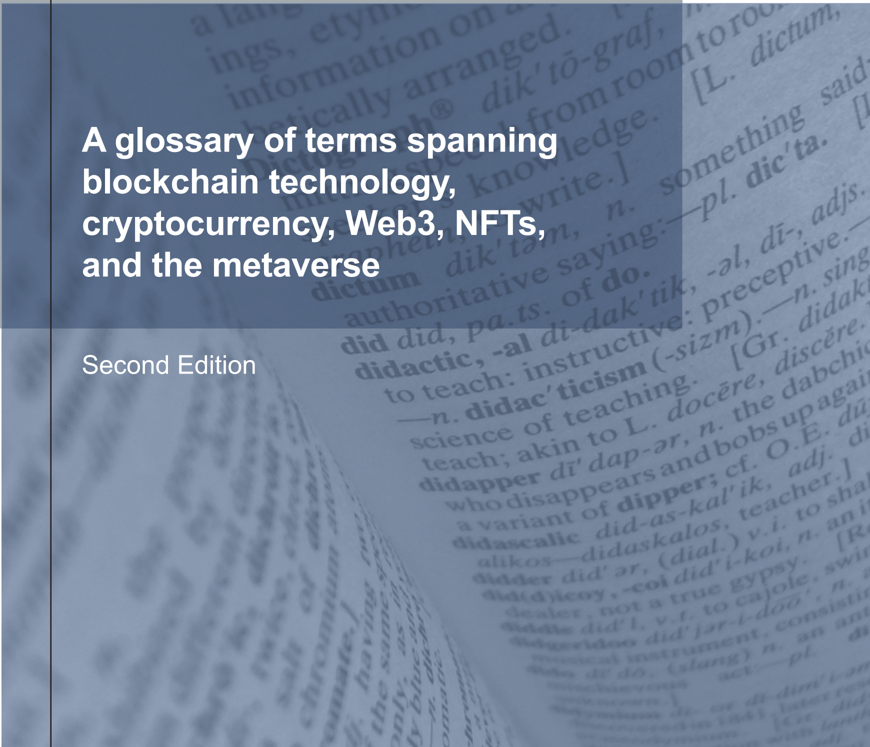
LATHAM & WATKINS LLP

The BOOK *of* JARGON®

Blockchain, Crypto & Web3



A glossary of terms spanning blockchain technology, cryptocurrency, Web3, NFTs, and the metaverse

Second Edition

The Book of Jargon® — Blockchain, Crypto & Web3 is one in a series of practice area-specific glossaries published by Latham & Watkins. The definitions provide an introduction to each term and may raise complex legal issues on which specific legal advice is required. The terms are also subject to change as applicable laws and customary practice evolve. The information contained herein is not legal advice and should not be construed as such. If you have questions about the terms or suggestions for additional terms, please email fintechglossary@lw.com.

2FA: acronym for Two-Factor Authentication.

51% Attack: when one or more persons collectively control more than 50% of a network's computing power and maliciously use their Hashing Power to reverse Confirmed Transactions, interfere with the process of recording new Blocks, prevent new transactions from gaining Consensus, allow Double Spending of the local currency, or take other actions to undermine the integrity of a Blockchain.

Accidental Fork: typically occurs when two or more Miners discover a Block at almost the same time, Forking the chain. Thanks to Consensus, Accidental Forks are usually quickly identified and resolved (i.e., one chain becomes longer than the other, and the network eventually abandons the Blocks that are not in the longer chain).

Account Tree: a core component of the "Mini-Blockchain" scheme that was proposed by J.D. Bruce in order to solve the Blockchain Scalability problem. An Account Tree is a self-contained balance sheet that acts as a database for all non-empty Addresses. The arboreal component of this term's name comes from the Hash tree structure of the database.

Address: a unique identifier of alphanumeric characters that represents a virtual destination for accepting and sending a Blockchain transaction.

Administrator: "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency." The Administrator is considered to be an MSB (in the absence of an applicable exemption) if the Virtual Currency in question is Convertible Virtual Currency.

Reference: FinCEN, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (March 18, 2013).

Agreement Ledger: a Distributed Ledger used by two or more parties to negotiate and reach an agreement.

Airdrop: a giveaway of Tokens to the Wallets (Software) of users, typically for marketing purposes and increasing awareness of a particular Cryptocurrency. Airdrops are usually either free or occur in return for the user's efforts to generate publicity, such as subscribing, posting, or sharing information about the Cryptocurrency on social media. Airdrops are basically the crypto-equivalent of Oprah's famous giveaway moment: "You get some Coins! You get some Coins! Everybody gets some Coins!"

Algorithm: a system for solving a specific class of problems. Algorithms are the step-by-step instructions given to a computer in order to produce a desired outcome. In the Cryptocurrency world, each Consensus model follows a certain Algorithm.

All Time High (ATH): the highest historical price reached by an investment product.

In contrast, see All Time Low.

All Time Low (ATL): the lowest price for a given Cryptocurrency since inception / first listing on a market or Exchange.

In contrast, see All Time High.

Altcoin: short for “alternative coin,” Altcoin initially referred to any Cryptocurrency other than Bitcoin, though more recently it has been used to refer to any Cryptocurrency other than the group of the most popular Cryptocurrencies, which includes Bitcoin and Ether.

Alternative History Attack: an attack in which a person submits for Consensus a transaction to pay a seller while simultaneously Mining a Fork of the same Blockchain that includes a transaction returning the payment to the attacker. The seller in this case will not receive the payment if the length of the chain on which the transaction is confirmed is shorter than the alternative chain released by the attacker.

Alternative Trading System (ATS): a trading Platform with fewer regulations than a national securities Exchange. ATSs aim to find counterparties for transactions, while also providing enhanced privacy. Large trade orders listed through an ATS are not reported on national Exchange order books. For this reason, ATSs are sometimes referred to as “dark pools.”

AML: acronym for Anti-Money Laundering.

AML Officer: the designated person responsible for managing an entity’s AML Program and ensuring compliance with the AML Program and the BSA, and, often, training other employees on their obligations under the BSA. The AML Officer can be held personally liable for failure to comply with the obligations of the role. Every entity subject to the requirements of the BSA and its implementing regulations must have an AML Officer (also known as a BSA Officer).

AML Program: the policies and procedures that must be developed, implemented, and maintained by entities subject to the BSA to ensure compliance with the BSA and its implementing regulations. An AML Program must be appropriately tailored to the entity’s business model and risk profile.

Anchor: essentially a Blockchain-based signature that can be put into codes or physical products and cannot be removed or changed; verification of the Anchor is synonymous with verification of the authenticity of the product. An Anchor can be a microchip or an optical code, and can be used to reduce counterfeit goods or trace stolen goods.

Announcement (ANN): a term often used in online forums to refer to communications of a new ICO or new product or service.

Anonymity: something made or done by an unknown person or group (i.e., no username is associated with the action).

Anti-Money Laundering (AML): a set of laws and regulations designed to ensure that financial services companies do not aid in criminal and/or terrorist enterprises, aka the rules in place to deter the next Breaking Bad car wash. Efforts to combat money laundering and terrorism finance include KYC requirements, Suspicious Activity Reports, and Currency Transaction Reports, all of which require financial institutions to investigate and report any customers or transactions that could be furthering a criminal enterprise. AML obligations can be burdensome, but failure to comply can result in heavy criminal and civil penalties. Global AML obligations differ by jurisdiction.

Application Program Interface (API): software code that enables communication between independent systems, such as computer programs and applications, in the form of a request-response message. For example, travel aggregators submit flight date, departure location, and destination through the APIs of airlines' websites and receive prices for flights meeting those specifications in response.

Application-Specific Integrated Circuit (ASIC): a computer chip specifically designed to do one task, as opposed to general-purpose hardware such as CPUs. For example, Bitcoin ASIC Miners are designed to be more efficient in Mining Bitcoin than standard laptops or desktop computers.

ASICs are one of three main types of hardware that can be used for Mining Cryptocurrency, alongside CPUs and GPUs, and are generally the most efficient type due to greater computing capacity and reduced electricity consumption, which results in a higher chance of earning rewards and lower operating costs.

Arbitrage: the trading of an Asset in order to take advantage of price discrepancies for the Asset, such as when the Asset is trading on different markets or Exchanges.

Artificial Intelligence (AI): a branch of computer science concerned with building smart machines capable of performing actions or tasks commonly associated with intelligent beings. The digital voice assistants on mobile phones and home devices are commonly used applications of AI. The most famous AI in fiction is HAL 9000 in the 1968 film 2001: A Space Odyssey, in which HAL (Heuristically programmed Algorithmic computer) systematically kills the crew of the Discovery One spaceship.

Ashdraked: to lose all funds in an investment; specifically, when shorting Bitcoin. The term originated when a trader, Lord Ashdrake, lost all funds shorting Bitcoin in 2014-2015.

Asset: an item, object, or thing of value, whether tangible or intangible, that can be transferred from one person or location to another person or location.

Asset Token: a category of Tokens that represent a "real world" asset or product — such as a Commodity (e.g., gold, diamonds, oil) or Currency — as opposed to Utility Tokens, which provide the holder with access to or the ability to do something on a relevant network. An Asset Token is also known as an Asset-Backed Token.

Asymmetric-Key Cryptography: an Encryption technique that uses a Public Key and a Private Key, either of which can be used to encrypt or decrypt data. Asymmetric-Key Cryptography can be used in the following ways:

Scenario 1: The intention is to ensure only Andy can read messages from Bertha and Charlie, since they trust him. Bertha and Charlie each use a Public Key (which is known to everyone) to encrypt their messages before sending them to Andy. Andy uses a Private Key (which is known only to himself) to decrypt the messages. Bertha and Charlie are assured that their messages are secured, since only the Private Key can decrypt their messages, and only Andy holds the Private Key.

Scenario 2: The intention is to ensure only Andy can send messages to Bertha and Charlie, since they trust him. This time, Andy uses the Private Key to encrypt his messages before sending them to Bertha and Charlie. Bertha and Charlie use the Public Key to decrypt the messages. Bertha and Charlie are assured that it is Andy who is the sender, since only the Private Key can encrypt such messages, and only Andy holds the Private Key.

Asymmetric-Key Cryptography is also known as Public-Key Cryptography. Contrast this technique with Symmetric-Key Cryptography, in which the same key is used to both encrypt and decrypt data.

