# Onchain Glossary



## **Onchain-specific terms**

## 

## B

### Basic Collection

The Originals collection is the basics of our brand and is always available for purchase. It’s refreshed once per year, and the products are made from premium, heavyweight cotton. They carry visible elements of the Onchain brand. For more details regarding the products, see the [Onchain store](https://onchain.org/store/).

### Business Membership

The "business membership" is tailored for companies, allowing multiple employees to access the membership portal simultaneously.

The standard membership perks contains access to all reports, store items, Onchain and partner events, Discord access and more.

## C

### Collab Collections

Our [store](#_r5tlxdwn9a7) aims to offer “stylish, cool, and modern” fashion products. The original collection is our first step in that direction, earning us the necessary experience in this field.

This is where the Collab collections become important. The strategy involves regularly partnering with established artists to produce new collections aligned with our goals. Ideally, these artists will be digital creators with their own [NFT](#_gb6irmgmwah2) collections. By collaborating with them, we can attract their audience to the Onchain brand, and they will be incentivized through revenue sharing.

Each collaboration NFT should serve a distinct purpose. For example:

* **Onchain Honorary**: Acknowledging individuals who are honorary members of the Onchain Club.
* **Onchain x Dmitri Cherniak**: An artistic collaboration featuring Dmitri Cherniak, combining his exceptional talent with Onchain's innovative ethos.

## D

### DeSci Vision for Onchain

The "internal rationale" for evolving Onchain.org into a more decentralized-based Web3 research platform was largely driven by Onchain's vision and mission. This transformation is a natural progression in our quest to enhance [Web3](#_bfv0v93yygtt) research and ultimately create a better "world" where utilizing onchain solutions brings meaningful improvements.

## E

### Entrepreneurs

An entrepreneur builds onchain use cases that address both of our external goals. Both [non-Web3](#_uavulu456m8f) and native [Web3](#_bfv0v93yygtt) entrepreneurs already understand [blockchain](#_8snqzngpz4dk) technology and Web3. With our resources, we inspire and enable them to conceptualize and build their own Onchain use cases.

## M

### Magazine

The magazine mainly serves as a source of information about how [blockchain](#_8snqzngpz4dk) improves the world in various aspects of life. The Onchain research reports are repurposed by breaking down their content into several shorter articles in our digital magazine. The idea is to help [entrepreneurs](#_qps56dehn5c9), start-ups, and investors find solutions for their own challenges.

We also address current topics of interest to our target audience. New magazine articles are distributed through our social media channels.

### Membership Experiences

Membership experiences (perks and utilities) are the benefits our members receive when joining Onchain. The “must-have” experiences will currently include the following:

* [NFT](#_gb6irmgmwah2) traits
* Membership art concept
* Main membership utility
* NFT main membership perks
* Onchain gamification system
* Onchain identity and Onchain DeSci platform

See [Onchain Founding Membership](#_8lymhrx57k91) for a detailed breakdown of the perks.

### Non-Web3 Businesses

Non-[Web3](#_bfv0v93yygtt) businesses, sometimes also referred to as [Web 2.0](#_pm4f9jb1dx9i) businesses, are businesses that have not engaged in Web3 so far. Many businesses can benefit from implementing [blockchain](#_8snqzngpz4dk) technology; often, there is simply a knowledge gap. Onchains’ [research](#_863he3sz6kbn) supports those businesses that desire to engage with Web3 but lack the knowledge or creativity to come up with promising Onchain use cases. Ultimately, targeting [non-Web3 businesses](#_uavulu456m8f) can pave the way for tailored studies and further collaborations.

## O

### Onchain AG

[Onchain](https://onchain.org/) [AG](https://www.grantthornton.ch/globalassets/1.-member-firms/switzerland/insights/pdf/2023/ag-factsheet-en.pdf) is an entity based in Zug, Switzerland. Our goal is to provide practical knowledge that helps businesses understand and apply blockchain solutions to their current and future challenges.

### Onchain Foundation

The Onchain Foundation is a non-profit collective of individuals passionate about [blockchain](#_8snqzngpz4dk) and its potential to improve the world for all humans. Our mission is to drive the adoption of blockchain-based solutions that empower businesses and [entrepreneurs](#_qps56dehn5c9) to innovate and thrive. Committed to sustainability, diversity, and inclusion, the Onchain Foundation champions a decentralized future where technology serves as a catalyst for economic growth and equitable opportunity.

### Onchain Founding Membership

The Onchain founding membership offers a one-time opportunity to become one of Onchain Foundation’s 2,500 founding members and will be launched on the [Ethereum](#_x0vjx0qw1jzd) [blockchain](#_8snqzngpz4dk). Some of the perks include the following:

* NFT traits (rarity card)

The [NFT](#_gb6irmgmwah2) distribution is split into two parts. Once it is minted, the member will receive a membership card of one of the 5 rarities on offer.

* Membership art concept

Eligibibility for the [PFP](#_h0fmb4yhz3qg) NFT drop a few weeks after the minting. PFPs, designed by a well-renowned NFT artist, will replace membership cards that provide the full membership experience.

* Main membership utility

Full, lifetime access to all the published research reports. Lifetime membership of the current and any future versions of the platform.

For a more detailed description of the perks see [Onchain.org](http://onchain.org).

## P

### Print Magazine

The Onchain print magazine is designed to capitalize on the advantages of providing a non-digital magazine. These include distributing it to enterprises (e.g., Axel Springer, Porsche, Google, Amazon) and co-working spaces (e.g., Full Node, Wework)

This should, in turn, attract large [non-Web3](#_uavulu456m8f) audiences and introduce them to the possibilities and use cases blockchain offers in the real world.

We offer it to lifetime members as an additional membership perk and distribute it to partners and thought leaders as an incentive to join our [DeSci](#_mdpmlzu1d050) platform.

## R

### Reports

Onchain publishes solution-oriented [blockchain](#_8snqzngpz4dk) [research reports](https://onchain.org/research/), providing valuable insights that bridge the gap between theory and real-world applications. Our reports are designed to attract more people and businesses to Onchain. In addition to the reports, we also offer regular [magazine](#_8tdbra6h492j) articles and a [print magazine](#_ds52jw7f05t4), delivering the latest expert analysis to our audience.

### Research

Onchain employs two key research methodologies: the deductive approach, where we start with a hypothesis to prove or disprove, and grounded theory, where we build theories from collected data without prior assumptions. Our process involves identifying topics, conducting thorough research, and engaging thought leaders for insights. We regularly review and refine our findings until we reach conclusive results, culminating in a structured report.

## S

### Store

Onchain manages an online store that sells high-quality fashion products with a premium experience. The goal is to establish a positive brand for the [Onchain Foundation](#_5zirlyub6fyd), which will result in a solid revenue stream. The products do not create the perception of merchandise items but rather of a regular fashion brand like [Off-White](https://www.off---white.com) or [The Giving Movement](https://thegivingmovement.com). The Onchain store offers [Web3](#_bfv0v93yygtt) clothing products manufactured in sync with the environment. Durable clothing with unique replaceable collab tags comes in sustainable packaging to minimize waste and environmental impact.

In addition, Onchain offers unique velcro artwork tags, including project specific tags with company logos or artwork, and finally [NFT](#_gb6irmgmwah2) specific tags.

## 

## **Blockchain/Web3-related terms**

## A

### Account

An account consists of a unique identifier/address, a balance of [tokens](#_6nf3qhiytmx0), and possibly some additional properties used in other parts of the [blockchain](#_8snqzngpz4dk) application.

### Account Abstraction

Account abstraction in [blockchain](#_8snqzngpz4dk) refers to separating fund control from the execution of [smart contracts](#_jyc0nzbj202w). In other words, it allows smart contracts to manage funds without users having to transfer control of their assets to the contract. This concept is crucial in blockchain as it can significantly enhance user experience and security without requiring users to give up full access to their [wallets](#_cfytv3vwtr4w).

### Active Delegate

An active delegate can mostly be considered a [forging](#_pyv9s4k7hf4q) delegate who can forge new blocks. [Active delegates](#_kdqozjfokhx2) often participate in consensus protocols, where they validate [transactions](#_9xn3i92u2dqg), propose [blocks](#_2ywt2dbofdd1), and contribute to blockchain governance. Their actions directly impact the [consensus mechanism](#_hwg650g688zp) by influencing how consensus is reached.

### AirDrop

An AirDrop is the distribution of free [tokens](#_6nf3qhiytmx0) or cryptocurrencies to a large number of [wallet](#_cfytv3vwtr4w) addresses. [Blockchain](#_8snqzngpz4dk) projects often use this distribution as a marketing or promotional strategy to increase awareness, reward existing users, or attract new users to their platform.

