



# The Blockchain Super Glossary

SPONSORED BY

**Cascadia Blockchain Council (@WTIA)**

**@CascadiaCouncil**

MANAGED/CREATED BY

**@ArryinSeattle**

# Background

I started this back in 2018 for myself with the help of our intern, Jasper Weed, because there are so many words in this space, and SO many different variations on even the same single word, like “blockchain.”

A perspective: “There is no [official] definition, and that’s deliberate. If something is poorly defined, as an entrepreneur you can claim you’re building it even if you’re not. The lack of codification works to the benefit of people in the industry.” -Nic Carter

**Devil's in the details.** 

**We need to do better.**

**Be better.**

Currently, there is a complete lack of precision when it comes to verbiage, the words that we use when we speak about this emerging technology industry with others. The onus of driving the use of precise words is *on each of us in this community* - not others. People will make blanket statements about blockchain, we need to ask, what do YOU mean when you say blockchain? The media will make broad generalizations about crypto, we need to ask, what specific part of crypto are they trying to refer to?

*We need to be VERY specific when talking about Bitcoin, blockchain, crypto. There are nuances, context, and boundaries that need to be CLEARLY understood.* I see it over and over again: policy, government, academia, entrepreneurs and innovators, and investors. It’s only getting worse.

We as an industry do a terrible job of practicing the use of precise language ourselves AND we do a terrible job of clarifying/demanding more thoughtful clarity from others.

Let's get better about being thoughtful, precise, and intentional with our words - ESPECIALLY when talking about anything in the bitcoin, blockchain, DLT, crypto, metaverse and web3 world.

That's the ONLY way we'll be able to accelerate progress forward, together.

BTW, if you want to learn more, and have a more curated hand-held experience with this space, I teach a class on Bitcoin, blockchain and crypto fundamentals - you can check it out [here](#). I'm also an adjunct professor with Portland State University.

-----

# Table of Contents

[51% Attack](#)

## A

[Actor](#)

[Address \(also known as “Addy”\)](#)

[Agreement Ledger](#)

[AirDrop](#)

[Altcoin](#)

[AML](#)

[Accidental Fork](#)

[Ape in](#)

[API](#)

[Artifacts](#)

[ASIC](#)

[Atomic Swap](#)

[Atomic Transaction \(Double-Spending-Problem\)](#)

[Attestation Ledger](#)

[AshDraked](#)

[ATH](#)

[Audit](#)

[Augmented Reality \(AR\)](#)

## B

[Bag](#)

[Bagholder](#)

[Banking Secrecy Act \(BSA\)](#)

[Bear](#)

[Bearish](#)

[Bit](#)

[Bitcoin \(BTC\)](#)

[bitcoin](#)

[Block](#)

[Blockchain](#)

[Blockchain \(Private\)](#)

[Blockchain \(Public\)](#)

[Blockchain \(Public Permissioned\)](#)

[Block Ciphers](#)

[Block Explorer](#)

[Block Height](#)

[Blockchain Multi-Tier Decision Framework \(BMDF\)](#)

[Block Reward](#)

[Block Time](#)

[Blue Chip](#)

[BTC](#)

[BTD](#)

[BTFD](#)

[Bull](#)

[Bullish](#)

[Bull Trap](#)

[Bytecode \(EVM\)](#)

[Byzantine Fault Tolerance \(BFT\)](#)

[Byzantine Generals Problem](#)

## C

[CBDC](#)

[CCO](#)

[CCO](#)

[Central Ledger](#)

[Centralized](#)

[Certificate Authority \(CA\)](#)

[Chain Linking](#)

[Chain of Custody](#)

[Chaincode](#)

[Choyna](#)

[Cipher](#)

[Client](#)

[Closed Source](#)

[CNFT](#)

[Coin](#)

[Coinbase](#)

[Command-Line Interface \(CLI\)](#)

[Compound](#)

[Cold Wallet](#)

[Cold Storage](#)

[Confirmation](#)

[Consensus](#)

[Consensus Mechanism](#)

[Consensus Point](#)

[Consensus Process](#)

[Consortium](#)

[Cryptoanalysis](#)

[Cryptocurrency](#)

[Cryptography](#)

[Currency](#)

[Custody](#)

## **D**

[DAC](#)

[DAO](#)

[\(The\) DAO](#)

[DApp](#)

[DDOS](#)

[Dead Cat Bounce](#)

[Decentralized](#)

[Decentralized Content \(DeCo\)](#)

[Decentralized Exchange \(DEX\)](#)

[Decentralized Identifier](#)

[Decentralized Society \(DeSoc\)](#)

[Decentralization](#)

[DevOps](#)

[Digital Asset](#)

[Decentralized Application \(DApp\)](#)

[Decryption](#)

[DeFi](#)

[Degen](#)

[Delist](#)

[Derivative](#)

[Difficulty](#)

[Digital Asset](#)

[Digital Commodity](#)

[Digital Identity](#)

[Digital Signature](#)

[Digital Signature \(Multi-signature\)](#)

[Digital Signature \(Ring\)](#)

[Directed Acyclic Graph \(DAG\)](#)

[Distributed](#)

[Distributed Ledger](#)

[Difficulty](#)

[Direct Acyclic Graphs \(DAGs\)](#)

[DLT \(Distributed Ledger Technology\)](#)

[dNFTs](#)

[Double Spend](#)

[Dox](#)

[DPoS](#)

[Drop](#)

[Dump](#)

[DYOR](#)

## **E**

[ELI5](#)

[Elliptic Curve Cryptography \(ECC\)](#)

[Encryption](#)

[ERC20 Token Standard](#)

[ERC-223](#)

[ERC-721](#)

[ERC-4907](#)

[Ether \(ETH\)](#)



[Ethereum \(ethereum\)](#)

[Ethereum Classic](#)

[Ethereum Enterprise Alliance \(EEA\)](#)

[EVM \(Ethereum Virtual Machine\) Code](#)

[EVM \(Ethereum Virtual Machine\)](#)

[EWASM](#)

[Exchange](#)

## **F**

[FA](#)

[Faucet](#)

[Fiat](#)

[Finality \(Instant Finality\)](#)

[Financial Crimes Enforcement Network \(FINCEN\)](#)

[Flipping](#)

[Floor price](#)

[fNFT](#)

[FOMO](#)

[FORGING](#)

[Fork](#)

[Fractionalized](#)

[Fren](#)

[FUD](#)

[Fungible](#)

[Fungible token](#)

[Futures Derivative](#)

## **G**

[GameFi](#)

[Gas](#)

[Gas Price](#)

[Genesis Block](#)

[GM](#)

[GN](#)

[Gossip Protocol](#)

[Governance](#)

[Graphical User Interface \(GUI\)](#)

[Gwei](#)

## **H**

[Halving](#)

[Hard Fork \(See also, Fork\)](#)

[Hardware Wallet](#)

[Hash](#)

[Hash Collision](#)

[Hash Function](#)

[Hashcash](#)

[Hashgraph](#)

[Hashgraph Consensus Mechanism](#)

[Hashrate](#)

[Hexadecimal Notation](#)

[HODL](#)

[Hodler](#)

[Honeypot Scam](#)

[Hot Wallet](#)

[Howey Test](#)

[Hyperledger Fabric](#)

## **I**

[Identity](#)

[Immutable](#)

[Immutability](#)

[Impermanent Loss](#)

[Initial Coin Offering \(ICO\)](#)

[Initial Token Offering \(ITO\)](#)

[Institutional Investor](#)

[Intentional Fork](#)

[Interchange](#)

[Interworking](#)

[InterPlanetary File System \(IPFS\)](#)

[Interoperability](#)

[IP-NFT](#)

[IYKYK](#)

## **J**

[Journal Entry](#)

[JOMO](#)

## **K**

[Key Pair](#)

[Keys](#)

[KYC](#)

## **L**

[Ledger](#)

[LFG](#)

[Light Client](#)

[Lightning Network](#)

[Lindy Effect](#)

[Liquid](#)

[Liquidity](#)

[Liquidity Mining](#)

[List](#)

[Litecoin \(LTC\)](#)

[Long](#)

## **M**

[Mainnet](#)

[Market Cap](#)

[MCAP](#)

[Maximum Coin Supply](#)

[mBTC](#)

[Memory Pool \(mempool\)](#)

[Merkle Proof](#)

[Merkle Root](#)

[Merkle Tree](#)

[Metadata](#)

[Metaverse](#)

[Miner](#)

[Miner \(CPU\)](#)

[Miner \(GPU\)](#)

[Miner \(ASIC\)](#)

[Mining](#)

[Mining Pool](#)

[Mint](#)

[Mises, Ludwig von](#)

[Moon](#)

[Mooning](#)

[Money](#)

[Money Transmitters](#)

[Multi Signature](#)

[Multi Party](#)

## **N**

[Network](#)

[NFA](#)

[NGMI](#)

[Node \(Full Node\)](#)

[Node \(Light\)](#)

[Node \(Web3\)](#)

[Nonce](#)

[Non-Fungible](#)

[Non-Fungible Token \(NFT\)](#)

[Non-Fungible Visualizations \(NFV\)](#)

[Normie](#)

## **O**

[OFAC](#)

[Off-Ledger Currency](#)

[Offchain](#)

[OG](#)

[Onchain](#)

[On-Chain Analysis](#)

[One-of-One](#)

[On-Ledger Currency](#)

[Opcode](#)

[Open Banking](#)

[Open Finance](#)

[Open source](#)

[Options Derivative](#)

[Oracle](#)

[OTC](#)

## **P**

[P2P](#)

[Paper hands](#)

[Participant](#)

[Peer](#)

[Peer to Peer \(P2P\)](#)

[Permissioned](#)

[Permissioned Ledger](#)

[Permissionless](#)

[PFP](#)

[Play to Earn \(P2E\)](#)

[POAP](#)

[Portfolio](#)

[PoS/Pow Hybrid](#)

[Pre-Sale](#)  
[Private Blockchain](#)  
[Private Blockchain](#)  
[Private Currency](#)  
[Private Key](#)  
[Private Key Infrastructure \(PKI\)](#)  
[Probably Nothing](#)  
[Proof of Activity](#)  
[Proof-of-Authority](#)  
[Proof of Burn](#)  
[Proof of Capacity](#)  
[Proof of Creativity](#)  
[Proof of Elapsed Time \(PoET\)](#)  
[Proof of Identity](#)  
[Proof of Importance](#)  
[Proof of Liquidity](#)  
[Proof-of-Stake](#)  
[Proof of Stake \(Delegated\)](#)  
[Proof of Work](#)  
[Proof-of-Work \(Delegated\)](#)  
[Protocol](#)  
[Provenance](#)  
[Provably](#)  
[Provably Fair](#)  
[Pseudonym](#)  
[Pseudonymity](#)  
[Public Blockchain](#)  
[Public Key](#)

[Pump](#)

[Pump & Dump](#)

## **Q**

[QR Code](#)

## **R**

[Raids](#)

[ReFi](#)

[Rekt](#)

[Rentable NFT](#)

[Reverse Indicator](#)

[Replicated Ledger](#)

[Ring Signature](#)

[Ripple](#)

[Roadmap](#)

[RSI](#)

[Rug](#)

## **S**

[Safu](#)

[Sandwich Attack](#)

[Satoshi](#)

[Satoshi Nakamoto](#)

[Scalability](#)

[Scarcity](#)

[Script](#)

[Secure Hash Algorithm \(SHA\)](#)



[Securities and Exchange Commission \(SEC\)](#)

[Security Token Offering \(STO\)](#)

[Seed Phrase](#)

[Seed Plate](#)

[Segregated Witness, or SegWit](#)

[Self-Sovereign Identity \(SSI\)](#)

[Semi-Fungible Token \(SFT\)](#)

[SHA 256](#)

[Sharding](#)

[Shill](#)

[Shiller](#)

[Shitcoin](#)

[Short](#)

[Sidechain](#)

[Cryptographic Signature](#)

[Simple Agreement for Future Tokens \(SAFT\)](#)

[Simplified Payment Verification \(SPV\)](#)

[Singleton](#)

[Slippage](#)

[Smart Contract](#)

[Soft Fork](#)

[Solidity](#)

[Soulbound token \(SBTs\)](#)

[Spot Market](#)

[Stablecoin](#)

[Staking](#)

[State Channel](#)

[State Machine](#)

[Stream Ciphers](#)

[Store of Value](#)

[Sweep](#)

[Swing](#)

## **T**

[TA](#)

[Tangle](#)

[Taxonomy](#)

[Testnet](#)

[Token](#)

[Token \(Non Fungible\)\(NFT\)](#)

[Token \(Security\)](#)

[Token \(Stable\)](#)

[Token \(Utility\)](#)

[Token Generation Event](#)

[Tokenization](#)

[Tokenomics](#)

[Tokenless Ledger](#)

[Total Circulating Coin Supply](#)

[Total Coin Supply](#)

[Total Value Locked \(TVL\)](#)

[Transaction](#)

[Transactions as Proof of Stake \(TaPoS\)](#)

[Transaction Block](#)

[Transaction Fee](#)

[Transactions Per Second \(TPS\)](#)

[Transaction Pool](#)

[Transparency](#)

[Trust](#)

[Trustless](#)

[TS](#)

[TTM](#)

[Turing Complete](#)

[Turing Machine](#)

## **U**

[uBTC](#)

[uNFT](#)

[URI](#)

[Utility](#)

[Unpermissioned Ledgers](#)

[Unspent Transaction Output](#)

## **V**

[Validator](#)

[Vapourware](#)

[Virtual Currency - See Digital Asset](#)

[Virtual Machine](#)

[Virtual Reality \(VR\)](#)

[Vyper](#)

## **W**

[WAGMI](#)

[Wallet \(Crypto\)](#)

[Wallet \(Cold\)](#)

[Wallet \(Warm\)](#)

[Wallet \(Hot\)](#)

[Wallet \(Multisignature\)](#)

[Web1](#)

[Web2](#)

[Web3](#)

[Web Assembly \(WASM\)](#)

[Whale](#)

[Wen](#)

[Wen Moon](#)

[Whitepaper](#)

[White list](#)

## **X**

[xBT](#)

[XRP](#)

## **Y**

[Yield](#)

[Yield Farming](#)

## **Z**

[Zeppelin/Open Zeppelin](#)

[Zero Knowledge Proof](#)

# Super Glossary

## 51% Attack

A 51% attack refers to a bad actor who gains control of the majority of CPUs in a cryptocurrency mining pool, or the overall hash rate. Hashing secures the blockchain. Any entity that obtains 51% of the overall hash rate AND gets 6 confirmations, has the power to rewrite the transaction ledger, roll back transactions, and spend them again (i.e. Double Spend). Without the 6 confirmations, then the entity can only censor or prevent. Such attacks are generally limited to smaller blockchains with fewer nodes (than the Bitcoin blockchain) because they're more susceptible to a single person seizing control based on a Proof of Work (PoW) consensus mechanism.