And you thought your anti-virus software was complicated …

Astroturfing: the process by which sponsors of a Cryptocurrency (or others who are financially interested in its success) falsely portray positive messages relating to that Cryptocurrency in a way that makes it appear as if such messages originated from grassroots participants in the Cryptocurrency market. This is usually done to generate buzz or hype around a Cryptocurrency.

The term is derived from AstroTurf, a brand of artificial grass, as a play on the word “grassroots” — the implication being that instead of organic grassroots support for the Cryptocurrency, there is an artificial appearance of support.

See also Shilling.

Atomic Swap: a Smart Contract that enables the simultaneous P2P exchange of one Digital Asset for another without using a Centralized Exchange, which can occur Off-Chain or Cross-Chain.

Attestation Ledger: the little black book of Cryptocurrency that is distributed among all participants of a network, providing evidence of every individual transaction, agreement, commitment, and statement that takes place.

Augmented Reality (AR): an immersive experience created by integrating computer-generated virtual objects or sensory stimuli into the user’s real-world environment. Also known as mixed reality and computer-mediated reality. In contrast, see Virtual Reality.

In contrast, see Virtual Reality.

See also Spatial Computing.

Automated Market Maker: the Protocol underlying most DeFi Exchanges, which utilize Liquidity Pools to facilitate trades requested by buyers and sellers without having to wait for a match.

Avatar: a digital icon or figure representing a particular person on a Web2 or Web3 platform, with the simplest iteration being the ubiquitous profile picture.

B2B: acronym for “business to business” transactions, which don’t involve consumers or individuals. B2B transactions often occur in the supply chain (e.g., a retailer purchasing mining equipment from a wholesaler).

B2C: acronym for “business to consumer” transactions. B2C transactions often occur in retail settings (e.g., a consumer purchasing mining equipment from a retailer).

Bag: a slang term for the Tokens or Coins in a person's portfolio. While Bags can vary in size, usually someone will refer to their holdings as a Bag only when they are holding a large amount of Cryptocurrency, usually of one type.

Bagholder: a person who keeps their Bag even when market forces indicate that some Tokens or Coins should be sold.

See also HODL.

Balance Attack: an attack against POW Consensus model methods in which a person splits Miners into two groups with equal Mining power (Group A and Group B), and then submits a transaction to only the Nodes associated with Group A (e.g., a transaction in which the attacker spent Coins) while Mining a different transaction (e.g., a transaction in which the attacker received Coins) alongside Group B. When the two groups attempt to reconcile the transactions, Group B will theoretically have a longer chain that will receive Consensus and be added to the main Blockchain. As a result, the attacker's account will not register the Coins that were spent, regardless of whether the attacker received products or services as a result.

Bandwidth: the maximum amount of data that can be transmitted across a path in a fixed period of time.

Bank Secrecy Act (BSA): a US law, originally passed in 1970 and amended multiple times over the years, most extensively by the USA PATRIOT Act of 2001, requiring financial institutions to aid the US government in detecting money laundering and terrorism finance. Despite its name, the BSA applies to more than just banks: casinos, MSBs, Broker-Dealers, commodities brokers, and more all must comply with certain obligations. The BSA is enforced by FinCEN.

Bear: a large mammal with thick fur and a short tail. Also an investor who is pessimistic about the state of the market for a given Cryptocurrency. Just as the mammal will often forage for seeds and grubs in the forest, a Bear will attempt to make profits from falling Cryptocurrency prices.

In contrast, see Bull.

Bearwhale: a not entirely mythical creature, the Bearwhale owns a considerable portion of any given Cryptocurrency and believes prices will fall.

Bear Trap: a situation in which the price of a Cryptocurrency goes down rapidly before sharply rising back up, "trapping" Bearish speculators who sold their position.

In contrast, see Bull Trap.

Bit: a sub-unit of value equivalent to one micro-bitcoin, or one-millionth of a bitcoin.

Bitcoin/bitcoin: the OG Cryptocurrency, Bitcoin is the most popular and highest-traded Cryptocurrency by volume. It was introduced by Satoshi Nakamoto as the first Open Source software providing a Decentralized Network and Protocol that uses Cryptography and other processes to regulate its creation and the verification of transactions.

bitcoin (lowercase): often used when referring to the term as a unit of measure (e.g., Alice sent Bon two bitcoins).

Bitcoin Improvement Proposal (BIP): a proposal to the Bitcoin community to improve the Protocol. Usually, someone (anyone, no credentials required) submits a draft to the Bitcoin community, and others can provide comments and edits; the author then may revise the BIP accordingly. If the community does not provide enough support for the BIP, the author may withdraw it – or the community may reject it. If there is consensus, the BIP will be adopted by the Bitcoin community. That said, the adoption of a BIP does not mandate any changes — Bitcoin community developers can choose to implement the BIP or ignore it.

Bitcoin Standard Transaction Type: the current transactions that can be performed and completed on the Bitcoin Blockchain. Although many transaction types can be represented in the scripting language (the computer code that gives instructions with each transaction), only a limited number of Bitcoin Standard Transaction Types are accepted by the Bitcoin network and Miners.

Bitcoin Transaction Locktime: the earliest time at which a Miner may include a particular transaction in the Miner's Merkle Root for inclusion on the main Blockchain. Bitcoin Transaction Locktime may be tied to a Block Height or specified as a date and time.

BitLicense: a state license issued by the NYSDFS that is generally required for any person or entity that wishes to engage in certain Cryptocurrency-related activities in the State of New York or with residents of the State of New York.

Reference: 23 N.Y. Comp. Codes R. & Regs. §§ 200.1 *et seq*.

Block: files in which data pertaining to a Cryptocurrency network is permanently recorded. A Block functions like a discrete entry in a ledger to permanently store records of transactions which, once written, cannot be altered or removed. Every time a Block is completed, a new Block is formed in the Blockchain.

Block Data: a component of a Block that contains a list of validated and authentic transactions. Whenever a Node publishes a Block, the Block contains a Block Header and Block Data.

Block Explorer: short for “Blockchain explorer,” a Block Explorer is a web-based tool that allows an individual to search for information on a Blockchain. Although functionality varies among the different Block Explorers, typically they allow searches relating to the Blocks that exist within a particular Blockchain (e.g., the creation date and size of a Block, or the transactions and corresponding Addresses contained within such Block), as well as specific transaction identification numbers and Addresses.

Block Header: Metadata included in every Block that provides a summary of the data in the Block. A Block Header typically includes information about the version of the Block, the Hash Digest of the previous Block (although this will not be present in the Block Header of the first Block of a Blockchain), a summary of all the transactions in the Block (the Merkle Root), a time stamp, the Bit field, and the Nonce of the Block.

Block Height: with respect to a Block on a Distributed Ledger, the number of Blocks preceding the Block in question — i.e., the number of Blocks between that Block and the Genesis Block (which always has a Block Height of zero) — on the relevant Blockchain.

Block Reward: the Cryptocurrency awarded by a Blockchain network to eligible Miners for each Block they Mine successfully. Better than a hand-knitted Christmas sweater.

Block Time: the amount of time it takes to create a new Block in the Blockchain.

Block-Withholding Attack: a category of attacks that may undermine the integrity of a Blockchain by exploiting the financial incentives of POW Consensus models.

In one version of the attack, a malicious Miner will join multiple Mining Pools in order to receive a portion of the Block Reward earned by the “victim” pool for the malicious Miner’s partial POW, while secretly aiding the “loyal” Mining Pool to complete the Block and receive the full POW Block Reward.

In an alternative version, a malicious Miner will not publish a completed Block so that other Miners will work to Mine Blocks that will become Orphans while the malicious Miner has a head start on Mining the next Block and earning the Block Reward.

Blockchain: an Immutable digital Ledger that chronologically records computationally verified transactions or other data.

See also Blockchain 1.0, Blockchain 2.0, and Blockchain 3.0.

Blockchain 1.0: the first implementation of DLT, which verified and recorded Cryptocurrency transactions on a Blockchain.

See also Bitcoin.

Blockchain 2.0: the second implementation of DLT, which created exchangeable Non-Native Tokens and enabled Smart Contracts, which automatically execute predefined actions on a Blockchain upon the occurrence of predefined conditions.

See also Ethereum.

Blockchain 3.0: the third implementation of DLT, which introduced innovations intended to resolve Blockchain issues relating to Scalability, Interoperability, Governance, privacy, and sustainability with the intention that such enhancements enable DLT to become the technical architecture powering the digital economy and Internet of Things.

Blockchain Network User: a person (natural or otherwise) who uses a Blockchain network. Each transaction on a Blockchain network involves Blockchain Network Users.

Bollinger Band: a Technical Analysis tool developed and trademarked by its namesake, John Bollinger, in the 1980s. A Bollinger Band contains a set of trend lines typically plotted two standard deviations away from the simple moving average of an Asset's price. Investors often use the tool to infer when an Asset is Oversold (i.e., near or below the lower band) or Overbought (i.e., near or above the upper band).

Bot: automated software that is used to conduct trades and execute transactions on behalf of human investors. There are many types of Crypto trading Bots, which can be free or subscription-based.

Bounty: a reward, usually an amount of Cryptocurrency, given to a person in order to encourage certain behaviors or as a reward for performing certain tasks. For example, a Bounty might be awarded to a person for promoting a Cryptocurrency on social media or reporting to the network developer any bugs or other issues that are encountered when using a software platform.

See also Airdrop.

Bribery Attack: an attack in which a person creates a Fork by paying other Miners to work on the attacker’s chosen Blocks instead of the longest chain, allowing the attacker to carry out detrimental activities such as double spending.

See also Double Spend (Attack).

Broker-Dealer: a company that buys and sells securities (i) on a principal basis for its own account (a dealer) and/or (ii) on behalf of its customers (a broker). Unless otherwise exempt, a Broker-Dealer must register with the SEC pursuant to the Securities Exchange Act of 1934. Since many Tokens and Cryptocurrencies have been found to be Securities, more crypto-focused businesses have been required to register with the SEC and operate pursuant to the Exchange Act and its implementing regulations.

Brute Force Attack (BFA): an old yet still used attack method in which hackers attempt to crack a Private Key via multiple guess attempts until one works.