### Artificial Intelligence

Artificial intelligence (AI) involves creating machines that think and act like humans, performing tasks considered "smart." AI processes large amounts of data differently from humans and aims to recognize patterns, make decisions, and judge like humans. It encompasses applications that perform complex tasks previously requiring human input, such as online customer communication. Often used interchangeably with [machine learning](#_u2b3qeqlulz2) (ML) and [deep learning](#_l9e5xcqc4pt9), AI refers to systems that operate under varying conditions without significant human oversight. AI models have the ability to learn from experience to improve performance.

### Automated Market Maker

An Automated Market Maker (AMM) is the most common [decentralized exchange](#_fbb45ne6rra2) (DEX) type that uses a liquidity pool of tokens to set asset prices automatically. Instead of an order book that most centralized or traditional exchanges use, AMMs rely on a mathematical formula to balance the token ratios in the liquidity pool. For example, to exchange [ETH](https://ethereum.org/en/) for [USDC](https://www.usdc.com/), a user adds ETH to the pool and receives USDC in return, with the exact amount determined by the pool's current ratio and formula. In this way, AMMs ensure constant liquidity and allow for seamless trading without the need to match buyers and sellers. While larger trades may experience some slippage due to their impact on the pool's balance, AMMs have become a cornerstone of decentralized finance ([DeFi](#_2lv6e6f1qe6h)), offering 24/7 trading of diverse tokens and democratizing access to financial markets.

## B

### Betanet

A temporary, public testing network. It serves as an intermediary step where users can test and identify potential issues before a [mainnet](#_450acasitat1) launch.

### BFT - Byzantine Fault Tolerance

In a system where components must agree to reach a consensus, Byzantine failures (usually caused by errors that are hard to detect) will prevent those components from reaching an agreement. A Byzantine Fault-Tolerant system ensures that measures are taken to manage such failures.

### BIP - Bitcoin Improvement Proposal

A Bitcoin Improvement Proposal (BIP) can be defined as a standard for proposing changes to the Bitcoin protocol. For example, [BIP39](https://www.cypherock.com/blogs/post-what-is-bip39) is one of many BIPs. This particular proposal describes the implementation of mnemonic code or a mnemonic sentence and how to create a human-readable mnemonic sentence, including how to convert that mnemonic into a seed.

### Bitcoin

Bitcoin is a digital currency designed to eliminate the need for central authorities like banks or governments. Instead, it leverages [blockchain](#_8snqzngpz4dk) technology to facilitate [peer-to-peer](#_9na4jkgk27ua) transactions on a decentralized network. Transactions are authenticated via Bitcoin’s proof-of-work ([PoW](#_gaszuat04k0c)) [consensus mechanism](#_hwg650g688zp), which rewards cryptocurrency miners for validating [transactions](#_9xn3i92u2dqg).

### Bitcoin Cash

Bitcoin Cash is a [hard fork](#_xkd96wh9j2yj) of the [Bitcoin](#_z63eovl5i5h1) network, developed as an electronic cash payment system. Its cryptocurrency, Bitcoin Cash (BCH), was created to be more practical for everyday [transactions](#_9xn3i92u2dqg) than Bitcoin (BTC). The Bitcoin Cash protocol features a larger [block size](#_ra2iqpo9crap), facilitating its use as a payment system by offering lower transaction fees compared to Bitcoin.

### Blockchain

A blockchain is a public [ledger](#_t8l3pyq2rjsz) of [transactions](#_9xn3i92u2dqg) maintained and verified by a decentralized, peer-to-peer ([P2P](#_9na4jkgk27ua)) network of computers using a [consensus mechanism](#_hwg650g688zp) to confirm data. Each computer in the network keeps its own copy of the shared record, making it nearly impossible for a single computer to alter past transactions or for malicious actors to compromise the network.

It can be considered a database that keeps a continuously growing list of records known as [blocks](#_2ywt2dbofdd1). These blocks are cryptographically linked, and each block contains a cryptographic [hash](https://de.wikipedia.org/wiki/Hash) of the previous block, the transaction data, and a [timestamp](#_lwyyltqpi4qg).

### Blockchain Application

A [blockchain](#_8snqzngpz4dk) application is any application that uses its own blockchain as a database layer. For example, it can be an application running on its own blockchain built with a software development kit (SDK).

### Blockchain App

Short form of [blockchain application](#_8qlxa2ecpp4u).

### Blockchain Tetralemma

The blockchain tetralemma is based on the [blockchain trilemma](#_e6n7t3n34hzq), which consists of decentralization, security, and [scalability](#_vndwes9ui21). It includes these three aspects but adds a fourth, usually profitability. As with the trilemma, trying to optimize all four of these aspects simultaneously is challenging.

### Blockchain Trilemma

The blockchain trilemma highlights the difficulty of simultaneously optimizing three crucial factors in blockchain technology: decentralization, security, and [scalability](#_vndwes9ui21). Achieving the highest levels in all three aspects simultaneously is a challenging task.

### Block

Blocks are files on a [blockchain](#_8snqzngpz4dk) where [transaction](#_9xn3i92u2dqg) data are permanently recorded. They contain recent transactions that the network still needs to validate. Once a block is validated, it is closed, and a new one is created for subsequent transactions. A unique number identifies each block, which contains encrypted information from previous blocks and new transactions. After the network has verified a block and its contents, new blocks can be generated.

### Block Height

The number of [blocks](#_2ywt2dbofdd1) in the blockchain between the [genesis block](#_70yembjtxggh) and the block of the specified block height.

### Block Size

Blockchain network protocols consist of [blocks](#_2ywt2dbofdd1) of data organized in a continuously updating, chain-like structure—hence the term "[blockchain](#_8snqzngpz4dk)." Each block contains transactions processed on the network, with the size or time interval of these blocks determined by the governance of the specific blockchain.

### BSC - Binance Smart Chain

BSC is a high-performance blockchain compatible with the Ethereum Virtual Machine ([EVM](#_plrv2iycqghx)) and equipped to support [smart contracts](#_jyc0nzbj202w).

## C

### Centralized Exchange

A Centralized Exchange (CEX) is an online platform that enables internet users to buy, sell, and swap crypto assets. CEXs are operated and owned by a single entity. They act as intermediaries between buyers and sellers and are bound to comply with the laws and regulations of the jurisdiction in which they operate.

A CEX platform maintains an order book for buy and sell orders, where traders specify the amount and price of [tokens](#_6nf3qhiytmx0)/[coins](#_ucpw7joemcgz) they wish to trade. It helps conduct these [transactions](#_9xn3i92u2dqg) by providing liquidity for the tokens/coins it supports on its platform.

Some examples of CEXs are [Binance](https://www.binance.com/en), [Coinbase](https://www.coinbase.com/en-de/), [Kraken](https://www.kraken.com/), and [HTX](https://www.htx.com/).

### CDBC

A central bank digital currency ([CBDC](https://thefintechtimes.com/what-is-a-central-bank-digital-currency-cbdc/)) is a digital representation of a country's central bank money or [fiat currency](#_kyjp1yp9zxud) that is not backed by a physical commodity like gold or silver.

### Coin

A coin is classed as a form of money and is native to its [layer 1](#_iapi07uv3y4r) blockchain. Its primary purpose is to act as a [store of value](#_golgj63geowj) and a medium of exchange, which can be equated to other forms of currency. Examples of coins are (BTC) [Bitcoin](#_z63eovl5i5h1), (ETH) [Ethereum](#_x0vjx0qw1jzd), and (LTC) [Litecoin](https://litecoin.org/).

### Coinbase Transaction

A generation transaction, commonly referred to as a coinbase transaction, is the initial [transaction](#_9xn3i92u2dqg) in a [block](#_2ywt2dbofdd1) on the [Bitcoin](#_z63eovl5i5h1) [blockchain](#_8snqzngpz4dk). It specifies the recipient(s) of the block reward. Unlike standard transactions that include both input and output data, a generation transaction creates new bitcoin (BTC) directly from the [protocol](#_v8qwd73s4svs), so it does not need input data.

### Cold Wallet

A cold wallet can be considered a digital safe for your cryptocurrency. It's a type of wallet that is kept offline, making it highly secure against online threats; unlike a [hot wallet](#_j4o7kb8ei7i), which is always connected to the internet for easy access, a cold wallet is disconnected, protecting your assets from hackers. It can be thought of as storing your valuables in a secure vault instead of carrying them around. Examples of cold wallets include hardware wallets like Ledger and Trezor and paper wallets, where private keys are printed on paper and stored safely.

