A2F BLO

All About Fintech

Web 3.0

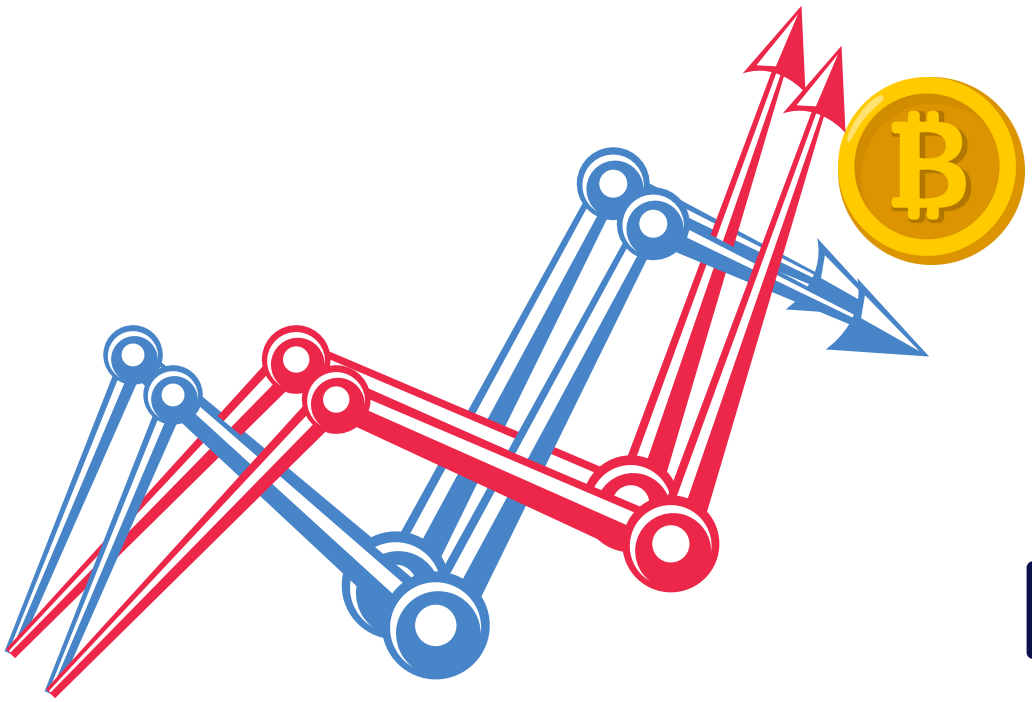
Part 3 of Terminologies

INITIAL COIN OFFERING (ICO)

A digital currency (web 3.0 tokens) is used to raise funds through an initial coin offering (ICO).

It is more common for cryptocurrency projects that have not fully developed their blockchain-based products, services, or platforms.

Early supporters of Initial Coin Offerings usually hope and expect the digital token (or coin) and company to be successful, potentially resulting in a good return on investment (ROI).



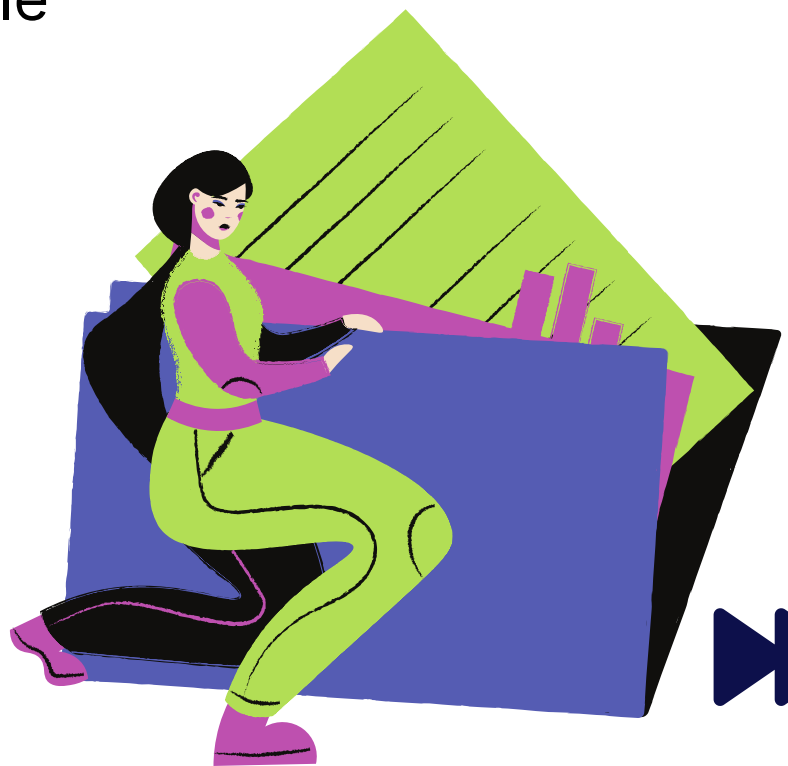
A2F BLOGS
All About Fintech

INTERPLANETARY FILE SYSTEM (IPFS)

The IPFS file system is an open-source project. With IPFS, the Internet could be transformed. There will be one file system shared by all devices, but it won't be the same as the Web today.

Comparing IPFS to HTTP, IPFS offers many advantages, including resistance to censorship, data integrity, lower operational costs, better performance, and security.

NFT systems are leveraging IPFS to ensure the uniqueness of the file



LIQUIDITY POOL

A liquidity pool generates a pool of coins or tokens that are then locked into smart contracts through crowdsourcing.

Although locked, these Cryptos are being utilized for loans, exchanges, and other applications.

