wasteful than PoW, but is still often used together with it to provide added security to the network.

CASPER

Casper is a security-deposit based economic consensus protocol. This means that nodes, so called “bonded validators”, have to place a security deposit (an action we call “bonding”) in order to serve the consensus by producing blocks. If a validator produces anything that Casper considers “invalid”, the deposit is forfeited along with the privilege of participating in the consensus process.

consensus

The agreement among all nodes in the network about the state of the Ethereum network.

homestead

Homestead is the second major version release of the Ethereum platform. Homestead includes several protocol changes and a networking change that makes possible further network upgrades: EIP-2 Main homestead hardfork changes; EIP-7 Hardfork EVM update (DELEGATECALL); EIP-8 devp2p forward compatibility. Homestead will launch when block 1,150,000 is reached on the Mainnet. On the Testnet, Homestead will launch at block 494,000.

metropolis

The third stage of Ethereum’s release. This is the stage when the user interfaces come out (e.g. Mist), including a dapp store, and non-technical users should feel comfortable joining at this point.

serenity

The fourth stage of Ethereum’s release. This is when things are going to get fancy: the network is going to change its mining process from Proof-of-Work to Proof-of-Stake.

frontier

Ethereum was planned to be released in four major steps with Frontier being the name for the first phase. The Frontier release went live on July 30th, 2015. The command line Frontier phase was mainly meant to get mining operations going with the full reward of 5 ether per block and also to promote the emergence of ether exchanges. Frontier surpassed earlier modest expectations and has nurtured tremendous growth of the ecosystem.

olympic
The Frontier pre-release, which launched on May 9th 2015. It was meant for developers to help test the limits of the Ethereum blockchain.

morden
Morden is the first Ethereum alternative testnet. It is expected to continue throughout the Frontier and Homestead era.

testnet
A mirror network of the production Ethereum network that is meant for testing. See Morden.

private chain
A fully private blockchain is a blockchain where write permissions are kept centralized to one organization.

consortium chain
A blockchain where the consensus process is controlled by a pre-selected set of nodes.

micropayment
A micropayment is a financial transaction involving a very small sum of money (<1 USD) and usually one that occurs online.

sharding
The splitting of the space of possible accounts (contracts are accounts too) into subspaces, for example, based on first digits of their numerical addresses. This allows for contract executions to be executed within 'shards' instead of network wide, allowing for faster transactions and greater scalability.

hash
A cryptographic function which takes an input (or 'message') and returns a fixed-size alphanumeric string, which is called the hash value (sometimes called a message digest, a digital fingerprint, a digest or a checksum). A hash function (or hash algorithm) is a process by which a document (i.e. a piece of data or file) is processed into a small piece of data (usually 32 bytes) which looks completely random, and from which no meaningful data can be recovered about the document, but which has the important property that the result of hashing one particular document is always the same. Additionally, it is crucially important that it is computationally infeasible to find two documents that have the same hash. Generally, changing even one letter in a document will completely randomize the hash; for example, the SHA3 hash of "Saturday" is `c38bbc8e93c09f6ed3fe39b5135da91ad1a99d397ef16948606cdcbd14929f9d`, whereas

the SHA3 hash of “Caturday” is `b4013c0eed56d5a0b448b02ec1d10dd18c1b3832068fbbdc65b98fa9b14b6dbf`. Hashes are usually used as a way of creating a globally agreed-upon identifier for a particular document that cannot be forged.

crypto-fuel
Similar to ‘gas’, referring to the amount of cryptocurrency required to power a transaction.

cryptoeconomics
The economics of cryptocurrencies.

protocol
A standard used to define a method of exchanging data over a computer network.

block validation
The checking of the coherence of the cryptographic signature of the block with the history stored in the entire blockchain.

blocktime
The average time interval between the mining of two blocks.

network hashrate
The number of hash calculations the network can make per second collectively.

hashrate
The number of hash calculations made per second.

serialization
The process of converting a data structure into a sequence of bytes. Ethereum internally uses an encoding format called recursive-length prefix encoding (RLP), described in the RLP section of the wiki.

double spend
A deliberate blockchain fork, where a user with a large amount of mining power sends a transaction to purchase some produce, then after receiving the product creates another transaction sending the same coins to themselves. The attacker then creates a block, at the same level as the block containing the original transaction but containing the second transaction instead, and starts mining on the fork. If the attacker has more than 50% of all mining power, the double spend is guaranteed to succeed eventually at any block depth. Below 50%, there is some probability of success, but it is usually only substantial at a depth up to about 2-5; for this reason, most cryptocurrency exchanges, gambling sites and financial services wait until six blocks have been produced (“six confirmations”) before accepting a payment.