### Consensus Mechanism

A [blockchain](#_8snqzngpz4dk) [consensus mechanism](#_hwg650g688zp) refers to a protocol unanimously adopted by all nodes in a blockchain network to validate and incorporate new [blocks](#_2ywt2dbofdd1) into the blockchain. Different types of consensus mechanisms exist, such as [PoW](#_gaszuat04k0c), [PoS](#_d4wssg7vism7), and [DPoS](#_nf1l4s244xux). The primary function of the consensus mechanism is to ensure all [nodes](#_b98tv6rmjwvj) within the network reach agreement on the order and validity of the [transactions](#_9xn3i92u2dqg).

### Cross Chain Communication

Cross-chain communication enables interaction and value exchange between different [blockchain](#_8snqzngpz4dk) networks, such as [token](#_6nf3qhiytmx0) transfers and data sharing, making it crucial to blockchain [interoperability](#_t34379a5wn8). Advancements in blockchain technology are expected to improve, resulting in cross-chain communication, allowing seamless data exchange across hundreds or even thousands of networks in the future.

### Crypto-off-Ramp

Crypto-off-ramps are services that enable cryptocurrencies or [tokens](#_6nf3qhiytmx0) to be converted back into [fiat currency](#_kyjp1yp9zxud), facilitating the transition from digital assets to traditional financial institutions. Crypto off-ramps are required to convert digital asset holdings into [fiat](#_kyjp1yp9zxud).

### Crypto-on-Ramp

A crypto-on-ramp is a website or app that enables users to purchase crypto [tokens](#_6nf3qhiytmx0) and other digital currencies using [fiat](#_kyjp1yp9zxud) money such as US Dollars, Euros, British pounds, etc.

## D

### DAO - Decentralized Autonomous Organization

A decentralized autonomous organization (DAO) operates without central leadership. Decisions originate from the community and are governed by a set of rules enforced on a [blockchain](#_8snqzngpz4dk).

### Dai

Dai is a crypto asset that attempts to maintain a stable 1:1 value with the U.S. dollar by locking other crypto assets in contracts.

### dApp - Decentralized Application

A decentralized application is created on a decentralized network, integrating a [smart contract](#_jyc0nzbj202w) and a user interface on the front end.

### Decentralized/Decentralization

Decentralization is a core feature of [blockchain](#_8snqzngpz4dk) technology, reducing or even eliminating intermediaries across industries. For instance, decentralized finance ([DeFi](#_2lv6e6f1qe6h)) platforms bypass banks, allowing profits and governance to be shared with users and the community. A decentralized network also allows crowd sourced consensus, making it difficult for any single entity to control or censor data. However, many experts believe that greater decentralization can reduce network throughput.

### Decentralized Artificial Intelligence

Decentralized Artificial Intelligence (DAI) can be described as [artificial intelligence](#_3kavnkyx503a) models trained and executed on decentralized networks that eliminate reliance on a single entity for control or data storage.

### Decentralized Storage Network

A Decentralized Storage Network (DSN) offers users [peer-to-peer](#_9na4jkgk27ua) (P2P) access to buy or rent data storage space. Clients use end-to-end encryption to securely transmit P2P files, which are protected by cryptographic proofs. Examples of decentralized storage networks include [Sia](https://sia.tech/), [Filecoin](https://filecoin.io/), and [Storj](https://www.storj.io/), which seek to mitigate the risks of data failures associated with centralized cloud storage providers. While many DSNs are built on [blockchain](#_8snqzngpz4dk) technology, others may employ different decentralized network architectures.

### Deep Learning

Deep learning (DL) is a subset of [machine learning](#_u2b3qeqlulz2) in which algorithms with multiple successive layers (known as neural networks) can extract features from the input data and make predictions like classic machine learning algorithms.

### DeFi - Decentralized Finance

DeFi is a financial framework built on decentralized [blockchain](#_8snqzngpz4dk) protocols. It enables [peer-to-peer](#_9na4jkgk27ua) transactions without relying on traditional intermediaries such as banks or brokers. It employs [smart contracts](#_jyc0nzbj202w), granting users access to diverse financial products and services without a central authority.

### Degen

A "Degen" is a slang term in the cryptocurrency community for traders who take high risks and speculate without doing thorough research or due diligence. These individuals often ignore important metrics, tokenomics, fundamental analysis, and technical analysis, instead making investment decisions based on superficial aspects like a token's logo or a catchy slogan.

### DeSoc - Decentralized Social Networks

Decentralized Social Networks (DeSoc) are social platforms built on decentralized technologies, including [blockchain](#_8snqzngpz4dk) and other distributed [ledger](#_t8l3pyq2rjsz) technologies. Unlike traditional social networks controlled by centralized entities, DeSoc platforms give users ownership and control over their data, content, and social connections. Examples of blockchain-based DeSoc platforms include [Farcaster](https://www.farcaster.xyz/) and [Lens](https://www.lens.xyz/), while non-blockchain examples include [Mastodon](https://joinmastodon.org/) and [BlueSky](https://bsky.social/about). These networks enhance privacy, security, and censorship resistance by distributing governance and eliminating single points of failure. Despite their benefits, such as user empowerment and new monetization models, DeSoc platforms face challenges in scaling, adoption, and providing a user experience comparable to traditional social media.

### Devnet

A [blockchain](#_8snqzngpz4dk) network for development purposes. For example, the [Lisk software development kit](https://lisk.com/sdk) (SDK) provides a dedicated [genesis block](#_70yembjtxggh) and configurations to conveniently set up a local Devnet while developing a blockchain application.

### DePIN - Decentralized Physical Infrastructure Network

DePIN is a concept whereby token rewards incentivize the creation and enhancement of physical infrastructure in the real world. The aim is to transition from a centralized to a decentralized model. Utilizing [blockchain](#_8snqzngpz4dk) technology and [token](#_6nf3qhiytmx0) rewards establishes and upkeeps decentralized physical infrastructure, encompassing wireless networks, cloud services, and power grids.

### DeSci - Decentralized Science

Decentralized Science (DeSci) uses b[lockchain](#_8snqzngpz4dk) and [Web3](#_bfv0v93yygtt) technologies to make scientific research more accessible, transparent, and efficient. By decentralizing funding, data management, and peer review, DeSci overcomes the limitations of traditional scientific institutions. This approach fosters broader participation and interdisciplinary collaboration and ensures the integrity of research. DeSci is instrumental in translating scientific advancements into practical applications, particularly in areas like healthcare and biotechnology, contributing to innovation across various industries.

### DEX - Decentralized Exchange

A Decentralized Exchange (DEX) is an online platform that enables users to buy cryptocurrencies directly through [peer-to-peer](#_9na4jkgk27ua) transactions without any middleman. Examples include [Binance](https://www.binance.com/en), [Coinbase](https://www.coinbase.com/en-de/), and [Bitstamp](https://www.bitstamp.net/). Unlike traditional centralized exchanges, where a third-party entity manages user funds and oversees [transactions](#_9xn3i92u2dqg), a DEX operates on a [peer-to-peer](#_9na4jkgk27ua) basis.

### DLT - Distributed Ledger Technology

Distributed Ledger Technology (DLT) is a decentralized [peer-to-peer](#_9na4jkgk27ua) digital system that records [transactions](#_9xn3i92u2dqg) simultaneously across multiple locations. Utilizing cryptography and [consensus mechanisms](#_hwg650g688zp), DLT enables participants to share an unalterable copy of the same [ledger](#_t8l3pyq2rjsz).

[Blockchain](#_8snqzngpz4dk) is one of the four types of DLTs, whereby its transaction records are kept in the [ledger](#_t8l3pyq2rjsz) as a chain of [blocks](#_2ywt2dbofdd1).

### Double Spending Problem

The double spending problem is a significant risk associated with digital currencies, where the same funds can potentially be duplicated and spent more than once. In contrast, with [fiat currency](#_kyjp1yp9zxud), once the spender hands over physical cash, it cannot be used again. However, with digital currency, [blockchain](#_8snqzngpz4dk) systems are specifically designed to prevent the same digital [coin](#_ucpw7joemcgz) or [token](#_6nf3qhiytmx0) (e.g., [Bitcoin](#_z63eovl5i5h1)) from being sent to multiple addresses. The risk of double spending in cryptocurrencies is reduced through various mechanisms ensuring all transactions' authenticity.

### DPoS - Delegated Proof of Stake

[DPoS](https://lisk.com/documentation/lisk-sdk/v5/modules/dpos-module.html#dpos) is the mechanism for determining eligible [block](#_2ywt2dbofdd1) creators. It is achieved by voting for registered delegate accounts, which can then create blocks depending on their vote weight. It is part of a [blockchain's](#_8snqzngpz4dk) consensus algorithm.