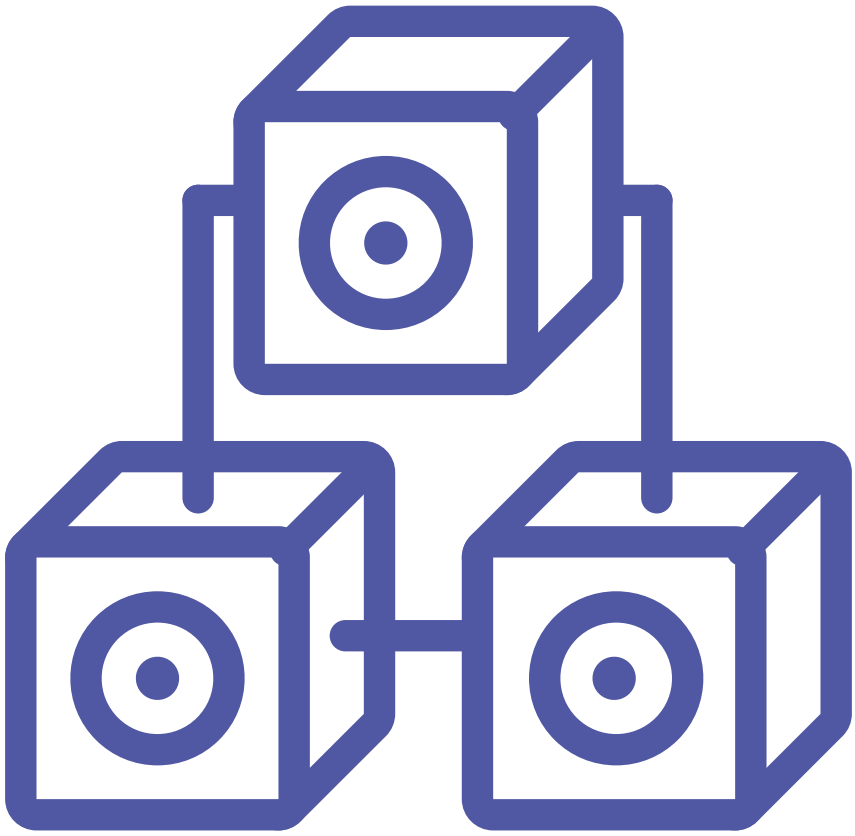
The liquidity pool is operated based on the automated market makers (AMM)

LAYER 1

Layer-1 network refers to a blockchain

Bitcoin, Litecoin, and Ethereum, for example, are Layer-1 blockchains.

Layer-1 scaling solutions augment the base layer of the blockchain protocol itself in order to improve scalability.

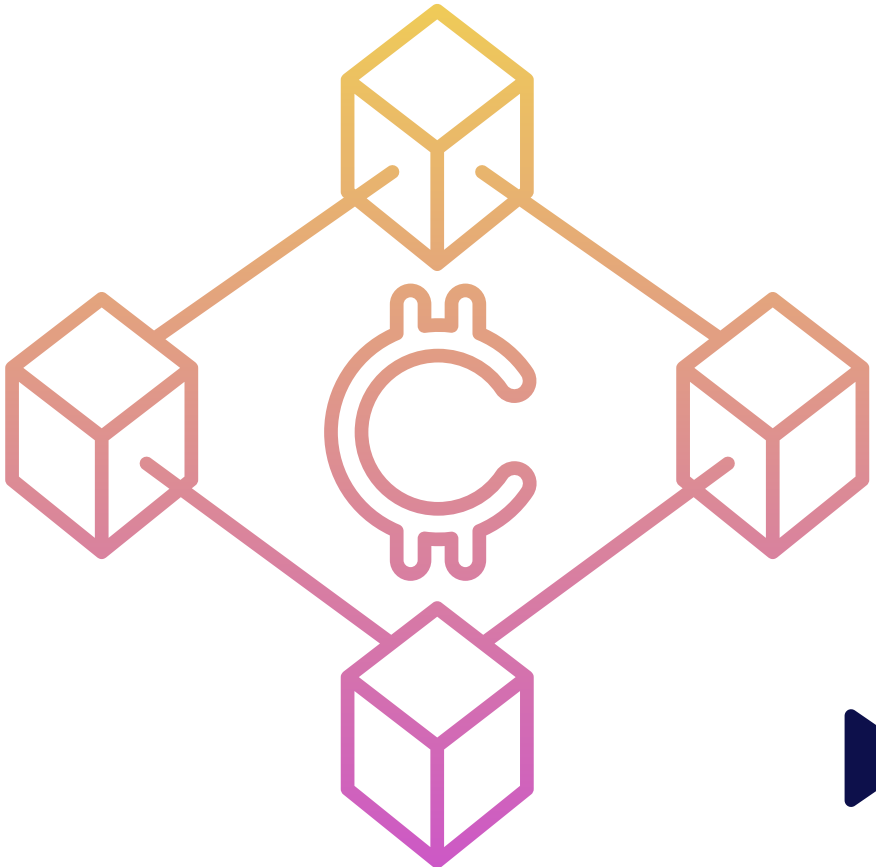


LAYER 2

A layer 2 system is a secondary framework built on top of an existing blockchain system.

Protocols such as these are aimed at solving the problems relating to transaction speed and scaling that the layer 1 networks face.

Major examples of layer 2 solutions are the Bitcoin Lightning Network, Polygon and the Ethereum Plasma.



MAINNET

Mainnet is the term for when a blockchain protocol has been fully developed and deployed.

This means that cryptocurrency transactions are broadcasted, verified, and recorded on a distributed ledger.

MEMPOOL

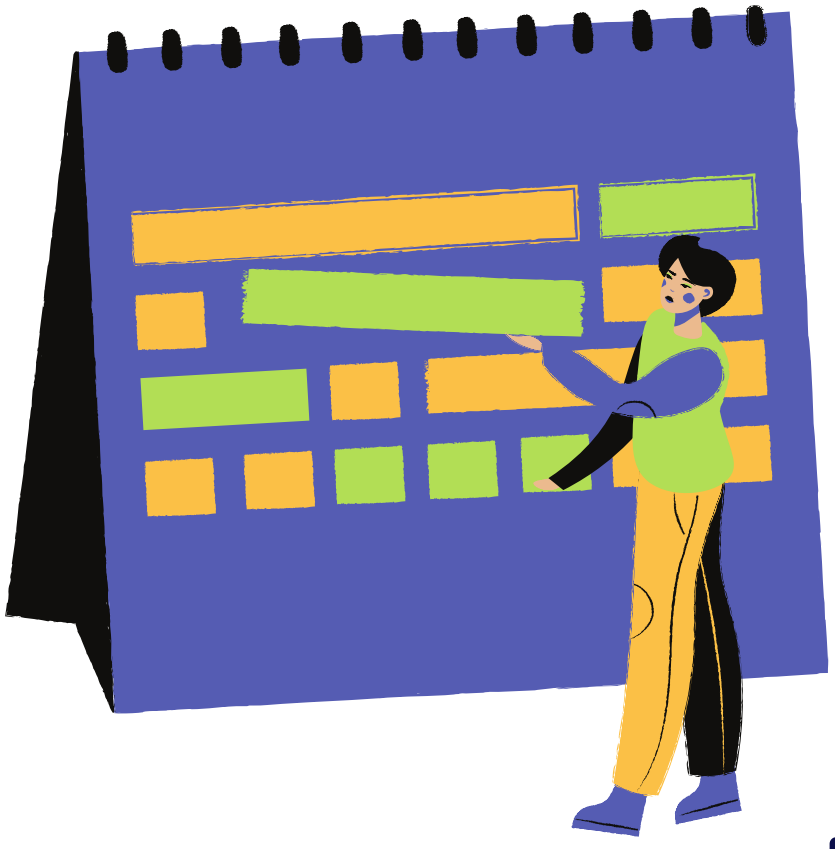
A mempool (a contraction of memory and pool) is a way for cryptocurrency nodes to store unconfirmed transactions.