---

## Actor

An actor is an entity that participates in a network.

---

## Address (also known as “Addy”)

An address is the public identifier of a crypto "account" used to transact on a blockchain network for digital assets. An address is a string of alphanumeric characters, and can also be represented as a scannable QR code. A blockchain address is similar to an email address: by giving someone your address, they can send digital assets to you at that address, from their own address.

A classic bitcoin address might look like:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa - consisting of a string of letters and numbers (base 58) starting with a “1” (number one).

Each blockchain has its own address format, and may have more than a single format. Bitcoin, for example, currently has 3 distinct mainnet address formats.

CAUTION: Blockchains generally provide no way to recover assets sent to an incorrect address. Check the recipient address very carefully when sending!

---

### **Agreement Ledger**

An agreement ledger is a distributed ledger that is used by two or more parties to negotiate and reach agreement.

---

### **AirDrop**

An AirDrop is the act of distributing tokens or cryptocurrencies to a set of predetermined addresses. Predetermined addresses can be selected by inviting participants to register, or by identifying participants who have already met some criteria (e.g.: hold certain assets, or performed certain actions).

---

### **Altcoin**

An altcoin is any digital currency or cryptocurrency alternative to Bitcoin. Altcoin was originally an abbreviation of “Bitcoin Alternative”. Today it’s an abbreviation of “Alternative Coin”. Many altcoins are forks of Bitcoin with changes to the Proof-of-Work algorithm or other properties of the network. Litecoin, Dogecoin, and Bitcoin Cash are a few examples that have minor changes. Ethereum is the largest altcoin, with substantial differences introduced.

---

## **AML**

AML stands for Anti Money Laundering. Anti-money laundering (AML) refers to the laws, regulations and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income, through the process of money laundering. Though anti-money laundering laws cover a limited range of transactions and criminal behavior, their implications are far-reaching.

---

## **Accidental Fork**

An accidental fork happens when two or more miners find a block at almost the same time. One chain becomes longer than the other chain, and the network will eventually abandon blocks that are not in the longer chain. The blocks that are abandoned are called “orphaned blocks” - and are added to the mempool, where miners will re-verify them.

---

## **Ape in**

To “ape in” (or just “ape”) means to become part of a project by buying a coin, or an NFT, but usually by acquiring a large stake, or paying a significant amount.

---

## **API**

API stands for Application Programming Interface, a software intermediary that helps two separate applications communicate with one another. They define methods of communication between various components.’

---

## **Artifacts**

Artifacts are the ‘ingredients’ of a token. These consist of Classifications – the bases of all tokens; Behaviors and Behavior Groups – capabilities and/or restrictions; Properties and Property Sets – values set within tokens; Control Messages – contractual interfaces.<sup>2</sup>

---

## **ASIC**

ASIC stands for “Application Specific Integrated Circuit”, and are custom silicon chips specifically designed to do a single task. For Bitcoin, ASICs are designed to efficiently process the SHA-256 hashing problems to mine new Bitcoins.

---

## **Atomic Swap**

Decentralized exchange of assets between two different blockchain networks without the use of an exchange (i.e. Bitcoin to Ethereum).

---

## **Atomic Transaction (Double-Spending-Problem)**

Atomic Transaction ensures that either the completion of a transaction in both sides (debit / credit) sides of a transaction are complete or nothing is none of them are registered at all (i.e. Hedera Hashgraph).

---

## **Attestation Ledger**

Attestation ledger is a distributed ledger showing a durable record of agreements, commitments or statements that provides evidence (or



“attestation”) that these agreements, commitments, or statements were made.

---

### **AshDraked**

AshDraked is a slang term used to let others know that you have lost all of your money.

---

### **ATH**

ATH is an acronym for “All Time High”.

---

### **Audit**

An audit is an unbiased and formal examination and evaluation of the financial statements of an individual, organization or financial situation (Investopedia). An audit involves an assessment that recorded transactions are supported by evidence that is relevant, reliable, objective, accurate, and verifiable.

---

### **Augmented Reality (AR)**

AR is not fully immersive submissive like VR. Usually accessed through AR glasses or mobile devices, the user can see computer based images layers placed on top of the real world.

---

## **Bag**

All the crypto, or NFTs that a person holds.

---

## **Bagholder**

Bagholder is a slang term to describe a person who holds a certain position of a certain cryptocurrency that decreases in value until the value is ultimately near or at zero.

---

## **Banking Secrecy Act (BSA)**

The BSA is a law that passed in 1970 that regulates the detection and prevention of money laundering. It is also known as the Currency and Foreign Transactions Reporting Act, is a U.S. law requiring financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering.

---

## **Bear**

Bear is a word to describe a pessimistic individual whose sentiment is that the price on a stock, crypto, or asset will continue to fall/is falling.

---

## **Bearish**

Expecting that the price or value might go down in the future. The opposite of bullish.

---

## **Bit**

Bit is a common unit to designate a sub-unit of Bitcoin. 1,000,000 bits is equal to 1 Bitcoin (BTC). It is a smaller unit of Bitcoin.

---

## **Bitcoin (BTC)**

Bitcoin (uppercase) is the most well known cryptocurrency, based on the proof-of-work blockchain. Bitcoin was created in 2009 by an unknown creator, Satoshi Nakamoto, and its technology was outlined in a whitepaper titled, "Bitcoin: A Peer-to-Peer Electronic Cash System". Bitcoin established the first decentralized digital asset and uses blockchain technology to create a digital asset that is entirely decentralized and managed across a wide network of computers (nodes) rather than by a single centralized entity.

First cryptocurrency built on a PoW blockchain in 2009. The creator is unknown and goes by the pseudonym Satoshi Nakamoto. Concept outlined in a whitepaper released in 2008.

---

## **bitcoin**

The lowercase bitcoin is a specific collection of technologies used by Bitcoin. The cryptocurrency, Bitcoin, is one of the technologies in bitcoin. What? Which technologies? Confusing, remove.

---

## **Block**

A block is a digital record or transaction in the electronic ledger entered into a blockchain. Blocks hold collections of valid transactions (or a set of updates) that are hashed and encoded into a Merkle Tree to the blockchain ledger. Each block includes the cryptographic hash of the prior block in the

blockchain, linking them together, forming a chain. A block is limited by the amount of data it can hold in its virtual container of transactions with corresponding data. Roughly every 10 minutes, a bitcoin node receives these blocks, validates all transactions in them, and then applies the updates to the global ledger.

A bitcoin miner is tasked to validate all transactions in the block and then solve a complicated mathematical equation that cryptographically ties this block to previous blocks. Once broadcast to other nodes and miners, this block is added to the string of blocks that make up the chain. The whole blockchain is a publicly viewable record that keeps track of every transaction that has ever occurred within that digital asset.

A batch of transactions written to the blockchain. Every block contains information about the previous block, thus chaining them together.

---

## **Blockchain**

A blockchain is a type of distributed ledger, composed of unchangeable (immutable), digitally recorded and validated data in chronologically ordered packages called blocks, managed by a cluster of computers, not owned by any single entity. Each block is then 'chained' to the next block, using a cryptographic signature, creating a long chain. The nature of the cryptographic tie from one block to previous blocks means that previous blocks cannot be altered by anyone. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions.

A publicly-accessible, unchangeable, digital ledger used to store and transfer information without the need for a central authority. Blockchains are the core technology on which cryptocurrency protocols like Bitcoin and Ethereum are built.

---

## **Blockchain (Private)**

A private blockchain is a blockchain that is only accessible to those with permission to access (read, write, modify).

---

## **Blockchain (Public)**

A public blockchain is a blockchain that is accessible to everyone and does not require special permission to access it.

---

## **Blockchain (Public Permissioned)**

A public permission blockchain is a blockchain that is publicly viewable but only permissioned parties can write to it.

---

## **Block Ciphers**

Block ciphers are a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to a block of data at once as a group rather than to one bit at a time.

---

## **Block Depth**

Block Depth is the position index of a block pertaining to the latest block.

---

## **Block Explorer**

Block explorers are a type of online tool (software) used to view all transactions, past and current, on the blockchain. They provide useful information such as transactions, verification of transactions, network hash rate and transaction growth. There are several block explorers available on the web for various cryptocurrencies. Block Explorers are often used to confirm that a transaction is complete (6 confirmations for Bitcoin is considered secure).

---

## **Block Height**

Block height refers to the global number of blocks connected together in the block chain, at the present time. For example, Height 0, would be the very first block, which is also called the Genesis Block. The fifth block to be added will have a height of four because four blocks came before it. As of October 2018, the Bitcoin block height is almost 550,000 and the Ethereum block height is almost 6,500,000.

---

## **Blockchain Multi-Tier Decision Framework (BMDF)**

The BMDF provides a holistic view of blockchain that accounts for the business objectives and unique criteria of each specific industry and use case.

---

## **Block Reward**

Block rewards are rewards given to a miner which has successfully hashed a transaction block. The first miner to solve the proof-of-work puzzle in a block receives a block reward of new coins in the native cryptocurrency as incentive, or compensation for the miner's expenditure in solving the puzzle. Block rewards can be a mixture of coins and transaction fees, depending on the

policy used by the cryptocurrency in question, and whether all of the coins have already been successfully mined.

---

## **Block Time**

Block Time is the average time it takes for a network to generate one block in a blockchain.

---

## **Blue Chip**

Blue chips within traditional finance are stocks that are a reliable investment. There are now blue chip cryptocurrencies - stablecoins, as well as blue chip NFTs that are usually found in expensive, “premium” projects with high floor prices, high utility, and relatively low price volatility.

---

## **BTC**

BTC is the original shorthand for *bitcoin*. This designation is often used on digital asset exchanges to denominate a bitcoin's current value. However, there has been an increase in the use of XBT as an alternate designation. The reason for this is that the International Organization for Standardization (ISO), which keeps a listing of all currencies, uses X to symbolize a currency that is not attached to a specific country (which is the case for all digital assets, because they are decentralized). Fidelity Digital Assets uses the XBT currency code.

---

## **BTD**

BTD is an acronym for the slang phrase, “Buy the Dip.”

---

## **BTFD**

BTFD is an acronym for the slang phrase, “Buy the F\*\*\*king Dip.” (delete one star, or take out the “k”)

---

## **Bull**

Bull is used to portray the sentiment that the price is moving upward.

---

## **Bullish**

“Bullish” means that you believe that the value (price) of crypto or an NFT will rise which is usually characterized by long strategies (*see Hodl, Hodler*).

---

## **Bull Trap**

A bull trap is when a downward price trend briefly reverses, moves upward and then continues its downward motion.

---



## **Bytecode (EVM)**

Smart contract code is usually written in a high level programming language such as Solidity. This code gets compiled to something called the EVM bytecode which gets deployed to the Ethereum blockchain. This is very similar to a programming language like Java where the code gets converted to JVM bytecode.

---

## **Byzantine Fault Tolerance (BFT)**

A characteristic of a distributed system to reach consensus at any time when no more than one third of its actors are malicious.

A subset is asynchronous Byzantine Fault Tolerance (aBFT) that takes into account the delay or loss of a message too (i.e. Hedera).

---

## **Byzantine Generals Problem**

Byzantine Generals' Problem is defined as a situation where spread out units need to coordinate their behavior or action but cannot trust each other to get organized. Byzantine describes the Byzantine Empire, this was the eastern part of Europe controlled by the Roman Empire from approximately 330 AD to 1453 AD. Byzantine Generals' Problem is an allegorical made up, historical situation where multiple generals and their individual armies have surrounded a city to attack it. The majority of the generals must somehow coordinate a decision to either attack or retreat at the same time, otherwise, the situation will end in a major failure.

---

## **CBDC**

CBDC is your Central Bank Digital Currency. CBDCs are not cryptocurrencies. They are similar to the centralized fiat currencies in that they are government controlled. The government decides on the supply and can increase/decrease the supply.

---

## **CCO**

CCO stands for “Community Contribution Opportunity” and is different from an ICO or DAICO, because its contributions don’t have to take the form of money. A CCO is a product managed by a community rather than a small team and their investors. (DAOhaus). The process of a community forming a DAO around a particular project / product in order to support its ongoing development or survival as a community owned resource.

---

## **CC0**

CC0 stands for “Creative Commons Zero” or no intellectual property rights reserved by the creator of a piece of art / content. This happens by default after a certain amount of time has expired, but it can also happen if the creator decides to immediately waive their IP rights, otherwise known as “public domain” meaning that anyone is free to create content using that intellectual property.

---

## **Central Ledger**

A central ledger refers to a ledger maintained by a central agency.