BSA: acronym for Bank Secrecy Act.

BTC: the Ticker symbol for Bitcoin.

Bubble: a surge in Asset prices unwarranted by the fundamentals of the Asset and driven by exuberant market behavior.

BUIDL: a misspelling of “build” that is used to urge Cryptocurrency users to focus on building and contributing to a specific Blockchain or Cryptocurrency project, rather than passively holding the Cryptocurrency.

See also HODL.

Bull: a male cow, typically with large horns and a reputation for a fierce disposition, with the exception of Ferdinand. The term also comes from traditional stock market concepts and refers to a person with optimism for future Cryptocurrency prices.

In contrast, see Bear.

Bull Run: a sustained and significant rise in the listed price of a Token, either singly or in the Cryptocurrency market in general, over a period of time, buoyed by market optimism and a positive outlook on the industry.

Bull Trap: in relation to a Cryptocurrency whose price has slumped, a pattern of price movements or other signals that convinces investors that a rally is underway. Sometimes also referred to as a “suckers’ rally.”

Investors who establish Long Positions in a given Cryptocurrency as a result of a Bull Trap may find themselves “trapped” when the market price falls again.

In contrast, see Bear Trap.

Burn: the destruction of one or more Coins or Tokens. Burning can be used as the proof component of a Consensus model, as a mechanism for the payment of dividends or Transaction Fees, or in the case of an ICO, as a way to eliminate any Coins or Tokens that are not sold to buyers by the end of the ICO (which also has the effect of limiting the total supply, and therefore potentially increasing the price of the Coin or Token).

Buy the Dip (BTD): the act of purchasing an Asset after a sharp price decline, with a belief that the Asset is undervalued.

Buy Wall: the result of one very large buy order or multiple large buy orders placed at the same price in the order book of a particular market, preventing the market price from dropping below the amount at which the buy orders were placed.

In contrast, see Sell Wall.

Byzantine Fault Tolerance: fault-tolerant Protocols used in the Consensus layer of Blockchain systems (e.g., POS and POW).

Byzantine Generals’ Problem: an issue of trust that underlies any system without a central, responsible authority. If there is a disagreement between people as to the past or present, and there is no arbiter of truth, how can the system work? Satoshi Nakamoto solved this issue for the Blockchain with Consensus (specifically, POW), which requires people to agree on a shared history and reality so that everyone can trust the transactions being conducted and stored.

In the hypothetical Byzantine Generals’ Problem described by computer scientist Leslie Lamport in 1982, a set of generals need to be coordinated in their attack in order to succeed, but are spread throughout a large area. Thus, they need to rely on messengers to share information between the various armies. But can they rely on the messengers — or on each other? The uncertainty ensures that the military campaign — or system — is at risk.

Candlestick: a graphing technique used to display the price movement of an Asset. Each Candlestick’s shape varies based on the high, low, open, and closing prices of an Asset over a specific period of time. Also a suitable housewarming gift.

Central Bank Digital Currency (CBDC): a digital form of Fiat Currency that is issued and regulated by a nation’s monetary authority or central bank and maintained in a Centralized Ledger. A CBDC has the same functions and legal tender status as Fiat.

Central Processing Unit (CPU): the part of the computer that processes and executes instructions (akin to the human brain).

Centralized Exchange: an Exchange operated by a central party or Intermediary, typically in exchange for a Transaction Fee.

In contrast, see Decentralized Exchange.

Centralized Finance (CeFi): when one central party is responsible for Cryptocurrency and Token transactions, such as a Centralized Exchange or a custodial Wallet provider.

In contrast, see Decentralized Finance.

Centralized Ledger: a Ledger maintained by a single central person or institution.

In contrast, see Distributed Ledger.

Centralized Network: in a network in which the parties that can participate and transact on a Blockchain are known, and access rights are controlled and not available to the public.

In contrast, see Decentralized Network.

See also Private Blockchain.

Chain Split: a break in digital recordings. With Cryptocurrency, only one recording should be made at a time. However, if the network of users managing the Cryptocurrency technology disagree on how the Block should be made, they may split off, each forming their own chain of recordings. A Chain Split occurred in 2016 with Ethereum, resulting in Ethereum and Ethereum Classic.

Chaincode: a program, written in a prescribed language, that runs on top of a Blockchain to implement the logic of the relevant application. For example, Chaincode checks to ensure that Bitcoin sellers actually have bitcoin in their Wallet (Software). Chaincode is also known as a Smart Contract.

Chainwashing: when vendors use the word “Blockchain” as a marketing buzzword, regardless of whether they possess an economically viable Blockchain-based product.

Change: European Cryptocurrency Exchange.

Chargeback: the reversal of a credit card transaction made with a merchant, usually at the request of a credit card user, and conducted by the bank that issued the credit card. Users whose credit cards are stolen may request a Chargeback when unauthorized purchases are made on their stolen cards.

Chargeback fraud is a risk for banks and merchants, as fraudsters may use the process to attempt to reverse payment for legitimate purchases.

Proponents of Cryptocurrency say using Virtual Currency mitigates or eliminates such risk, since payments are transferred directly from person to person.

Checksum: a digit representing the sum of the correct digits in an Address against which comparisons can be made to detect errors in the data. Checksum helps users avoid sending Cryptocurrency to the wrong person.

Child Chain: a separate Blockchain attached to a parent Blockchain, or Side Chain. Child Chains are intended to allow a Blockchain network to Scale globally, as users can transfer Assets between the parent Blockchain and the Child Chain. Child Chains also separate transactions and data that do not affect security from those that do, which leads to a smaller Block size. Thus, Child Chain Blocks can be verified more quickly than Blockchain Blocks, increasing the number of transactions that can be processed per second. An example is Ignis, which is a Child Chain on the Ardor network.

Cipher (or Cypher): an Algorithm for Encryption or Decryption of data. Also the evil dude in *The Matrix*.

Circulating Supply: the number of Coins or Tokens currently issued and available to the market.

See also Max Supply.

Client: end-user software that facilitates Private Key generation and security as well as payment transfer on behalf of a Private Key and other services.

Cloud Mining: a Mining method whereby Miners rent or invest in cloud-based Mining capacity to avoid the hassle of maintaining a Mining Rig at home.

See also Mining Contract.

Coin: a type of Cryptocurrency that operates on its own Blockchain and is independent of any other Blockchain (e.g., Bitcoin, which operates and functions on the Bitcoin Blockchain).

Cold Storage: the storage of Bitcoin, Ether, or other Virtual Currency offline, such as on a USB drive or in physical form like in a Wallet (Hardware), rather than in a Wallet (Software) or other online Stored Value tool.

Cold Wallet: see Cold Storage and Wallet (Hardware).

Collective Investment Scheme: an investment pool, such as a unit of funds that are managed on behalf of investors. Collective Investment Schemes may be more specifically defined or conditioned depending on the jurisdiction.

Commodity: in the CFTC regulatory context, the definition is very broad and includes all goods and articles, and all services, rights and interests, in which contracts for future delivery are dealt in, presently or in the future. Since 2014, the definition of Commodity has been understood to include Virtual Currency. Individualized things (e.g., antiques, paintings) and Securities are expressly excluded from this definition, as are — wait for it — onions and movie ticket receipts.

Commodity Futures Trading Commission (CFTC): the US agency tasked with regulating the Swaps, Futures, and retail leveraged Commodities markets. The CFTC also retains general enforcement authority to police fraud and manipulation in cash or "spot" commodities markets.

Community Governance: a system in which a community, rather than a central governing body, makes decisions with respect to a Protocol. The community uses Governance Tokens to signify each party's vote on a given matter. While founders and early investors typically hold the majority of Governance Tokens, allowing them to control outcomes (much like shareholder votes), the community makes far more decisions than shareholders usually do.

See also DeFi.

Complete Block: a complete set of the most recent transactions that have been successfully mined (not including transactions that have been included in other Blocks). A Complete Block is added to a Blockchain and gives way to the next Block in the chain.

See also Mining.

Composability: the interoperability of components (i.e., Protocols) within a design system (e.g., Ethereum). Stacking Open Source and Permissionless Protocols to achieve creative financial objectives is a central feature of DeFi. The process is sometimes described as playing with "money Legos."

Confirmation: the verification and legitimization of Blocks on a Blockchain by Miners. When a Block has been verified, it is accepted and added to the Blockchain, and the transactions in that Block are then considered to have one Confirmation. The number of Confirmations that a transaction has increases with each subsequent Block that is added to the Blockchain.

In practice, for security purposes, an individual or an exchange may require a transaction to have a certain number of Confirmations before it considers the transaction final and delivers the goods or services being purchased with Cryptocurrency.

Confirmed Transaction: a transaction executed on a Blockchain and evidenced in a Block. One or more Confirmations complete a transaction.

In contrast, see Unconfirmed Transaction.

Conflict: a situation in which participants disagree about the state of the system (e.g., when multiple Blocks are published to a Blockchain at approximately the same time, resulting in conflicting versions of the Blockchain). It is important for Conflicts to be resolved in order to prevent a Hard Fork.

Conflict Resolution: the rules by which a Blockchain network resolves Conflict among its Blockchain Network Users. The Conflict is resolved through publication of the next valid Block to a version of the Blockchain. The other versions of the Blockchain then become Orphans.

Consensus: a process to achieve agreement by the majority of peers within a Distributed Network. Achieving Consensus means the group of peers participating in a Blockchain have evaluated and agreed on the state of the Blockchain, most commonly when there is an addition to the Blockchain.

A key part of any Blockchain is how it achieves Consensus. One method is the use of Algorithms (e.g., POS, POW).

Consortium Blockchain: a Blockchain with set Permissions, allowing for greater control over the network while maintaining the security features of a Public Blockchain. Consortium Blockchains are semi-Decentralized and controlled by a group of approved individuals.

Consumer Token: a Token that provides the holder access to a specific set of goods, services, or content on a Blockchain. It is designed for consumptive use as opposed to serving as a medium of exchange or representing a form of ownership or right to a revenue stream.

Convertible Virtual Currency: a Virtual Currency that can be exchanged for and has an equivalent value in Currency and/or can be used in place of Currency (i.e., for the purchase of goods or services).

Reference: FinCEN, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (March 18, 2013).

Co-Signer: a person or entity that has partial control and access over a Cryptocurrency Wallet.