Transactions that have not yet been included in a block are placed here as a waiting room.

MINING

Mining coin is a technical term that refers to the process of generating new coins or verifying transactions across the blockchain network.

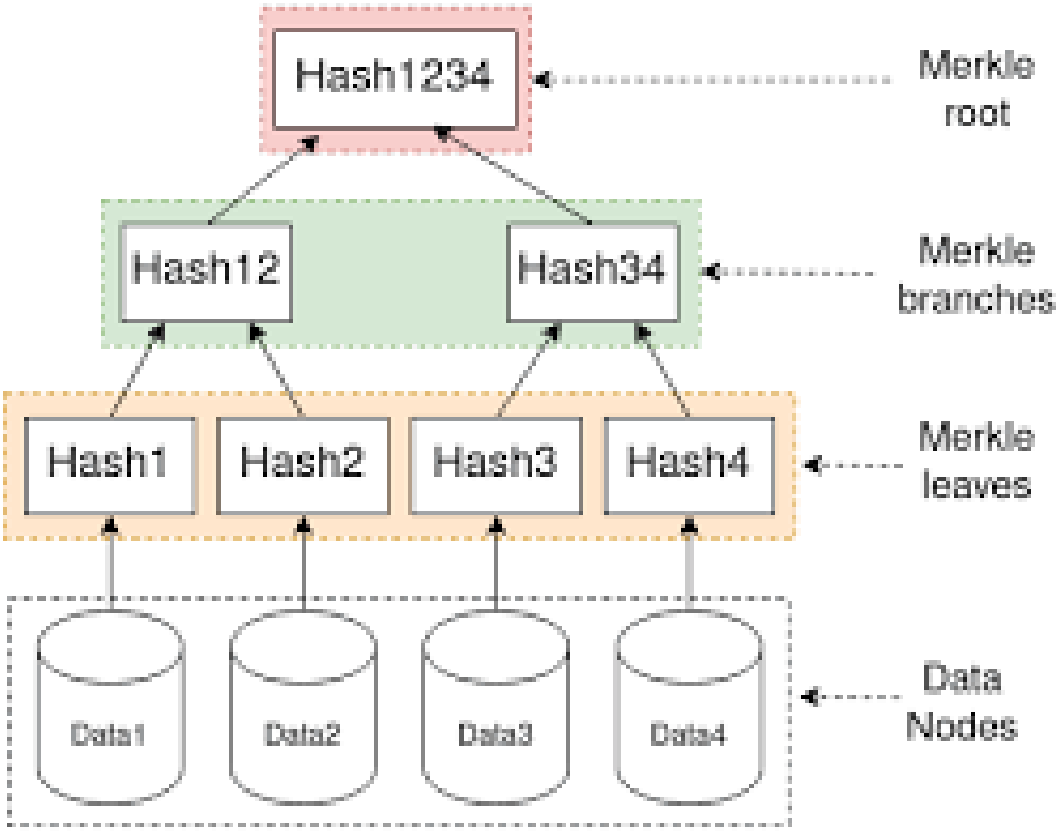
Every transaction is verified by miners to ensure that it is very difficult and expensive to duplicate resources.



MERKLE TREE

The Merkle tree is a way of organizing and structuring large amounts of data to make it easier to manage.

The Merkle tree is used to structure transaction data in cryptocurrency and blockchain in a way that is less resource-intensive.

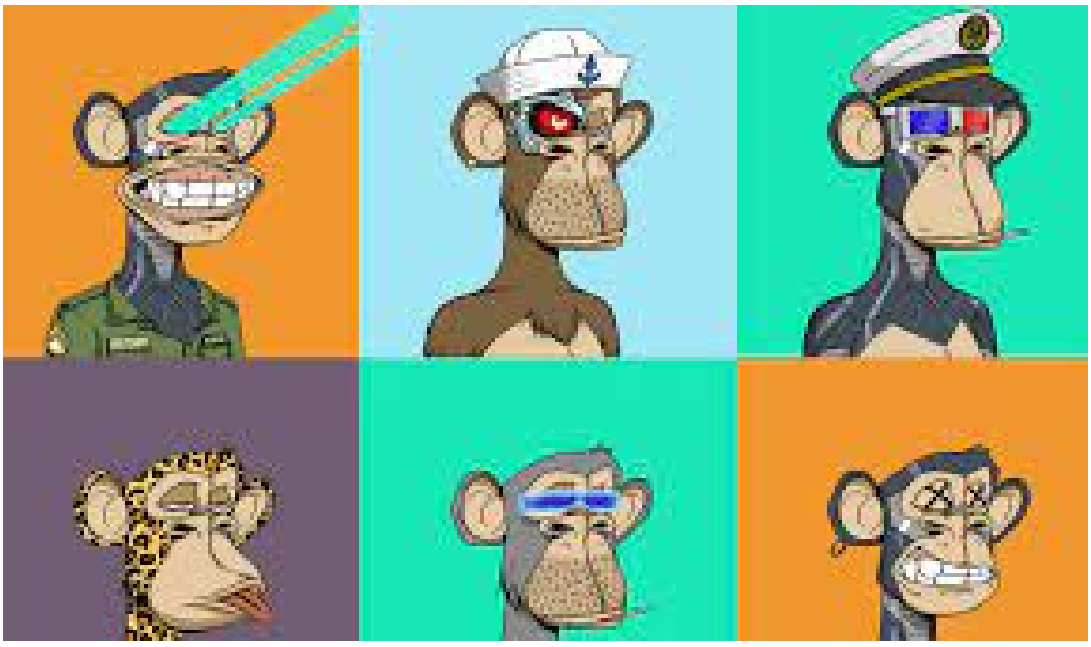


NON-FUNGIBLE TOKEN (NFT)

The tokenized versions of digital and real-world assets are known as NFTs.

Within a blockchain network, they serve as verifiable proofs of ownership and authenticity.

Digital scarcity is introduced by NFTs since they are not interchangeable.