SPV client
A client that downloads only a small part of the blockchain, allowing users of low-power or low-storage hardware like smartphones and laptops to maintain almost the same guarantee of security by sometimes selectively downloading small parts of the

state without needing to spend megabytes of bandwidth and gigabytes of storage on full blockchain validation and maintenance. See light client.

uncle

Uncles are blockchain blocks found by a miner, when a different miner has already found another block for the corresponding place in the blockchain. They are called “stale blocks”. The parent of an Uncle is an ancestor of the inserting block, located at the tip of the blockchain. In contrast to the Bitcoin network, Ethereum rewards stale blocks as well in order to avoid to penalize miners with a bad connection to the network. This is less critical in the Bitcoin network, because the Block Time there is much higher (~10 minutes) than on the Ethereum network (aimed to ~15 seconds).

GHOST

Greedy Heaviest-Observed Sub-Tree is an alternative chain-selection method that is designed to incentivize stale blocks (uncles) as well, thus reducing the incentive for pool mining. In GHOST, even the confirmation given by stale blocks to previous blocks are considered valid, and the miners of the stale blocks are also rewarded with a mining reward.

merkle patricia tree

Merkle Patricia trees provide a cryptographically authenticated data structure that can be used to store all (key, value) bindings. They are fully deterministic, meaning that a Patricia tree with the same (key,value) bindings is guaranteed to be exactly the same down to the last byte and therefore have the same root hash, provide O(log(n)) efficiency for inserts, lookups and deletes, and are much easier to understand and code than more complex comparison-based alternatives like red-black trees.

DAG

DAG stands for Directed Acyclic Graph. It is a graph, a set of nodes and links between nodes, that has very special properties. Ethereum uses a DAG in Ethash, the Ethereum Proof of Work (POW) algorithm.The Ethash DAG takes a long time to be generated, which is done by a Miner node into a cache file for each Epoch. The file data is then used when a value from this graph is required by the algorithm.

uncle rate

The number of uncles produced per block.

issuance

The minting and granting of new cryptocurrency to a miner who has found a new block.

presale

Sale of cryptocurrency before the actual launch of the network.

static node

A feature supported by Geth, the Golang Ethereum client, which makes it possible to always connect to specific peers. Static nodes are re-connected on disconnects. For details, see the section on static nodes.

bootnode
: The nodes which can be used to initiate the discovery process when running a node. The endpoints of these nodes are recorded in the Ethereum source code.

exchange
: An online marketplace which facilitates the exchange of crypto or fiat currencies based on the market exchange rate.

compiler
: A program that translates pieces of code written in high level languages into low level executable code.

genesis block
: The first block in a blockchain.

network id
: A number which identifies a particular version of the Ethereum network.

block header
: The data in a block which is unique to its content and the circumstances in which it was created. It includes the hash of the previous block's header, the version of the software the block is mined with, the timestamp and the merkle root hash of the contents of the block.

pending transaction
: A transaction that is not yet confirmed by the Ethereum network.

block propagation
: The process of transmitting a confirmed block to all other nodes in the network.

sidechain
: A blockchain that branches off a main blockchain and checks in periodically with the main blockchain. Besides that it runs independently from the main chain, and any security compromises in the sidechain will not affect the main chain.

pegging
: Locking down the exchange rate of the coins/tokens in two chains (usually a main and a side chain) in a certain direction.

2-way pegging
: Locking down the exchange rate of the coins/tokens in two chains (usually a main and a side chain) in both directions.

trustless
: Refers to the ability of a network to trustworthily mediate transactions without any of the involved parties needing to trust anyone else.

faucet
: A website that dispenses (normally testnet) cryptocurrencies for free.

checksum

A count of the number of bits in a transmission that is included with the unit so that the receiving end can verify that the entirety of the message has been transmitted.