---

## **Centralized**

Centralized means a single and/or central source of control and authority. A typical centralized blockchain system is the private blockchain, since it is governed/managed by a single group or organization.

---

## **Certificate Authority (CA)**

A Certificate Authority is a centralized authority that ensures public and private keys match in a private key infrastructure.

---

## **Chain Linking**

Chain linking is the process of connecting two blockchains with each other, thus allowing transactions between the chains to take place. This will allow blockchains like Bitcoin to communicate with other sidechains, allowing the exchange of assets between them.

---

## **Chain of Custody**

Chain of custody is the entire chain of ownership of a widget during its lifestyle from materials to the end user.

---

## **Chaincode**

Chaincode is another word for smart contract.

---

## **Choyna**

Choyna is another word for China.

---

## **Cipher**

A cipher is the algorithm used for the encryption and/or decryption of information. In common language, 'cipher' is also used to refer to an encryption message, also known as 'code'.

---

## **Client**

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

---

## **Closed Source**

Closed source is the source code of the proprietary software that is not opened to the public except the owner.

---

## **CNFT**

The "C" of this acronym is the name of the blockchain Cardano from which the NFTs are sold, "Cardano-NFT".

---

## **Coin**

A coin or altcoin is a representation of digital asset value that is generated via its own independent blockchain.

---

## **Coinbase**

Coinbase is an application that is an easy to use crypto-currency exchange, based in the US. (There are many other US based exchanges, and their sizes may vary over time.).

Coinbase can also be a technical term. The coinbase is the content of the 'input' of a generation transaction. While regular transactions use the 'inputs' section to refer to their parent transaction outputs, a generation transaction has no parent, and creates new coins from nothing.

---

## **Command-Line Interface (CLI)**

Command line interface is a text based user interface.

---

## **Compound**

Compound is the ability of a sum of money to grow exponentially over time through the repeated addition of earnings to the principal amount.

---

## **Cold Wallet**

A cold wallet is an offline wallet that is disconnected from the internet at all times.

---

## **Cold Storage**

Cold storage is a mechanism where private keys used to sign withdrawal transactions are kept in secure locations that are not connected to the internet. It is one of many security techniques used by Fidelity Digital Assets to secure customers' funds.

---

## **Confirmation**

A confirmation means that the blockchain transaction has been verified by the network, processed and highly unlikely to be reversed. This happens through a process known as mining, in a proof-of-work system (e.g. Bitcoin). Transactions receive a confirmation when they are included in a block and for each subsequent block. Once a transaction is confirmed, it cannot be reversed or double spent. The more confirmations a transaction has, the harder it becomes to perform a double spend attack. Even a single confirmation can be considered secure for low value transactions, although for larger amounts like \$1000 USD, it makes sense to wait for 6 confirmations or more. Each confirmation exponentially decreases the risk of a reversed transaction.

---

## **Consensus**

The process of how a group of peers within a network determines truth, usually through algorithms to establish rules regarding the addition of blocks and validation of nodes.

---

## **Consensus Mechanism**

Various types of consensus mechanism used to validate a transaction designed to achieve Byzantine Fault Tolerance. (A consensus mechanism refers to any number of methodologies used to achieve agreement, trust, and security across a decentralized computer network. -Investopedia)

---

## **Consensus Point**

A point – either in time, or defined in terms of a set number or volume of records to be added to the ledger – where peers meet to agree to/on the state of the ledger.

---

## **Consensus Process**

The consensus process a group of peers responsible for maintaining a distributed ledger uses to reach consensus on the ledger's contents.

---

## **Consortium**

A consortium blockchain is a private blockchain network where the consensus process is controlled by a pre-selected set of nodes. For example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which ten must sign every block for the block to be valid. The right to read the blockchain may be public or restricted to the participants. There are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state. These blockchains may be considered “partially decentralized”.

---

## **Cryptoanalysis**

Cryptoanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required to do so.

---

## **Cryptocurrency**

Cryptocurrency (also known as digital assets and digital currencies) is a form of digital currency based on mathematics and transferable electronically, where encryption techniques, consensus mechanisms, and code are used to regulate the generation of units of currency and verify the transfer of funds.

A digital asset designed to be used as a medium of exchange.

Cryptocurrencies are borderless, secure, and maintained by blockchains, as opposed to centralized banks or governments - the ideal definition. Not all cryptocurrencies are the same. The ideal definition best can be applied to Bitcoin.

---

## **Cryptography**

Cryptography is a method for securing communication (protecting data by encrypting and decrypting information) using math, logic, and code. The main example of cryptography in cryptocurrency is the asymmetric-key cryptography used in the Bitcoin network. Bitcoin addresses generated for the wallet have matching private keys that allow for the spending of the cryptocurrency. The corresponding public key coupled with the private key allows funds to be unlocked. This use of cryptography makes it nearly impossible for anyone to spend funds from another user. This is one example of cryptography in action. In the word, cryptography: "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing".



---

## **Currency**

Currency is money that is accepted or in use.

---

## **Custody**

Custody is a service in which a financial institution or other entity holds property on behalf of a customer.

---

## **DAC**

A DAC (Decentralized Autonomous Community or Corporation) is a collaborative governance structure around a community-based, or corporation-based system with agreed upon guidelines written on the blockchain.

---

## **DAO**

A DAO (Decentralized Autonomous Organization) in general is a governance structure that contains a set of predefined rules in a smart contract to review “good behavior” and penalize “bad behavior”. Generally, Decentralized Autonomous Organizations can be thought of as corporations that run without any human intervention and surrender all forms of control to an incorruptible set of business rules.

Also called a DAC - a Decentralized Autonomous Corporation. An organization based on open-source code and governed by its users. DAOs typically focus on a specific project or mission and are governed by community-agreed upon guidelines written on the blockchain.

---

## **(The) DAO**

The DAO is also known as the digital decentralized autonomous organization (DAO) - The DAO served as a form of investor-directed venture capital fund that sought to provide enterprises with new decentralized business models. Built on the Ethereum blockchain, The DAO's code was open source and caused a soft and a hard fork.

---

## **DApp**

A DApp stands for Decentralized Application. Decentralized applications that retrieve some or all of their data from a blockchain network, typically Ethereum. To be considered a text-book DApp, it must be completely open-source, operate autonomously, and have no entity controlling the majority of its crypto tokens.

---

## **DDOS**

DDOS is a denial-of-service attack that is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

---

## **Dead Cat Bounce**

A dead cat bounce is a small recovery in prices after a big downward movement. From the phrase : “Even a dead cat (thrown off a roof) bounces.”

---

## **Decentralized**

Decentralized means to distribute the administrative powers or functions of (a central authority) over a less concentrated area: to decentralize the national government. to disperse (something) from an area of concentration: to decentralize the nation's industry. A decentralizedDecentralized system is a system without central authority or decision making. See definition for cryptocurrency.

Not controlled by a single institution or authority, but distributed among a variety of computers, networks and nodes.

---

## **Decentralized Content (DeCo)**

Decentralized Content (DeCo) is a form of on-chain content distribution that seeks to eliminate intermediaries, allowing each user to directly receive the real benefits that their content has generated. Components of DeCo could include: decentralized storage, public blockchain ownership registration, and automated revenue to creators.

---

## **Decentralized Exchange (DEX)**

Decentralized Exchanges are a method to buy or sell cryptocurrencies without the use of an arbiter, or market maker. Price is determined solely via bids and asks.

---

## **Decentralized Identifier**

Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID identifies any subject (e.g., a

person, organization, thing, data model, abstract entity, etc.) that the controller of the DID decides that it identifies (W3C Definition).

---

## **Decentralized Society (DeSoc)**

Decentralized Society (DeSoc) was coined related to Soulbound Tokens (SBTs) which were proposed in May 2022 by economist & social technologist E. Glen Weyl, lawyer Puja Ohlhaver, and Ethereum creator Vitalik Buterin. A terminology, technology, and theory to counterbalance Web3's movement toward hyper-financialization into something more inclusive, democratic, and decentralized.

---

## **Decentralization**

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

---

## **DevOps**

DevOps is a set of practices in which a company combines software development with the process of software technical operations.

---

## **Digital Asset**

A digital asset is the recommended description for this emerging asset class. Several other terms, such as *cryptocurrencies*, *crypto assets*, *virtual currencies*, and *crypto tokens*, are also used in this evolving market.

---

## **Decentralized Application (DApp)**

Decentralized Applications are an open source, trustless software application with the backend code running on a decentralized peer-to-peer network (a decentralized blockchain network) rather than a centralized server.

---

## **Decryption**

Processing of turning cipher-text into readable plain text message.

---

## **DeFi**

Financial decentralized applications (dApps) and tools built on the blockchain. Short for “decentralized finance,” an umbrella term for a variety of financial applications geared toward disrupting financial intermediaries.

---

## **Degen**

A person that spends a significant amount of time and their own money to “go all in” on NFTs, often referred to as going “full degen”.

---

## **Delist**

To “delist” is to take down an NFT item from an auction, or marketplace.

---

## Derivative

A derivative in the finance world is a financial contract which depends on another asset to retain its value. This could be either a contract or a security. When it comes to the cryptocurrency world, however, this word takes on a slightly new meaning and usually refers to a contract signed by two or more parties to purchase a certain cryptocurrency at a certain price. If the specified cryptocurrency changes price before the time of the contract completion, its value will be influenced. There are three main types of derivatives and these are swaps, futures, and options.

---

## Difficulty

The level of difficulty to verify blocks in a blockchain network, usually refers to Proof of Work.

---

## Digital Asset

The definition of a digital asset is *“anything that exists in binary (‘1’s and 0’s) data which is self-contained, uniquely identifiable, and has a value or ability to use.”* When the term originated in the mid-90s, digital assets were items such as videos, images, audio, and documentation. Since then, technological advances have given the term new life. Today, blockchain technology allows us to tokenize nearly everything we own. Consequently, items that were once non-liquid such as debt can now be traded between anyone, anywhere, in person, or across the internet. This ability to tokenize any item creates entirely new digital asset classes in the market. These new asset classes continue to develop. As such, lawmakers continue to adjust regulations to account for the new efficiency that these services bring.

---

## Digital Commodity

A digital commodity is a scarce, electronically transferrable, intangible commodity with a market value. See also the definition for “*Digital Asset*”.

---

## Digital Identity

Digital identity is about protecting identifying information that is collected and about customer identity management (business data, sensitive versus non-sensitive non sensitive data, passport, date of birth, Driver’s ID, etc...). There are different realms in the identity framework: government, civil society, commercial and employment.

---

## Digital Signature

A digital signature is a mechanism that uses public-key cryptography to create unforgeable proof that a transaction is authorized by the owner of the coins. Generated by public key encryption, a digital signature is a code attached to an electronically transmitted document to verify its contents. The most common algorithm used by digital assets is the Elliptic Curve Digital Signature Algorithm (ECDSA), though there are many such algorithms, including Schnorr and BLS signatures, whose use is increasing. The signature itself is a 65-byte number, which in combination with a message and a public key can be validated by the signature algorithm.

---

## Digital Signature (Multi-signature)

A Digital Signature (multi-signature) is when more than one signature is used to sign a transaction.

---

## **Digital Signature (Ring)**

A Digital Signature (Ring) is the signing of a transaction by a group of people who had keys.

---

## **Directed Acyclic Graph (DAG)**

Graph structures without recursive routes, creating links between blocks, transactions and data storage structures.

---

## **Distributed**

Distributed computing is a model in which components of a software system are shared among multiple computers. Even though the components are spread out across multiple computers, they are run as one system.

---

## **Distributed Ledger**

Distributed ledgers are a type of database that are spread across multiple sites, countries or institutions. Records are stored one after the other in a continuous ledger. Distributed ledger data can be either “permissioned” or “unpermissioned” to control who can view it.

---

## **Difficulty**

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



---

## **Direct Acyclic Graphs (DAGs)**

A non-blockchain database structure, DAGs are another form of consensus when it comes to managing data. The theory of DAGs advantage over blockchain are: no transaction fees since transactions are approved as users contribute to the security of the network by confirming past transactions, and some DAGs are asynchronous meaning that not all transactions occur at the same time as they do in a blockchain database structure.

---

## **DLT (Distributed Ledger Technology)**

Distributed Ledger Technology (DLT) is a larger class of technology which includes blockchain, where transactions are recorded in multiple copies without central authority or data storage, whether they are permissioned or unpermissioned.

---

## **dNFTs**

dNFTs can stand for both “distributed” or “dynamic” NFT. The (distributed) NFT was starting to be termed/described in <sup>1</sup>2019 (see also fNFTs - fractionalized NFTs). The (dynamic) NFT is more recent, with a full breakdown of this evolving NFT operability through <sup>2</sup>Chainlink labs.

---

<sup>1</sup> <https://medium.com/quillhash/partial-ownership-on-eos-773aea600e3>

<sup>2</sup> <https://blog.chain.link/what-is-a-dynamic-nft/>

---

## Double Spend

Double spend refers to a scenario, for example in the Bitcoin network, where someone tries to send a bitcoin transaction to two different recipients at the same time, or when the same digital tokens are spent or used twice. It is creating two conflicting transactions. This is prevented by the Bitcoin network and double-spends are not allowed. Once a bitcoin transaction is confirmed, it makes it nearly impossible to double spend it. The more confirmations that a particular transaction has, the harder it becomes to double spend the bitcoins. This is arguably the primary innovation of the Bitcoin blockchain—an algorithm for preventing double-spends. However, in combination with a *51% Attack*, an attacker can cause one conflicting transaction to be replaced with another if he or she controls 51% or more of the hashrate. See *51% Attack*.

---

## Dox

To “dox” is to reveal private information.