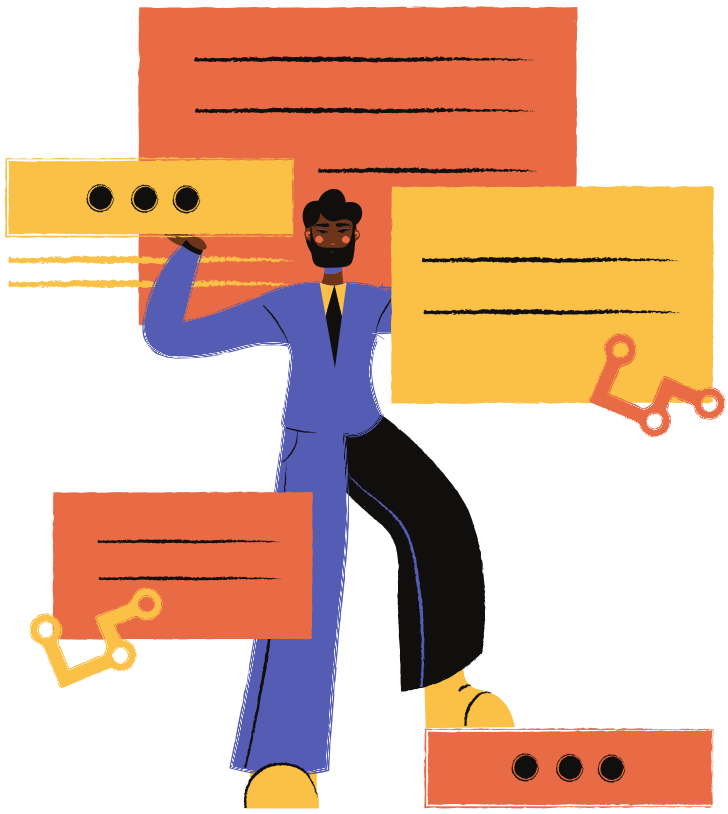
A2F BLOGS
All About Fintech

NONCE

Nonces are numbers or values that can only be used once.

Cryptographic hash functions and authentication protocols often use them.

Nonces refer to pseudo-random numbers that are used as counters in blockchain technology.



OFF-CHAIN

Off-chain transactions take place outside the blockchain. They can be conducted in several ways.

1. Transacting parties can enter into a transfer agreement.
2. A third party can guarantee the transaction's honor.
3. Participants purchase coupons in exchange for crypto-tokens and give the codes to others so they may redeem them.

POLKADOT

Polkadot is a decentralized blockchain network protocol designed to enable independent blockchain networks to communicate with each other through cross-chain interoperability.

A hybridized Nominated Proof-of-Stake (NPoS) consensus methodology is used by Polkadot, utilizing the GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement) and BABE (Blind Assignment for Blockchain Extension) mechanisms.

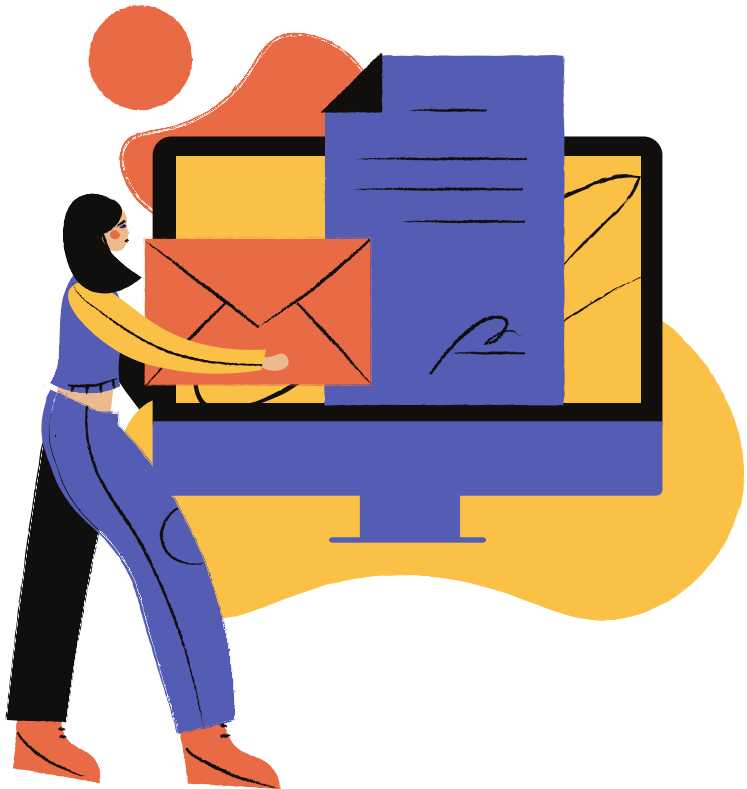
A2F BLOGS
All About Fintech

PROOF OF STAKE (POS)

Proof of Stake (PoS) is a consensus mechanism in which validators are selected based on the number of coins they stake.

In this case, stake refers to validators committing funds to the system. The only way validators can participate in creating new blocks is by locking their coins.

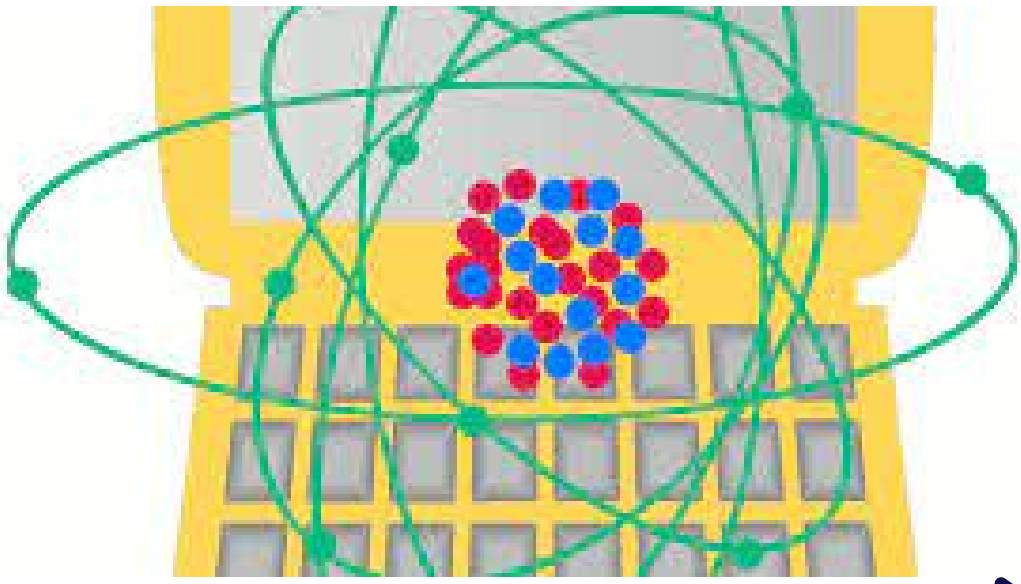
It is the most common protocol for Web 3.0 applications