ICAP

Interexchange Client Address Protocol, an IBAN-compatible system for referencing and transacting to client accounts aimed to streamline the process of transferring funds, worry-free between exchanges and, ultimately, making KYC and AML concerns a thing of the past.

private key

A private key is a string of characters known only to the owner, that is paired with a public key to set off algorithms for text encryption and decryption.

public key

A string of characters derived from a private key that can be made public. The public key can be used to verify the authenticity of any signature created using the private key.

encryption

Encryption is the conversion of electronic data into a form unreadable by anyone except the owner of the correct decryption key. It can further be described as a process by which a document (plaintext) is combined with a shorter string of data, called a key (e.g. `c85ef7d79691fe79573b1a7064c19c1a9819ebdbd1faaab1a8ec92344438aaf4`), to produce an output (ciphertext) which can be "decrypted" back into the original plaintext by someone else who has the key, but which is incomprehensible and computationally infeasible to decrypt for anyone who does not have the key.

digital signature

A mathematical scheme for demonstrating the authenticity of a digital message or documents.

port

A network port is a communication endpoint used by a one of the existing standards of establishing a network conversation (e.g. TCP, UDP).

RPC

Remote Procedure Call, a protocol that a program uses to request a service from a program located in another computer in a network without having to understand the network details.

IPC

Interprocess communication (IPC) is a set of programming interfaces that allow a programmer to coordinate activities among different program processes that can run concurrently in an operating system.

attach

The command used to initiate the Ethereum Javascript console.

daemon

A computer program that runs as a background process instead of in direct control by an interactive user.

system service
See base layer service

base layer service
Services such as SWARM and Whisper which are built into the Ethereum platform.

js
Javascript.

syncing
The process of downloading the entire blockchain.

fast sync
Instead of processing the entire block-chain one link at a time, and replay all transactions that ever happened in history, fast syncing downloads the transaction receipts along the blocks, and pulls an entire recent state database.

ASIC
Application-specific integrated circuit, in this case referring to an integrated circuit custom built for cryptocurrency mining.

memory-hard
Memory hard functions are processes that experience a drastic decrease in speed or feasibility when the amount of available memory even slightly decreases.

keyfile
Every account's private key/address pair exists as a single keyfile. These are JSON text files which contains the encrypted private key of the account, which can only be decrypted with the password entered during account creation.

ICAP format
The format of the IBANs defined using the Inter-exchange Client Address Protocol.

block(chain) explorer
A website that allows easy searching and extraction of data from the blockchain.

geth
Ethereum client implemented in the Golang programming language, based on the protocol as defined in the Ethereum Yellow Paper.

eth
Ethereum client implemented in the C++ programming language, based on the protocol as defined in the Ethereum Yellow Paper.

ethereumjs
Ethereum client implemented in the Javascript/Node programming language, based on the protocol as defined in the Ethereum Yellow Paper.

pyethereum

Ethereum client implemented in the Python programming language, based on the protocol as defined in the Ethereum Yellow Paper.

ethereumj
Ethereum client implemented in the Java programming language, based on the protocol as defined in the Ethereum Yellow Paper.

ethereumh
Ethereum client implemented in the Haskell programming language, based on the protocol as defined in the Ethereum Yellow Paper.

parity
Ethereum client implemented in the Rust programming language, based on the protocol as defined in the Ethereum Yellow Paper.

difficulty
In very general terms, the amount of effort required to mine a new block. With the launch of Homestead, the difficulty adjustment algorithm will change.

account
Accounts are a central part of the Ethereum network and are an essential part of any transaction or contract. In Ethereum, there are two types of accounts: Externally Owned accounts (EOA) and Contract accounts.

HLL (obsolete)
Acronym for Higher Level Language, which is what Serpent and Solidity are. HLL is what early Đapp developers called Ethereum programming languages that did not touch the low level elements. This phrase has been phased out.

CLL (obsolete)
Acronym for C Like Language, which Mutan was. This acronym has been phased out.

ES1, ES2, and ES3 (obsolete)
"Ethereum Script" versions 1,2 and 3. There were early versions of what would become the Ethereum Virtual Machine (EVM).

log event
Contracts are triggered by transactions executed as part of the block verification. If conceived of as a function call, contract execution is asynchronous, and therefore they have no return value. Instead contracts communicate to the outside world with log events. The log events are part of the transaction receipt which is produced when the transaction is executed. The receipts are stored in the receipt trie, the integrity of which is guaranteed by the fact that the current root of the receipt trie is part of the block header alongside the roots of state and state-trie. In a broad sense from the external perspective receipts are part of the Ethereum system state except that they are not readable contracts internally.