---

## DPoS

Delegated Proof of Stake (DPoS) is a consensus algorithm that was developed to secure a blockchain by ensuring representation of transactions within it. DPoS is a technology-based democracy that uses voting and elections to protect blockchain from malicious attack and centralization.

---

## Drop

Another word for “*launch*” within the NFT industry. Not to be confused with “airdrop”.

---

## **Dump**

To dump is to do a sale of your tokens as a result of market pressure.

---

## **DYOR**

DYOR stands for Do Your Own Research.

---

## **ELI5**

ELI5 stands for Explain to me like I'm 5.

---

## **Elliptic Curve Cryptography (ECC)**

Elliptic Curve Cryptography is the preferred public-key cryptography approach for cryptocurrencies to authorize asset transfer. It is favored over older mechanisms based on prime numbers because of the relatively small size of keys and digital signatures and is based on solving equations using an elliptic curve with values in a finite field. The most common elliptic curves used for digital assets are called secp256k1 (e.g., Bitcoin, Ethereum) and ed25519. They are accompanied by an algorithm to create *digital signatures* that can be publicly validated.

---

## **Encryption**

Encryption is the process of turning a readable plain clear-text message (plaintext) into a data stream (cipher-text). Cipher-text looks like a meaningless and random sequence of bits.

---

## **ERC20 Token Standard**

ERC20 Token stands for Ethereum Request for Comment followed by the assignment number and is a fungible Ethereum token type. A technical standard for smart contracts the majority of Ethereum tokens follow. Essentially a list of rules an Ethereum token has to implement to be compliant and function within the Ethereum network.

---

## **ERC-223**

Token Standard: ERC223 is a token standard with a focus on security that allows token transfers to act as ETH transactions, using event handling (transaction management) to prevent lost tokens. This standard is an improvement on the ERC20 critical bug.

---

## **ERC-721**

Token Standard: ERC721 is a non-fungible Ethereum token standard. Non-fungible meaning that the token standard is used to represent a unique digital asset that is not interchangeable.

---

## **ERC-4907**

On June 28, 2022, the “rentable” NFT standard ["EIP-4907"](#) from the NFT rental marketplace Double Protocol, passed Ethereum final review and became the 30th ERC standard with the status of "Final". An extension of ERC-721, ERC-4907 implements the time-limited role of 'user' and authorizes automatic expiration through the innovative 'expires' function. The expires feature no longer requires owners to withdraw user rights – often complicating the simultaneous leasing of NFT assets – and results in reduced gas costs.

---

## **Ether (ETH)**

Ether is the integral element (i.e. native cryptocurrency) of the Ethereum Blockchain network and is a tradeable digital asset. Ether functions as a fuel of the Ethereum ecosystem. Ether acts as a medium of incentive or form of payment for the network participants to execute their requested operations on the network. The focus of Ether tokens is not as a store of value, but as a system for creating and paying for the execution of smart contract logic (transaction fees, miner rewards, and other services).

---

## **Ethereum (ethereum)**

Ethereum is an open software, decentralized, blockchain-based computing platform where developers build, deploy and run decentralized applications that contribute to the value of ETH cryptocurrency ecosystem. Decentralized applications include smart contracts. Ethereum is a public blockchain network. In ethereum blockchain, mining computers work to earn ETH, a digital asset that supports the Ethereum network.

A public blockchain serving as the foundation for decentralized applications. Ethereum is a Turing complete language, allowing users to write and deploy complex, self-executing smart contracts which live on the blockchain.

---

## **Ethereum Classic**

Ethereum Classic is a blockchain that was formed from a split from Ethereum after a hard fork.

---

## **Ethereum Enterprise Alliance (EEA)**

The EEA is a group of enterprise partners that are committed to support the development of Ethereum.

---

## **EVM (Ethereum Virtual Machine) Code**

EVM code is the programming language in which accounts on the Ethereum blockchain can contain code. The EVM code associated with an account is executed every time a message is sent to that account, and has the ability to read/write storage and itself send messages.

---

## **EVM (Ethereum Virtual Machine)**

The Ethereum Virtual Machine (EVM) is Turing complete and a state machine that allows anyone, anywhere to execute arbitrary EVM Byte Code. EVMs uses bytecode to process transactions and perform state transitions for the ethereum blockchain. All Ethereum nodes run on the EVM, and are the same for every node in the network. The project is designed to prevent denial-of-service attacks. It is home to smart contracts based on the Ethereum blockchain.

---

## **EWASM**

EWASM is a web assembly of the EVM that gives additional functionality for the blockchain.

---

## **Exchange**

An exchange is a place or a platform to buy, sell and/or trade cryptocurrencies, using both fiat currencies and other digital assets. The exchange charges fees in many cases for transactions, withdrawals, or deposits. Exchanges are a way to link your fiat funds to a location where you can purchase cryptocurrency. There are centralized exchanges for cryptocurrency like Coinbase and there are decentralized exchanges that do not have a central authority.

---

## **FA**

FA stands for Fundamental Analysis.

---

## **Faucet**

Faucet is a website or app that gives out small amounts of cryptocurrencies, sometimes as a reward for completing tasks. Used on testnets to get native assets for development testing, etc.

---

## **Fiat**

Fiat is government-issued currency and backed by a central government, for example: USD, EUR, CNY, JPY. The government's debt and/or paper is used as money and the government is able to increase its supply as it sees fit. Using

other forms of money for exchange, or attempting to create more of the government's money is at the risk of punishment by the government.

Government issued currency that is not backed by a physical commodity, such as gold or silver, but rather by the government that issued it.

---

### **Finality (Instant Finality)**

Finality of settlement ensures that transactions made over payment networks will, at some point, be complete and not subject to reversal even if the parties to the transaction go bankrupt or fail.

---

### **Financial Crimes Enforcement Network (FINCEN)**

FINCEN is the US federal agency responsible for investigating and prosecuting financial crimes.

---

### **Flipping**

Flipping is to trade an asset (like an NFT) quickly for a profit.

---

### **Floor price**

The “floor” means the lowest price that an NFT can be purchased. (see also “sweep the floor”)

---



## **fNFT**

NFTs that are “fractionalized” and are subject to being issued as a security under the Howie Test.

---

## **FOMO**

FOMO stands for Fear of Missing Out.

---

## **FORGING**

“Forging” describes the creation of a physical good from an NFT, such as receiving a physical fashion product after buying the NFT.

---

## **Fork**

A fork creates an alternative version of a blockchain and occurs when the rules of the blockchain are changed and forces the creation of a new digital asset (if there is contentious disagreement among the network participants, or some nodes don't upgrade in time). A fork causes two or more chains to run simultaneously on different parts of the network. They can be either accidental or intentional. This may result from an upgrade to the features of the blockchain, a bug in the consensus algorithm, or changes to the node software. Alternatively, a hard fork may result in a continuation of the network structure if all the participants agree to the changes, install new node software, and update dependent software-like wallets. Soft forks are backward-compatible software updates to a digital asset blockchain, and are minor modifications of the original code (but with a new genesis block). Soft forks do not result in a physical split of the blockchain into two digital assets. The new soft fork does not share any history with the original cryptocurrency. An example of a soft fork is: Litecoin which is a Soft-Fork of Bitcoin. Litecoin is

a separate cryptocurrency from Bitcoin, and does not share any history, but does share the original code-base.

---

## **Fractionalized**

Fractionalized means a portion of one unit of cryptocurrency or a portion of an asset.

---

## **Fren**

A term meaning “friend” in NFT communities.

---

## **FUD**

FUD stands for Fear, Uncertainty and Doubt.

---

## **Fungible**

Fungible means a widget could be exchangeable with another widget such as conversion of USD with Euros.

---

## **Fungible token**

A digital asset representing value that can be divided into smaller fractions like one bitcoin into satoshi. A fungible token (unlike a non-fungible token) is a type of cryptographic token that is a digital asset that is interchangeable and is used for exchange of value on a blockchain network. Examples of

fungible tokens: 5 quarters on a table, each valued at 25 cents; 10 \$100 dollar bills on a table, each valued the same; 10 brand-new #2 pencils out of a box; 10 first-class postage stamps.

---

## **Futures Derivative**

Futures, just like when it comes to fiscal currency, are an agreement or obligation for a buyer to buy certain assets at a later date (or for a seller to sell at a certain point or date). However, as far as futures go, these are often only available for currencies such as Bitcoin or Ethereum which are popular and hold a large share of the cryptocurrency market.

---

## **GameFi**

GameFi, is the combination of gaming and blockchain-powered financialization. Traditional game systems and companies own every aspect of the users experience while playing the game. In GameFi, users have the ability to earn digital assets like NFT's, own them, and keep them stored in decentralized networks. GameFi is also known as play-to-earn since players are rewarded with ownable assets for their in-game efforts.

---

## **Gas**

Gas is a way to measure the computational steps necessary (or computational difficulty) for a transaction (in processing a smart contract function) on the Ethereum network that then equates to a fee for network users. More intensive actions (or more complicated smart contract functions) require more gas. Every transaction on ethereum requires a gas limit and a fee - and miners have a choice of including the transaction and/or collecting the fee. For most operations it is ~3-10, although some expensive operations have expenditures up to 700 and a transaction itself has an expenditure of 21000.

A fee paid by a user to conduct a transaction or execute a smart contract on the Ethereum blockchain. This fee is dependent upon the transaction's complexity as well as the current demand on the network.

---

## **Gas Price**

Gas price is the number of tokens charged as a fee to write a transaction to a public blockchain. Such tokens are utilized to reward a miner who validates the transaction.

---

## **Genesis Block**

Genesis block is the very first original block in a block chain. It does not reference any prior block, and all subsequent blocks will reference the genesis block.

---

## **GM**

NFT Twitter language for “good morning”, but also “hi”, “bye”, “please”, “thank you” and/or what’s up.

---

## **GN**

NFT Twitter language for “good night”.

---

## **Gossip Protocol**

Gossip protocol is a system in which actors in a network exchange information with other actors.

---

## **Governance**

Governance is the principles and rules governing an entity, group or organization.

---

## **Graphical User Interface (GUI)**

GUI is an interface of how information is displayed to the user.

---

## **Gwei**

Gwei is a denomination of the cryptocurrency Ether (ETH), which is used on the Ethereum network, typically used in gas context.

---

## **Halving**

Halving is the process where the number of a cryptocurrency is decreased by 50%, every 4 years. Digital asset miners are compensated, or *rewarded*, for their work, which aids the process of validating and processing transactions. In Bitcoin, the reward amount for successfully mining a block is cut in half every four years. This is done to control the distribution of new digital assets in circulation. It is the technical mechanism by which the creator implemented the monetary policy of the system. Bitcoins have a finite supply, which makes

them a scarce digital commodity. The total amount of bitcoins that will ever be issued is 21 million. The final halving will take place in the year 2140.

---

### **Hard Fork (See also, Fork)**

A hard fork is a rule change to the blockchain protocol that makes previously invalid blocks/transactions valid, and therefore requires all users to upgrade their clients (known as flag day). In case of a hard fork, all nodes meant to work in accordance with the new rules need to upgrade their software. A hard fork is the splitting of a digital asset's blockchain in a backward-incompatible way, resulting in two distinct digital assets. The code and data are replicated from the original digital asset to create the new one, adding backward-incompatible changes. Once the hard fork occurs, the two digital assets are non-fungible with each other but share some transaction and ledger history.

Hard forks occur for two key reasons: The first is when competing visions of a digital asset's future development fail to reach agreement. The second is unforeseen bugs or intentional fixes to system-critical issues. When a hard fork occurs, developer and miner support are key components in determining whether the digital assets gain or lose value and relevance.

If poorly implemented, hard forks can also cause instability in the digital asset's network, because of transactions that may be valid on both networks. Coordination of flag days is extremely difficult and, as digital asset networks grow, may become impossible. For this reason, some digital assets such as Bitcoin do not use hard forks as an upgrade mechanism. It's also a split in the blockchain of a particular crypto-currency into two (2) block-chains. This results in two (2) cryptocurrencies with a common shared history (the original blockchain). An owner of the original cryptocurrency, after the hard fork, now owns both cryptocurrencies after the hard fork. An example of a Hard Fork is the split of Bitcoin (BTC) to Bitcoin (Core) (BTC), and Bitcoin Cash (BCH). Original owners of Bitcoin, own both Bitcoin and Bitcoin Cash.

---

## Hardware Wallet

A hardware wallet is a physical device like the famed Ledger Wallet that can be connected to the web and interact with online exchange, but can also be used as cold storage.

---

## Hash

Hash is a function that converts one value to another, or the function of mapping data of a variable size to a new set of data at a fixed size so that reverse computation is nearly impossible. The output of a Hash is known as a “hash value” or “digital fingerprint”. Hashing data is a common practice in computer science and is used for several different purposes. Examples include cryptography, compression, checks, generation, and data indexing. Hashing is a natural fit for cryptography because it masks the original data with another value.

A hash function can be used to generate a value that can only be decoded by looking up the value from a hash table. The table may be an array, database, or other data structure. A good cryptographic hash function is non-invertible, meaning it cannot be reverse engineered. Cryptographic hash functions require specific properties to be considered secure, and different digital assets may use different hash functions. The SHA-256 hashing algorithm is used in Bitcoin, and SHA-3 with Ethereum, for example. The hash is used to confirm coin transactions on the blockchain. Each block in the blockchain contains the hash value that validated the transaction before it and its own hash value.

---

## Hash Collision

Hash collision is two inputs that go to the same output hash.

---

## **Hash Function**

Hash function is the cryptographic function that maps data of arbitrary size to fixed size values.

---

## **Hashcash**

Hashcash is a proof-of-work system used to limit denial-of-service attacks and email spams, and more recently has become known for its use in bitcoin (and other cryptocurrencies) as part of the mining algorithm.