CPU: acronym for Central Processing Unit.

Creator Economy: a subset of the global or domestic economy that is based on independent creators or "solopreneurs" who monetize their creativity through content creation. The Creator Economy is facilitated by Web2 and Web3 as creators earn revenue on video apps, social media platforms, NFT marketplaces, Metaverse games, etc. The Creator Economy runs on likes, shares, retweets, followers, and subscribers.

Cross-Chain: an exchange of one Digital Asset for another directly between the respective Blockchains for the two Digital Assets in question.

See also Atomic Swap.

Cross-Chain Atomic Swap: an Atomic Swap in which the exchange of two Digital Assets occurs Cross-Chain.

Crowdsourcing: a method of fundraising whereby developers solicit donations from the public in exchange for certain benefits if the project is successful. Crowdsourcing can be used to fund a Blockchain project, with the promise that participants will be issued Tokens at launch.

Crypto: short for Cryptocurrency.

Crypto-to-Crypto Exchange: an Exchange that permits users to trade one or more types of Cryptocurrency for another Digital Asset (as opposed to a Fiat Exchange, which permits users to trade Fiat for Cryptocurrency). A Crypto-to-Crypto Exchange is also known as a Pure Cryptocurrency Exchange or an Altcoin Exchange.

Crypto Climate Accord (CCA): an agreement among Cryptocurrency businesses and individuals to bring the Cryptocurrency industry to zero carbon emissions by 2030. Many observers and industry participants believe that certain Cryptocurrency processes (e.g., Proof of Work Mining and Minting) need to become more energy efficient in order to become widely accepted. Proponents of the CCA therefore argue that the agreement is good for the industry and the environment.

Crypto Valley: an Ecosystem in Switzerland and Liechtenstein that has become a business hub for VASPs. Switzerland has favorable tax and regulatory systems, as well as an educated workforce, and is actively recruiting Cryptocurrency businesses to relocate in the country. Many such businesses are based in Zug, outside of Zurich.

Cryptoasset Trading Platform (CTP) : a Platform that facilitates the secondary trading of Cryptocurrency Assets.

Cryptocurrency: a type of Virtual Currency that incorporates Cryptography to enhance its security. Most, but not all, Cryptocurrencies are Decentralized.

Cryptographic Digest: the output of a Cryptographic Hash Function.

See also Hash Digest.

Cryptographic Hash Function: a special class of Hash Function that has certain properties in order to make it secure and ideal for cryptographic purposes, including the following: (i) it is deterministic, meaning the Hash Function always produces the same result; (ii) it is fast, meaning it returns the Hash of an input very quickly); (iii) it is pre-image resistant, which basically means that it is virtually impossible to determine the original input data from its Hash value; and (iv) even a small change in the input data would result in a massive change to the Hash value (known as the “avalanche effect”).

A well-known example of a Cryptographic Hash Function is SHA-256, which Bitcoin uses.

Cryptographic Nonce: an arbitrary number used only once in a cryptographic communication.

Cryptography: information and communication techniques for securing information in computer systems from malicious third parties known as adversaries.

Cryptojacking: a form of cyberattack in which the attacker obtains unauthorized access to a computer in order to secretly Mine Cryptocurrency.

Cryptonetwork: the mechanism used by Cryptocurrencies to disaggregate information while keeping the system as Decentralized as possible.

CryptoPunks: a collection of 10,000 algorithmically generated and unique Profile Picture NFTs on the Ethereum Blockchain. CryptoPunks are a mere 24 x 24 pixels in dimension, but the collection is one of the most followed in the NFT market, and rare “Punks” have changed hands for millions of dollars.

Currency: money (in whatever form: coin, paper, or other representation) that is designated as legal tender, circulated by a government, and generally accepted as a medium of exchange in its country of issuance.

See also Fiat.

Custodian: the party responsible for storing Cryptocurrency and other Digital Assets.

Custody: the concept of ownership and/or control over a particular Asset. One notable aspect of having Custody includes holding the Private Key to a Wallet (Software) or Wallet (Hardware) that holds the Asset(s) in question. Custody often involves an external Custodian or Exchange, while Self-Custody is popular among those who prefer HODLing their Cryptocurrency free of Intermediaries.

Cypherpunk: a person who advocates for the widespread use of Cryptography and anonymous systems in order to foster privacy online. While the term predates Cryptocurrency and the Blockchain, Cypherpunks are often (but not always) aligned with the Cryptocurrency and Blockchain ethos. Eric Hughes, the original Cypherpunk, coined the term in 1993 with “A Cypherpunk’s Manifesto.” In the manifesto, Hughes argues that guaranteeing privacy in an electronic age requires “anonymous transaction systems” using electronic money, which governments or corporations are unlikely to create. Instead, he says, society needs to come together and deploy the required systems in order to maintain privacy. Satoshi Nakamoto may have achieved the Cypherpunk goal with the Blockchain.

DAO: acronym for Decentralized Autonomous Organization.

Dapp: short for Decentralized Application.

Data Silo: a collection of information in an organization that is isolated from and not accessible by other parts of the organization, analogous to how grain is stored in silos on farms.

Database: a virtual library of all the transactions that take place in crypto-land.

Date of Launch: when an ICO puts Tokens up for sale.

DDOS: acronym for Distributed Denial of Service.

Dead Cat Bounce: when a cryptoasset that has been declining in value due to selling pressure gets a sudden but temporary improvement in price.

Decentralized: when the functions and power of an activity or organization are dispersed and Peer to Peer, rather than concentrated in a central location or authority.

Decentralized Application: a digital program that runs on a P2P network of computers and utilizes Smart Contracts to access a Blockchain network and enforce each term of agreement between two parties.

Decentralized Autonomous Cooperative: an organization controlled by users that is likely to have some form of autonomous Governance to address issues of corporate responsibility.

Decentralized Autonomous Organization (DAO): an organization that operates autonomously in accordance with preset rules, utilizing a Blockchain and coordinated through a distributed Consensus model. The DAO, established in 2016 utilizing Ethereum, was an example of this type of organization.

Decentralized Exchange (DEX): a Platform that enables P2P Cryptocurrency and/or Token transactions without an Intermediary that manages a Centralized Ledger or controls user funds.

In contrast, see Centralized Exchange.

Decentralized Finance (DeFi): the economic paradigm shift enabled by Decentralized technologies, particularly Blockchain networks and Decentralized Applications. Proponents of DeFi imagine a global open alternative to every financial service used today, including savings, loans, trading, insurance, etc., accessible to anyone in the world with a smartphone and an internet connection.

Decentralized Network: a network in which any party can participate and upload information onto a Blockchain. Bitcoin is the most well-known example of a Decentralized Network.

In contrast, see Centralized Network.

See also Public Blockchain.

Decoupling: when an Altcoin no longer follows the price trend of Bitcoin or other highly traded Cryptocurrencies (i.e., when the price of Bitcoin increases, the price of the Altcoin decreases, and vice versa).

Decryption: the conversion of encrypted data back into its original form.

In contrast, see Encryption.

Deflation: the reduction of the general price levels in an economy. In the Cryptocurrency context, this may occur when demand for a specific Cryptocurrency decreases, which results in the decrease of the value or price of such Cryptocurrency.

In contrast, see Inflation.

Delegated Proof of Stake (DPOS): a Consensus method whereby users of a Blockchain vote on a certain number of "witnesses" who are paid to validate transactions and create Blocks, with the weight of a user's vote being proportionate to the percentage of applicable Tokens that he or she owns (see POS). While witnesses may prevent specific transactions from being included in a Block, they cannot change the details of a transaction and are thus equivalent to Miners in a POW Consensus model. Voting for witnesses is a continuous process, with each witness being at risk of replacement.

Demurrage: the cost associated with holding Currency over time; basically, a carrying cost to discourage the hoarding of Currency and encourage circulation.

Depository Trust and Clearing Corporation (DTCC): a post-trade financial services company that provides clearing and Settlement services to the financial markets in the United States.

Depth Chart: a visual representation of the supply and demand of a particular stock, Commodity, or Digital Asset. The chart usually has two lines, one representing buy orders for the subject asset of the chart, and another representing sell orders. The vertical axis indicates the amount of the subject asset, while the horizontal axis indicates the spot price for the subject asset.

Derivative: a financial instrument through which specific financial risks related to another financial instrument, indicator, or Commodity can be traded in financial markets. While Derivatives are treated as separate from the underlying transaction to which they are linked, the value of a Derivative derives (get it?) from the underlying financial instrument.

Examples include: (i) contracts to buy or sell something for future delivery, such as Forwards and Futures Contracts; (ii) contracts involving an option to buy or sell financial or non-financial instruments or items at a fixed price in the future, such as Options; (iii) contracts to exchange one cash flow for another, such as Swaps; and (iv) many combinations of the foregoing.

Deterministic Wallet: a Wallet (Hardware) or Wallet (Software) that uses a Seed Phrase to generate pairs of Public Keys and Private Keys.

DEX: acronym for Decentralized Exchange.

Digital Asset: an Asset that is digitally represented on an electronic medium or stored on a digital device.

Digital Commodity: a Commodity in non-physical form with some level of relative value that can be exchanged for other value, such as cash or Bitcoin.

Digital Currency: a digital representation of Currency.

See also Central Bank Digital Currency, Fiat, Virtual Currency, Cryptocurrency, and Stored Value.

Digital Identity: digital representation and storage of information used by computers to represent a real-world person or entity that arises from the input and use of such information on the internet. Digital Identity can be used to authenticate and verify a person or entity across systems or networks. Historically, personal information has been collected and stored in centralized repositories controlled by specific entities, but on a Blockchain, identity authentication and verification can be Decentralized and potentially more secure.

Digital Signature: a technological tool used to sign documents electronically that verifies the identity of the signer. Each signer uses a Private Key to produce a unique Digital Signature, which includes a time stamp and can only be decrypted by the signer's Public Key — which the signer shares with a counterparty. This technology allows parties to trust each other's identities, as well as to ensure that any agreements have not been amended or tampered with.

Digital Twin: a virtual counterpart of a physical object, service, process, or system, updated in real time and used to simulate or test the real-world object, service, process, or system. Not to be confused with an Avatar.

