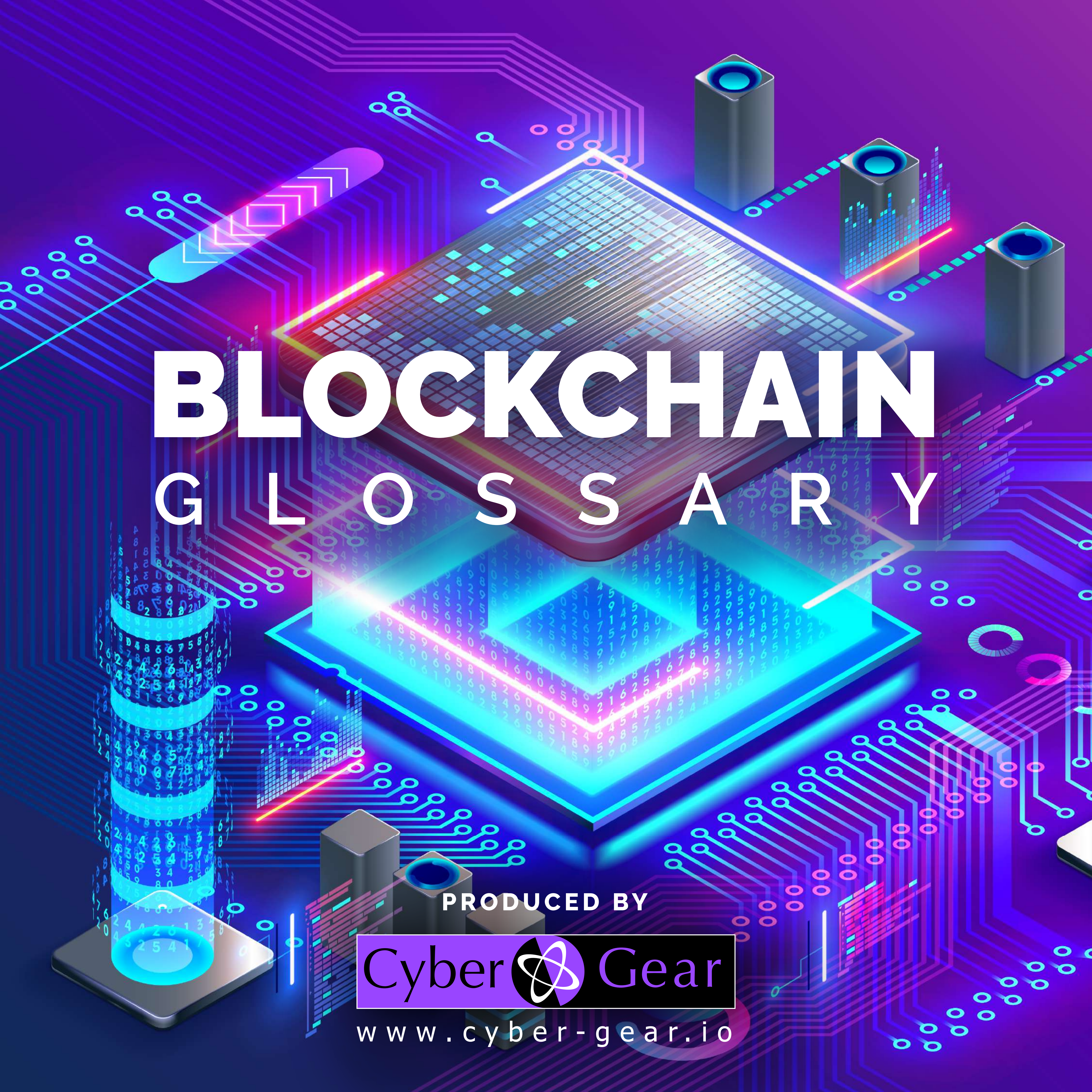

BLOCKCHAIN GLOSSARY

PRODUCED BY

Cyber Gear

www.cyber-gear.io

ABI (APPLICATION BINARY INTERFACE)

An interface between two binary program modules, often one program is a library and the other is being run by a user.

ACCOUNT

A public and private keypair that “holds” your funds.

Your funds are actually stored on the blockchain, not in the wallet or account. Just like your Reddit account has a username (public) and password (private), so does your Ethereum account–the difference being that you are the custodian of your Ethereum keys, while Reddit holds your login information for their site. For additional security, you can use a password to encrypt your private key which would result in a username (public) and password (private) and password for that password (private + more secure). See also ‘keystore file’.

ADDRESS / PUBLIC KEY

Used to send and receive transactions on a blockchain network. An address is an alphanumeric character string, which can also be represented as a scannable QR code. In Ethereum, the address begins with 0x. For example: 0x06A85356DCb5b307096726FB86A78c59D38e08ee.

AIR-GAPPING

A method for securing computers in which the device does not connect to the internet or any other open networks.

AIRDROP

A token distribution method used to send cryptocurrency or tokens to wallet addresses. Sometimes airdrops are used for marketing purposes in exchange for simple tasks like reshares, referrals, or app downloads.

ALTCOIN

Any digital currency alternative to Bitcoin. Many altcoins are forks of Bitcoin with minor changes (e.g., Litecoin).

ALPHA

Alpha is valuable information shared before it hits the general public on upcoming drops, news, updates, and more.

AMA

Ask Me Anything.

APE IN

To invest in an NFT without too much research, often based on FOMO.

AR

Augmented Reality is the tech used to create an overlay of digital information of visuals, sounds and haptics.

ATH

All-Time High of a crypto asset.

ATL

All-Time Low of a crypto asset.

ATOMIC SWAP

A cross-chain trading mechanism that enables users to exchange one cryptocurrency for another without the need for a centralized exchange.

AVATAR

A profile pictures style NFT that can also represent a 3D version that can be used in blockchain gaming and the metaverse.

AML
(ANTI-MONEY LAUNDERING)

A set of international laws enacted to diminish the potential for criminal organizations or individuals to launder money. These rules and laws are applied to cryptocurrencies with varying effects in different jurisdictions.

API (APPLICATION PROGRAMMING INTERFACE)

A software intermediary that allows two separate applications to communicate with one another. APIs define methods of communication between various components.

ASIC (APPLICATION SPECIFIC INTEGRATED CIRCUIT)

ASICs are silicon chips designed to do a specific task. In ASIC use for mining cryptocurrencies, the ASIC will perform a calculation to find values that provide a desired solution when placed into a hashing algorithm.

ATTESTATION

Under the Proof of Stake mechanism (on the Beacon Chain), every validator other than the one proposing a new block will provide an attestation, or vote, in favor of a block with which it agrees, hereby forming consensus and confirming the block and the transactions it contains. See also ‘Proof of Stake'.

BEACON CHAIN

The Beacon Chain (always capitalized) is one element in the infrastructure being built to scale Ethereum, and is the foundation for a transition from a Proof of Work (PoW) consensus mechanism to Proof of Stake (PoS). For more information, see this guide.