---

## **Hashgraph**

Hashgraph is a patented distributed ledger technology developed by Leemon Baird and is the intellectual property of the Swirlds Corporation.

---

## **Hashgraph Consensus Mechanism**

Hashgraph consensus mechanism is a consensus mechanism using the gossip protocol on the Hedera blockchain platform.

---

## **Hashrate**

Hashrate is the number of hashes that can be performed by a bitcoin miner in a given period of time (usually a second). The hash rate is the measuring unit of the processing power of the Bitcoin network. The Bitcoin network must make intensive mathematical operations for security purposes. When the network reached a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per second. When miners run software to create blocks, the



algorithm they run is called a hash. Miners compute a lot of hashes; the sum of how many hashes they compute in a given unit of time is called their *hash rate*. Hash rate is directly correlated with miner earnings. Increasing one's hash rate by installing new mining devices increases the miner's profits. As of October 2018, all bitcoin miners combined compute 50 EH/s (50,000,000,000,000,000,000 hashes per second), which is more computations than all the world's other computers combined. These computations are of special purpose, useful only for mining bitcoin and cannot be repurposed to solve other problems. Hash functions are commonly used for proof-of-work algorithms and are integral to digital signature algorithms.

---

## **Hexadecimal Notation**

Hexadecimal notation is raw data in base 16.

---

## **HODL**

HODL means holding your cryptocurrency through a bear market. Also known as “Hang on for Dear Life”. What began as a typing error on a Bitcoin forum in 2013 has become a beloved rally cry for long-time bitcoiners. It expresses the belief that long-term value is better obtained by holding a digital asset rather than actively trading it. Don't rush to correct someone when you see this term; instead, ask them to tell you the story.

---

## **Hodler**

a person that hodles. (see HODL definition)

---

## Honeypot Scam

A honeypot scam is a scam whereby an attacker baits a smart contract they created with their own crypto then tricks a victim into depositing their crypto. The contract has a trap door that locks-away the victims crypto and the attacker can withdraw the victims crypto at their leisure.

---

## Hot Wallet

A hot wallet is a wallet that is directly connected to the internet at all times. For this reason, hot wallets are considered to have lower security than a cold storage system or hardware wallet.

---

## Howey Test

The [Securities Act of 1933](#) and the [Securities Exchange Act of 1934](#) dictate much of the U.S. government's approach to financial regulation, even nearly 100 years after they were established. Under these acts, transactions which qualify as "investment contracts" are considered [securities](#), meaning that they are also subject to specific requirements related to disclosure and registration. Digital assets and tokens may be classified as a security based on the "Howey Test" (see token definitions).

---

## Hyperledger Fabric

Hyperledger Fabric is a private permission blockchain offered by IBM and hosted by The Linux Foundation.

---

## **Identity**

Identity is the unique representation of a human being, entity, organization, machine, application or computer.

---

## **Immutable**

Immutable means an inability to be altered or changed over time. This refers to a ledger's inability to be changed by a single administrator, all data once written onto a blockchain can be altered.

---

## **Immutability**

Immutability is a characteristic, property or attribute where something cannot be changed.

---

## **Impermanent Loss**

Impermanent loss happens when you provide liquidity to a liquidity pool, and the price of your deposited assets changes compared to when you deposited them. The bigger this change is, the more you are exposed to impermanent loss. In this case, the loss means less dollar value at the time of withdrawal than at the time of deposit.

---

## **Initial Coin Offering (ICO)**

An Initial Coin Offering (also called an ICO) is an event in which a new cryptocurrency sells advance tokens from its overall coinbase, in exchange for

upfront capital. ICOs are frequently used for developers of a new cryptocurrency to raise capital.

---

### **Initial Token Offering (ITO)**

Initial Token Offerings are similar to ICOs (initial coin offerings), but different in that not every blockchain project that is tokenized has developed a new coin. A project built on the Ethereum network that is tokenized using ETH would be considered an ITO, the project isn't launching a new coin, just a new application on an established coin platform.

---

### **Institutional Investor**

Institutional investor examples include hedge funds, investment advisors, pensions and endowments, mutual funds, and family offices.

---

### **Intentional Fork**

An intentional fork helps to reverse and repair the damages related to hacking or a catastrophic bug on a blockchain.

---

### **Interchange**

The action of interchanging things, especially information. *Synonyms:* exchange · trading · trade · swap · swapping · barter · bandying · give and take. The interchange is an electronic transfer of information. In the business world, this usually involves financial data. Banks are common users of interchange data because they issue credit cards and debit cards. The action of

interchanging things, especially information. synonyms: exchange · trading · trade · swap · swapping · barter · bandying · give and take

---

## **Interworking**

The state or an instance of two or more things working with or being made to work with each other based on a common language or understanding and not based on technology.

---

## **InterPlanetary File System (IPFS)**

IPFS is a distribution protocol that started as an open source project at Interplanetary Networks. The p2p method of storing and sharing hypermedia in a distributed file system aims to help applications run faster, safer and more transparently. IPFS allows objects to be exchanged and interact without a single point of failure. IPFS creates trustless node interrelations.

---

## **Interoperability**

Interoperability is the characteristic, property or attribute where two different systems could communicate and exchange data.

Being able to seamlessly travel between virtual spaces with the same virtual assets, such as avatars and digital assets.

---

## **IP-NFT**

The IP-NFT was created from [@cl2pp](#) (Twitter), a web3 developer and Product Manager at Molecule, for "Creating legal agreements between two parties for

(pre-patent) biopharma assets is complicated, in-transparent and lengthy” - and therefor by “accounting for the sensitivity of early-stage IP. Molecule is utilizing the power of Ethereum and NFTs to standardize the process of creating and transacting around the early-stage biopharma IP: The IPNFT is born." (@Molecule Twitter thread March 29, 2022)

---

## IYKYK

Stands for “if you know, you know” and implies that a piece of news about NFTs will make sense to some ‘insiders’ and not to other people. (see also *Probably Nothing*)

---

## Journal Entry

A journal entry is the method used to record all individual financial transactions made by a company into its journal. To put it more simply, it is the daily accounting input written in the journal for each business event.

---

## JOMO

JOMO is the Joy of Missing Out.

---

## Key Pair

The term *key pair* describes public and private keys used in public-key (or *asymmetric*) cryptography, where the key used to encrypt data is different from the key used to perform decryption. In Bitcoin, public keys are used as a transaction output in addresses, functioning similarly to an account number

or payment instruction, while the private key is known only to the funds' owner and can be used to sign transactions moving those funds.

---

## Keys

Keys are long numeric codes that are involved in digital asset transactions, often encoded as hex or alphanumeric strings. *Asymmetric* key cryptography provides a strong security layer in which two different keys are created—a public key that is shared to encrypt a message, and a private key that is confidential to decrypt or sign a message. In Bitcoin these asymmetric keys are used to create digital signatures instead of encryption, which can be validated by everyone. There are two kinds of keys: public and private.

---

## KYC

Know Your Customer is the process of identifying and verifying the identity of its clients depending on jurisdiction and legal requirements.

---

## Ledger

A ledger is the principal book or an append-only computer file for recording and totaling economic transactions measured in terms of a monetary unit of account by account type, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account. Traditional accounting practices use a ledger to keep track of money movements in and out of accounts, with each party keeping its own ledger and requiring reconciliation between the ledgers of different parties. The Bitcoin network maintains a public ledger that records all transactions. As transactions are executed, updates to the ledger *blocks* containing sets of recent transactions are distributed to millions of computers around the world. Because of the wide distribution of the ledger history, no central point of

failure exists, and therefore it is practically impossible for the ledger to be altered by either malice or mistake. The transactions recorded on the Bitcoin ledger are unalterable, permanent, and nearly impossible to erase.

---

## **LFG**

In NFT culture means “let’s f\*cking go” and is often associated with a rocket ship emoji and equates to being very bullish and hyped about something.

---

## **Light Client**

A light client is a wallet which does not download and validate the full blockchain (see Node). Generally they are wallets (particularly on mobile devices) and rely on a server to supply them with transactions. In order to have full security for assets, a *full node* is generally required. A light client mechanism was originally proposed by Satoshi Nakamoto called Simple Payment Verification (SPV). Although it was initially deemed to be unworkable, several improvements have been made since. This is an area of active research and development.

---

## **Lightning Network**

The Lightning Network (LN) is the Layer 2, or secondary layer on the Bitcoin blockchain optimized for speed and cost. It enables fast transactions amongst users/participating nodes. It was proposed as a solution to the bitcoin “scalability problem” which creates payment channels outside of the main base blockchain, while still benefiting from the Bitcoin Blockchain’s security and decentralization. Elizabeth Stark is the CEO and Co-founder of the Lightning network. The Lightning Network can allow for millions of transactions per second that can settle at practically no cost.



The Lightning Network can process a million transactions per second. The main Bitcoin blockchain can process around 7 transactions a second.

---

## **Lindy Effect**

An idea that the future life expectancy of some non-perishable things like a technology or an idea is proportional to their current age, so that every additional period of survival implies a longer remaining life expectancy.

---

## **Liquid**

“Liquid” means a project has a lot of buyers and sellers who want to buy and sell. Liquid buyers have cash to spend.

---

## **Liquidity**

Liquidity is the ability of a monetary medium to be bought and sold without too much loss. The more people accept a monetary medium, the more liquid it is. The more trading and transactions of a monetary medium, the more liquid it is.

---

## **Liquidity Mining**

Liquidity mining is the process by which a yield farmer obtains a new token as well as mining rewards in exchange for the farmer’s liquidity.

---

## List

To “list” is to put an NFT up for sale. (see also *Delist*)

---

## Litecoin (LTC)

Litecoin is a peer-to-peer cryptocurrency based on the Scrypt proof-of-work network. Sometimes referred to as the silver of bitcoin's gold. Litecoin was an early bitcoin spinoff or altcoin, founded by Charlie Lee in October 2011. Litecoin was a fork of the Bitcoin Core client, differing primarily by having a decreased block generation time (2.5 minutes), increased maximum number of coins, different hashing algorithm (Scrypt, instead of SHA-256)

---

## Long

Long is a positive perception of a coin.

---

## Mainnet

Mainnet is the production version of a blockchain.

---

## Market Cap

Market Cap stands for market capitalization. The term *market capitalization* comes from the world of equities and is determined by multiplying the total outstanding shares of an asset by the last available share price. The term has been adopted for use in the digital asset space and is computed by multiplying the total coin supply by the current market value of each coin. Some prefer the term *implied network value*, as the coins are digital assets of

decentralized networks rather than shares in a company. MarketCap is commonly associated with the website CoinMarketCap in the crypto community, a market cap is the total value held in a cryptocurrency. The website lists nearly all cryptocurrencies' market caps and serves as a major point of reference for investors.

---

## **MCAP**

MCAP is the market capitalization of the coin.

---

## **Maximum Coin Supply**

Maximum Coin Supply is the total number of coins that can be minted for a particular digital asset. Most digital assets have been designed with caps on the total supply that can be created by the network in an attempt to drive value by creating digital scarcity. A digital asset's maximum coin supply is a fundamental feature of its design, and some have no fixed maximum supply at all. Bitcoin's maximum coin supply is set at 21 million.

---

## **mBTC**

An mBTC is one thousandth of a bitcoin, or 0.001 BTC. A bitcoin can be split into very small parts. Each bitcoin is divisible to the eighth decimal place, so each bitcoin can be split into 100,000,000 units (*satoshis*). It is also called a *millibitcoin*. See also uBTC and Satoshi.

---

## Memory Pool (mempool)

Memory Pool is where unconfirmed transactions reside until they are confirmed in a block. High mempool size means more network utilization and typically higher transaction fees.

---

## Merkle Proof

Merkle Proof is the process of climbing a Merkle Tree from the leaf to the root level used to determine whether data belongs to the Merkle Tree, prove the validity of data without storing the entire data set and without revealing the data set or their subset.

---

## Merkle Root

Merkle Root is the cryptographic hash of all transaction hashes in a blockchain network.

---

## Merkle Tree

A Merkle tree, also called a Hash Tree, is a binary tree data structure in which a set of data can be compactly committed to so that it cannot be modified. A Merkle tree is a data tree where every leaf node contains the cryptographic hash of a block of data, and every non-leaf node contains the cryptographic hash of its children. It works by hashing together pairs of data (leaf nodes), hashing the pairs of the pairs from that hashing and so on, in pairs, until there is a single hash remaining. This is known as the *Merkle Root* and is a compact commitment to the entire set of data. Most digital assets use Merkle Trees to ensure that the set of transactions in a block are unmodified. A Merkle Tree also has a feature where by presenting a list of hashes which indicate a branch of the tree, a single element can be proven to be present in the tree.

This is the fundamental tool used by Satoshi Nakamoto in his “Simple Payment Verification” (SPV) proposal.

---

## **Metadata**

The stored data that provides more detailed information about the data with which it is associated.

---

## **Metaverse**

The metaverse is an umbrella term used to describe a group of 3D, interactive virtual environments. Accessible through virtual reality, augmented reality, game consoles, mobile devices, or conventional computers. Blockchain technology plays a key role in the transactions that occur in the metaverse.

---

## **Miner**

A miner is an actor in a blockchain network that creates and submits new blocks to the blockchain.

---

## **Miner (CPU)**

A CPU miner uses its central processor to validate and produce blocks.

---

## **Miner (GPU)**

A GPU miner uses its graphics processor to validate and produce blocks.

---

## **Miner (ASIC)**

An ASIC miner uses an application-specific integrated circuit (ASIC) to validate and produce blocks.

---

## **Mining**

Mining is the process by which transactions are verified, blocks are created, validated, submitted and added to a blockchain. This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies. Miners perform all the same duties as nodes, and additionally attempt to solve a proof-of-work puzzle that, given a successful solution, gives them the right to publish a block of new transactions and allocate new coins to themselves. They do this by computing a hash repeatedly with different inputs, creating a proof-of-work algorithm. Mining is competitive and requires powerful dedicated hardware, energy consumption, and time.