Directed Acyclic Graph (DAG): a directed graph data structure with a topological ordering that only goes one way from an earlier edge to a later edge, making it impossible to traverse the entire graph starting at one edge. DAG-based DLTs validate each new transaction with a predetermined number of previous transactions, eliminating the need for Miners' confirmation and improving the speed and efficiency of a Distributed Ledger.

Discord: a voice, video, and text-messaging Platform favored by the NFT and DeFi communities.

Discount Token: a Token that provides its holder with a specific claim to receive discounts at some point in the future on transactions executed on the relevant Protocol, per the terms of the Discount Token.

Distributed Denial of Service (DDOS) Attack: a malicious attempt to disrupt the ability of a server, service, or network to handle normal traffic volume by overwhelming the target or its infrastructure with data or requests.

Distributed Ledger: a Database split across every computer that elects to run Blockchain software. Data can be with or without Permissions to control who views it.

In contrast, see Centralized Ledger.

Distributed Ledger Technology (DLT): an umbrella term with no single accepted definition that is typically used to describe Blockchain technology and systems that utilize a Distributed Ledger to store data and a Consensus model rooted in Cryptography to facilitate Decentralized control by system participants.

Distributed Network: a P2P network in which the participants can communicate directly with one another, without any Intermediary or centralized point.

Do Your Own Research (DYOR): pretty basic advice (whether in the Cryptocurrency market or otherwise). When a Token issuer excitedly promotes a new partnership or an ICO, members of the Cryptocurrency community will advise potential investors to DYOR and not trust the hype.

Dogecoin: a Shiba Inu-themed Cryptocurrency designed by Billy Markus and Jackson Palmer. Dogecoin was originally intended to poke fun at speculation in the Cryptocurrency market. However, with a Market Capitalization consistently in the top 20 of all Digital Assets, Dogecoin packs a bite and has gained legitimate traction as an Altcoin.

Dolphin: persons or entities with significant Cryptocurrency holdings (e.g., between 100 and 500 bitcoins). Dolphins are bigger than Fish but smaller than Whales.

Dominance: an index that compares Market Capitalization of Bitcoin with the overall Market Capitalization of all other Cryptocurrencies in existence.

Double Spend (Attack): an attack on a Blockchain network in which a person purposely attempts to disrupt or discredit the network by exploiting a Double Spend (Problem) and using or spending the same Virtual Currency multiple times.

Double Spend (Problem): the risk that a single unit of Virtual Currency (e.g., one bitcoin) can be spent multiple times. Bitcoin has attempted to solve this problem by using a Distributed Ledger and POW Consensus model; if a transaction is not included in the Blockchain, it is not considered valid. The more data in the Blockchain, the harder it is to double spend or otherwise create fraudulent transactions.

Dox/Doxxing: the act of publicly revealing someone's personal and private information online (e.g., publishing someone's mobile number or address in a chat room or on social media), often with the malicious intent to harass or cause harm. Derived from the phrase "dropping docs."

Drop: short for Airdrop.

Dump: to sell all of your Tokens at once or within a short period of time.

Dumping: the decline in price of an Asset generated by collective sell-offs.

Dust Transaction: a transfer of Cryptocurrency value that is too small to be processed because the value is less than the cost of the Transaction Fee. Dust Transactions are therefore considered to be uneconomic.

DYOR: acronym for Do Your Own Research.

Ecosystem: the world in which Cryptocurrency lives and operates. Ecosystems can be viewed in bubbles (the Ethereum Ecosystem, the Bitcoin Ecosystem, etc.) or as a whole. Ecosystems include Coins, Tokens, Wallets, Exchanges, Blockchain, Protocols, applicable laws and regulations, and users. Anything that allows Cryptocurrency to increase in popularity and utility, as well as the stumbling blocks to its success, is part of the Ecosystem.

E-Currency: a digital representation of Currency or Fiat.

EIP: acronym for Ethereum Improvement Proposal.

E-Precious Metal: a digital or electronic certificate representing an ownership stake in one or more precious metals, such as gold or silver.

Elliptic Curve Digital Signature Algorithm (ECDSA): a cryptographic Algorithm that is widely used among Blockchains for the purpose of Digital Signature and/or Public Key exchange.

Emission: the speed at which new Cryptocurrency coins are created and released.

Encryption: the process of converting plain text or data into a random and unreadable sequence of text or data in order to, among other things, prevent unauthorized access or use of such text or data.

In contrast, see Decryption.

End User License Agreement (EULA): an agreement that gives a software application user the right to use the application on the condition that the user follow the terms set out within.

An EULA is often the one thing standing between people and their sweet, sweet content.

Enterprise Ethereum Alliance (EEA): an industry organization launched in 2017 whose goal is to build, promote, and support Ethereum-based technologies, including the development of industry best practices and standards.

Environmental, Social, and Governance (ESG): the three factors that are considered by an increasing number of businesses, investors, and other stakeholders (alongside more traditional factors) in a variety of decision-making processes (e.g., the undertaking of ESG due diligence as part of an investment, the preparation of ESG-related disclosures by a company, or the preparation of a report by ESG research providers). In the Cryptocurrency context, ESG plays a role in debates over the environmental impact of Proof of Work versus Proof of Stake Consensus mechanisms, as well as appropriate governance in Decentralized arrangements.

ERC: acronym for Ethereum Request for Comment (Token Standard).

ERC-1155: an Ethereum Token standard developed in 2018 that allows for the use a single Smart Contract to create a bundle of NFTs, with each tied to a single set of Metadata, and for which ownership of each NFT is not individually tracked. This arrangement is useful in applications like games, for which millions of game Tokens (pieces, accessories, etc.) can exist among users, and tracking individual Token ownership across multiple Smart Contracts can be a hindrance to transfer.

See also Ethereum Request for Comment (ERC) Token Standard.

ERC-20: an Ethereum Token that reflects the standard for all Smart Contracts on the Ethereum Blockchain by proposing a series of rules by which all Ethereum Tokens must abide. Almost all Ethereum Tokens are ERC-20 compliant, and the use of ERC-20 helps developers more easily create Tokens.

ERC-721: the most widely used Smart Contract standard on Ethereum for Minting NFTs.

See also Ethereum Request for Comment (ERC) Token Standard.

Escrow: the concept of holding signed documents, Assets, or other property to prevent them from becoming operative, or holding proceeds until a specific event (e.g., “We will hold the documents in Escrow until the Private Sale is complete,” or “The funds used to purchase the Tokens will be held in Escrow until the Tokens are delivered”).

ETH: the Ticker symbol for Ether.

Ether: the Token for the Ethereum Blockchain. Ether is often described as the Gas powering the Ethereum network, since it provides incentive for Miners and developers to keep the network safe and efficient. As with other Tokens, Ether can be traded and appreciates or depreciates in value.

Ethereum: an Open Source distributed Public Blockchain and operating system with Smart Contract functionality that went live on July 30, 2015. Ethereum provides a Decentralized Turing Complete virtual machine, the EVM, which can execute Scrypts using an international network of public Nodes. In the Ethereum Blockchain, Miners work to earn Ether.

Ethereum 2.0: an obsolete name for the massive upgrade to the Ethereum Public Blockchain that is taking place over the course of 2020-2022. In early 2022, Ethereum core developers announced the preferred terms “execution layer” and “consensus layer” to describe the network upgrade known as “the merge” (execution layer + consensus layer = Ethereum). The upgrade is meant to address some of the larger problems inherent in the original Ethereum network, including energy consumption, Scalability, lag time, and network security. The network will move from a Proof of Work model to a Proof of Stake model, which should address many of the above issues.

Ethereum Improvement Proposal (EIP): a document that provides information to the Ethereum community or describes standards for Ethereum.

Ethereum Request for Comment (ERC) Token Standard: a Protocol intended to create deterministic standards that is submitted to the Ethereum community for approval.

For example, ERC-20 is the technical standard to identify and provide information about a Token (e.g., total supply, balance) and permit the request and transfer of such Token. ERC-20 is intended to enable developers to easily create Fungible Tokens representing a medium of value that will be predictably usable. Conversely, ERC-721 is the technical standard for identifying unique Assets, such as a certificate of ownership, that are not divisible or Fungible.

Ethereum Virtual Machine (EVM): software Protocols contained in each Full Node of the Ethereum Blockchain that can perform any computation coded by developers regardless of the programming language.

See also Turing Complete.

Exchange: a website on which you can buy, sell, or exchange Cryptocurrency for either Fiat or other Cryptocurrency.

Exchange Traded Fund (ETF): a collection of stocks or bonds that can be bought in one transaction at one price. There are both Blockchain ETFs (instruments that hold the stock of companies with Blockchain projects or Assets) and Cryptocurrency ETFs (instruments that hold multiple Tokens or Coins).

Exchanger: “a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.”

Reference: FinCEN, FIN-2013-G001, Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (March 18, 2013).

Exit Scam: a fraudulent practice in which a Cryptocurrency promoter launches an ICO and then vanishes with investors’ money during or after the offering.

Fat Protocol: a theory that first emerged in 2016 in a paper by Joel Monegro, who opined that one of the fundamental differences between the internet (a centralized system) and Blockchains (Decentralized systems) is the relative “thickness” of Protocols and applications (here, thickness is a proxy for value). According to Monegro, the value of Public Blockchains is found in the Protocol layer, whereas internet value is derived from the application layer. Monegro argues that popular internet sites, search engines, social networks, and other applications (or their data) provide value and returns for investors, whereas the underlying infrastructure creates value in the Blockchain Ecosystem. Public Blockchains have shared data and Tokens of some sort that provide access to the system — this adds up to a Fat Protocol and thin application stack.

Not everyone agrees with this theory, especially as a long-term prospect. Some people say the value of the Protocol decreases each time there is a Hard Fork, which leads to fewer users and transactions in that Protocol (some users take their business to the new Protocol). While the theory does appear to be a potent one for investors, on the Ethereum side, it looks like applications may overtake the Protocol in Market Capitalization and value.

Faucet: a Cryptocurrency Reward System in the form of a website or app that distributes Coins (usually in tiny fractions) in exchange for the completion of certain tasks such as solving captchas.

Fault Tolerance: the capacity for a given system to operate as intended even if certain components fail.

Fear of Missing Out (FOMO): the reason you attend a party when you really wanted to have a quiet night at home. In the Cryptocurrency context, FOMO can drive a person to rush to buy a Coin or Token when the value of that Cryptocurrency (or the market, generally) rises, lest they miss a chance to become a millionaire.