BITCOIN (BTC)

A decentralized blockchain that specifically transacts tokens between accounts.

Bitcoin is the original blockchain-based cryptocurrency. Bitcoin uses Unspent Transaction Outputs (UTXOs) to store data and a Proof-of-Work (PoW) consensus algorithm.

BEAR MARKET

A market condition in which prices are falling and investor sentiment is negative.

BULL MARKET

A market condition in which prices are rising and investor sentiment is positive.

BLOCK

Think of a blockchain as consisting of a ledger that is being constantly updated, and those changes synced between any number of different nodes (indeed, “distributed ledger technology” is another phrase used to describe it).

After a certain number of transactions have been added to the ledger and consensus has been reached among the nodes that the transactions are valid, then they are cryptographically locked into a “block” and officially recorded. This “block” forms the basis for the next one; in this way, they are all linked together in a chain, hence—blockchain.

BLOCK, CANONICAL

A block that has been included in the primary blockchain and is directly or indirectly referenced by future blocks. Blocks that are not canonical may have been valid but were discarded in favor of the canonical block.

BLOCK EXPLORER

A tool that allows users to view and search the contents of the blockchain.

BLOCK, GENESIS

The original block in a blockchain. The genesis block has a block height of zero, and all other blocks are intrinsically linked to it.

Genesis blocks can be configurable to create a fork of a chain for purposes such as pre-loading accounts with tokens for a test network or specifying different block parameters.

BLOCK HEIGHT

The number of blocks connected together in the blockchain. For example, Height 0 would be the very first block, which is also called the Genesis Block.

BLOCK REWARD

The reward given to a miner after it has successfully hashed a transaction block. Block rewards can be a mixture of coins and transaction fees. The composition depends on the policy used by the cryptocurrency in question, and whether all of the coins have already been successfully mined. The current block reward for the Bitcoin network is 12.5 bitcoins per block.

BLOCK TIME

When we talk about ‘block time’, we’re referring to how long it takes for a block of transactions (see ‘block’) to be confirmed by the network, either by miners under PoW or by validators under PoS. See also ‘Proof of Work’, ‘Proof of Stake’.

BLOCKCHAIN

A method of storing data in discrete sections (blocks) that are linked together. Blockchains specify criteria for what data can be stored in a block and reject invalid data.

The submission of blocks to a decentralized blockchain is governed by its consensus mechanism.

BLOCKCHAIN 1.0

The generation of blockchain technology that focused on performing simple token transactions. Blockchain 1.0 chains have limited scope and ability, but served to prove the fundamental technologies of blockchains and show that a market existed for those technologies.

Bitcoin was the first of the Blockchain 1.0 generation.

BLOCKCHAIN 2.0

The generation of blockchain technology that enabled smart contracts and generalized processing on chain. Blockchain 2.0 chains are typically built on Turing-complete programming languages and provide expanded capabilities beyond simple peer-to-peer (P2P) value exchange.

Ethereum was the first of the Blockchain 2.0 generation.

BLOCKCHAIN 3.0

The generation of blockchain technology that focuses on scalability and interoperability. This generation of blockchain typically enables the use of smart contracts.

Blockchain 3.0 chains are currently in early development with no front-runners as of yet. Two promising Blockchain 3.0 projects are SkyCoin and EOSIO.

BOUNTY / BUG BOUNTY

A reward offered for exposing vulnerabilities and issues in computer code.

BRAIN WALLET

A blockchain account generated from a seed phrase or password or passphrase of your choosing. Humans are not capable of generating enough entropy, or randomness, and therefore the wallets derived from these phrases are insecure; brain wallets can be brute forced by super fast computers. For this reason, brain wallet are insecure and should not be used. See also ‘Seed phrase / Secret Recovery Phrase’.

BTD

Buy The Dip.

BUIDL

Ostensibly coined (see what we did there) by Gitcoin's Kevin Owocki. It reflects the Ethereum-focused mindset of not just investing in a cryptocurrency as a store of value, but rather investing in it as an ecosystem and a platform for public goods and software; it complements, in this sense, the now-infamous HODL.

BYTECODE

Bytecode is a “low-level” computer language, that is, meant to be processed by a computer, rather than a “high-level”, more human-readable, language. In Ethereum, higher-level Solidity is compiled into Ethereum bytecode, which is read by the Ethereum Virtual Machine (EVM).

BYZANTIUM FORK

A “hard fork” in the Ethereum network that occurred in October of 2017. For detailled information, see here; see also “hard fork”.

BYZANTINE FAULT TOLERANCE

The ability of a network to properly reach consensus at any time, assuming that no more than 1/3 of its actors are malicious.

BFT

A property of a distributed system in which it can continue to function correctly even if some of its components fail or behave maliciously.

INTERLEDGER PROTOCOL (ILP)

A protocol that enables payments between different ledgers and networks.

CERTIFICATE AUTHORITY (CA)

A centralized authority that correlates identities with a public/private key pair in a private key infrastructure.

CENTRALIZED EXCHANGE (CEX)

A cryptocurrency exchange that is controlled by a centralized authority.

CEX

Centralized Exchange.

CMC

Coinmarketcap.

CT

Crypto Twitter.

CLIENT (ETHEREUM)

An Ethereum client is software that accesses the Ethereum blockchain via a local computer and helps to process transactions. A client usually includes a cryptocurrency software wallet.

CLOSED SOURCE

Closed source software is proprietary software with source code that cannot be accessed by the public. The compiled binaries may be available in the form of an executable program (files that end in .exe, .dpkg, etc.) but are not human-readable or available for modification by anyone but the original software developer.

CODEFI

Derived from “Commerce & Decentralized Finance”, Codefi, part of ConsenSys, is building a suite of commerce and financial applications.

COIN

A coin, in cryptocurrency, is a representation of digital asset value that is generated via its own independent blockchain.

COLD WALLET / COLD STORAGE

An offline wallet that is never connected to the internet. These wallets protect cryptocurrencies from getting hacked online.

COLD STORAGE

A method of storing cryptocurrencies offline to protect them from hackers.

COMMAND-LINE INTERFACE (CLI)

A text-based user interface.

CLIs can provide more core functionality and access to system resources than a graphical user interface (GUI), but at the cost of usability. Because of this, CLIs are generally directed toward developers over the average user. They can be used to demonstrate the functionality underlying a program without expending development time building a more robust user interface.

CONFIRMATION

A confirmation happens when the network has verified the blockchain transaction. Under a Proof of Work (PoW) consensus mechanism, this happens through a process known as mining; under Proof of Stake (PoS), the process is known as validation. Once a transaction is successfully confirmed it theoretically cannot be reversed or double spent. The more confirmations a transaction has, the harder it becomes to perform a double spend attack.

CONSENSUS

The process used by a group of peers, or nodes, on a blockchain network to agree on the validity of transactions submitted to the network. Dominant consensus mechanisms are Proof of Work (PoW) and Proof of Stake (PoS).