## E

### EIP

An EIP is a formal recommendation for updates and changes to the [Ethereum](#_x0vjx0qw1jzd) network. The acronym EIP stands for “Ethereum Improvement Proposal,” the Ethereum community members use them to contribute to the Ethereum network's further development.

### EoT - Economy of Things

The Economy of Things goes beyond the [Internet of Things](#_ijykk3nl8f24) by letting devices independently make money and trade the value they create. In contrast to the [Internet of Things,](#_ijykk3nl8f24) where devices are contextually aware and linked, the Economy of Things turns devices into economic agents. It's a system of decentralized and borderless economic connections between machines and people, allowing them to become increasingly autonomous and economically independent.

### ERC

ERC is a technical standard used on the Ethereum [blockchain](#_8snqzngpz4dk) for [smart contracts](#_jyc0nzbj202w). It stands for “Ethereum Request for Comment.” The [ERC-20](#_qgc30b1rcbrm) standard was originally implemented in 2015, allowing developers to establish their own tokens by adhering to it.

### ERC-20 Token

ERC-20 [tokens](#_6nf3qhiytmx0) are Ethereum-based tokens with standardized features. These ensure compatibility can be maintained with the broader [blockchain](#_8snqzngpz4dk) ecosystem. Simply put, ERC-20 serves as the technical standard governing the implementation of [tokens](#_6nf3qhiytmx0) through [smart contracts](#_jyc0nzbj202w) on the [Ethereum](#_x0vjx0qw1jzd) [blockchain](#_8snqzngpz4dk).

### ERC-721 Token

ERC-721 is a standard for non-fungible tokens ([NFTs](#_gb6irmgmwah2)) representing unique ownership. It is more intricate than [ERC-20](#_qgc30b1rcbrm), featuring optional extensions and distributed across multiple contracts.

### Ethereum

Launched in 2015, Ethereum is a decentralized, blockchain-based platform designed as a global supercomputer to support a range of interoperable [decentralized applications](#_p34magdiaafq) (dApps) using token economies and [smart contracts](#_jyc0nzbj202w). It operates on self-executing smart contracts that eliminate the need for intermediaries. The network is powered by its native cryptocurrency, ether (ETH), which covers [transaction](#_9xn3i92u2dqg) fees. Ethereum is open-source, programmable, private, and censorship-resistant, serving as the foundation for a decentralized internet that has led to innovations such as Initial Coin Offerings (ICOs), [stablecoins](#_repprl2yp93), and decentralized finance ([DeFi](#_2lv6e6f1qe6h)) applications.

### EVM - Ethereum Virtual Machine

The EVM is a vital component of the [Ethereum](#_x0vjx0qw1jzd) platform. It enables developers to build [dApps](#_p34magdiaafq) and [smart contracts](#_jyc0nzbj202w). EVM is instrumental in powering most of the [dApps](#_p34magdiaafq) built today. It also facilitates the execution of [smart contracts](#_jyc0nzbj202w) and supports Ethereum's goals of achieving user adoption and decentralization.

## F

### Faucet

In the [blockchain](#_8snqzngpz4dk) world, a faucet is generally defined as a tool that allows users to receive a certain amount of [tokens](#_6nf3qhiytmx0) for free.

### Fiat Currency

A fiat currency is a form of government-issued money used as legal tender by the citizens of a particular country, government, or region. Unlike currencies backed by physical commodities such as gold or silver, fiat currencies are backed by the issuing government. As a government-regulated instrument, fiat currency serves as a medium of exchange, a [store of value](#_golgj63geowj), and a unit of account. For money to be considered fiat, it must be durable, portable, divisible, uniform, widely accepted, and have a limited supply. Most paper currencies, such as the euro, yen, and U.S. dollar, are examples of fiat currencies.

### Forging

Forging is the process of creating new [blocks](#_2ywt2dbofdd1) on a [blockchain](#_8snqzngpz4dk). Rewards can be paid to the participants with cryptocurrencies and fees. Similar to mining in [Bitcoin](#_z63eovl5i5h1) or [Ethereum](#_x0vjx0qw1jzd), forging validates [transactions](#_9xn3i92u2dqg) but operates differently in ecosystems like proof-of-work [(PoW](#_gaszuat04k0c)) and proof-of-stake ([PoS](#_d4wssg7vism7)). A more in-depth explanation of forging can be found [here](https://0-100.io/glossary/forging).

### Fork

A fork can be defined as an occurrence of a [blockchain](#_8snqzngpz4dk) diverging into two forward paths in the network. In other words, an alternative version of the blockchain is created by simultaneously generating two [blocks](#_2ywt2dbofdd1) on different parts of the network. See [hard fork](#_xkd96wh9j2yj) and [soft fork](#_c3chqpff729z).

### Fungible Token

A fungible [token](#_6nf3qhiytmx0) is a digital asset created to have the same value and be interchangeable with other tokens of its kind. Fungibility is a key principle in traditional finance and economics, closely linked to government-issued money or [fiat currency](#_kyjp1yp9zxud).

## G

### Gamification

Gamification involves adding fun and interactive gaming features to non-game situations to boost interest and encourage specific behaviors. Crypto platforms use game-like elements such as rewards, badges, or levels to motivate users to participate and actively explore different features. This creates a feeling of accomplishment and progress, ultimately increasing user engagement and building long-term loyalty.

### Generative AI

Generative AI models can create new data like images, video, audio, or text. While not directly used in core [blockchain](#_8snqzngpz4dk) functions, generative AI has the potential to create new user experiences within [Web3](#_bfv0v93yygtt) environments.

### Genesis Block

The genesis [block](#_2ywt2dbofdd1) describes the very first block in the [blockchain](#_8snqzngpz4dk). It defines the initial state of the blockchain at the start of the network. A genesis block must be given to the application, and all networks should have a different genesis block.

## H

### Hard Fork

A hard fork is a software update that lacks backward compatibility. A hard fork occurs when new rules are introduced into the [blockchain](#_8snqzngpz4dk) code that is incompatible with the previous version's rules. [Nodes](#_b98tv6rmjwvj) that don't update their software become unable to communicate with those that have, sometimes leading to a split in the blockchain into two separate networks—one following the old rules and the other operating under the new, updated rules. For instance, [Bitcoin Cash](#_8g271frbyle0) was created after a hard fork of the [Bitcoin](#_z63eovl5i5h1) blockchain.

### Hash

Hashing is the process of converting an input of any size into a fixed-size output using a mathematical function known as a hash function. These functions are considered one-way, meaning they cannot be reversed to retrieve the original input. Unlike encryption, which aims to conceal data in transit or at rest, hashing is mainly used to verify data authenticity. It also plays a crucial role in securing network components, such as passwords and sensitive information, by storing them as hashes—the outputs generated by hash functions.

### 

### Hot Wallet

A hot [wallet](#_cfytv3vwtr4w) is like a digital wallet for everyday spending—always connected to the internet for quick transactions, like buying something or sending money. This convenience comes with a higher risk of hacking, similar to the risk of carrying cash. While hot wallets are ideal for easy access and frequent use, they aren't the best for storing large amounts of cryptocurrency long-term. For that, [cold wallets](#_ayl1ky9g5rj3) kept offline and secure from online threats, are preferred.

## I

### Interoperability

Interoperability is like speaking multiple languages fluently, allowing different [blockchain](#_8snqzngpz4dk) networks to communicate seamlessly. This means that [smart contracts](#_jyc0nzbj202w) on different blockchains can interact with each other, and it is possible to transfer assets and data between blockchains without needing a central authority. It can be thought of as trading [Bitcoin](#_z63eovl5i5h1) for [Ethereum](#_x0vjx0qw1jzd) directly, such as swapping your dollars for euros without needing a bank. The key difference here is that it is possible to natively swap [tokens](#_6nf3qhiytmx0) across different blockchain networks without relying on a central entity.

### 

### IoT - Internet of Things

This is a collective network of connected devices and technology, enabling communication between the devices, both with the cloud and among themselves.

## J

### JavaScript

JavaScript (JS) is a popular programming language for creating complex features and web applications. It is also the official programming language used by [Lisk](https://lisk.com/).

## K

### KYC

Know Your Customer (KYC) is a regulatory compliance process that businesses use to verify the identity and assess the risk level of their customers. This typically involves users providing official identification, such as a passport or driver's license. KYC regulations mandate that financial firms collect personal data on their customers and confirm the legitimacy of the individuals or clients they serve.