QUANTUM COMPUTING

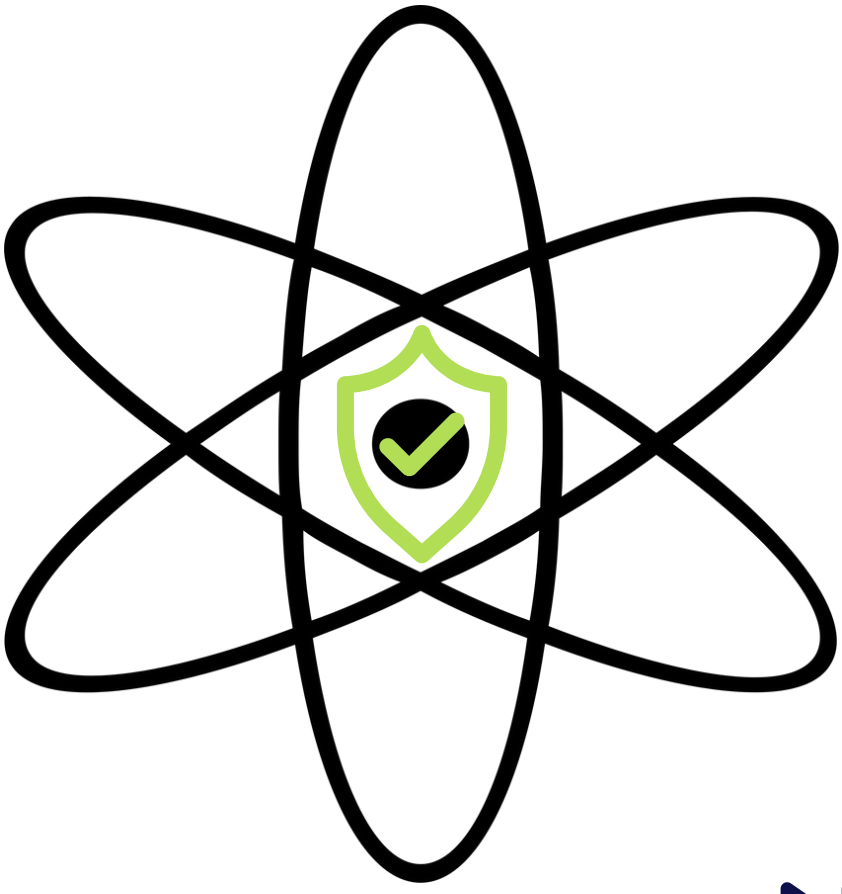
In quantum computing, computations are based on quantum properties, such as superposition, interference, and entanglement. Quantum computers are devices that perform quantum computations.

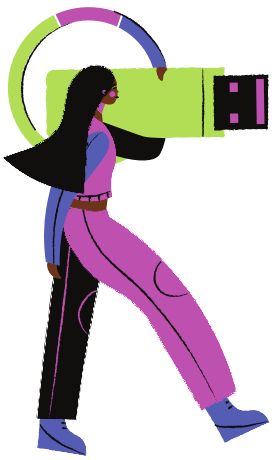
Particles in quantum computing can exist in superposition. The particles represent qubits instead of bits, and can take the value of either 1, 0 or both simultaneously.



QUANTUM RESISTANCE

Cryptography that is quantum-resistant aims to deliver secure functions and protocols even if large-scale quantum computers are built with fault-tolerant hardware.

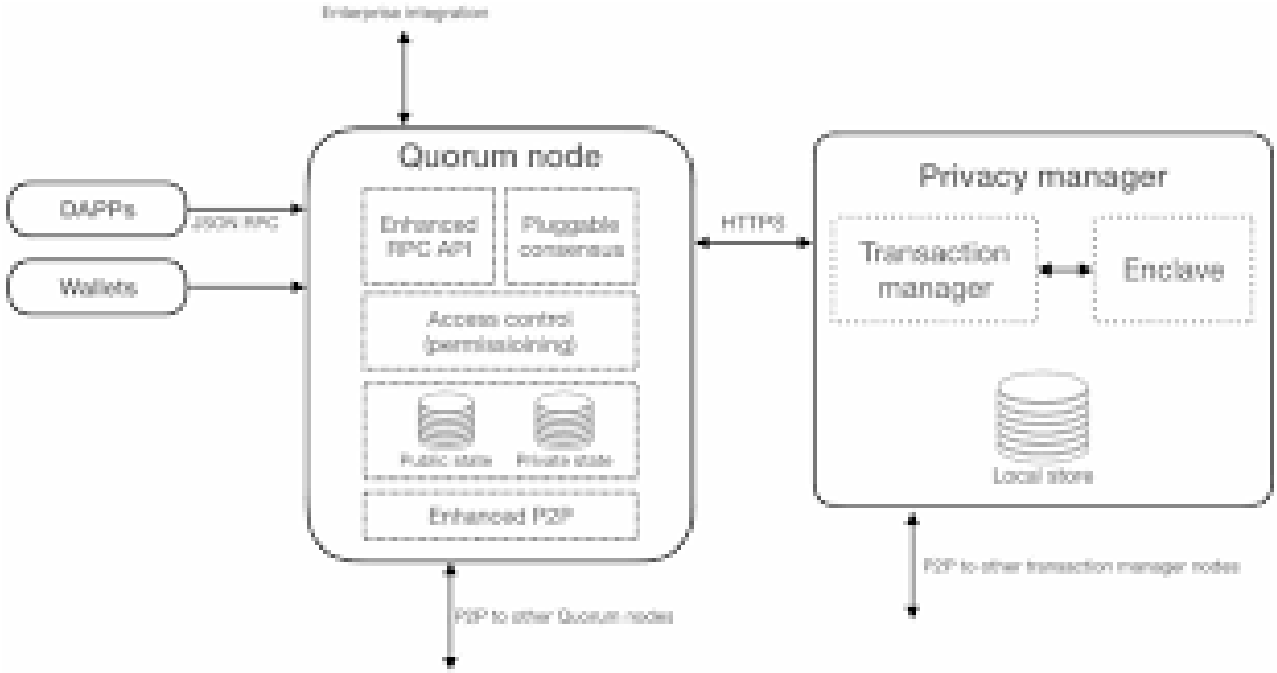




QUORUM

Quorum is a modified version of the Ethereum network that is specifically tailored for business applications and other services.