CONSENSYS

Short for Consensus Systems, ConsenSys is the software engineering leader of the blockchain space. But you're here, so you already knew that.

CONSORTIUM

A private blockchain network run by a company or a group of companies. Consortium chains deal with information that would not be appropriate for public release but still needs to be immutably communicated between two parties.

CRYPTO

Even though this prefix is originally Greek, our current usage comes from cryptography. Technologies that are referred to with the blanket term of “crypto” tech are underlain by cryptographic tools and processes (such as public/private key pairs) that enable them, and enable them to be secure. Of course, “cryptocurrency” often gets shortened to simply “crypto”, so this emerging field is full of instances where something “crypto” is being added to or shortened.

CRYPTOCURRENCY

Digitally distributed and traded currencies for which proof of ownership is established via cryptographic methods. For example, Ether cannot be transferred from an account without having control of the private key that is associated with that account.

CRYPTOGRAPHY

A method for secure communication using code. Symmetric-key cryptography is used by various blockchain networks for transfer of cryptocurrencies. Blockchain addresses generated for wallets are paired with private keys that allow transfer of cryptocurrency. Paired public and private keys allow funds to be unlocked.

CROSS-CHAIN

Refers to the ability of different blockchain networks to communicate and exchange data with each other.

CURRENCY

A system of abstract representations of the ability to reconcile debts that is generally accepted or in use. Money is a currency. In the United States of America, the U.S. Dollar is the national currency.

DAO

A Digital Decentralized Autonomous Organization (DAO, pronounced like the Chinese concept) is a powerful and very flexible organizational structure built on a blockchain.

Alternatively, the first known example of a DAO is referred to as The DAO. The DAO served as a form of investor-directed venture capital fund, which sought to provide enterprises with new decentralized business models. Ethereum-based, The DAO's code was open source. The organization set the record for the most crowdfunded project in 2016. Those funds were partially stolen by hackers. The hack caused an Ethereum hard-fork which lead to the creation of Ethereum Classic.

DAPP

Short for decentralized application, a software application that runs on a blockchain network.

DCA

Dollar Cost Averaging.

DEFI

Decentralized Finance

DEGEN

Short for “Degenerate"- someone who is over enthusiatsic about a project or invests without doing any prior research or due diligence.

DECENTRALIZATION

The transfer of authority and responsibility from a centralized organization, government, or party to a distributed network.

DECENTRALIZED APPLICATION (DAPP)

An open source, software application with backend code running on a decentralized peer-to-peer network rather than a centralized server. You may see alternate spellings: dApps, DApps, Dapps, and Đapps.

DECENTRALIZED EXCHANGE (DEX)

A decentralized exchange is a platform for exchanging cryptocurrencies based on functionality programmed on the blockchain (i.e., in smart contracts). The trading is peer-to-peer, or between pools of liquidity. This is in contrast with a centralized exchange, which is more akin to a bank or investment firm that specializes in cryptocurrencies. There are important technical and regulatory differences between the two which are constantly evolving.

DEPOSIT

Digital property put into a contract involving a different party such that if certain conditions are not satisfied that property is automatically forfeited to the identified counterparty.

DERIVE / DERIVATION

To derive something is to obtain it from an original source. In the context of crypto-technology, we often discuss “deriving” wallets and accounts from seed phrases / Secret Recovery Phrases.

DECENTRALIZED AUTONOMOUS ORGANIZATION (DAO)

A company or group of like-minded entities that operate based on the rules set forth in a smart contract. DAOs are used to transform business logic into software logic recorded on a blockchain.

DEVCON

This is shorthand for the Ethereum Developers' Conference.

DIFFICULTY

The concept outlining how hard it is to verify blocks in a blockchain network during Proof of Work mining. In the Bitcoin network, the difficulty of mining adjusts every 2016 blocks. This is to keep block verification time at ten minutes.

DIFFICULTY BOMB

The difficulty bomb, along with the Beacon Chain and others, is an element of Ethereum's upgrade to Ethereum 2.0 and a Proof of Stake (PoS) consensus mechanism. As the name indicates, the difficulty bomb is a mechanism that will increase the block verification difficulty, making it more expensive and difficult–eventually, prohibitively so–to mine a new block. The intention is to force the shift to PoS consensus. See also ‘Proof of Stake'.

DIGITAL ASSET

A digital commodity that is scarce, electronically transferable, and intangible with a market value.

DIGITAL IDENTITY

An online or networked identity adopted by an individual, organization, or electronic device.

DIGITAL SIGNATURE

A code generated by public key encryption and attached to an electronically transmitted document in order to verify the contents of the document.

DIAMOND HANDS

When someone holds a crypto asset or an NFT regardless of any bad press it may receive. Similar to HODL.

DIRECTED ACYCLIC GRAPH (DAG)

A directed graph structure (e.g., flow chart) that has no recursive routes (i.e., traversing the graph will never go twice through the same route or branch).

DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

A type of cyber-attack in which the perpetrator continuously overwhelms the system with requests in order to prevent service of legitimate requests.

DISTRIBUTED LEDGER

A type of database which spreads across multiple sites, countries, or institutions. Records are stored sequentially in a continuous ledger. Distributed ledger data can be either “permissioned” or “unpermissioned” to control who can view it.

DOUBLE SPEND

An event during which someone on the Bitcoin network tries to send a specific bitcoin transaction to two different recipients at once. However, as each bitcoin transaction is confirmed, double spending becomes almost impossible. The more confirmations that a particular transaction has, the decreased likelihood of double spending successfully.

DOUBLE SPEND ATTACK

A malicious attempt to convince two separate parties that one of two conflicting transactions is valid. In such a situation, both transactions appear individually valid, but their combination is not. Thus, only one is included in the blockchain.

Due to the nature of blockchain reorganizations (natural forks), simply showing that a transaction is included in a block is not enough to verify that it is immutable. Transactions are only immutable once they have reached a depth in the chain where a chain reorganization is unlikely to affect them.

DYOR

Do Your Own Research

EIP (ETHEREUM IMPROVEMENT PROPOSAL)

EIPs describe standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards. They are, precisely, proposals for modifications to the network and the way it functions.

ENCRYPTED VS UNENCRYPTED KEYS

As discussed elsewhere, public and private crypographic key pairs are one of the technologies that underpins crypto-currencies and “crypto” tech in general. In MetaMask, an unencrypted private key is 64 characters long, and it is used to unlock or restore wallets. An encrypted key is also 64 letters long and is a regular private key that has gone through the process of encryption.

ENUM

Short for ‘enumeration' - a fixed list of possible values.
The list of US states could be considered an enum.

ENCRYPTION

There are many types of encryption, but for our purposes, it is a process that combines the text to be encrypted (plaintext) with a shorter string of data referred to as “a key” in order to produce an output (ciphertext). This output can be “decrypted” back into the original plaintext by someone else who has the key.There are many types of encryption, but for our purposes, it is a process that combines the text to be encrypted (plaintext) with a shorter string of data referred to as “a key” in order to produce an output (ciphertext). This output can be “decrypted” back into the original plaintext by someone else who has the key.