## L

### Layer 1

A layer 1 [blockchain](#_8snqzngpz4dk) serves as the foundational blockchain upon which secondary blockchain networks and applications can be constructed. L1s offer the fundamental infrastructure and security necessary for the operation of [layer 2](#_ws5uenk1b9qm) blockchains. Good examples of Layer 1 networks are [Bitcoin](https://bitcoin.org/en/), [Ethereum](https://ethereum.org/en/), and [Solana](https://solana.com/).

### Layer 2

A Layer 2 network encompasses any off-chain network, system, or technology constructed on top of a [layer 1](#_iapi07uv3y4r) [blockchain](#_8snqzngpz4dk). This extends the capabilities of the underlying base layer network. [Layer 2](#_ws5uenk1b9qm) networks can be employed to enhance blockchain functionalities and reduce the load on its parent network, enabling features like increased transaction throughputs. Examples of well-known [layer 2](#_ws5uenk1b9qm) networks are [Polygon](https://polygon.technology/), [Arbitrum](https://arbitrum.io/), and [Lisk](https://lisk.com/).

### Layer 3

Layer 3, commonly known as the application layer, is built on top of [layer 1](#_iapi07uv3y4r) (the base [blockchain](#_8snqzngpz4dk)) and [layer 2](#_ws5uenk1b9qm) (scaling solutions). While layers 1 and 2 address infrastructure and [scalability](#_vndwes9ui21), layer 3 is dedicated to developing user-facing applications and protocols. This layer includes decentralized applications ([dApps](#_p34magdiaafq)), decentralized finance ([DeFi](#_2lv6e6f1qe6h)) platforms, and other blockchain-based services directly interacting with users.

### Ledger

A ledger is a record-keeping system for tracking financial transactions. [Blockchains](#_8snqzngpz4dk) are often referred to as distributed ledgers.

### Lightning Network

The Lightning Network is a [layer 2](#_ws5uenk1b9qm) scaling solution that operates on top of [blockchains](#_8snqzngpz4dk) like [Bitcoin](#_z63eovl5i5h1). It establishes a private, two-way channel between users, allowing multiple [transactions](#_9xn3i92u2dqg) to occur off the main blockchain. These transactions are later consolidated and recorded as a single transaction on the main blockchain. This approach, applied across numerous transactions, reduces network congestion and enhances [scalability](#_vndwes9ui21).

### LSK

The token used in the [Lisk](https://lisk.com/) [Mainnet](#_450acasitat1).

## M

### 

### Machine Learning (ML)

A core [AI](#_3kavnkyx503a) technique in which algorithms learn from data to make predictions or decisions without explicit programming.

### Mainnet

A [mainnet](https://lisk.com/documentation/lisk-core/v3/index.html#mainnet) is a fully developed, functional, and independent [blockchain](#_8snqzngpz4dk) that runs on its own network and uses its own protocol and technology.

### Merkle Trees

A Merkle tree is a data structure made up of data-converting [hashes](#_kmyyb7hvd01t) used by [blockchains](#_8snqzngpz4dk) to verify information securely. It summarizes all the [transactions](#_9xn3i92u2dqg) in a [block](#_2ywt2dbofdd1) by generating a digital fingerprint (i.e., a single [hash](#_kmyyb7hvd01t)) representing the entire set of transactions.

### Metaverse

The metaverse is an immersive, multi-dimensional environment. It is a virtual reality world where people can interact with each other and digital objects as if they were in the same physical space. It represents a future iteration of the internet with persistent virtual worlds for socializing, working, gaming, and shopping, creating an evolved, three-dimensional cyberspace.

### Mining Pool

A mining pool aggregates, or "pools," the [hash](#_kmyyb7hvd01t) rate of participating crypto miners to collectively mine [blocks](#_2ywt2dbofdd1) and share the associated block rewards. This approach offers miners a more consistent return on their efforts and enables smaller operations to compete with larger mining farms. Mining pools are blockchain-specific and typically charge a fee of 0–2% of all block rewards.

### Module Asset

A module asset allows a module to execute specific state changes on the [blockchain](#_8snqzngpz4dk) based on [transactions](#_9xn3i92u2dqg). A transaction with the corresponding module and asset ID needs to be sent to the [blockchain](#_8snqzngpz4dk) application to trigger the logic defined in a particular module asset. The data provided in the transaction asset provides the required input data to execute the desired state changes.

### Multi-Signature Wallet

A multi-signature (multi-sig) [wallet](#_cfytv3vwtr4w) is a type of wallet that requires multiple keys to sign a [transaction](#_9xn3i92u2dqg) before it can be executed. In contrast, standard wallets need only a single signature to authorize transactions.

## N

### Network Graph

A network graph (force-directed graph) is a mathematical structure used to represent relationships between points in an aesthetically pleasing manner visually. It illustrates how subjects are interconnected, with entities displayed as [nodes](#_b98tv6rmjwvj) and their relationships represented by lines.

### Nonce

A nonce (short for "number only used once") is a number added to the data in a [block](#_2ywt2dbofdd1) before it is [hashed](#_kmyyb7hvd01t) during the Proof of Work ([PoW](#_gaszuat04k0c)) mining process.

### Natural Language Processing (NLP)

NLP enables [AI](#_3kavnkyx503a) to understand and generate human language. NLP can be used to analyze sentiment in social media data on [blockchains](#_8snqzngpz4dk) or to create chatbots for interacting with [decentralized applications](#_p34magdiaafq) (dApps).

### Network Effects

Network effects happen when a product or service becomes more valuable as more people use it. This, in turn, increases the value of the service or product for the existing users, encouraging new users to join and increasing its value further in a positive feedback loop.

### NFT - Non Fungible Token

NFTs are digital assets in the form of unique cryptographic [tokens](#_6nf3qhiytmx0). Examples can represent real-world objects such as art, music, games, and videos, which, due to their uniqueness, can result in them becoming collectible items of value.

### Node

A blockchain node is typically a device, such as a computer, that participates in a [blockchain](#_8snqzngpz4dk) network by running the network's protocol software. This enables it to validate transactions contribute to network security, and ensure consensus on a public [ledger](#_t8l3pyq2rjsz). Nodes communicate with each other, and a greater number of nodes increases the network's decentralization.

## O

### Off Chain Assets

Off chain assets in crypto are [tokens](#_6nf3qhiytmx0) or [coins](#_ucpw7joemcgz) that are stored off of the [blockchain](#_8snqzngpz4dk). For example, in a [cold wallet](#_ayl1ky9g5rj3) or a third-party intermediary.

### Optimism

[Optimism](https://app.optimism.io/superchain/) is a [Layer 2](#_ws5uenk1b9qm) scaling solution built on top of the [Ethereum](#_x0vjx0qw1jzd) [blockchain](#_8snqzngpz4dk). It addresses the challenges faced by running on the Ethereum network. Optimism developed the [OP](#_rmnwg3e8bdm1) [Superchain,](#_3nwwic71lhxy) a network of interconnected [layer 2](#_ws5uenk1b9qm) [blockchain](#_8snqzngpz4dk) networks built using its open-source OP Stack, which was designed to provide enhanced [scalability](#_vndwes9ui21), [interoperability](#_t34379a5wn8), and flexibility for decentralized application development.

### OP Chains

The [Superchain](#_3nwwic71lhxy) is a network of [layer 2](#_ws5uenk1b9qm) chains called OP (over powered) chains that share security, a communication layer, and an open-source technology stack. Unlike other multi-chain designs, these chains are standardized and intended to be used interchangeably.

### Optimistic Rollups

Optimistic [rollups](#_wv0k85ev2c62) accumulate transactions on the respective chain and bundle them into a batch (rollup). These are then submitted for execution on the mainchain. The term "optimistic" is used as these transactions are considered to be valid unless proven otherwise within a specified time period. This reduces the number of computations and results in lower gas fees. Furthermore, a “fraud-proof” mechanism is deployed.

### Oracles

Oracles are third-party services that provide external real-world data to [blockchain](#_8snqzngpz4dk) protocols, often to [smart contracts](#_jyc0nzbj202w). They enhance the blockchain’s functionality by securing, verifying, and validating its data, as blockchains and [smart contracts](#_jyc0nzbj202w) are typically closed systems. Oracles can be either decentralized, drawing from multiple data sources, or centralized, controlled by a single entity. An essential use of blockchain oracles is delivering price and data feeds for the trustless execution of smart contracts in the [DeFi](#_2lv6e6f1qe6h) sector.

### Orphan Block

An orphan block (or stale block) is a [block](#_2ywt2dbofdd1) that gets rejected by the [blockchain](#_8snqzngpz4dk) network due to the simultaneous mining of two blocks. Although theoretically, a [soft fork](#_c3chqpff729z) occurs when two blocks are mined at the same time; orphaned blocks typically affect only a few subsequent blocks. These blocks are valid and verified but serve no purpose once rejected and exist in isolation from the main blockchain.