In contrast, see JOMO.

Fear, Uncertainty, and Doubt (FUD): an emotional state that can be triggered by major swings in the crypto-market. FUD was common in 2018 when Cryptocurrency prices changed dramatically by the minute, building and destroying fortunes.

Federated Blockchain: a Permissioned Blockchain that is governed by a group of persons or entities rather than one person or entity.

See also Consortium Blockchain.

Fiat: a Currency that is declared legal tender by a governmental entity that is not backed by a physical Commodity and has little to no intrinsic value (e.g., US dollars and euros).

Fiat Exchange: an Exchange that permits users to employ traditional payment methods (e.g., a credit card, a bank account, or cash) to exchange Fiat for one or more types of Cryptocurrency.

Finality: an assurance or guarantee that a Cryptocurrency transaction cannot be altered, reversed, or canceled after completion. Finality is used to measure the amount of time a person must wait for a reasonable guarantee that the executed Cryptocurrency transaction will not be reversed or changed.

Financial Crimes Enforcement Network (FinCEN): a bureau of the US Department of the Treasury in charge of administering the BSA.

FinCEN: acronym for Financial Crimes Enforcement Network.

Finney: a smaller denomination of Ether (0.001 ether). Named after Hal Finney, one of the first Bitcoin developers. Other subdivisions of Ether (in progressively smaller units) are called Szabo, Gwei, Mwei, Kwei, and Wei. 1000 Ether are referred to as kether, grand, or Einstein.

Finney Attack: a type of Double-Spend (Attack) that can be performed only in the presence of one-confirmation vendors. An attacker Mines a Block and includes a transaction that sends the Coins included in a transaction in that Block back to himself, without including the transaction in the Block. Once the attacker has found the Block, rather than broadcasting his Block, he sends the Coins to the merchant of the duplicated transaction. Once that merchant has accepted payment and provided the goods and services, the attacker broadcasts his Block, which overrides the merchant's transaction and sends the Coins back to the attacker.

Fish: a person who holds an insignificant amount of Cryptocurrency relative to the size of the market. The term is named for a person's exposure to market movements caused by Whales. A Fish is also known as a Minnow.

See also Dolphin.

Flip/Flipping: purchasing a Cryptocurrency Asset with the intent of selling it for a quick profit rather than HODLing it.

Flippening: the moment (currently hypothetical) when Ethereum's Market Capitalization overtakes Bitcoin's and Ethereum becomes the No. 1 Cryptocurrency. Flippening can also be used generically to refer to any Digital Asset, Commodity, or stock overtaking any other in Market Capitalization.

Floor Price: the lowest price (rather than the average price) at which an NFT in a collection can be bought. NFT bargain hunters are often said to "buy the floor," scooping up the cheapest NFT in a collection.

See Sweep the Floor.

Forge/Forging: creating new Tokens in POS systems. Forging is also known as Minting.

Fork: when a Blockchain splits into two branches. For example, if two Miners find a Block at the same time, typically subsequent Blocks are added to only one of the Blocks, while the other Block is abandoned by the network.

Additionally, a Fork may be introduced if the developers of a Blockchain wish to amend the rules of the network.

See also Accidental Fork, Hard Fork, and Soft Fork.

Formal Verification: the use of formal mathematical methods to prove that a given code or software program correctly matches its specification.

Forward: an agreement between two parties to buy or sell a specific Asset when it hits a specific price sometime in the future. A Forward contract is usually used for the purpose of hedging.

Fractionalization: generally, the proportional segmentation of Asset ownership. In the context of Blockchain and NFTs, Fractionalization has exploded in popularity, as Asset fractions can be cheaper and traded more quickly with lower transactional costs. Increased Fractionalization in turn offers more Liquidity to the underlying Asset.

Fractionalized NFT: an NFT that is divided into fractions (each fraction is usually represented as Fungible ERC-20 Tokens). This allows several people or entities to pool resources and collectively own a fractional Token of a single (and possibly very expensive) NFT.

Fraud Proof: a message alerting Lightweight Nodes (which do not independently validate Blocks and are susceptible to accepting invalid Blocks that Full Nodes identify as valid) that a Block is invalid and should not be added to the Blockchain.

Frictionless: a trading environment with no costs or restraints on initiating or completing transactions.

Frontier, Homestead, Metropolis, Serenity: the four planned stages in the development of Ethereum.

Full Node: a Node that fully verifies all of the rules of Bitcoin by downloading every Block and transaction and checking them against Bitcoin's Consensus and rules.

Fundamental Analysis: the attempt to determine the actual value of an Asset based on extrinsic (macro- and microeconomic) factors, rather than the value at which such Asset is currently trading or otherwise valued. The goal is to determine whether an Asset is over- or undervalued (and then act accordingly).

See also Technical Analysis.

Fungible/Fungibility the quality of a good or Asset that allows it to be interchanged one-to-one with other individual goods or Assets of the same type. Commodities, common shares, Options, Fiat bills, and most Cryptocurrency Tokens are examples of Fungible goods. Unique pieces of art, and by definition NFTs, are generally non-Fungible.

Futures/Futures Contract: an agreement providing for the delivery of Commodities or financial instruments at a specific time in the future. A Futures Contract represents a set quantity of a Commodity or financial asset, can be traded only in multiples of that amount, and can be either physically or cash-settled. Futures Contract indicia include: (i) a standardization of terms; (ii) the opportunity to offset; (iii) the right to liquidate rather than take physical delivery; and (iv) no specified right to any particular lot of Commodity.

In contrast, see Spot Trade.

Gains: increases in the value of an Asset. Gains can be realized as profits when an Asset is sold at a price higher than the original purchase price. Cha-ching.

GameFi: a mix of Blockchain-based video gaming and DeFi, based on a Play-to-Earn model in which players receive financial rewards (usually in the form of Cryptocurrency, in-game Tokens, and NFTs) for completing gameplay objectives. Often associated with the Metaverse.

Gas: the fee charged to a person in order to engage in a transaction or other operation on a Blockchain network. On the Ethereum network, Gas is the amount of Ether required to process a transaction or run a Smart Contract or Decentralized Application.

Gas Limit: the maximum amount of Gas that an Ethereum user is willing to pay for the execution of a transaction.

See also Gas Price.

Gas Price: the price an Ethereum user is willing to pay for a transaction. The initiator of a transaction chooses and pays the Gas Price of the transaction. Setting a higher Gas Price incentivizes Miners to prioritize that transaction over others.

See also Gas Limit.

Gas War: when network participants try to obtain priority positioning in Blockchain transactions by paying above the network average for Gas on their submitted transaction. Paying more to obtain priority is usually done to gain a fleeting advantage or avoid a steep loss, or to secure an NFT in an in-demand Drop. Gas War is also known as Priority Gas Auction (PGA).

Generation Transaction: a type of transaction on the Bitcoin Blockchain created by a Miner to claim the Block Reward and any Transaction Fees arising from transactions included in a Block. A Generation Transaction, also known as a Coinbase Transaction, is always the first transaction in a Block.

a type of transaction on the Bitcoin Blockchain created by a Miner to claim the Block Reward and any Transaction Fees arising from transactions included in a Block. A Generation Transaction, also known as a Coinbase Transaction, is always the first transaction in a Block.

Genesis Block: the first Block of a Blockchain. The first Genesis Block was the first Block of the Bitcoin Blockchain, released by Satoshi Nakamoto on January 3, 2009.

A popular bit of trivia is that Nakamoto left a message in the code of the first Genesis Block containing the headline of British newspaper The Times on January 3, 2009: "Chancellor on brink of second bailout for banks." This message serves as a time stamp for the Genesis Block, perhaps a commentary on the central bank system, and a possible indication that Nakamoto is British or was living in England at the time.

Get Off Zero: the exhortation by Digital Asset enthusiasts to those on the sidelines to dip their toes into the investment waters through the purchase of a small, comfortable amount of Digital Assets.

Git: an Open Source and distributed version control system. Git is a software that tracks changes and coordinates work upon different source codes.

GM: a commonly used greeting in the cryptosphere meaning "good morning," regardless of the actual time. Conveys the feeling of a bright, sunny future for the Crypto conversationalists.

Gold-Backed Cryptocurrency: one version of a Stablecoin; each Coin or Token issued is backed by gold held by the Cryptocurrency issuer. Some Coins represent actual ownership of the underlying gold, while other Coins use the gold to stabilize the value. Purchasing the Coin does not convey any rights to the underlying Asset.

Governance: a system for managing and implementing changes to Cryptocurrency Blockchain Protocol.

Governance Token: a Token that represents voting rights on a Blockchain project. Governance Tokens are mostly associated with DeFi projects, since they allow many parties to be involved in the Governance, including decisions normally undertaken by the officers or directors of a company. Many DeFi projects issue Governance Tokens to users based on certain terms, or simply Airdrop them at set times. While not exactly like Utility Tokens, Governance Tokens are perhaps better understood as shares in a project instead of a Cryptocurrency.

Governance Vote: a vote by holders of Governance Tokens on a proposal related to the Blockchain or Protocol associated with the Token. A Governance Vote can impact, among other things, Blockchain functions, features, fees, and strategic development.

Goxxed/Goxed: to have suffered losses or other ongoing issues due to the failure of Japanese Cryptocurrency Exchange Mt. Gox. Generally, describes the victims of a Cryptocurrency Exchange that (i) discontinues operations due to technical or system issues, (ii) is forced to shut down, or (iii) files for bankruptcy.

Graphical Processing Unit (GPU): a computer chip that is designed to perform mathematical calculations necessary for rendering images and boosting the performance of video and graphics on computers.

GPUs are also one of the three main types of hardware that can be used for Mining Cryptocurrency, alongside ASICs and CPUs. In this regard, GPUs are generally faster than CPUs and more flexible than ASICs.

Green Bitcoin: in keeping with the goals of the Crypto Climate Accord, developers are working on creating a sustainable Cryptocurrency that would not use as much energy as Bitcoin or most other Cryptocurrencies. While no one has yet created a fully net zero Cryptocurrency, several developers are providing more sustainable options.

Group Mining: Mining as part of a Mining Pool.

Gwei: a small value denomination equal to 1/1,000,000,000 of an Ether.