ENTERPRISE ETHEREUM ALLIANCE (EEA)

A group of Ethereum core developers, startups, and large companies working together to commercialize and use Ethereum for different business applications.

ENTROPY

In the context of cryptography, ‘entropy’ refers to ‘randomness’; generally, the more random something is (the more entropy it has), the more secure it is.

EOA

Externally Owned Account

EOSIO

EOS is a Blockchain 3.0 chain that focuses on transaction throughput. It uses a Delegated Proof-of-Stake (DPoS) consensus mechanism and web assembly (WASM) for smart contracts.

EPOCH

An epoch, in general, is a measure of time, or of blockchain progression, on a given blockchain. For the Ethereum Beacon Chain, an epoch consists of 32 slots, each lasting 12 seconds, for a total of 6.4 minutes per epoch. There is additional functionality built upon the epoch measure in the Beacon Chain to help ensure security and proper operation of the Chain.

ERC-20

A standard for fungible tokens on the Ethereum network.

ERC-721

A standard for non-fungible tokens (NFTs) on the Ethereum network.

ERC-20 TOKEN STANDARD

ERC is the abbreviation for Ethereum Request for Comment and is followed by the assignment number of the standard. ERC-20 is a technical standard for smart contracts which is used to issue the majority of tokens (in particular, cryptocurrency tokens) extant on Ethereum. This list of rules states the requirements that a token must fulfill to be compliant and function within the Ethereum network.

ELI5

Explain It (to me) Like I'm 5.

ERC-721 TOKEN STANDARD

As stated above, this is another standard for Ethereum smart contracts, which allows for the issuance of a non-fungible token, also known as an NFT. This token standard is used to represent a unique digital asset that is not interchangeable.

ETHER (ETH)

Ether is the native currency of the Ethereum blockchain network. Ether—also referred to as ETH (pronounced with a long "e", like "teeth" without the "t")—functions as a fuel of the Ethereum ecosystem by acting as a medium of incentive and form of payment for network participants to execute essential operations. The cryptocurrency of Ethereum has a lowercase e. The plural of ether is just ether; its abbreviation is ETH, with a space: I have 10 ETH.

ETHEREUM

Ethereum is a decentralized Blockchain 2.0 chain. It was the first major smart contract platform and has widespread support from Fortune 500 companies through the Ethereum Enterprise Alliance (EEA).

Ethereum currently uses a Proof-of-Work (PoW) consensus algorithm, but future changes to the protocol will update it to a more scalable algorithm, most likely based on Proof-of-Stake (PoS).

ETHEREUM ENTERPRISE ALLIANCE (EEA)

A collection of medium- to large-sized companies that have publicly committed to supporting the development of Ethereum and the creation of applications for the protocol.

Double spend attacks can be mitigated by waiting to ensure that a transaction is confirmed by the network and is acceptably immutable before acting on it.

ENS

The Ethereum Name Service is a protocol to assign human-readable and easy-to-remember addresses to Ethereum addresses and assets, homologous to the traditional internet's DNS.

ERC

Ethereum Request for Comment, or ERC, is a bit of a misnomer, as it is used to refer to suggestions for modifications that have already made it through the Ethereum Improvement Protocol (EIP) process and have been made standard on Ethereum. An ERC is, essentially, a set of standards for a given operation or topic on the Ethereum network.

EVM (ETHEREUM VIRTUAL MACHINE)

The EVM is a virtual machine that operates on the Ethereum network. It is Turing complete and allows anyone, anywhere to execute arbitrary EVM bytecode. All Ethereum nodes run on the EVM. It is home for smart contracts based on the Ethereum blockchain.

EWASM

A web assembly (WASM) version implemented by the Ethereum Virtual Machine that provides additional functionality for blockchains.

EXCHANGE

A place to trade cryptocurrency. Centralized exchanges, operated by companies like Coinbase and Gemini, function as intermediaries, while decentralized exchanges do not have a central authority.

EXCHANGE, DECENTRALIZED

A cryptocurrency exchange that is hosted entirely through a DApp on a blockchain.

Decentralized exchanges typically do not allow the exchange of cryptocurrency to fiat. Decentralized exchanges are more difficult than standard exchanges to regulate or sanction.

FAUCET

A faucet is an application, sometimes a very simple website, other times more complex, that dispenses cryptocurrency for use on test networks only. These faucets are used by developers to test out dapps or smart contracts before deploying them on Ethereum Mainnet, or users who want to practice an action on the blockchain with no risk. Tokens dispensed by a test faucet stay on the test networks and cannot be exchanged for mainnet equivalents.

FIAT

A nationally adopted currency with government support, such as U.S. Dollars or Euros. Fiat currencies are desirable due to their legal status and traditional use.

FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN)

The U.S. federal agency responsible for investigating and prosecuting financial crimes, such as money laundering.

FinCEN regulations cover many aspects of cryptocurrency use.

FINAL, FINALITY

A transaction is considered “final” once it can no longer be changed. In a sense, this happens once there are sufficient confirmations of the transaction, but for all intents and purposes, a transaction is final once the block that contains it is mined or validated. Keep in mind that this reflects a fundamental rule of blockchains: unlike traditional financial systems where charges can be “reversed”, there is no “undoing” a transaction on the blockchain. Once finality is reached, the transaction is immutable.

FINNEY

A denomination of ether.

FLIP

To mint an NFT and sell soon after for a profit.

FLIPPENING

This has not happened yet, but some people believe Ethereum will be more valuable than Bitcoin in the future.

FLOOR

The lowest price of an NFT within a particular collection.

FOMO

Fear of Missing Out.

FORK

A fork creates an alternative version of a blockchain, and are often enacted intentionally to apply upgrades to a network. Soft Forks render two chains with some compatibility, while Hard Forks create a new version of the chain that must be adopted to continue participation. In the instance of a contentious Hard Fork, this can create two versions of a blockchain network.

FORK, HARD

A fork that is permanently incompatible with the original network.

Hard forks typically change transaction data structures, consensus algorithms, or add/remove blocks that would not have otherwise been included.

FORK, SOFT

A fork that is compatible with the data on the original chain.

Blocks created on the original chain after a soft fork would be valid on the forked chain; however the reverse does not have to be true.

FUD

Fear, Uncertainty, Doubt.

GAMEFI

A term used in blockchain games that have a financial return for players.

GM/GN

Good Morning / Good Night.

GMI

Gonna make it.

GAS

A measure of the computational steps required for a transaction on the Ethereum network. This then equates to a fee for network users paid in small units of ETH specified as Gwei. See also “ether (denominations)”.

GAS LIMIT

The gas limit is the maximum amount you're willing to pay for any given transaction to go through the Ethereum network. Another way of looking at it is as a "rough estimate" of how much computing power your transaction will take.