## P

### Passphrase

A passphrase can be described as an extended password. It is a string of words used for authentication, usually 15 characters or more.

### Peg

Pegs are mechanisms that link the value of one asset to another on a 1:1 basis. They are mainly used to enable the trading of different assets, which is often limited due to varying [blockchain](#_8snqzngpz4dk) protocols. Pegging allows users to exchange assets pegged at a 1:1 ratio with their native assets while potentially enjoying lower [transaction](#_9xn3i92u2dqg) fees and faster confirmation times.

### PFP - Picture-for-Profile

A PFP [NFT](#_gb6irmgmwah2), which stands for Picture-for-Profile Non-Fungible Token, is a unique digital image created to be the owner's personal profile picture.

### POAP - Proof of Attendance Protocol

A Proof of Attendance Protocol refers to [NFTs](#_gb6irmgmwah2) that prove a person has attended a particular event. These badges are supported by a cryptographic record and sent to a person’s [wallet](#_cfytv3vwtr4w) as a reward for participating in certain activities.

### PoS - Proof of Stake

Proof of Stake (PoS) is a consensus mechanism used to achieve agreement over a distributed network. With PoS, the consensus is determined based on each user's stake in the network.

In PoS networks, participants are incentivized to stake native [coins](#_ucpw7joemcgz) in [validator](#_9rjlm127n8um) [nodes](#_b98tv6rmjwvj), which involves validating [transactions](#_9xn3i92u2dqg) and earning rewards. By staking, users help secure and stabilize the network while earning interest on their investment. Validator nodes are randomly selected to validate [block](#_2ywt2dbofdd1) data and generate the next block, earning native coins as a reward. A strong network of nodes enhances security, resilience, and computational power. Additionally, PoS systems often allow validator nodes to participate in decentralized governance by voting on important updates and decisions. PoS networks already demonstrate faster speeds, greater [scalability](#_vndwes9ui21), and improved energy efficiency compared to Proof of Work ([PoW](#_gaszuat04k0c)) [blockchains](#_8snqzngpz4dk).

### PoW - Proof of Work

Proof of Work is a type of [consensus mechanism](#_hwg650g688zp) used to achieve agreement over a distributed network. With PoW, in order to complete the [transactions](#_9xn3i92u2dqg) on a given network, the miners have to solve complex mathematical problems to be rewarded with the tokens. In a nutshell, the PoW consensus algorithm is used to confirm transactions and produce new [blocks](#_2ywt2dbofdd1) to the chain. Miners have to compete against each other to complete transactions on the network and receive rewards. Hence, the PoW mechanism allows consensus to be reached while simultaneously maintaining network security.

### Private Key

[Public-key](#_mbetrrmjke3o) cryptography (asymmetric cryptography) is a specialized cryptographic system that uses pairs of long alphanumeric keys that must be used together. Public keys serve as [wallet](#_cfytv3vwtr4w) addresses that can be shared with others, while private keys, known only to their owner, provide access to funds. These keys are generated through cryptographic algorithms that solve mathematical problems to create a one-way function.

### Protocol

A [blockchain](#_8snqzngpz4dk) protocol refers to a specific blockchain platform or network, such as the [bitcoin](#_z63eovl5i5h1) protocol. It can also denote a set of rules that govern interactions within a blockchain network, including [consensus](#_hwg650g688zp), network participation, and [transaction](#_9xn3i92u2dqg) validation.

### Protocol Layer

The protocol layer comprises the core [blockchain](#_8snqzngpz4dk) [consensus mechanism](#_hwg650g688zp) and [nodes](#_b98tv6rmjwvj) that form the foundation of a blockchain. It can also include external [layer 2](#_ws5uenk1b9qm) systems like [sidechains](#_y36i1sccj9ww) and virtual machines. Typically, this layer refers to the underlying architecture of all [layer 1](#_iapi07uv3y4r) blockchain networks. It contains elements such as [node](#_b98tv6rmjwvj) addresses, error reporting, interface identification, network synchronization, state changes, and the processing of network [transactions](#_9xn3i92u2dqg).

### Public Address

A public address is an abbreviated form of a user’s public cryptographic key. It is used to receive [transactions](#_9xn3i92u2dqg) via a [blockchain](#_8snqzngpz4dk) network protocol and often serves as a substitute for a public key.

### Public Key

A public key is a cryptographic code that allows you to receive cryptocurrency [transactions](#_9xn3i92u2dqg). Paired with a [private key](#_644bfddu7tz0), it can be shared publicly, enabling others to send transactions. However, the private key is required to "unlock" and prove ownership of the received cryptocurrency. Typically, a public key is presented as an address, a shortened version of the public key itself. The private key, in contrast, should always remain confidential.

### Public Key Cryptography

Public-key cryptography (PKC) is a cryptographic system that uses paired alphanumeric keys: [public keys](#_mbetrrmjke3o), which can be shared with others, and [private keys](#_644bfddu7tz0), known only to their owner. Public keys are used to receive cryptocurrencies on the [blockchain](#_8snqzngpz4dk) and, in combination with the corresponding [private key](#_644bfddu7tz0), to send them. These keys are generated through cryptographic algorithms that create one-way functions. Public-key cryptography is also referred to as asymmetric cryptography.

### P2P - Peer-to-Peer

A peer-to-peer network is a group of [nodes](#_b98tv6rmjwvj) (devices) that make up a decentralized network that can collectively share and store data, whereby each node acts as an individual peer.

## Q

### QR Code

A quick response (QR) code is a type of matrix barcode that uses a machine-readable optical label, often scanned with a mobile phone, to store sensitive information about the item it’s attached to. QR codes typically contain data for tracking, locating, or identifying that links to a mobile app or website. They store data using four standardized encoding methods (byte/binary, alphanumeric, numeric, and kanji).

## R

### RaaS - Rollups-as-a-Service

A RaaS consists of different rollups, namely a custom-built solution. These are considered to be simplified, elastic, flexible, ‘pay-as-you-go’ models designed to reduce complexity.

### Recovery Phrase/Recovery Seed Phrase

A recovery phrase, also known as a "seed phrase" or "recovery seed phrase," is a 12, 18, or 24-word code used as a backup to regain access to a cryptocurrency [wallet](#_cfytv3vwtr4w) if the [private key](#_644bfddu7tz0) is lost. This phrase corresponds to information stored within the wallet that can unlock the private key needed to restore access.

### ReFi - Regenerative Finance

ReFi is an alternative financial system emphasizing the promotion and restoration of sustainability and resilience, not just monetary gains. In the [blockchain](#_8snqzngpz4dk) ecosystem, this is often referred to as a cryptocurrency project that utilizes its platform for investments in sustainability, encompassing environmental, social, and financial stability and growth.

### Rollups

A rollup is a type of modular [layer 2](#_ws5uenk1b9qm) scaling solution that conducts [transactions](#_9xn3i92u2dqg) off the main [blockchain](#_8snqzngpz4dk) to lower transaction costs and enhance throughput on the mainchain. It enhances [scalability](#_vndwes9ui21) and performance by reducing the computational load on the primary [layer 1](#_iapi07uv3y4r) chain.

### Rug Pull

A rug pull in crypto is a scam where the developers of a cryptocurrency project suddenly withdraw all the investors' funds and disappear. This often happens with meme [coins](#_ucpw7joemcgz) or new projects that seem promising but have malicious intentions. Essentially, investors are left with worthless [tokens](#_6nf3qhiytmx0) as the coin's value drops drastically or the project is abandoned entirely.

### RWA - Real-World Assets

Real-world assets encompass a wide range of physical, digital, or data-based assets that derive their value from existing outside the [blockchain](#_8snqzngpz4dk). Tokenizing RWAs involves creating a digital twin that resides on a blockchain.

## S

### Scalability

The scalability of a [blockchain](#_8snqzngpz4dk) refers to its capacity to handle [transactions](#_9xn3i92u2dqg), store data, and achieve consensus effectively as the network expands with the addition of more users.

### Scrypt

Scrypt is the [hash](#_kmyyb7hvd01t) function used by [Litecoin](https://litecoin.org/) to convert an input of letters and numbers into an encrypted output. While it differs from the [SHA-256](#_6crh7u2zfcea) hash function used by [bitcoin](#_z63eovl5i5h1), it operates within a similar [Proof of Work](#_gaszuat04k0c) (PoW) [consensus mechanism](#_hwg650g688zp). Scrypt was initially designed to restrict mining to [CPUs](https://www.arm.com/glossary/cpu#:~:text=The%20CPU%2C%20also%20referred%20to,programs%20running%20on%20the%20device.) and [GPUs](https://www.intel.com/content/www/us/en/products/docs/processors/what-is-a-gpu.html), although scrypt-capable [ASICs](https://getbtcz.com/what-is-an-asic/#:~:text=Application%2Dspecific%20integrated%20circuit%20(abbreviated,after%20CPUs%2C%20GPUs%20and%20FPGAs.) have since been developed.