Hack: the act of exploiting the security vulnerabilities of a Cryptocurrency, Exchange or Wallet (Software) to steal Cryptocurrency. In 2018, Hacks led to over US$1.5 billion in Cryptocurrency theft.

Halving/Halvening: when the reward for Mining Bitcoin transactions is cut in half. Halving happens with every 210,000 Blocks Mined, which is about every four years. In addition to reducing the reward, Halving also reduces the pace at which new bitcoins join the Circulating Supply. Halving is intended to control Inflation.

Hard Cap: the maximum amount of funds intended to be raised in an ICO, such that if the amount is reached, the ICO will cease accepting funds.

Hard Fork: a Fork in which two or more competing and incompatible implementations of a Distributed Ledger result following the proposal by one or more developers of a modification to a Decentralized Network that is not accepted by a majority of Miners and users, but that is nonetheless accepted by a substantial plurality of Miners and users.

See also Accidental Fork and Soft Fork.

Hash: output emitted from the Algorithm maintaining Consensus on a Blockchain. Each Block contains a Hash value that validated the transaction before it.

Hash Chain: a name for a data structure in which data is combined into Blocks, with each Block containing a Hash Digest of the previous Block. This Hash Digest should provide evidence of tampering, as any modification to a Block in the Hash Chain will result in a different Hash Digest being recorded in the subsequent Block.

See also Tamper Evident.

Hash Crash: a precipitous drop in computing power for the Blockchain.

See also Hash Rate.

Hash Digest: the output of a Hash Function that is usually a set of alphanumeric characters of fixed length. A Hash Digest is also known as a Hash Value or Hash Code.

See also Hash and Hashing.

Hash Function: any function that can be used to map data of various sizes to data of a fixed size (or a Hash).

Hash Rate: the number of Hashes that a given processor can calculate in a defined period of time.

See also Hash Crash.

Hashing: the process of reducing all transactions conducted on a Blockchain to an output with a fixed length. Each Hash becomes equal in length, making the data uniform and manageable. Bitcoin, for example, uses SHA-256 so that each transaction input results in a 256-bit output.

Hashing Power: the speed at which a Cryptocurrency Mining device operates.

See also Hash and Hash Rate.

HD Wallet: short for Hierarchical Deterministic Wallet.

Hidden Cap: when ICO issuers keep the amount of capital they wish to raise a secret. The ostensible goal is to incentivize smaller investors to participate in an ICO; large investors may not be willing to invest without knowing the intended Circulating Supply.

Hierarchical Deterministic Wallet (HD Wallet): a Wallet using the Hierarchical Deterministic (HD) Protocol, which creates a hierarchical tree-like structure of Private Keys and Public Keys from a single master Seed Phrase.

HODL: a misspelling of "hold" that refers to the act of maintaining ownership of an Asset for a long period of time regardless of market sentiment and volatility. HODL has also been interpreted as an acronym for "Hold On for Dear Life."

See also BUIDL.

HODLACL: acronym for "Hold on for Dear Life and Complain a Little."

See also HODL.

Homomorphic Encryption: another term for Public Key / Private Key Encryption.

Honeypot: a decoy computer system designed to lure hackers into attempting to gain unauthorized access to an information system in order to detect, analyze, counteract, and/or repel such behavior.

Hosted Wallet: a Wallet (Software) provided by a company that stores the users' Private Keys. Hosted Wallets function like a traditional banking mobile application.

Hot Storage: a type of digital storage that provides immediate access and is typically connected to other computers, networks, or the internet.

In contrast, see Cold Storage.

Hot Wallet: a Wallet (Software) that is online or otherwise connected to the internet to enable Hot Storage and that is used to allow faster access to the stored Cryptocurrency. Since Hot Wallets are connected in some manner to the internet, they are often targeted by malicious actors and hackers and therefore seen as risky.

In contrast, see Cold Wallet.

Howey Test: a test established in a 1946 case decided by the US Supreme Court that determines whether an Asset constitutes an "investment contract," a species of Security under US law, which in turn informs the SEC's approach in determining whether a Digital Asset is a Security. Specifically, the Howey Test examines whether an Asset involves an investment of money in a common enterprise in which the investor is led to expect profits derived from the entrepreneurial or managerial efforts of one or more third parties.

HTTP (Hypertext Transfer Protocol): the communications Protocol used to connect a client (e.g., a desktop, laptop, mobile device, etc.) to servers on the internet or a local network (intranet). HTTP is used to send and receive information, webpages, and files, and underpins Web2.

Hybrid POW/POS: a Consensus model that uses elements from both the POW Consensus Model and the POS Consensus model.

The exact elements and mechanisms vary depending on the Algorithm, but one example of a hybrid system is when POW Miners create new Blocks, and POS Miners vote on whether the Blocks are to be confirmed.

See also Proof of Work and Proof of Stake.

Hyperledger/Hyperledger Foundation: an Open Source umbrella project for the collaborative development of Blockchain-based Distributed Ledgers and related tools, started in December 2015 by the Linux Foundation.

Immutable: an adjective meaning unchanging or unable to be changed that is used to describe one of the perceived benefits of Blockchain: that once a Block is written to a Blockchain, it cannot be changed. (Rewriting a Blockchain is not impossible, but it involves enormous complexities.)

Impermanent Loss: when the Tokens provided to a Liquidity Pool by a Liquidity Provider dip in value such that the Liquidity Provider's deposited Tokens are worth less than when they were originally deposited. The Liquidity Provider only suffers an actual loss if the Tokens are withdrawn at a lower value.

Incentive Mechanism: the process of providing Blockchain users with a reward for conducting certain activities within the Blockchain network. The most well-known example is the system of Bitcoin Mining, whereby Miners are rewarded with bitcoins in return for the successful publishing of Blocks.

See also Block Reward.

Inflation: an economic term for what happens when prices for goods and services steadily or abruptly rise (due to increased Currency supply, higher wages, supply chain disruptions, etc.), resulting in a decline in purchasing power (e.g., "I used to be able to go to the movies for five dollars!").

In contrast, see Deflation.

Initial Bounty Offering (IBO): the limited-time process by which a new Cryptocurrency is made public and distributed to people who invest their skills and time to earn rewards in the new Cryptocurrency.

In contrast, see Initial Coin Offering.

Initial Coin Offering (ICO): a fundraising method through which an entity creates a certain amount of Tokens or Coins and sells them to the public.

In contrast, see Initial Bounty Offering.

Initial Exchange Offering (IEO): the use of one or more Exchanges by a Cryptocurrency startup to conduct an offering of its Tokens or Coins. Such Exchanges can administer a Smart Contract for the offering or the marketing of the offering. The Exchanges act as Intermediaries between the Token or Coin buyers, in contrast with an ICO, in which a Cryptocurrency issuer directly sells Tokens or Coins to buyers.

Initial Token Offering (ITO): an offering of tokens with proven (or unproven) intrinsic utility in the form of software or usage in an Ecosystem. These offerings are conducted in a manner similar to an ICO.

Instamine: when a Cryptocurrency allows Miners to obtain a lot of Coins or Tokens in a short period. Instamining can be a purposeful promotion to drum up interest in a new Cryptocurrency. Conversely, Instamining can be accidental if the Cryptocurrency issuer does not adjust the difficulty of the Mining algorithm and Miners take advantage to obtain a large market share of the Circulating Supply.

Interface: a device or program connecting two items of hardware or software so that they can be operated jointly or communicate with each other. Interface may also refer to the means by which a user might interact with a computer system or technological product.

Intermediary: a third party that facilitates the trading of Assets, whether on an Exchange or OTC, typically in exchange for a Transaction Fee.

A Custodian is a type of Intermediary that holds customers' Assets for safekeeping in order to minimize the risk of misappropriation, misuse, theft, or loss.

See also OTC Broker and Self-Custody.

Interoperability: the ability of different Blockchain solutions to recognize and interact with each other. If Blockchains are not interoperable, an Intermediary is needed to validate and execute the transactions between the different Blockchains, which is anathema to the concept of Blockchain.

InterPlanetary File System (IPFS): a Decentralized, Peer-to-Peer file sharing and storage network built on the Ethereum Blockchain. IPFS is often used to store files, websites, applications, and NFT data in a distributed manner, with persistent content identifiers that provide numerous advantages over traditional HTTP arrangements (which are subject to the risk of Rug Pulls).

IOTA: a Blockchain network designed and developed to record and execute transactions between devices operating in the Internet of Things Ecosystem.

Irreversible Transaction: a transaction that cannot be undone. In the world of Cryptocurrency, this is the Bitcoin solution to the Double Spend (Problem). Once a transaction conducted in Bitcoin is executed on the Blockchain (execution includes POW and Hashing), the transaction is final.

See also Immutable.

Joy of Missing Out (JOMO): the happiness or excitement a person feels when they decide not to take part in an activity or event. Investors or traders who did not participate in the latest and greatest ICO that subsequently crashed in value may experience JOMO.

In contrast, see Fear of Missing Out.

Key: see Private Key, Public Key, View Key.

Know Your Customer (KYC): the requirement, pursuant to the BSA, that financial institutions conduct due diligence on their customers prior to engaging in transactions with them. The goal is to avoid inadvertently engaging in criminal activity by furthering money laundering, terrorism finance, other criminal enterprises, or engaging in business with persons on the OFAC sanctions list. The KYC process is tailored to the activity, the financial institution, and the person, so that the level of due diligence is commensurate with the risk presented to the institution.

Know Your Transaction (KYT): the general compliance process used to identify fraudulent transactions. The goal is to spot potentially risky transactions and unusual behavior that may signify money laundering or other criminal activity.

Lambo: an expression of Cryptocurrency success. Lambo originates from Lamborghini, the car crypto-traders hope to buy when they become crypto-millionaires.

Latency: the time it takes for data to go from one Node to another.

Layer 1/Layer 2: usually discussed in the context of Scalability, Layer 1 refers to the basic architecture of the Blockchain, which provides the foundation on which to build Layer 2, which is the overlaying network. Scalability issues can be addressed at Layer 1 or Layer 2; if they are addressed at Layer 1, Sharding needs to be implemented or fundamental changes to the Consensus Protocol need to be made. On the other hand, Layer 2 solutions can be less fundamental (not messing with the underlying Blockchain architecture). The Lightning Network is a popular Layer 2 solution.