GAS PRICE

The gas price is what it sounds like: the cost the network is paid for the computational work being performed in a given transaction. It is paid in units of ETH called Gwei. Depending on network congestion, the gas price may vary significantly.

GENESIS BLOCK

The initial block of data computed in the history of a blockchain network.

GOSSIP PROTOCOL

A process by which actors in a network exchange information with all other members.

When an actor receives new information, it relays it to every other actor it's connected to that does not already have that information. Since all actors are cumulatively connected, eventually they all receive the information.

GRAPHICAL USER INTERFACE (GUI)

A way of displaying information to the user through stylized, on-screen elements, such as windows and taskbars.

GWEI

A minuscule and common denomination of ETH, and the unit in which gas prices are often specified. See ‘ether (denominations)’ entry for more information.

HALVING

Many cryptocurrencies have a finite supply, which makes them a scarce digital commodity. For example, the total amount of Bitcoin that will ever be issued is 21 million. The number of bitcoins generated per block is decreased 50% every four years. This is called “halving.” The final halving will take place in the year 2140.

HARD FORK

A hard fork occurs when there is a change in the blockchain that is not backward compatible (not compatible with older versions), thus requiring all participants to upgrade to the new version in order to be able to continue participating on the network. See also “fork”.

HARDWARE WALLET

A physical device that can be connected to the web and interact with online exchanges, but can also be used as cold storage (not connected to the internet).

HASH

The output of a cryptographic function that maps inputs to specific, but seemingly arbitrary, outputs. Hashes are used to efficiently identify data.

HASH COLLISION

Two inputs that map to the same output hash.

While hash collisions are possible, providing two sets of meaningful data whose hashes collide is nearly impossible. Hashes are one-way streets; they can be constructed from data, but data cannot be reconstructed from hashes.

HASHGRAPH

A decentralized ledger that uses a gossip protocol to communicate transactions and a tangle-style consensus mechanism.

HASHRATE

The rate at which a particular machine can perform a specific hashing function.

Hashrate is similar to general CPU speed, but where processor speed is measured based on the number of arbitrary instructions a machine can carry out per second, hashrate is measured based on the number of times a machine can perform that specific function per second, allowing application-specific integrated circuits (ASIC) to have a much higher hashrate than a processor with the same clock speed.

HASH FUNCTION

A cryptographic function that maps inputs to specific, but seemingly arbitrary, outputs.

Hash functions and their qualitative differences are an incredibly important field of research in cryptography.

HD WALLET

Hierarchical Deterministic wallets were first created for Bitcoin, and enable the creation of a very large number of accounts based on an initial seed phrase. This technology was later adopted in Ethereum wallets; when restoring a MetaMask wallet from the Secret Recovery Phrase, for example, if you “create” accounts, they will be the same accounts as previously created from that same phrase; they are derived from it.

HEXADECIMAL

Hexadecimal is a base 16, rather than base 10, counting system. Used all over Ethereum for a variety of things, a hexadecimal string is comprised of the numbers 0 1 2 3 4 5 6 7 8 9 and letters A B C D E F.

HODL

Hold On for Dear Life.

HOT WALLET / HOT STORAGE

A wallet that is directly connected to the internet at all times, for example one that is held on a centralized exchange. Hot wallets are considered to have lower security than cold storage systems or hardware wallets.

HYPERLEDGER

Hyperledger is an ecosystem of open-system tools, libraries, and products designed to enable and support enterprise-grade blockchain technology. In general, the products focus on creating solutions for permissioned blockchains–that is, non-public blockchains, with alternative consensus mechanisms other than Proof of Work (PoW) or Proof of Stake (PoS).

That said, there are use cases where such institutions would want to integrate with public blockchains, and for that reason Hyperledger Besu and Hyperledger Burrow are actively developed projects, the former being a Java-based Ethereum client, the latter being a smart contract platform which supports EVM bytecode.

IDENTICON / ADDRESSIDENTICON / ADDRESSICON

The colorful blob of colors that corresponds to your address. It is an easy way to see if your address is correct. More specifically, you can choose between jazzicons (created by the MetaMask team!) or blockies.

IGO

Initial Game Offering.

INO

Initial NFT Offering.

INITIAL COIN OFFERING (ICO)

Much like an initial public offering of stock, an initial coin offering is a way for a tokenized business to generate investment from the public.

ICOs are regulated by the Securities and Exchange Commission (SEC), even if the tokens are not specifically securities because the language used in promoting a sale can serve to classify tokens as a security offering.

INTEROPERABILITY

The ability of different blockchain networks to communicate

IMMUTABLE

Refers to the fact that once data is added to the blockchain, it cannot be changed or deleted.

IMMUTABILITY

The inability to be altered or changed. This is a key element of blockchain networks: once written onto a blockchain ledger, data cannot be altered. This immutability provides the basis for commerce and trade to take place on blockchain networks.

INSTANTIATE(D)

To provide an instance of or concrete evidence in support of (a theory, concept, claim, or the like).

INVARIANT

A function, quantity, or property that remains unchanged when a specified transformation is applied.

INITIAL COIN OFFERING (ICO)

Much like an initial public offering of stock, an initial coin offering is a way for a tokenized business to generate investment from the public.

ICOs are regulated by the Securities and Exchange Commission (SEC), even if the tokens are not specifically securities because the language used in promoting a sale can serve to classify tokens as a security offering.

INTERPLANETARY FILE SYSTEM (IPFS)

A decentralized file storage and referencing system for the Ethereum blockchain. IFPS is an open source protocol that enables storing and sharing hypermedia (text, audio, visual) in a distributed manner without relying on a single point of failure. This distributed file system enables applications to run faster, safer and more transparently.

IPFS

Inter Planetary File System

ITO

Initial Token Offering.

JOMO

Joy of Missing Out.

KEYSTORE FILE

A keystore file is a special, encrypted version of a private key in JSON format. See also ‘private key’.

KNOW YOUR CUSTOMER (KYC)

A process in which a business must verify the identity and background information (address, financials, etc) of their customers. For example, current regulations and laws require banks and other financial institutions to keep and report customers' personal information and transactions.

LAYER 2

Layer 2 is a set of upcoming scaling solutions for Ethereum.

LEDGER NANO S

A hardware wallet that is used to store cryptocurrencies offline.

LIGHT 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.

LIQUID DEMOCRACY (DELEGATIVE DEMOCRACY)

A government system where votes can be delegated or proxied to other individuals such as friends, politicians, or subject matter experts. For example, in a liquid democracy, Bernadette could give Ahmad her vote and Ahmad would then vote for both himself and Bernadette. A liquid democracy has been explored as a governance mechanism for Decentralized Autonomous Organizations where every participant is able to vote or delegate their vote to another individual.

LIQUIDITY

The availability of liquid assets to a company or market. An asset is considered more liquid if it can easily be converted into cash. The harder the ability to turn an asset into cash the more illiquid the asset. For example, stocks are considered relatively liquid assets as they can be easily converted to cash while real estate is considered an illiquid asset. The liquidity of an asset affects its risk potential and market price.