### Sharding

Sharding is a technique used to partition a [blockchain](#_8snqzngpz4dk) network or other computer networks or databases to distribute computational and storage workloads across a wider set of devices or [nodes](#_b98tv6rmjwvj). This approach enhances the system's throughput and [transaction](#_9xn3i92u2dqg) speed by having each node maintain information related only to its specific shard or partition. Since each node handles only a fraction of the network's total transactional load, the network's overall processing capabilities and resilience are significantly improved. Consequently, sharding has enabled many blockchain networks to achieve faster transaction speeds, greater security, and better suitability for widespread enterprise use.

### SHA-256

SHA-256 is part of the SHA-2 cryptographic [hash](#_kmyyb7hvd01t) function family, developed by the National Security Agency ([NSA](https://www.nsa.gov/)) and later became well-known as a core component of the [bitcoin](#_z63eovl5i5h1) [blockchain](#_8snqzngpz4dk) network. As a Secure Hash Algorithm (SHA), SHA-256 secures data using a cryptographic mathematical operation to generate a unique 256-bit, 64-character sequence of letters and numbers, known as a hash, from an input. These functions are typically designed to be one-way operations, making it nearly impossible to reverse-engineer the original data from its hash value.

### Sidechain

A sidechain is an external secondary [blockchain](#_8snqzngpz4dk) protocol linked to a primary blockchain network (mainchain). Sidechains enable the transfer of data and value between themselves and the mainchain and often use a different [consensus mechanism](#_hwg650g688zp). This allows for greater flexibility and [scalability](#_vndwes9ui21), as systems with robust sidechain [interoperability](#_t34379a5wn8) can cater to a wider range of enterprise and individual users. Some sidechains facilitate asset transfers between multiple protocols, like [Ethereum](#_x0vjx0qw1jzd) and [Bitcoin](#_z63eovl5i5h1), while others enhance [layer 2](#_ws5uenk1b9qm) scaling solutions to boost the mainchain's [transaction](#_9xn3i92u2dqg) speeds.

### Smart Contract

A smart contract is a self-executing code or protocol that automatically enforces a set of instructions verified on the [blockchain](#_8snqzngpz4dk). These contracts are trustless, autonomous, decentralized, and transparent, becoming irreversible and unmodifiable once deployed. While they have many applications, some of the most common include financial contracts like loans, derivatives, and trading. They are also used in legal agreements, identity management, and various other scenarios. Popular in decentralized finance [(DeFi](#_2lv6e6f1qe6h)), [smart contracts](#_jyc0nzbj202w) can be combined into decentralized applications ([dApps](#_p34magdiaafq)) to perform more complex functions.

### Smart Contract Wallet

A [smart contract](#_jyc0nzbj202w) wallet is a decentralized application ([dApp](#_p34magdiaafq)) built on a [blockchain](#_8snqzngpz4dk) that enables users to manage their digital assets using smart contract code.

### Soft Fork

A soft fork is a backward-compatible blockchain update, allowing [nodes](#_b98tv6rmjwvj) with updated software to remain interoperable with those running the older version. Unlike a [hard fork](#_xkd96wh9j2yj), where only new [blocks](#_2ywt2dbofdd1) are valid, soft forks involve less drastic protocol changes.

### Source-Code Fork

A source-code fork is a type of [hard fork](#_xkd96wh9j2yj) where the original source code is used from an existing [blockchain](#_8snqzngpz4dk) network to create a new one. As with all hard forks, source-code forks can render previously invalid [blocks](#_2ywt2dbofdd1) and [transactions](#_9xn3i92u2dqg) on the blockchain valid, requiring all [nodes](#_b98tv6rmjwvj) from the previous network to upgrade to the latest software protocol. Additionally, like other hard forks, source-code forks are not backward-compatible, meaning they cannot be reverted to their prior state.

### Stablecoin

A stablecoin is a digital currency designed to maintain a stable value. Most stablecoins are directly linked to a specific [fiat currency](#_kyjp1yp9zxud) or tangible commodity, such as the [Gemini Dollar](https://www.gemini.com/dollar) (GUSD), which is pegged 1:1 to the U.S. dollar. However, some stablecoins achieve price stability through collateralization with other cryptocurrencies or algorithmic management of [token](#_6nf3qhiytmx0) supply. Since stablecoins maintain a relatively constant value, they are intended for use rather than as an investment.

### State Data

State data is a snapshot of all data stored on the [blockchain](#_8snqzngpz4dk) at a specific moment in time. This includes account balances, [smart contract](#_jyc0nzbj202w) details, and other relevant information. The blockchain's state is dynamic, changing with each [transaction](#_9xn3i92u2dqg) and smart contract execution.

### Store of Value

A store of value is an asset that is anticipated to retain its value or purchasing power over time and can be reliably accessed and exchanged in the future. Historically, [fiat currency](#_kyjp1yp9zxud), real estate, and precious metals like gold and silver have been considered reliable stores of value. As [blockchain](#_8snqzngpz4dk) technology becomes more mainstream, many people also view certain cryptocurrencies, especially [bitcoin](#_z63eovl5i5h1) (BTC), as an effective store of value.

### Superchain

The Superchain is a concept designed by [Optimism](#_6960v6fqzhyt). It comprises a network of [layer 2](#_ws5uenk1b9qm) chains, referred to as [OP Chains](#_rmnwg3e8bdm1), that jointly utilize security, a communication layer, and an open-source technology stack. The Superchain builds interconnected layer 2 [rollup](#_wv0k85ev2c62) networks, or OP chains' that share the standardized OP Stack architecture for seamless interaction, as opposed to creating isolated [blockchains](#_8snqzngpz4dk).

Unlike multi-chain designs, these chains are standardized and meant to function as interchangeable resources.

### Sybil Attack

A Sybil attack is an online security breach where an attacker creates numerous fake identities that function as [nodes](#_b98tv6rmjwvj) to overwhelm and disrupt a target network. These attacks exploit the way legitimate nodes connect with each other. Sybil attacks can be particularly harmful to systems where new nodes can be created and synchronized with relative ease.

## T

### Testnet

An official testing network is an instance of a [blockchain](#_8snqzngpz4dk) used for testing purposes. It consists of the same version of the mainnet underlying software. All testing and experimentation can be performed on the testnet without jeopardizing the actual mainnet.

### Timestamp

A timestamp is a digital record that marks a [transaction's](#_9xn3i92u2dqg) precise moment. Timestamps logged onto a blockchain’s [ledger](#_t8l3pyq2rjsz) are immutable and uniquely correspond to the specific transaction they record.

### Token

A token represents a physical or virtual object or an abstract concept like a gift.

In the digital world, tokens vary. Crypto tokens function as digital keys on specific [ledgers](#_t8l3pyq2rjsz), unlike digital [coins](#_ucpw7joemcgz) that are central to their systems.

A [token](#_6nf3qhiytmx0) is different from a coin in that it is created on top of an existing chain, as opposed to a coin that is native to its [layer 1](#_iapi07uv3y4r) [blockchain](#_8snqzngpz4dk). Crypto tokens serve multiple purposes beyond currency, such as providing access to services or representing ownership of digital art. There are generally five types of digital tokens: payment, utility, security, equity, and [NFTs](#_gb6irmgmwah2).

### Token Liquidity

Token liquidity refers to the ease with which a digital [token](#_6nf3qhiytmx0) can be converted into digital assets or cash without impacting its price. Having good liquidity reduces investment risk and, crucially, facilitates the creation of an exit strategy, making it more straightforward to sell.

### Tokenization

Tokenization involves transforming an asset or its ownership rights into distinct units known as [tokens](#_6nf3qhiytmx0). Tokens are digital representations of an asset on a [blockchain](#_8snqzngpz4dk) and generally serve as indicators of ownership for valuable assets.

### TPS - Transactions per Second

The transactions per second (TPS) denotes the number of [transactions](#_9xn3i92u2dqg) a [blockchain](#_8snqzngpz4dk) network can handle in one second.

### Transaction

A transaction involves a contract, or agreement, such as a transfer, or exchange of assets between two or more parties. A [blockchain](#_8snqzngpz4dk) transaction is a transfer of value from one address on a network to another. Simply put, it is a transmission of data across the network of computers within the blockchain system.