---

## **Mining Pool**

Mining Pool is A group of miners that work together to generate the next block in a blockchain with the goal to increase efficiency. Due to the variance of whether a given miner will win a block or not, miners often band together into mining pools. In a mining pool, one node validates transactions and distributes a candidate block to multiple different miners. By agreeing to share winnings if one of the miners in the pool wins the block, pools help reduce variance for its members.

---

## **Mint**

Means to issue a piece of art on the blockchain, either by the artist or the collector.

---

## **Mises, Ludwig von**

Ludwig Heinrich Edler von Mises (29 September 1881 – 10 October 1973) was an Austrian School economist, historian, logician and sociologist. Mises wrote and lectured extensively on the societal contributions of classical liberalism. He is best known for his work on praxeology, a study of human choice and action.

---

## **Moon**

Moon means an expected upward movement of price.

---

## **Mooning**

An NFT project that is growing rapidly. (see also *Moon,TTM*)

---

## **Money**

Money is a current medium of exchange in the form of coins and banknotes; coins and banknotes collectively.

---

## **Money Transmitters**

Money transmission is the movement of money from one entity to another through an intermediary.

---

## **Multi Signature**

Multi-signature (multisig) addresses allow multiple parties to require more than one key to authorize a transaction. The needed number of signatures is agreed at the creation of the address. Multi signature addresses have a much greater resistance to theft. Multi-signature, or multi-sig, is a feature of bitcoin and other digital assets that requires that multiple private keys be used to sign a transaction and move funds. Practically speaking, multisig can be used to add an extra layer of security to digital asset transactions by requiring an additional approval from a third party before a transaction is approved. Digital asset custodians typically use multisig wallets and processes to help secure client funds.

---

## **Multi Party**

Multi Party is relating to, or involving multiple and usually more than two parties. The rapid innovations in multiparty systems empower business ecosystems to operate in a shared data construct.

---

## **Network**

Network is a number of actors connected for a common purpose.

---



## **NFA**

Is a disclaimer acronym that means “not financial advice” and used when promoting to clearly state they are not liable for the financial future and outcome of the person who listens to the advice.

---

## **NGMI**

means “not gonna make it” and is used to describe people and projects that are not expected to last long in the NFT space. (see also *WAGMI*)

---

## **Node (Full Node)**

A full node is a computer running software that fully validates transactions and blocks. Almost all full nodes also help the network by accepting transactions and blocks from other full nodes, validating those transactions and blocks, and then relaying them to further full nodes. A full node has a complete copy of the blockchain and fully enforces all of the rules of the blockchain. Most nodes are not full nodes and full nodes can be difficult to run due to their bulky size. A full node is a program that can fully validate transactions and blocks bolstering the p2p network. In Bitcoin, for example, *full nodes* download the entire blockchain and validate each transaction per the agreed-upon rules of the network and relay transactions and blocks to others.

---

## **Node (Light)**

A light node that has enough block data to validate the chain.

---

## **Node (Web3)**

Any device connected to a blockchain network. Blockchains are distributed peer to peer networks, nodes come together to create the network's infrastructure.

---

## **Nonce**

A nonce is a random number that is used to vary the input to a cryptographic hash function (see Hash), modifying the output in an unpredictable way. In the context of *proof of work*, the nonce is what miners repeatedly modify to find an output hash numerically smaller than the target, thereby winning the block.

---

## **Non-Fungible**

Non-fungible is a property of a widget that is not exchangeable with another widget.

---

## **Non-Fungible Token (NFT)**

An NFT is a special type of cryptographic token that is a representation of a unique digital asset that is not interchangeable. This is in contrast to cryptocurrencies like Bitcoin, and many network or utility tokens that are fungible in nature.

A non-fungible token is a digital certificate of authenticity used to assign and verify ownership of a unique digital or physical asset. Unlike fungible tokens, NFTs are not interchangeable with one another.

---

## **Non-Fungible Visualizations (NFV)**

Non-Fungible Visualizations (NFV) were first created by @programmable.art (Twitter) on Cardano as continual visual patterns of art.

---

## **Normie**

aName given to people outside the Web3, crypto, NFT, or Metaverse space.

---

## **OFAC**

The Office of Foreign Assets Control of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.

---

## **Off-Ledger Currency**

An off-ledger currency is minted off-ledger and used on-ledger. An example of this would be using distributed ledgers to manage a national currency.

---

## **Offchain**

Offchain transactions refer to those transactions occurring on a cryptocurrency network which move the value outside of the blockchain. Off-chain transactions are valid bitcoin transactions that are not sent to the

main Bitcoin network. New research using off-chain transactions is under development by several companies and enables a large increase in the effective transaction capacity of the network. They use multiple off-chain transactions to create a *payment channel* between counterparties. By keeping a valid signed transaction and *not* sending it to the blockchain, the parties in the payment channel can update their balances in real time, without having to wait for transactions to be mined. In the event of a dispute or one party going offline, the counterparties can send their transactions to the blockchain to settle. This technique is used by payment networks, such as the Lightning Network, and non-custodial trading. It is a major tool that allows blockchains to handle many more transactions than could ever be settled on the blockchain. Due to their zero/low cost, off-chain transactions are gaining popularity, especially among large participants.

---

## **OG**

OG stands for Original Gangster. OG is usually used to describe an old-school gangster, but can also be used to describe an original member of a gang, cultural movement or organization. In the technology world it refers to original developers or investors in a new technology.

---

## **Onchain**

Onchain transactions refer to those cryptocurrency transactions which occur on the blockchain - that is, on the records of the blockchain - and remain dependent on the state of the blockchain for their validity. Onchain data is stored on the blockchain.

---

## **On-Chain Analysis**

On-chain analysis is an emerging field in crypto, designed to help traders enhance their strategies. ... These analysts scrutinize blockchain data such as transaction details (like the sending and receiving addresses, amount sent in each transfer, or amounts remaining in an address), block details (like timestamps, fees, miner rewards, block weight, and addresses), and smart contract info to gain valuable insights. On-chain analytics refers to techniques that involve scrutinizing data stored on a blockchain network. This data typically includes block details, transactional data, and smart contract information. For blockchains that use smart contracts, on-chain analysis will also investigate the underlying code that controls the issuance and transfer of tokens.

---

## **One-of-One**

is the term for an NFT with only one existing edition issued by the creator. A unique and more scarce - therefore more valuable - NFT since only one exists. Also known as 1/1.

---

## **On-Ledger Currency**

On-ledger currency is minted on-ledger and used on-ledger. An example of this would be the cryptocurrency, Bitcoin.

---

## **Opcode**

Opcode is the basic command for a processor.

---

## **Open Banking**

Open banking is the term used to describe the use of open APIs that allow third party providers to build applications and services across a broad range of financial products.

---

## **Open Finance**

Open finance is the term used to describe the expansionists of Open Banking data sharing principles to allow third party providers to access consumer data across a broad range of financial products.

---

## **Open source**

Open source means software products that provide permission to use and modify the source code.

---

## **Options Derivative**

Options also function in the cryptocurrency world in the same way which they function in the fiscal world (a buyer or seller has the right but not obligation to buy or sell at a certain point) but similar to futures, these often aren't available for all cryptocurrencies on the market.

---

## **Oracle**

An Oracle helps communicate data using smart contracts connecting the real world and blockchain. The oracle finds and verifies events and gives this information to the smart contract on the blockchain.

---

## **OTC**

OTC stands for over the counter

---

## **P2P**

Peer-to-peer (P2P) refers to the decentralized interactions that happen between at least two parties in a highly interconnected network. P2P participants deal directly with each other through a single mediation point. A P2P network is created when two or more computer systems are connected to each other through the internet for file sharing and work distribution, all without a central server. Examples of P2P networks include file-sharing protocols like BitTorrent, the Invisible Internet Project (I2P) anonymity network, and digital asset protocols like Bitcoin and Ethereum.

---

## **Paper hands**

A person that has a low-risk tolerance for high volatility in the prices of their NFTs. They are known to sell quickly as the floor price drops, and usually buy high, get nervous, and sell low.

---

## **Participant**

Participant is an actor who can access the ledger: read records or add records to.

---

## **Peer**

A peer is an actor that shares responsibility for maintaining the identity and integrity of the ledger.

---

## **Peer to Peer (P2P)**

In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. P2P interactions are ones that happen between two actors in a network. In the case of Bitcoin, the network is built in such a way that each user is broadcasting the transactions of other users. And, crucially, no bank is required as a third party.

---

## **Permissioned**

Permissioned blockchains are a hybrid of public and private blockchains where anyone can access them as long as they have permission from the administrators to do so.

---

## **Permissioned Ledger**

A permissioned ledger is a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors — government departments or banks, for example — which makes maintaining a shared record much simpler than the consensus process used by unpermissioned ledgers. Permissioned block chains provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than an unpermissioned ledger.



---

## **Permissionless**

Permissionless is a blockchain-specific term that means that users do not require permission to use a blockchain protocol, DeFi platform, or related system.

---

## **PFP**

An acronym in texting, social media, and in NFT culture which means both picture for proof and profile pic.

---

## **Play to Earn (P2E)**

Concept of gaming in which a platform provides its players with a chance to earn in-game assets like tokens or NFTs that could have real monetary value.

---

## **POAP**

A Proof of Attendance Protocol (pronounced poh-ap) is a unique NFT (a “mini-NFT”) from a curated ecosystem - for the preservation of memories that is given to people to commemorate and prove they attended an event. By checking-in at different events, POAP collectors build a digital scrapbook where each POAP is an anchor to a place and space in time. (POAP.com)

---

## **Portfolio**

A portfolio is a collection of your tokens.

---

## **PoS/Pow Hybrid**

PoS/PoW hybrid is a combination of Proof of Stake (PoS) and Proof of Work (PoW) consensus protocols on a blockchain network. Blocks are validated from not only miners, but also voters (stakeholders) to form a balanced network governance.

---

## **Pre-Sale**

A term that replaces “white list” implying also a private list generated by NFT projects and communities that usually grants early access - this term is used by DE&I persons moving away from the affiliation between “white” and “exclusivity” or “VIP”. Often seen in BIPOC, women, or LGBTQIA NFT communities.

---

## **Private Blockchain**

Private blockchain is also known as private or permissioned blockchain, allows companies to create and centrally administer their own transactional networks that can be used inter- or intra-company with partners.

---

## **Private Blockchain**

A private blockchain is a closed network where blockchain permissions are held and controlled by a centralized entity. Read permissions are subject to varying levels of restriction.

---

## **Private Currency**

A private currency is a currency issued by a private individual or firm, typically secured against uninsured assets.

---

## **Private Key**

A private key in asymmetric cryptography is a unique string of characters or data (held in secret) that shows you have access and proves your right to spend the bitcoins in a specific wallet through cryptographic signature. It is used to compute digital signatures on data that can be verified using a Public Key. Your private key(s) are stored in your computer if you use a software wallet; they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin wallet.

Alphanumeric passcode required to withdraw assets from a blockchain wallet and authorize digital transactions. This passcode should never be shared over a network.

---

## **Private Key Infrastructure (PKI)**

PKI are rules and policies that manage identification through public key encryption.

---

## **Probably Nothing**

An ironic Twitter saying which implies that something is actually of value but usually only to some 'insiders' and not to other people. (see also *IYKYK*)

---

## **Proof of Activity**

Hybrid mechanism between Proof of Work and Proof of Stake.

---

## **Proof-of-Authority**

Proof-of-authority is a consensus mechanism in a private blockchain in which transactions are validated by certain known, approved accounts, called validators, who have the private key. Essentially, validators stake their reputation to the integrity of the blockchain. The right to validate the blocks is given to an actor with private key in a private blockchain.

---

## **Proof of Burn**

Proof of burn is the consensus mechanism where miners destroy their cryptocurrency in exchange for the right to mine blocks.

---

## **Proof of Capacity**

Proof of capacity is the consensus mechanism where mining rights are dependent on available hard drive space of mining devices.

---

## **Proof of Creativity**

A consensus mechanism created by Bella Irons with the children's software company LetsMOD out of Saratoga, CA in 2022, based on their internal software "creativity chain" ledger protocols.

---

## **Proof of Elapsed Time (PoET)**

A consensus mechanism that operates every node in the system must be (1) identifiable, and (2) accepted into the network where every participant is assigned a random amount of time to wait, and the first participant to finish waiting gets to commit the next block to the blockchain. Conceived by Intel in 2016 and can be used by Hyperledger Sawtooth, the theory of PoET is that by requiring each node to "rest", PoET is believed to be more energy efficient than PoS.

---

## **Proof of Identity**

Proof of identity is cryptographic evidence for a user's private key that is attached to a specific transaction.

---

## **Proof of Importance**

Proof of Importance recognizes that other factors can be taken into account when determining what nodes provide the most value to a network.

---

## **Proof of Liquidity**

Proof of liquidity is the cryptographic signed declaration by a third party auditor that an actor has the number of assets that he or she claims.

---

## **Proof-of-Stake**

Proof-of-stake is an alternative consensus mechanism to the proof-of-work system, in which your existing stake in a cryptocurrency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine. It's a consensus mechanism where the amount a miner could mine is dependent on the amount of cryptocurrency that the miner holds. In PoS-based cryptocurrencies the creator of the next block is chosen via various combinations of random selection and wealth or age (i.e., the stake). In POS, instead of miners, there are validators. The validators lock up some of their crypto as a stake in the ecosystem. Following that, the validators bet on the blocks that they feel will be added next to the chain. When the block gets added, the validators get a block reward in proportion to their stake

---

## **Proof of Stake (Delegated)**

Delegated proof of Stake consensus mechanism based on POS where miners are nominated.