LIGHTNING NETWORK

A scaling solution for Bitcoin that allows for instant and low-cost transactions.

METAVERSE

A virtual world or several worlds that host games, events, offices and much more.

MINT

To add a digital asset to the blockchain. Mainly used in NFTs.

MR

Mixed Reality.

MAINNET

The primary network where actual transactions take place on a specific distributed ledger. For example, The Ethereum mainnet is the public blockchain where network validation and transactions take place.

MARKET CAP

Short for Market Capitalization, this term refers to the total value held in a particular industry, market, company, or asset. For a publicly traded company, the market cap is the total dollar market value of a company's outstanding shares. For Bitcoin or Ethereum, the total market cap is a reflection of the current existing supply times the market price.

MERKLE TREE

A tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes.

MESH

ConsenSys Mesh is a network of loosely coupled, tightly aligned teams, products, and investments advancing the Ethereum ecosystem and the arrival of Web 3.0.

METAMASK

MetaMask, either in its mobile app form on iOS and Android, or in its browser extension form, is a tool to access and interact with blockchains and the decentralized web. Its functions include that of a wallet, a dapp permissions manager, and token swap platform.

MINING

The process by which blocks or transactions are verified and added to a blockchain using a Proof of Work (PoW) consensus mechanism. In order to verify a block a miner must use a computer to solve a cryptographic problem. Once the computer has solved the problem, the block is considered "mined" or verified. In the Bitcoin or Ethereum PoW blockchains, the first computer to mine or verify the block receives bitcoin or ether as a reward.

MINING POOL

A collection of miners who come together to share their processing power over a network and agree to split the rewards of a new block found within the pool.

MIST

Browser for installing and using Dapps.

MOONING

A term used to describe a rapid and significant increase in the price of a particular cryptocurrency.

MSP (MEMBERSHIP SERVICE PROVIDER)

A Hyperledger Fabric blockchain network can be governed by one or more MSPs.

MULTI SIGNATURE (MULTISIG)

A crypto-asset wallet that requires multiple keys to access. Typically, a specified number of individuals are required to approve or “sign” a transaction before they are able to

NGMI

Not Gonna Make It.

NFT

When discussing Non-Fungible Tokens (NFTs), “fungibility” refers to an object's ability to be exchanged for another. For example, an individual dollar is considered fungible as we can trade dollars with one another. Artwork is usually deemed non-fungible as paintings, sculptures, or masterpieces are likely to be unequal in quality or value. A non-fungible token is a type of token that is a unique digital asset and has no equal token. This is in contrast to cryptocurrencies like ether that are fungible in nature.

NO COINER

Someone who doesn't invest in crypto.

NOOB

A person who is new to crypto, NFTs and the rest of the blockchain.

NODE (FULL NODE)

Any computer connected to the blockchain network is referred to as a node. A full node is a computer that can fully validate transactions and download the entire data of a specific blockchain. In contrast, a “lightweight” or “light” node does not download all pieces of a blockchain’s data and uses a different validation process.

NONCE

The word ‘nonce’ has a few different meanings, and in different contexts, it ends up getting used a lot of different ways. Originally formed from a contraction of a phrase meaning “not more than once”, on the Ethereum mainnet, “nonce” refers to a unique transaction identification number that increases in value with each successive transaction in order to ensure various safety features (such as preventing a double-spend). Note that due to its broader use in cryptography, you may encounter ‘nonce’ being used differently on other sidechains or decentralized projects.

NOTHING AT STAKE PROBLEM`

This is caused by validator nodes approving all transactions on old and new software after a hard fork occurs.

NPM (NODE PACKAGE MANAGER)

Default package manager runtime environment node.js.

OG

Original Gangster is a term used to describe very early adopters and investors of blockchain tech.

OTC

Over the Counter are private deals in crypto between two parties.

OAUTH PROTOCOL

Open Authorization is a standard that is used by third party services to keep and distribute users information without exposing their password.

OMMER BLOCK

Under the Proof of Work (PoW) consensus mechanism, miners received rewards for being the first to mine a new block. However, at times a block would be mined just after, and in competition with, the last block; this block, known as an ommer and previously as an uncle, could get rolled into subsequent blocks and the miner of the original ommer would get a partial block reward. All of this functionality is deprecated as of the Beacon Chain.

ON-CHAIN GOVERNANCE

A system for managing and implementing changes to a cryptocurrency blockchain.

OPTIMISTIC ROLLUP

A rollup that assumes the validity and good faith of transactions, and only runs a fraud proof in the case of fraud being alleged.

ORACLE

Typically, an oracle is any entity or person that is relied on to report the outcome of an event. In a blockchain network an oracle (human or machine) helps communicate data to a smart contract which can then be used to verify an event or specific outcome.

ORDERER NETWORK

A computer network that allows nodes to share resources.

ORACLES

A mechanism that allows smart contracts to interact with external data sources.

P2P (PEER-TO-PEER)

P2P refers to interactions that happen between two parties, usually two separate individuals. A P2P network can be any number of individuals. In regards to a blockchain network, individuals are able to transact or interact with each other without relying on an intermediary or single point of failure.

P2E

Play To Earn is another term for GameFi used in blockchain gaming.

P2P

Peer-to-Peer.

PAPER HANDS

NFT collectors who sell too early.

PFP

Profile Picture.

PERMISSIONED BLOCKCHAIN

A blockchain network that is controlled by a centralized authority and requires permission to participate.

PERMISSIONLESS BLOCKCHAIN

A blockchain network that is open to anyone and does not require permission to participate.

POAP

Proof of Attendance Protocol.

PUMP N DUMP

A term used when an asset is hyped in order to raise the price only for a fraudulent group to then "dump" or sell their assets at a much higher price.

PARITY

Parity Technologies is the name of a blockchain technology company that is developing a number of significant projects in the Ethereum space; however, one of its first projects was an Ethereum client, now known as Parity Ethereum; often this client is simply referred to as ‘Parity’.

PERMISSIONED LEDGER

A blockchain network in which access to ledger or network requires permission from an individual or group of individuals, as opposed to a public blockchain. Permissioned ledgers may have one or many owners. Consensus on a permissioned ledger is conducted by the trusted actors, such as government departments, banks, or other known entities. Permissioned blockchains or ledgers contain highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is much easier to maintain and considerably faster than a public blockchain. For example, Quorum or Hyperledger Besu are permissioned ledgers that can be more easily set up for large enterprises. In contrast, the public Ethereum blockchain is a permissionless ledger which anyone can access.

PKI (PUBLIC KEY INFRASTRUCTURE)

A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

PLASMA

Plasma is a term that is used to refer to one of the scaling solutions being deployed to create Layer 2 of the Ethereum network. A Plasma network functions similarly to an Optimistic rollup, inasmuch as it relies on Layer 1 Ethereum mainnet to maintain the record of transactions, and as the source for arbitration or fraud resolution. However, a Plasma network differs in other important technical ways from rollups, and is currently limited to simple operations, such as swaps and token transfers.