### Trading Volume

In capital markets, trading volume refers to the quantity of a security traded within a specific time frame. It is usually reported as the number of shares exchanging hands during a trading session or period. Trading volume for any openly traded asset constantly fluctuates, and the direction and magnitude of these changes are key factors that many investors consider in their analysis.

### Transaction

In a blockchain context, a transaction (TX) typically refers to the exchange of various types of data between users on a [blockchain](#_8snqzngpz4dk) network. Depending on their origin, transactions can vary in speed, security, and privacy. The most common transaction type involves users exchanging network-specific [coins](#_ucpw7joemcgz) or [tokens](#_6nf3qhiytmx0).

### Transaction Fee

A number of [tokens](#_6nf3qhiytmx0) that is required to send a [transaction](#_9xn3i92u2dqg) on the respective [blockchain](#_8snqzngpz4dk).

### Transaction ID

A [hash](#_kmyyb7hvd01t) of a [transaction](#_9xn3i92u2dqg) that uniquely identifies a transaction.

### Transaction Message

A [transaction](#_9xn3i92u2dqg) message is a piece of data signed by an external party. It represents either a message or a new autonomous object.

Transactions are recorded into each [block](#_2ywt2dbofdd1) of the [blockchain](#_8snqzngpz4dk). A message is created by contracts interacting with each other or by a transaction.

### TVL - Total Value Locked

TVL is simply defined as the total value of cryptocurrency locked in a [smart contract](#_jyc0nzbj202w).

## U

### Unit of Account

A unit of account is a standard measure used to assess the value of goods or services. By assigning a specific measurement unit to an offering, its monetary value can be easily understood in abstract terms, eliminating the need for bartering. This function of providing a consistent measure of value is one of the three essential roles of money, alongside serving as a [store of value](#_golgj63geowj) and a medium of exchange.

### Utility Token

A utility t[oken](#_6nf3qhiytmx0) is a digital asset designed to provide its holder with access to a [blockchain](#_8snqzngpz4dk) protocol’s products or services. These tokens are meant for use within the blockchain's network rather than as investments. However, because the value of most utility tokens tends to fluctuate based on the network's popularity and adoption, many traders and crypto enthusiasts still buy them as speculative investments.

### UTXO - Unspent Transaction Output

UTXO is an unspent output. In other words, it can be thought of as an indivisible chunk of a [token](#_6nf3qhiytmx0) that is under the control of the [private keys](#_644bfddu7tz0) belonging to the owners.

## V

### Validator

In the context of [blockchain](#_8snqzngpz4dk) technology, a validator is an entity tasked with verifying and approving [transactions](#_9xn3i92u2dqg) submitted by users or blockchain clients. Each blockchain [protocol](#_v8qwd73s4svs) defines its own criteria for what qualifies as a validator and how these validators function. Most decentralized blockchain networks depend on some type of validator [node](#_b98tv6rmjwvj) to process on-chain transactions in a permissionless and distributed way.

### Vanity Address

Vanity addresses are cryptocurrency addresses customized according to specific parameters set by the user, making them more personal and easily recognizable while maintaining security. For example, [bitcoin](#_z63eovl5i5h1) vanity addresses are like regular addresses in functionality but include a personalized alphanumeric string, message, or special word chosen by the owner.

### Volatility

Volatility refers to the extent to which an asset's trading prices fluctuate relative to its average price over a specific period. The more volatile an asset is, the more frequently and significantly its price changes. Volatility is typically measured using standard deviations of logarithmic returns. Many investors monitor an asset's volatility to spot and exploit potential trading opportunities based on perceived price trends. However, excessive and unpredictable price swings often deter investors with lower risk tolerance.

### Volume

Volume measures how frequently a specific [coin](#_ucpw7joemcgz) or [token](#_6nf3qhiytmx0) is traded within a certain time frame. Investors use this metric to gauge the popularity of buying or selling an asset at any given moment. Volume indicates the total monetary value of a cryptocurrency traded over a period and is crucial because it significantly influences price, both in absolute and relative terms. See [trading volume](#_p1aqw23fgo0p).

## W

### Wallet

Wallets can be divided into three distinct categories: software, hardware, and paper wallets. Software wallets can be desktop, mobile, or online.  
In short, a wallet will store [public keys](#_mbetrrmjke3o) and [private keys](#_644bfddu7tz0) and can interface with various [blockchains](#_8snqzngpz4dk), enabling users to monitor their balance, send [tokens](#_6nf3qhiytmx0), and conduct other operations.

### Web2

Web 2.0 emerged in the early 2000s as a second wave of internet innovation characterized by its interactive, read-write design. Platforms like Amazon, Facebook, Airbnb, Alibaba, and X spearheaded this era by providing dynamic, multi-functional applications across various devices. However, Web 2.0 has faced criticism for being overly centralized and fostering excessive profit-driven practices, intrusive advertising, mass surveillance, reduced privacy, and widespread data theft.

### Web3

Web3 is the next generation of the Internet, in which all applications are decentralized and can run on the blockchain. Web3 enables most users to be linked through decentralized networks and maintain control over their own data.

The four core concepts of Web3 are decentralization, [artificial intelligence](#_3kavnkyx503a), and [machine learning](#_u2b3qeqlulz2), trustless and permissionless networks, and omnipresent connectivity.

The first version of the Web (Web 1.0) was the "read-only Web," and the second version added the ability to “write.” Web 2.0 is described as the "participative social Web." Web3 goes a step further and can be classed as the "read, write, own, Web." This stage shifts users away from centralized platforms such as Facebook and Google.

### Whitepaper

A whitepaper is a report-style document that explains a complex issue within a specific industry or field and outlines how an enterprise addresses that problem. Typically, whitepapers introduce a business model and development plan. In the context of [blockchain](#_8snqzngpz4dk), a whitepaper is often one of the first documents created once a project has a working product and initial funding. It also serves as a pitch to attract additional investors. Blockchain-specific whitepapers usually include details on the technical architecture, [token](#_6nf3qhiytmx0) economics, team, and other relevant information.

### Wrapped Token

A wrapped [token](#_6nf3qhiytmx0) is a digital asset tied to another cryptocurrency's value. It's called a wrapped token because the original asset is secured in a specialized digital vault, enabling the creation and use of the wrapped token on a different [blockchain](#_8snqzngpz4dk). This process allows the asset to benefit from the unique functionalities offered by different blockchains, thereby expanding its utility across various networks.

## Y

### Yellow Paper

In traditional contexts, a yellow paper can have a broader meaning. Still, in the [blockchain](#_8snqzngpz4dk) space, it usually refers to a highly technical document detailing the specific technical components of a blockchain or related system. Yellow papers are often more concise than white papers, focusing on the most complex technical aspects of a blockchain protocol.

### Yield Farming

Yield farming involves staking or locking up cryptocurrencies within a [blockchain](#_8snqzngpz4dk) protocol to earn tokenized rewards. Many decentralized finance ([DeFi](#_2lv6e6f1qe6h)) projects use yield farming to encourage users to provide liquidity and maintain network stability, as these projects operate without a centralized market facilitator.

## Z

### Zero Knowledge Proofs

A Zero-Knowledge Proof (ZKP) is a cryptographic method that offers enhanced privacy for users in digital transactions. Essentially, ZKPs allow one party to prove to another that they possess a particular piece of information without revealing any details about that information itself. These proofs enable the verification of information without disclosing any specifics about the underlying data or the identities of the parties involved in the transaction.

### Zero Knowledge Rollups

A zero-knowledge rollup (zk rollup) is a [layer 2](#_ws5uenk1b9qm) scaling solution that shifts computation by executing them off the main [blockchain](#_8snqzngpz4dk) (off chain) while still storing the [transaction](#_9xn3i92u2dqg) data on the main blockchain and retaining the [transaction](#_9xn3i92u2dqg) data on chain in a [layer 1](#_iapi07uv3y4r) network. By using [zero-knowledge proofs](#_72bbzn6c8m0t), off-chain computation results are proven valid on chain.

Unlike [optimistic rollups](#_eliy27jfc83), which assume transactions are valid and only verify them if challenged, zk-rollups immediately verify the validity of transactions using zero-knowledge proofs. This results in faster finality and increased security but can be more computationally intensive.

### Zero Knowledge Snarks

A Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk SNARK) is a cryptographic proof used to maintain privacy in blockchain-based distributed [ledger](#_t8l3pyq2rjsz) systems. It allows one party to prove they have specific information without revealing the actual data to the network by using a secret key before the transaction is broadcast. Zk SNARKs gained prominence with privacy-focused [blockchain](#_8snqzngpz4dk) protocols like [Zcash](https://z.cash/) and [Monero](https://www.getmonero.org/).