---

## **Proof of Work**

Proof-of-work is a system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof

of work. For Bitcoin, Proof of Work (PoW) is the mechanism by which Bitcoin creates a cost of production for the unit of account and ensures immutability of the ledger in a trustless manner. Because each update to the ledger *block* contains a costly proof of work, this cost makes it expensive to rewrite the ledger.

---

### **Proof-of-Work (Delegated)**

Delegated proof-of-work is a consensus mechanism based on POW where miners who solved the problem can sign the right to another miner to validate the block.

---

### **Protocol**

Protocol is a set of formal rules that dictate how data is exchanged and transmitted, especially across a network. This pertains to cryptocurrency in blockchain when referring to the formal rules that outline how these actions are performed across a specific network. Can also refer to a blockchain codebase itself (i.e. Bitcoin protocol, Ethereum protocol, etc).

---

### **Provenance**

Provenance is the product lifecycle including materials to the end user.

---

### **Provably**

Provably means to be with proof or in a provable manner.

---

## **Provably Fair**

Provably fair describes the verifiers that provide proof that results are fair, commonly used in association with blockchain-based gaming applications.

---

## **Pseudonym**

A Pseudonym is an identifier used by a person that can not be used to identify a specific person.

---

## **Pseudonymity**

Pseudonymity means using pseudonyms in online activity so that the activity is not attributable to a specific person. Public Blockchain: Public blockchain ledgers can be managed autonomously to exchange information between parties. There's no need for an administrator. In effect, the blockchain users are the administrator.

---

## **Public Blockchain**

A global public network where anyone participates in transactions, executes consensus protocol to help determine which blocks get added to the chain, and maintains the shared ledger.

---

## **Public Key**

A Public Key is a unique string of characters derived from its corresponding private key used to decrypt a message. A public key is obtained and used by anyone to encrypt messages before they are sent to a known recipient with



the correct matching private key for decryption. By pairing a public key with a private key trustless transactions are possible. The public key converts the message into an unreadable format and the corresponding private key makes it readable again for the intended party.

Also called a Wallet Address. It's used to point to your wallet address. This is an alphanumeric code that serves as the address for a blockchain wallet, similar to a bank account number. Other users can send digital assets to your wallet via your public key. Only you can access your wallet's contents using your private key.

---

## **Pump**

Pump is an upward price movement.

---

## **Pump & Dump**

Pump and dump is price manipulation where you artificially drive the price upwards to dump your shares on others for a profit.

---

## **QR Code**

Quick response (QR) codes are sometimes used in place of the long string of letters and numbers that make up a Bitcoin address like this:

16r61N8tB03FTQGwZCRXLLygNqVL8MEsrR. For convenience, wallets will provide the option of converting a Bitcoin address into a QR Code for use in sending or receiving, or to transact a coin exchange directly between two smartphones, for example.

## **Raids**

Are flash social media campaigns that respond to a single message in great volumes and used to keep the community engaged and/or promote a project.

---

## **ReFi**

“Regenerative Finance”. The current ReFi industry is almost exclusively pertaining to carbon markets and the purchase or sale of carbon credits which provide incentives for landowners NOT to develop forest areas.

---

## **Rekt**

Rekt is a slang term meaning wrecked, as in ruined, especially in reference to finances.

---

## **Rentable NFT**

See ERC-4907. An extension of ERC-721, ERC-4907 implements the time-limited role of 'user' and authorizes automatic expiration through the innovative 'expires' function.

---

## **Reverse Indicator**

Reverse indicator is someone who is generally wrong when predicting movements of price.

---

## **Replicated Ledger**

A replicated ledger is a ledger with one master (authoritative) copy of the data, and many slave (non-authoritative) copies.

---

## **Ring Signature**

A ring signature is a type of private key based cryptographic digital signature that is decrypted using multiple keys. In a peer-to-peer transaction, such as that used with cryptocurrencies, a ring signature enables an individual of a group to sign a transaction without revealing the identity of the actual signer.

---

## **Ripple**

Ripple is a payment network built on distributed ledgers that can be used to transfer any currency. The network consists of payment nodes and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships.

---

## **Roadmap**

A visual chart (sometimes supported with a document) that outlines an NFT's long-term value by listing the goals and strategies of an NFT project in order to communicate its long-term value.

---

## **RSI**

RSI stands for Relative Strength Index

---

## **Rug**

A “rug” is when somebody , or a project runs away with your crypto or NFTs by disappearing and deactivating everything having to do with the project or collection. Also known as a “rug pull”.

---

## **Safu**

Safu is a slang term meaning safe.

---

## **Sandwich Attack**

A sandwich attack is a near-simultaneous front and back-running attack that primarily targets decentralized finance protocols and services. This creates artificial price variations on the trade. How it works: Malicious traders identify pending transactions and place one order right before the victims trade and one right after it. The attacker is able to buy the asset at a lower price than the victim and sell the same asset for a higher price. The name comes from the victim’s pending transaction stuck in the middle.

---

## Satoshi

A Satoshi refers to the smallest unit of the Bitcoin cryptocurrency 0.00000001 BTC. A *satoshi* is currently the smallest denomination of bitcoin. A bitcoin can be split into one hundred million units. Each of these units is called a *satoshi*. So, a satoshi = 0.00000001 BTC. Named after the creator of the Bitcoin protocol Satoshi Nakamoto.

---

## Satoshi Nakamoto

Satoshi Nakamoto is an individual or entity who created the Bitcoin protocol having successfully solved the digital currency issue of the 'double spend'. Nakamoto first published his paper describing the project in 2008 and the first bitcoin software was released one year later.

---

## Scalability

Scalability is the change in the size or scale to handle the 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. It is the capability of a network to function when the number of actors increases significantly.

---

## Scarcity

Scarcity refers to all cryptocurrencies that contain an algorithmically enforced limit on the number of coins. This is different from traditional commodity and currency assets, in which either more commodities can be created (such as in gold mining) or more currency can be printed (fiat). Thus Bitcoin has a different (and stronger) form of scarcity than traditionally scarce assets.

---

## **Script**

Script is an alternative proof of work system, or algorithm to SHA-256, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC miners. Script is the POW used by Litecoin.

---

## **Secure Hash Algorithm (SHA)**

SHA is the cryptographic hashing function designed by the US National Security Agency.

---

## **Securities and Exchange Commission (SEC)**

The SEC is the US federal agency responsible for the regulation of securities.

---

## **Security Token Offering (STO)**

An STO is a token offering of tokens that are classified as a security.

---

## **Seed Phrase**

The seed phrase is used in the restoration of a lost wallet by using a random series of words.

---

## Seed Plate

The Seed Plate is typically a small metal sheet where people can engrave seed phrases onto to enable permanence and for safe keeping.

---

## Segregated Witness, or SegWit

Each transaction recorded on a blockchain has a signature that proves it is a valid transaction. How many can fit into each block depends on the maximum defined size of the block. Segregated Witness was one of many soft-fork upgrades to the Bitcoin network, and it altered the format of transactions. It moved some transaction data (*witness data*—signatures and scripts) outside of the main block, mainly in an effort to fix a technical deficiency called *transaction malleability*. By moving some data out of the main block, SegWit had the side benefit that it increased the effective block size of Bitcoin by up to 3.5 times, depending on uptake of the feature by users. As of October 2018, approximately 50% of the transactions on Bitcoin are using the SegWit transaction format.

---

## Self-Sovereign Identity (SSI)

SSI is an identity that is owned only by the user, typically built on a decentralized system that doesn't involve any third-party.

---

## Semi-Fungible Token (SFT)

Semi-Fungible Tokens (SFT) have a completely different use than NFTs. They are intended to be a widespread consumer product like cinema or concert tickets and is not the asset itself that is the value, but the series that presents unique characteristics.

---

## SHA 256

SHA 256 is the cryptographic function (with 256-bit digest) used as the basis for bitcoin's proof of work system.

---

## Sharding

Sharding is a way of partitioning to spread out the computational and storage workload across a P2P network so that each node isn't responsible for processing the entire network's transactional load. Instead, each node only maintains information related to its partition, or shard. Sharding is the making of a partition of a database from larger databases into smaller ones.

---

## Shill

To shill is to promote an NFT that you own, under possibly suspect reasons, a person that has a hidden motive to "sell".

---

## Shiller

A person who "shills" (see also *Shill*)

---

## Shitcoin

A shitcoin is an alt coin with minimal or no value.

---



## **Short**

Short means borrowing from an exchange to sell for profit with the expectation that price will go down.

---

## **Sidechain**

A sidechain is a blockchain that is linked to a main blockchain that performs certain tasks.

---

## **Cryptographic Signature**

A cryptographic signature is a mathematical mechanism that allows someone to prove ownership. In the case of Bitcoin, a Bitcoin wallet and its private key(s) are linked by some mathematical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

---

## **Simple Agreement for Future Tokens (SAFT)**

SAFT Agreements designed for investors to purchase tokens from a blockchain startup instead of equity.

---

## **Simplified Payment Verification (SPV)**

SPV is the process of verifying that a transaction is included in the Bitcoin blockchain without downloading the entire blockchain.

---

## **Singleton**

A singleton is a non-subdividable whole token with a quantity of 1. Generally used to represent digital or physical items where there will be a single owner. A singleton implies non-subdividable, so the decimal value for the base token should be 0 and a total Quantity be 1, both are established upon creation. This singleton is non-transferable and attestable.

---

## **Slippage**

Slippage is the difference between the expected price of a trade and the price when the order actually executes.

---

## **Smart Contract**

Smart contracts are scripts for business automation that execute when certain contractual conditions are met. Blockchain-based smart contracts are proposed contracts that can be partially or fully executed or enforced without human interaction. Smart contracts are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.

A self-executing contract with the terms directly written into lines of code, which exist across a blockchain network. The code controls the execution, and transactions are trackable and irreversible. Smart contracts allow transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

---

## **Soft Fork**

Soft fork is a rule change that creates blocks recognized as valid by the old software but not the new that can result in a potential divide in the blockchain as the old software generates blocks seen as invalid according to the new rules. A soft fork can be viewed as a backward-compatible software update for a digital asset blockchain. Soft forks can refine the governance rules and functions of a digital asset blockchain but, unlike hard forks, are compatible with the previous blockchain. This means that a soft fork does not result in a split of the blockchain into two digital assets. For a soft fork to be implemented, a specific level of readiness to enforce the new rules must be signaled by miners. Soft forks are optional for all users in the system, and it is not necessary for users to immediately upgrade, unless they want to use the new features. This kind of fork requires only a majority of the miners upgrading to enforce the new rules.

---

## **Solidity**

Solidity is the programming language developers use to write smart contracts on the Ethereum network. Solidity is the smart contract programming language built for the Ethereum Virtual Machine for implementing smart contracts on the Ethereum blockchain.

---

## **Soulbound token (SBTs)**

Soulbound Tokens (SBTs) were proposed in May 2022 by economist & social technologist E. Glen Weyl, lawyer Puja Ohlhaver, and Ethereum creator Vitalik Buterin. SBTs are a foundational building block, in an emerging Web3 trend known as the Decentralized Society (DeSoc) and were created to augment Web3's trajectory toward hyper-financialization to something more inclusive, democratic, and decentralized.

---

## Spot Market

A spot market is where financial instruments are exchanged for immediate delivery, such as commodities, currencies, and securities. Delivery, here, means cash exchange for a financial tool. In comparison, a futures contract is based on the delivery of the underlying asset at a future date.

---

## Stablecoin

A stablecoin is a type of cryptocurrency that's backed by a stable asset such as gold or traditional fiat currency, known as pegging. Blockchain is also being used to digitize other assets, such as cars, real estate and even artwork. Stablecoin is any cryptocurrency pegged to a stable asset, like fiat or gold. It theoretically remains stable in price as it is measured against a known amount of assets not subject to change.

A token with its value pegged to another asset. Stablecoins are usually backed by a fiat currency, like the U.S. dollar. It can also be pegged to physical assets like precious metals, or even other cryptocurrencies like bitcoin.

---

## Staking

Staking is the process of actively participating in transaction validation (similar to mining) on a proof-of-stake (PoS) blockchain. On these blockchains, anyone with a minimum-required balance of a specific cryptocurrency can validate transactions and earn Staking rewards. If anyone knows more about this or how I might use my new computer as a node for any type of crypto validation, I'm interested to learn.

---

## **State Channel**

State channel is a process where blockchain transactions are executed off chain and then written to the main blockchain as a single transaction.

---

## **State Machine**

A state machine is a model of computation.

---

## **Stream Ciphers**

Stream Ciphers is a method of encrypting text where a cryptographic key and algorithm are applied to each binary digit in a data stream one bit at a time.

---

## **Store of Value**

Store of Value is one of the core functions of money, alongside Medium of Exchange and Unit of Account. An asset is considered to be a good Store of Value if the purchasing power does not degrade over time.

---

## **Sweep**

“Sweep (the floor)” means to buy all of the NFTs in a collection at the floor price.

---

## **Swing**

Swing is the movement of price that goes upward and downward

---

## **TA**

TA stands for Technical Analysis

---

## **Tangle**

Tangle is the consensus mechanism in which transactions must confirm the validity of at least two prior transactions.

---

## **Taxonomy**

Taxonomy is the process or system of describing the way in which different things are related by putting them in groups. A token taxonomy describes how digital tokens relate to each other based on their artifacts.

---

## **Testnet**

Testnet is an alternative blockchain developers use to test applications. It is where an application is staged for testing before it goes onto the mainnet.

---

## **Token**

A Token represents an asset built on an existing blockchain (different from a coin). A token is a unit of value that can be acquired through the blockchain. A token is, very simply, a piece of data that stands in for another, more valuable piece of information. Tokens have virtually no value on their own - they are only useful because they represent something bigger.