POA, POS, POW

Acronyms standing for Proof of X consensus mechanisms: Assignment, Stake, Work. The “o” is lowercase since you wouldn't capitalize “of” when writing out the phrase. See also ‘consensus’, ‘Proof of Authority’, ‘Proof of Stake’, ‘Proof of Work’.

POS/POW HYBRID

A hybrid consensus model that utilizes a combination of Proof of Stake (PoS) and Proof of Work (PoW) consensus. Using this Hybrid consensus mechanism, blocks are validated from not only miners, but also voters (stakeholders) to form a balanced network governance.

PRIVATE BLOCKCHAIN

A blockchain or distributed ledger that has a closed network where participants are controlled by a single entity. A private blockchain requires a verification process for new participants. A private blockchain may also limit which individuals are able to participate in consensus of the blockchain network. See also ‘permissioned ledger’.

PRIVATE CURRENCY

A currency or token issued by a private individual or firm. Typically, the token or currency is limited to use within the network of that particular firm or individual. This is not to be confused with a “privacy cryptocurrency” which are cryptocurrency with specific privacy features, such as hidden user identities.

PRIVATE KEY

A private key is an alphanumeric string of data that, in MetaMask, corresponds to a single specific account in a wallet. Private keys can be thought of as a password that enables an individual to access their crypto account. Never reveal your private key to anyone, as whoever controls the private key controls the account funds. If you lose your private key, then you lose access to that account.

PRAGMA(S) OR PRAGMA-LINE

Defines which compiler version the smart contract uses.

PRIVATE BLOCKCHAIN

Blockchain that can control who has access to it. Contrary to a public blockchain a Private Blockchain does not use consensus algorithms like POW or POS, instead they use a system known as byzantine fault tolerant(BFT). BFT is not a trustless system which makes a BFT system less secure.

PROOF OF ACTIVITY

Active Stakeholders who maintain a full node are rewarded.

PROOF OF BURN

Miners send coins to an inactive address essentially burning them. The burns are then recorded on the blockchain and the user is rewarded.

PROOF OF CAPACITY

Plotting your hard drive (storing solutions on a hard drive before the mining begins). A hard drive with the fastest solution wins the block.

PROOF OF ELAPSED TIME

Consensus algorithm in which nodes must wait for a randomly chosen time period and the first node to complete the time period is rewarded.

PROOF OF STAKE (POS)

A consensus mechanism in which an individual or “validator” validates transactions or blocks. Validators “stake” their cryptocurrency, such as ether, on whichever transactions they choose to validate. If the individual validates a block (group of transactions) correctly then the individual receives a reward. Typically, if a validator verifies an incorrect transaction then they lose the cryptocurrency that they staked. PoS requires a negligible amount of computing power compared to Proof of Work consensus.

PROOF OF WORK (POW)

A consensus algorithm which requires a user to “mine” or solve a complex mathematical puzzle in order to verify a transaction. “Miners” are rewarded with Cryptocurrencies based on computational power.

PROTOCOL

A set of rules that dictate how data is exchanged and transmitted. This pertains to cryptocurrency in blockchain when referring to the formal rules that outline how these actions are performed across a specific network.

PUBLIC BLOCKCHAIN

A globally open network where anyone can participate in transactions, execute the consensus protocol to help determine which blocks get added to the chain, and maintain the shared ledger.

PUB/SUB

Publish/Subscribe

PUBLIC KEY CRYPTOGRAPHY

Encryption that uses two mathematically related keys. A public and private key. It is impossible to derive the private key based on the public key.

PUBLIC KEY

In cryptography, you have a keypair: the public and private key. You can derive a public key from a private key, but cannot derive a private key from a public key. The public key, therefore, is obtained and used by anyone to encrypt messages before they are sent to a known recipient with a matching private key for decryption. By pairing a public key with a private key, transactions not dependent on trusting involved parties or intermediaries. The public key encrypts a message into an unreadable format and the corresponding private key makes it readable again for the intended party, and the intended party only.

PUMP AND DUMP

A type of market manipulation in which a group of investors artificially inflate the price of a cryptocurrency and then sell it off for a profit.

PRIVACY COIN

A cryptocurrency that is designed to protect the privacy and anonymity of its users.

PROOF OF ELAPSED TIME

A consensus mechanism in which nodes are chosen randomly to validate transactions based on the amount of time they have waited.

PROOF OF HISTORY

A consensus mechanism in which nodes use a verifiable delay function to determine their turn to validate transactions.

QUANTUM COMPUTING

A cryptographic technique that allows one party to prove to another party that they know a particular piece of information without revealing the information itself.

QUANTUM PROOF

A blockchain resistant to attacks from quantum computers.

RAIDEN NETWORK

A scaling solution for Ethereum that allows for off-chain transactions.

REKT

Meaning wrecked, is when someone loses all of their investment.

RELAYER

Any party or entity which hosts an off-chain orderbook. Relayers help traders discover counter-parties and cryptographically move orders between them. 0x is an example of a popular Ethereum relayer protocol.

REST API (REPRESENTATIONAL STATE TRANSFER API)

Defines restraints based on http.

ROLLUPS

Rollups (pronounced “roll ups”) are one element in the set of tools and infrastructure being built as Layer 2, the scaling solutions for the Ethereum network. They consist, in general, of solutions in which the transaction data is still kept on Layer 1, the original Ethereum network, while transaction computation occurs on a side network, freeing up computational power on Layer. There are different ways of approaching this problem from a technical point of view, namely Zero Knowledge, or ZK, rollups, and Optimistic rollups.

RPC
(REMOTE PROCEDURE CALLS)

A protocol that is used from one program to request a service on another program located on a network.

RUG PULL

Similar to the traditional financial scam of a pyramid scheme, a ‘rug pull’ is a cryptocurrency or crypto-token based scam in which the creators of the token create hype, through injecting liquidity into their token, airdropping, and other schemes, and once investors pile in and boost the price of the token up to a certain point, the creators liquidate their share of the tokens, leaving their investors with next to nothing.

SATS

Standing for “Satoshis”, SATS are a denomination of a Bitcoin.

SHILL

To promote an NFT or coin, usually on social media.

SWEEP FLOOR

Buying multiple NFTs of the same collection at their floor price.

SATOSHI NAKAMOTO

A pseudonymous individual or entity who created the Bitcoin protocol, solving the digital currency issue of the “double spend." Nakamoto first published their white paper describing the project in 2008 and the first Bitcoin software was released one year later.

SCALABILITY

A change in size or scale to handle a network's demands. This word is used to refer to a blockchain project's ability to handle network traffic, future growth, and capacity in its intended application.

SDK

A software development kit provides the necessary tools for a developer to create software on a specific platform.