Although the Quorum blockchain is a bit ambiguous in its classification, it is considered to be a consortium or hybrid blockchain platform because it possesses both private (closed) and public (open) characteristics.

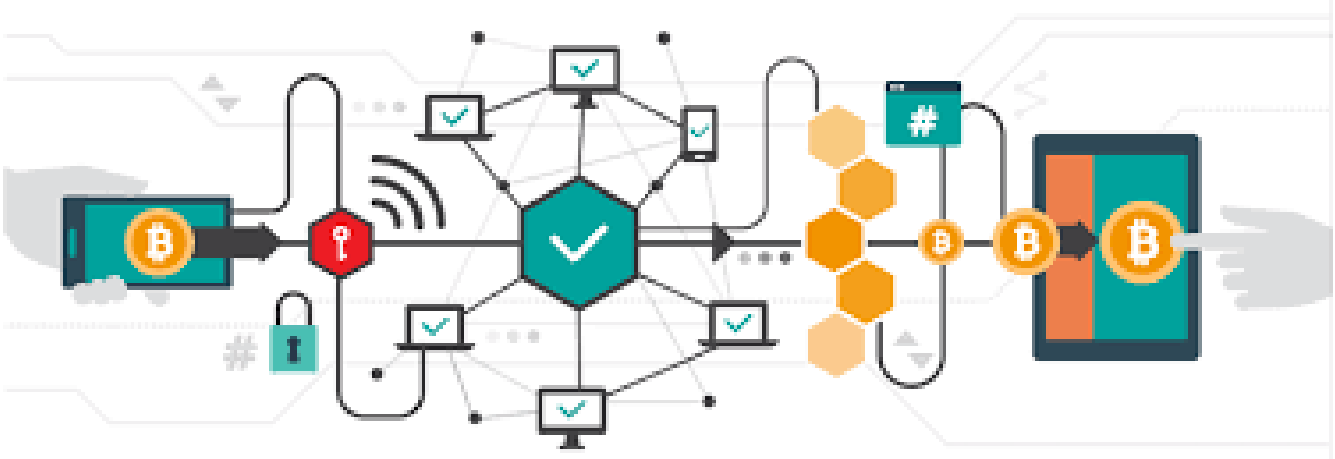


RAD

Radicle is a decentralized network for collaborative software development.

Radicle is a peer-to-peer (P2P) network built on Directed Acyclic Graph (DAG), offering optional Ethereum integration with blockchain-based functionalities.

RAD tokens can be used to vote for on-chain governance proposals and offer users discounted fees for using the platform's Ethereum-based tools.

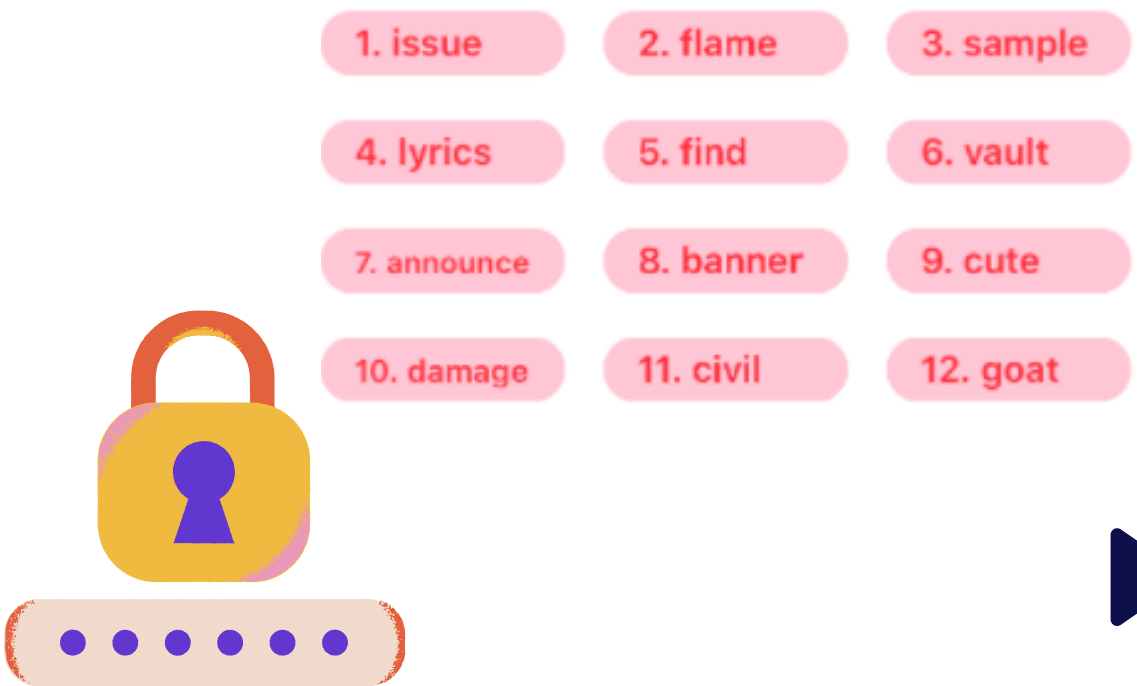


SEED PHRASE

A seed phrase is a collection of words that can be used to access your cryptocurrency wallet.

Seed phrases – as opposed to private keys – leave less room for human error when it comes to backups, as they're easier to record and transmit.

They can be used across hundreds, so that one seed can actually be used to recover an entire portfolio of coins and tokens.



STABLECOIN

Stablecoins are cryptocurrencies whose price remains stable over time.

Stablecoins are pegged to another asset in order to have their values fixed. The majority of them are pegged to the fiat currency

A stablecoin is mostly used to hedge against the volatility of cryptocurrency markets, although it can also serve as a decentralized stable currency in some circumstances

Types: Collateralised and Non-Collateralised

STABLECOIN

Stablecoins are cryptocurrencies whose price remains stable over time.