Unlike a coin, a token is a digital asset created on an existing blockchain. Tokens can be used to represent digital and physical assets, or used to interact with dApps.

---

### **Token (Non Fungible)(NFT)**

An NFT token is a token used to represent unique goods such as artwork or cards.

---

### **Token (Security)**

A security token is a token that represents a share of the company.

---

### **Token (Stable)**

A stable token is a token that has a relative fixed value in relation to another currency.

---

### **Token (Utility)**

A utility token is a token with a utility besides value.

---

## **Token Generation Event**

The Token Generation Event (TGE) is the first sale of a token and another word for Initial Coin Offering.

---

## **Tokenization**

Tokenization is the process of turning property, real property and other assets into tokens. The process of turning something with value into a unique representation of that value. Tokenization is the process of removing sensitive data from your business systems by replacing it with an undecipherable token and storing the original data in a secure cloud data vault. Encrypted numbers can be decrypted with the appropriate key. Tokens, however, cannot be reversed, because there is no mathematical relationship between the token and its original number.

---

## **Tokenomics**

Tokenomics is tokens + economics and is the token structure, management and distribution.

---

## **Tokenless Ledger**

A tokenless ledger refers to a distributed ledger that doesn't require a native currency to operate. It's a ledger that does not require a token to function.

---



## **Total Circulating Coin Supply**

Total circulating coin supply is the total number of coins that a particular digital asset has in circulation.

---

## **Total Coin Supply**

Total coin supply is the total number of coins that have been minted for a particular digital asset, although not all coins minted may be in circulation. It can also mean the total number of coins that will ever exist, as in 21 million for Bitcoin.

---

## **Total Value Locked (TVL)**

Total Value Locked is the total amount of digital assets being staked in a specific blockchain project and/or DeFi

---

## **Transaction**

A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. A transaction is also an input into a blockchain to transfer cryptocurrencies, execute smart contracts or perform another function.

---

## **Transactions as Proof of Stake (TaPoS)**

TaPoS is a technique for securing a network by preventing transactions from being applied to forks other than the one seen by the user at the time of signing the transaction. This protects a network against long-range reorganizations and protects the user from signing a transaction based upon a false view of the world. With TaPoS it is possible for centralized entities to operate a blockchain while ensuring that the chain cannot be reorganized without all other users updating their signatures. TaPoS works by incorporating a small amount of data from a recent block ID into the transaction so that any change to the blockchain invalidates the transaction.

---

## **Transaction Block**

Transaction block is the collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain.

---

## **Transaction Fee**

A transaction fee is a small fee imposed on some transactions sent across the bitcoin network, charged by the miner to conduct the transaction. The transaction fee is awarded to the miner that successfully hashes the block containing the relevant transaction. In Bitcoin, a transaction fee is not mandatory, nor is it prescribed by the code. Users can choose how much to pay for their transactions to be processed. That is why during times of network congestion, the average transaction fee goes up, as users are trying to incentivize miners to process their transactions over other users' transactions. On the other hand, when network traffic slows down, average transaction fees also decline.

---

## **Transactions Per Second (TPS)**

TPS is the measurement of speed of blockchain.

---

## **Transaction Pool**

Transaction pool is the list of all transactions in a network that has not been included in a block.

---

## **Transparency**

Transparency is a characteristic of a public blockchain where a transaction can be seen publicly.

---

## **Trust**

Trust means confidence in the integrity of an entity.

---

## **Trustless**

Trustless means that Trust that is built into a system with digital signatures, cryptography, consensus and verification so trust between two entities is trivialized and/or eliminated.

---

## **TS**

Means “Twitter Space”, a Twitter audio community application similar to Clubhouse.

---

## **TTM**

Means “to the moon” and is associated with the potential for amazing gain.

---

## **Turing Complete**

Turing complete is any machine that can calculate on a level equal to a programmable computer is Turing Complete or computationally universal. It is the ability of a programming language to simulate a Turing machine.

---

## **Turing Machine**

Turing machine is the ability of a machine to perform any algorithm that can be done by a computer.

---

## **uBTC**

uBTC is one millionth of a bitcoin, or 0.000001 BTC. It is also called microbitcoin.

---

## **uNFT**

uNFTs are “utility” NFTs. This term emerged in 2021 with a "classification guide" provided by Ron Jaradat of Liquiditeam and currently includes the subcategories of: gaming/Metaverse, gaming/items, fashion/luxury goods, Fine Art/Blue Chip Fractionalisation, gambling/sports, new idea, PFP, identity, ownership-based governance, ticket/token gates, DeFi, investment, science/research fundraising, wearable/brand marketing, music, gallery curation, food, arts (open, curated, traditional), and land (IRL, or virtual).

---

## **URI**

A Uniform Resource Identifier is a unique sequence of characters that identifies the location of an asset stored on a network.

---

## **Utility**

Means the non-monetary perks of an NFT, such as IRL events or merchandise, voting rights, or airdropped assets. Not all NFTs have utility.

---

## **Unpermissioned Ledgers**

Unpermissioned ledgers such as Bitcoin have no single owner — indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates censorship resistance, which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state

---

## **Unspent Transaction Output**

Unspent transaction output is the amount of cryptocurrency left remaining after a transaction is executed so that any unspent outputs are deposited back into a database as inputs when a transaction is completed. Bitcoin does not operate on the account model (like Ethereum) but on the unspent transaction output (UTXO) model. Every transaction has inputs and outputs. Outputs that have not been spent are the set of bitcoins in circulation (i.e., spendable bitcoins). Unspent outputs are used as inputs in new transactions.

---

## **Validator**

A Validator is a blockchain node that has permission to process transactions and create new blocks.

---

## **Vapourware**

Vapourware refers to a project that is never implemented.

---

## **Virtual Currency**

See Digital Asset

---

## **Virtual Machine**

A virtual machine refers to a computer operating system that runs parallel to another operating system.

---

## Virtual Reality (VR)

An immersive, computer-generated 3rd space usually accessed by a VR headset.

---

## Vyper

Vyper is a programming language for the Ethereum blockchain used to create smart contracts built for security and auditability.

---

## WAGMI

Means “we are going to make it” and is used to indicate a strong conviction or optimism for a successful outcome. (see also *NGMI*)

---

## Wallet (Crypto)

Wallet is a designated storage location for digital assets (cryptocurrency) that has an address used for sending and receiving funds to and from the wallet. The wallet can be online, offline, or on a physical device. A digital asset wallet is a piece of software that maintains keys and manages addresses. A wallet consists of a set of addresses. If the wallet has the private keys for these addresses, it is capable of sending transactions. If it does not have the private keys for these addresses, it is called a *watch-only wallet*, as might be used by an auditor.

A software application or hardware device used to store the private keys to blockchain assets and accounts. Unlike a traditional wallet, a blockchain wallet does not actually store the coins or tokens themselves. Instead, they store the private key that proves ownership of a given digital asset i.e. Metamask, Coinbase, Ledger, Trezor.

---

**Wallet (Cold)**

A wallet that is not connected to the Internet.

---

**Wallet (Warm)**

A wallet that is sometimes connected to the Internet.

---

**Wallet (Hot)**

A wallet that is connected to the Internet.

---

**Wallet (Multisignature)**

A wallet that requires multiple digital private key signatures to execute a transaction.

---

**Web1**

Was approximately 1990-2005. The first iteration of the web, commonly referred to as the “read-only” web. Static websites that displayed information. Little to no user interaction or user-generated content. The early internet used open protocols and was decentralized. Most of the value went to users and builders.

---



## **Web2**

Web2 refers to the version of the internet most of us know today. An internet that is dominated by companies that provide services in exchange for your personal data.

---

## **Web3**

Web3 in the context of Ethereum, refers to the decentralized apps that run on the blockchain. These are apps that allow anyone to participate without monetising their personal data. Some limitations include scalability (decentralization slows down transactions), user experience (it takes a lot of extra steps/software to interact with it), accessibility (it's not yet integrated in modern web browsers), and the cost (it's expensive to put anything on the blockchain). Benefits, mainly due to decentralization, include:

- Anyone on the network has permission to use the service. Service is permissionless.
  - No one can block you or deny you access to the service.
  - Payments are built in via ether (ETH).
  - Ethereum is turing-complete, which means that anything can be programmed on it.
- 

## **Web Assembly (WASM)**

WASM is a binary instruction format for a virtual machine.

---

## Whale

A whale is someone who owns a large number of coins that can manipulate price.

---

## Wen

Means “when” in NFT culture. (see also *wen moon*)

---

## Wen Moon

A common expression referring to the price of your NFT ascending to the moon, often accompanied by a rocket ship emoji. (see also *Wen*)

---

## Whitepaper

A whitepaper is an authoritative report or proposal that is used in the web 3.0 community as an integral marketing tool to attract investors, educate the public about the project, and present to venture capital firms. Almost every ICO or ITO has a whitepaper on their website that is essentially an informative sales pitch.

---

## White list

A private list generated by NFT projects and communities that usually grants early access to NFT drops through pre-approved crypto wallet holders, and normally subject to specific criteria. (see also *Pre-Sale*)

---

## **xBT**

xBT is another way to abbreviate or shorthand Bitcoin. While BTC was and often still is the original shorthand for *bitcoin*, there has been an increase in the use of the term XBT. The reason for this is that the International Organization for Standardization (ISO), which keeps a listing of all currencies, uses X to symbolize a currency that is not attached to a specific country (which is the case for all digital assets, because they are decentralized). Fidelity Digital Assets uses the XBT currency code.

---

## **XRP**

Formerly known as Ripple, XRP is the native cryptocurrency for the Ripple distributed ledger payment network. XRP acts as a bridge currency to other currencies. Ripple operates on an open source and peer-to-peer decentralized platform that allows for a seamless transfer of money in any form, whether fiat or cryptocurrency.

---

## **Yield**

Yield refers to earnings generated on an investment over a particular period of time, usually as a percentage based on the invested amount, current market value or face value of the investment including any interest or dividends.

---

## **Yield Farming**

Yield farming means to provide liquidity to a DeFi protocol to earn a portion of protocol revenue share, and a governance token which is then sold for additional profit (or yield).

---

## **Zeppelin/Open Zeppelin**

Zeppelin is a community of Smart Contract developers and battle-tested libraries of smart contracts for Ethereum and other blockchains

---

## **Zero Knowledge Proof**

Zero Knowledge Proofs (ZKPs) are an experimental technology that allows one to cryptographically prove a statement, without revealing the input data. For instance, one could prove that a transaction was included in the blockchain without telling you which transaction it is. One could also prove the ability to decrypt encrypted data, or the ability to spend from a certain address, or prove the amount of funds in your wallet without revealing any addresses (for instance, to satisfy an audit). ZKPs are being actively explored by a number of blockchain and cryptocurrency projects and are a fundamental piece of engineering infrastructure in the space. Zero knowledge proofs are an assertion to prove that a transaction is valid without having to reveal transaction details such as transaction amount, sender or recipient.

# Sources

- <https://www.blockchaintechnologies.com/glossary/>
- <https://blockgeeks.com/guides/blockchain-glossary-from-a-z/>
- <https://www.fidelitydigitalassets.com/digital-asset-basics>
- <https://medium.com/@michelletsng/a-glossary-of-blockchain-defi-terms-7308e48aab18>
- <https://hackernoon.com/blockchain-dictionary-f4d098c9ef89>
- Vocabulary: <https://bitcoin.org/en/vocabulary#address>
- <https://www.investopedia.com>
- <https://en.wikipedia.org>
- <https://coinmarketcap.com/alexandria/glossary>
- <https://consensus.net/knowledge-base/a-blockchain-glossary-for-beginners/>
- <https://a16z.com/2019/11/08/crypto-glossary/>
- <https://www.coingecko.com/en/glossary>
- Blockchain Definitions: <https://101blockchains.com/blockchain-definitions/>
- <https://cryptonews.com/exclusives/on-chain-analysis-data-providers-who-are-they-and-what-do-th-6962.htm>
- <https://medium.com/interdax/how-chain-analysis-helps-cryptocurrency-traders-dd4de03f823>
- <https://shemesh.larc.nasa.gov/fm/papers/Malekpour-2006-tm214322.pdf>
- <https://hedera.com/learning/what-is-asynchronous-byzantine-fault-tolerance-abft>
- <https://interwork.org/wp-content/uploads/2020/07/License-Diploma-spec.pdf>
- <https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp506.pdf?9024621c5b9f7d562ae3c657e40e013f>
- <https://dolomite-war-106.notion.site/Web3-Glossary-9ae15514178443dc98c1f9312bd2741b>
- <https://ethereum.org/en/developers/docs/web2-vs-web3/>

# Contributors

Name	Company	Email
Jasper Weed	Intern at Yellow Umbrella Ventures	
Arry Yu		
Dae Yu		
Adam Norris	Coding Dojo	
Elsa Velazquez	NA	
Michelle Tsng		
Jordan Odinsky		
"Tesa Ho"		
Paul Rapino	<a href="#">InterWork Alliance</a>	Paul.Rapino@Interwork.org
Ray Monner	Annie Stacks	
Kaliya IdentityWoman Young		
Alex Wick	Cascadia Carbon	
Maha Saad		

Luiz Lemos	Inovar.Tech	luiz.lemos@inovar.tech
Adam Laska		
Vikas Pandey	DevopsInternational B.V.	<a href="mailto:vikpande@devopsinternational.nl">vikpande@devopsinternational.nl</a>
Bella Irons	Academic Web3 Conference	Bella@academicNFTconference.com
Brook Riggio	Cofounder, Code Fellows	
Steve Cherewaty		
Dick Hardt	CEO, Hello.coop	