SEED (PHRASE) / SECRET RECOVERY PHRASE

The seed phrase, mnemonic, or Secret Recovery Phrase is a crucial part of public blockchain technology, originally created for Bitcoin, and goes by many names. However, they all refer to a set of ordered words which correspond to determined values. These values never change, and therefore the same string of words in the same order will always produce the same number–this is the underlying functionality that allows seed phrases to back up wallets.

SELF-EXECUTING

Functioning by itself, not controlled by any other party other than itself. Self-executing smart contracts cut costs/ overhead by removing the need for an arbitrator and trust toward a third party.

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).

SHARDING

Sharding refers to splitting the entire network into multiple portions called “shards.” Each shard would contain its own independent state, meaning a unique set of account balances and smart contracts. Usually, shards must be tightly coupled and side-chains must be loosely coupled.

SIDECHAINS

A sidechain is what it sounds like — it is a separate blockchain that is Ethereum-compatible. While a sidechain is a sort of scaling tool, as a class they aren't part of Layer 2; they simply represent a way in which developers can build and enable cheaper transactions for the user (on the sidechain, in sidechain-native tokens or currencies) while maintaining compatibility with the Ethereum network. This often requires routing tokens through a special portal or bridge, as sending tokens from a sidechain to Ethereum mainnet or vice versa would result in token loss.

SLASHING CONDITION

Under a Proof of Stake (PoS) consensus mechanism, a slashing condition is one that causes the validator's deposit to be destroyed when they trigger it.

SLOT

A slot, on the Ethereum Beacon Chain, is a 12-second period of time during which a new block may (or may not) be proposed. Every 32 slots composes an epoch.

SMART CONTRACT

Self executing contract with the terms of agreement written into the code.

SOFT FORK

A change to the software protocol where only previously valid blocks/transactions are made invalid. Since old nodes will recognize the new blocks as valid, a soft fork is backward-compatible. However, this can result in a potential divide in the blockchain, as the old software generates blocks that read as invalid according to the new rules.

SOLIDITY

The programming language developers use to write smart contracts on the Ethereum network. Try it out on Remix.

STABLECOIN

Any cryptocurrency pegged to a stable asset, like fiat currency or gold. It theoretically remains stable in price as it is measured against a known amount of an asset less subject to fluctuation. Always spelled as one word.

STATE

The set of data that a blockchain network strictly needs to keep track of, and that represents data currently relevant to applications on the chain.

STATE CHANNELS

State channels are part of the set of tools and platforms involved in scaling Ethereum and enabling Layer 2. While a complex topic, state channels are essentially methods through which the current ‘state’ of the blockchain can be exported, and based on that any given number of transactions can take place off-chain, and then be moved back onto the main Ethereum chain.

STO

Short for security token offering, a fundraising method in which tokens are sold that are backed by real-world assets.

SZABO

A denomination of ETH.

TGE

Token Generation Event.

TLT

Think Long Term.

www.cyber-gear.io

TPS

Transactions Per Second.

TX

Transaction.

TXID

Transaction ID.

TESTNET

An alternative blockchain developers use to test applications in a near-live environment.

TESTNET KOVEN

Ethereum testnet that uses Proof of Authority consensus, available through MetaMask.

TOKEN

A token represents an asset built on an existing blockchain. There are many types; see also ‘ERC-20' and ‘ERC-721' entries.

TRANSACTION BLOCK

A collection of transactions on a blockchain network, gathered into a set or a block that can then be hashed and added to the blockchain.

TRANSACTION FEE

A small fee imposed on some transactions sent across a blockchain network. The transaction fee is awarded to the miner that successfully hashes the block containing the relevant transaction.

TRUSTLESS

‘Trustless’ is a term that gets used a lot in the decentralized web, and it deserves some explanation. Traditionally, to call something ‘trustless’ would sound like a negative thing. In the context of decentralized technology, it has a more technical meaning: since everyone has a copy of the ledger of all transactions ever executed, there is no need for a third-party repository of ‘truth’ in whom trust resides. We don't rely on some centralized server somewhere that could be hacked or changed arbitrarily; anyone can verify the transactions themselves. In a way, the rules and assurances built into the blockchain provide the basis for greater trust, because the system works the same for everyone.

TREZOR

A hardware wallet that is used to store cryptocurrenciesoffline.

TURING COMPLETE

Any machine that can calculate on a level equal to a programmable computer is Turing Complete, or computationally universal. The EVM, despite not existing on a single physical computer, is Turing Complete.

UTILITY

A token with a use case such as a currency, digital collectables, exclusive access, governance, and many more.

VALIDATOR

A participant in Proof of Stake (PoS) consensus. On the Beacon Chain, validators need to stake 32 ETH, that is to submit a sort of security deposit, in order to get included in the validator set.

VALIDITY PROOF

The proof submitted along with certain types of rollups to prove that the transactions are valid.

VALIDIUM

One of the technologies developed for Layer 2 scaling of the Ethereum network.

VIPER

A programming language created to be a formal introduction to smart contracts.

VR

Virtual Reality.

WALLET

A designated storage location for digital assets (cryptocurrency) that has an address for sending and receiving funds. The wallet can be online, offline, or on a physical device.

WEN....

Short for “when”, this is often used as spammers on CT and communities eager to see a quick return of 1000x, “ wen lambo, wen moon wen token” etc

WGMI/WAGMI

We Gonna Make It / We All Gonna Make It.

WHALE

Someone who holds a vast amount of a particular cryptocurrency.

WHITELIST

An exclusive list that allows people the first opportunity to mint an NFT.

WEB3 / WEB 3.0

Web3, or Web 3.0, are terms used synonymously with “the decentralized web" and are often used to refer, broadly, to the blockchain and decentralized technology ecosystems as a whole.

XR

Extended Reality.

YOLO

You Only Live Once, a popular term which, when used in crypto, means to take a gamble on an investment/trade.

ZEPPELIN (OR OPEN ZEPPELIN)

Community of like minded Smart Contract developers.

ZK-SNARK

Zero-Knowledge Succinct Non-interactive ARguments of Knowledge are an incredible technology, and vital to the scaling of blockchain technology and the decentralized web. They are mathematically complex and can be daunting; this explanation from the Ethereum Foundation is a good primer.

ZERO ADDRESS

The Zero Address is an address on the Ethereum network that is the recipient of a special transaction used to register the creation of a new smart contract on the network.

ZK

Zero Knowledge.

ZK-SNARKS

A type of zero-knowledge cryptography which allows someone to prove that they know something without disclosing any additional information.

ZK-ROLLUPS

A Layer 2 scalability solution that allows blockchains to validate transactions faster.

1:1

One of One is a term used for unique art NFT digital collectables.

2FA

Two-Factor Authentication.

51% ATTACK

If more than half the computer power or mining hash rate on a network is run by a single person or a single group of people, then a 51% attack is in operation. This means that this entity has full control of the network and can negatively affect a cryptocurrency by taking over mining operations, stopping or changing transactions, and double-spending coins.