Stablecoins are pegged to another asset in order to have their values fixed. The majority of them are pegged to the fiat currency

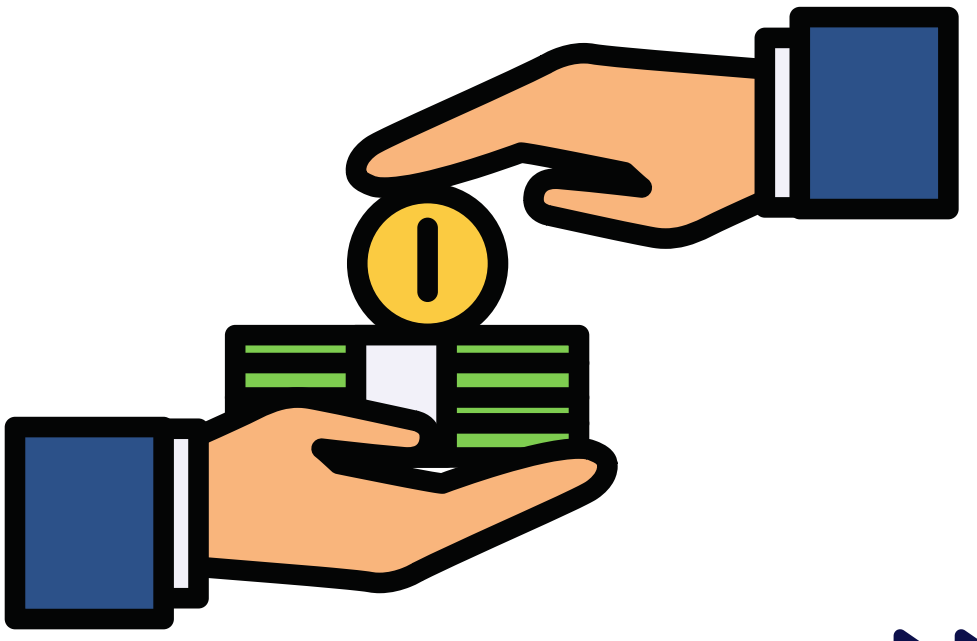
A stablecoin is mostly used to hedge against the volatility of cryptocurrency markets, although it can also serve as a decentralized stable currency in some circumstances

Types: Collateralised and Non-Collateralised

STORE OF VALUE

An asset that is able to avoid depreciation over a long period of time is called a store of value. An asset should have a value that is either stable or increases over time - but never decreases.

In addition to being a store of value, Bitcoin is often referred to as a "digital gold." Bitcoin is scarce and indestructible. It's a digital form of money that can't be copied or spent twice.



STATE CHANNEL

The state channel facilitates two-way communication between a blockchain and off-chain transactions by making use of a variety of mechanisms to improve transaction speed and capacity.

No immediate miner involvement is required to validate a transaction using a state channel. Rather, it is a network-adjacent resource that is protected by a multisignature or smart contract

TURING COMPLETE

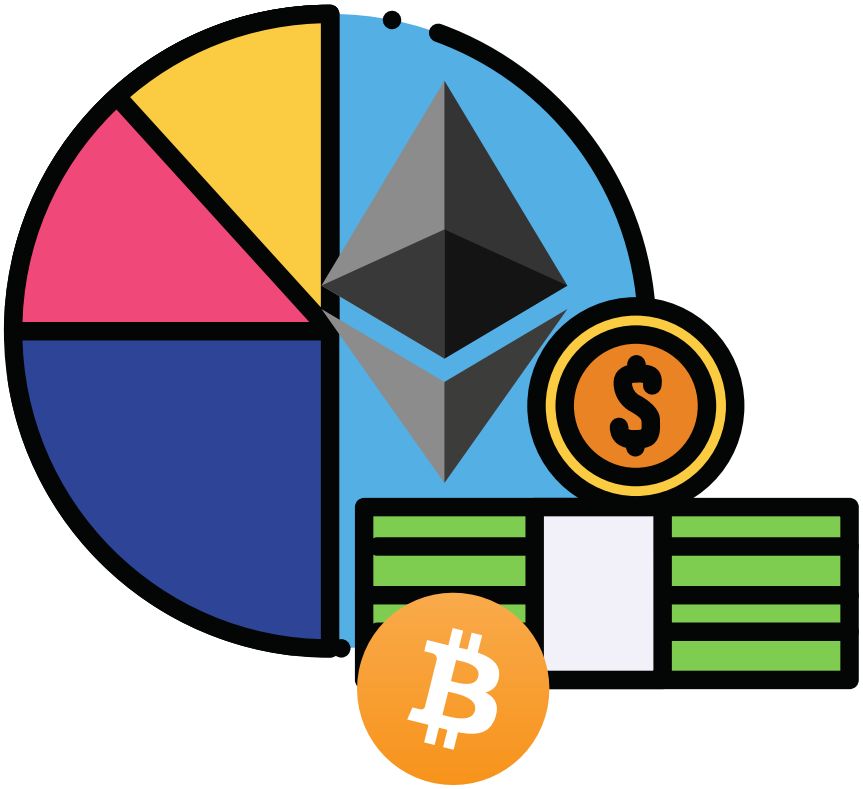
A Turing Complete machine can solve any computational problem, regardless of its complexity, given enough time and memory.

Most modern programming languages are Turing Complete (C++, Python, JavaScript, etc)

TOTAL VALUE LOCKED (TVL)

Total value locked (TVL) is a metric that measures the aggregate value of all crypto assets locked in decentralized finance (DeFi) protocols via smart contracts

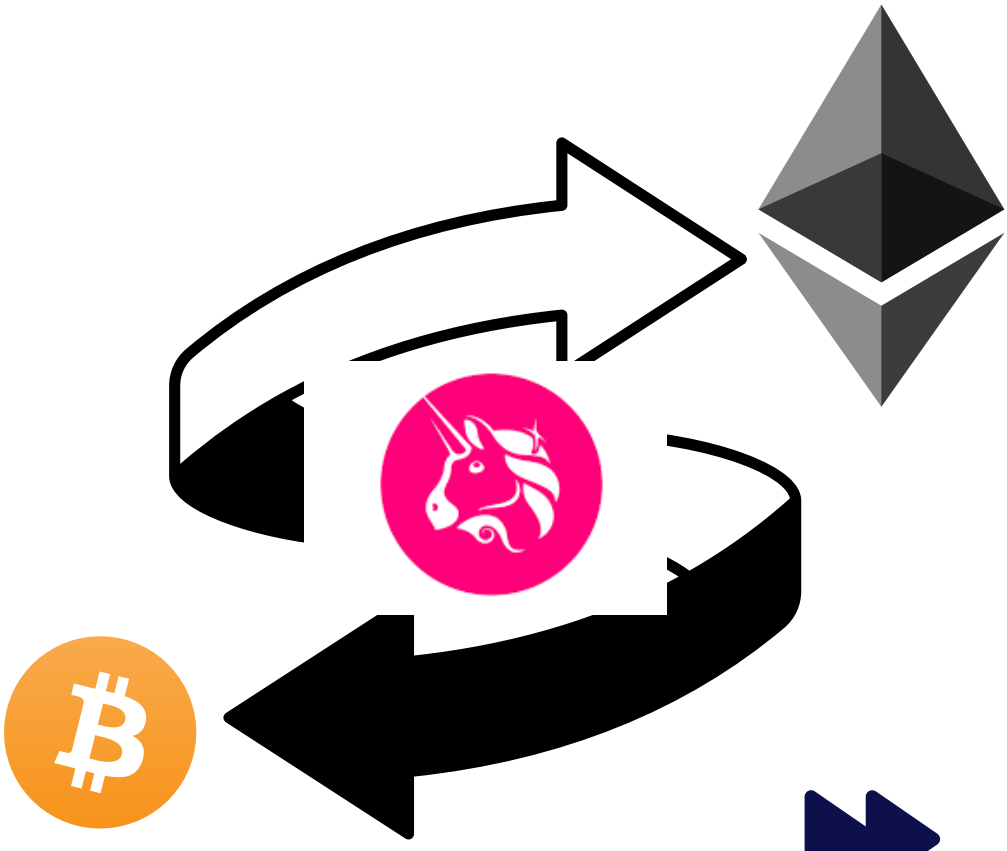
TVL data can also be further broken down and measure the DeFi value locked by purpose or type (such as lending and derivatives).



UNISWAP (UNI)

UniSwap is a decentralized exchange (DEX) that uses liquidity pools (LP) instead of order books and central facilitators.

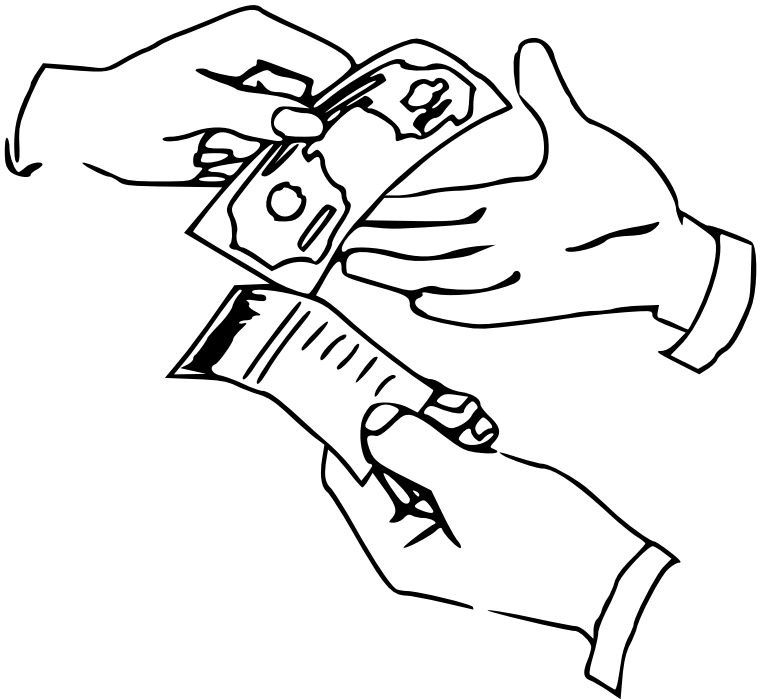
USWAP is powered by smart contracts that facilitate token swaps and provide incentives for liquidity providers to participate.



UNSPENT TRANSACTION OUTPUT (UTXO)

An unspent transaction output (UTXO) refers to a transaction output that can be used as input in a new transaction. In essence, UTXOs define where each blockchain transaction starts and finishes.

The UTXO model is a fundamental element of Bitcoin and many other cryptocurrencies.



VIRTUAL REALITY (VR)

Virtual Reality (VR) is a simulated virtual experience that is quite different from the real world.

Typically, VR takes two main forms: immersive VR, and text-based network VR (also called cyberspace).

Web 3.0 and Metaverse requires VR to provide end to end solutions

WRAPPED TOKENS

Cryptocurrencies that are wrapped around an asset represent the value of the asset they represent, and can often be redeemed for that asset.

The tokens usually take the form of ERC-20 tokens or other smart contract platform tokens. These tokens can therefore be exchanged for other tokens within a smart contract platform ecosystem (such as Ethereum).

YIELD FARMING

The practice of yield farming is to stake or lock up cryptocurrencies within blockchains to generate tokenized rewards.

Decentralized finance (DeFi) projects often use yield farming to encourage users to contribute to the network's liquidity and stability since these projects do not rely on a centralized market facilitator.

0X (ZRX)

0x is a protocol that facilitates the peer-to-peer (P2P) exchange of Ethereum-based assets.

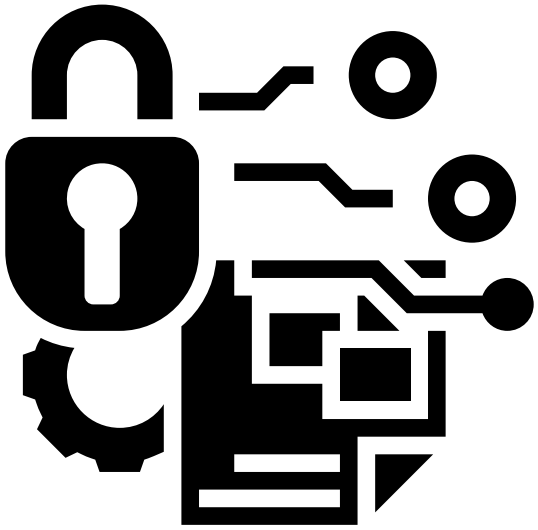
Built by 0x Labs, the protocol serves as an open standard and core DeFi building block for any developer needing exchange functionality.

0x offers secure, audited smart contracts; developer tools tailored to the 0x ecosystem; a decentralized global P2P order book (0x Mesh); and an API that provides easy access to aggregated liquidity sourced from a growing number of exchange networks

ZERO-KNOWLEDGE PROOFS

A zero-knowledge proof, sometimes also referred to as a ZK protocol, is a verification method that takes place between a prover and a verifier.

sing a type of proof known as a zero-knowledge Succinct Non-interactive Argument of Knowledge (zk-SNARK), privacy-focused cryptocurrencies such as Zcash are able to offer blockchain transactions with increased levels of privacy to their users. Ethereum is also working with zk-SNARK proofs since its Byzantium update in 2017.



A2F BLOGS

All About Fintech

The intent of this document is to express personal opinions only, and does not represent the views of any organization