Ledger: a written or computerized record of transactions in a monetary unit, reflecting debits and credits to applicable accounts in such monetary unit.

Leverage: the ability of a trader to borrow money against current funds to trade Cryptocurrency "on margin" on an Exchange.

Leverage Token: a Token, often in the form of an ERC-20 Token, that seeks to provide leveraged exposure (whether long or short) to the price performance of some other Digital Asset or Token. For example, a Token providing 3x long exposure to ETH price or a Token providing 3x short exposure to ETH price.

Lex Cryptographica: rules administered through self-executing Smart Contracts and DAOs.

Lightning Network: a payment Protocol that can be layered and operated on top of a Blockchain for the purpose of enabling instant, scalable transactions between participating Nodes.

Lightweight Node: a Node that can verify if a transaction has been included in a Block by downloading only the Block Header as opposed to the full copy of a particular Blockchain. The Node often passes its data to Full Nodes that support it in order to connect to the Blockchain.

Limit Buy: a Limit Order to buy an Asset when the price meets a specified amount.

Limit Order: an order to buy or sell a Cryptocurrency at a specified limit price or better.

In contrast, see Market Order.

See also Limit Buy, Limit Sell.

Limit Sell: a Limit Order to sell a Cryptocurrency when the price meets a specified amount.

See also Limit Buy and Limit Order.

Liquidity: the impact of individual trades (buy or sell) of an Asset on the market price. In a "highly liquid" Cryptocurrency market, it is relatively easy for that Cryptocurrency to be bought and sold by market participants without impacting the market price.

Liquidity Mining: see Yield Farming.

Liquidity Pool: the secret ingredient for a DEX's success. These Smart Contract-based pools hold Cryptocurrency supplied by Liquidity Providers, which allows DEXs to use Automated Market Makers to match trades rather than order book trading (which matches buy and sell orders). Liquidity Providers are incentivized to continue Staking Cryptocurrency by sharing in the returns, including Yield Farming, Governance Tokens, and receipt of trading fees.

Liquidity Provider: a person who Stakes or lends their Cryptocurrency to a Liquidity Pool (or other product or service).

See also Yield Farming.

Liquidity Provider (LP) Token: a Token issued to a Liquidity Provider on a Decentralized Exchange, which runs on an Automated Market Maker Protocol. LP Tokens represent a Crypto Liquidity Provider's share of a Liquidity Pool.

Locktime: see Bitcoin Transaction Locktime, Timelock / Locktime.

Long/Long Position: a position taken by an investor who expects the price of the investment to rise over time.

Mainnet: the operating copy of a Blockchain that effectuates the purpose of such Blockchain. For example, the Bitcoin Mainnet operates to transfer Bitcoin from one public address to another.

In contrast, see Testnet.

Margin Bear Position: a Short Position when Margin Trading.

Margin Bull Position: a Long Position when Margin Trading.

Margin Call: when a trader is required to deposit more funds into their margin account to reach the minimum Margin Trading requirements. If a trader does not deposit sufficient funds, their holdings are automatically liquidated to cover losses.

Margin Trading: using funds borrowed from a broker to make trades (for any Asset). Margin Trading allows investors to purchase more Assets (Coins, Tokens, or Securities) than they otherwise would be able to. Using borrowed funds means that both losses and Gains are increased, so it's important to DYOR on any purchases. Further, as the broker is providing a loan, the investor must pay interest on their margin.

Market Capitalization (Market Cap): the measure of the total market value of a given Asset. In the Crypto world, Market Capitalization = the supply of a Digital Asset in circulation x the current price.

Market Order: a buy or sell order that is sought to be executed immediately at the current market price of the Security, Token, or Coin.

In contrast, see Limit Order.

Markets in Crypto-Assets Regulation (MiCA): a proposed regulation by the European Commission that could profoundly impact Cryptocurrency activity in the EU; as drafted, it would impact any Cryptocurrency not issued by a governmental entity (i.e., CBDC) and especially Stablecoins.

Masternodes: Full Nodes that perform functionalities such as anonymizing transactions, clearing transactions, and participating in Governance and voting. Masternode owners are financially incentivized with Tokens, but need to commit an initial collateral of Tokens to get started.

Maximalist/Maxi: someone who is all in on a particular Token or sector. For example: Alice is a Bitcoin Maximalist, while Bob is a DeFi Maxi.

Max Supply: the best approximation of the maximum amount of Coins that will ever exist in the lifetime of a Cryptocurrency.

See also Circulating Supply.

MCAP: a type of Token that operates on the Ethereum Platform.

Meatspace/Meatverse: synonymous with Realverse, and a play on the “meta-” prefix in Metaverse.

Memecoin: a Token that is associated with a popular meme or theme, often created as a joke with little real-world utility (e.g., Dogecoin, Shiba Inu, Dogelon Mars, and other canine-themed Cryptocurrencies).

Mempool: a portmanteau of “memory” and “pool,” Mempools provide a vital buffer between the creation of Blocks. As a new Block is created, new transactions are created, validated, and propagated to the Miners working to create the next Block.

Mempool Congestion: a scenario in which a high transaction count (i.e., transactions waiting to be validated) in the Mempool delays transaction processing. Mempool Congestion can occur when the volume suddenly spikes and/or the processing power for a given volume of transactions drops.

Merkle Root: all of the transaction Hashes in a Block that are themselves Hashed, combining all of the information that came before it into a new Hash Digest.

See also Merkle Tree.

Merkle Tree: named after computer scientist Ralph C. Merkle, a data structure that results from the repeated application of a Hash Function to Blocks of data until there is a single Hash Digest (known as the Merkle Root) representing the entire data set.

A Merkle Tree has nothing to do with former German Chancellor Angela Merkel or Duchess of Sussex Meghan Markle.

Metadata: data that provides information about other data, but not the content of the data. In the context of NFTs, Metadata can be On-Chain or Off-Chain. Regardless, the Metadata describes the NFT's essential properties and contains the link to the underlying Digital Asset (often a JPEG file or video stored online).

MetaMask: a Cryptocurrency Wallet (Software) used to interact with the Ethereum Blockchain, and often used as a bridge to NFT apps to buy and sell ERC-20 assets.

Metaverse: a persistent set of online worlds that are interconnected within a single synchronous virtual universe in which physical reality, Augmented Reality, and Virtual Reality converge for communities of users or players. A Blockchain can be used as a Decentralized Ledger for Assets (from digital real estate and economic transactions to fashion and weapons represented as NFTs or Tokens) to be recognizable and trackable across the various interconnected worlds within a single Metaverse.

MEW: acronym for MyEtherWallet, one of the most widely used interfaces for transferring ETH and ERC-20 Tokens between Cold Storage (Wallet (Hardware)) and other addresses on the Ethereum Blockchain.

MicroBitcoin (uBTC): one-millionth of a bitcoin, or 0.000001 bitcoins or 100 satoshis. MicroBitcoin may also be referred to as "bits."

Microtransaction: a very small payment for a product or service online. Microtransactions are a commonly cited use case for a public, Permissionless Blockchain.

Miner: a person engaged in Mining, and an opportunity for computer geeks to sound tough when asked what they do. In addition, the Miners act almost as shareholders and earn voting rights when a change, such as a Fork, is proposed.

Mine/Mining: the activity of choice for people (now mostly large corporations) who would rather expend vast resources on solving extremely complex math problems with extremely fancy computers than just buy their Bitcoin like the rest of us. Mining is the process of putting more Bitcoin into circulation, and it is Miners who complete the POW to authenticate transactions on the Blockchain.

Mining Contract: an agreement where a user can rent, invest in, or otherwise pay for the output of Mining capacity.

See also Cloud Mining.

Mining Pool: a group of people who work together and combine their computing resources to increase the chance of successfully Mining a Block. The participants split the reward earned by the pool in relation to the share they contributed to Mining the Block.

Mining Rig: a computer configured for the purpose of Mining Cryptocurrency.

Mint/Minting: the creation of new Tokens.

In the context of POS systems, Minting is an Incentive Mechanism, or the equivalent of Mining in POW systems. Generally, while a Miner is rewarded with new Coins by using computing power to solve new Blocks, a minter is rewarded with new Coins based on how many existing Coins he or she already owns.

When someone Mints an NFT, they are writing the underlying Smart Contract code that governs the NFT's qualities, which are added to the Blockchain where the NFT is managed.

See also Staking and POS Consensus model.

Mixer: a service that allows Bitcoin users to hide the source of their bitcoins and where they are sending them. On a Public Blockchain, almost anyone can follow user transactions, and therefore mixing allows a user to become anonymous.

See also Tumbler.

Mnemonic Phrase: a list of words that can be used to access a Cryptocurrency Wallet (Software) or Wallet (Hardware). A Mnemonic Phrase is also known as a Seed Phrase.

Module (or Cryptographic Module): a combination of hardware, software, and/or firmware that implements security functions (including cryptographic Algorithms and Public Key / Private Key generation) and is contained within a cryptographic module boundary.

Money Services Business (MSB): a category of "financial institution" for the purposes of the BSA and its implementing regulations that includes the following sub-categories: (i) dealer in foreign exchange; (ii) check casher; (iii) issuer of traveler's checks or money orders; (iv) provider of Prepaid Access; (v) Money Transmitter; and (vi) US Postal Service; and (vii) seller of Prepaid Access.

Reference: 31 C.F.R. § 1010.100(ff).

Money Transmission: the act of receiving money or monetary value from one person for the purpose of delivering that money or monetary value either to another person or back to the sender at a different time or place. Under US state regulatory regimes, Money Transmission is also used to refer to the sale or issuance of Stored Value or payment instruments.

Money Transmitter: a person or entity that engages in, or holds itself out as engaging in, the business of Money Transmission.

Money Transmitter License: the license required in each US state and territory, except Montana, in order for a person or entity to engage in, or hold itself out as engaging in, the business of Money Transmission to residents of the respective state.

Some states have expressly amended their laws to require a person or entity to obtain a Money Transmitter License in order to provide certain Cryptocurrency-related products or services to residents of the state. In addition, some state regulators have interpreted the existing language of the relevant laws to capture certain Cryptocurrency-related products or services offered to residents of the state.

Moon/Mooning: a colloquial term used when a Cryptocurrency is experiencing a spike in its price, and hence is Mooning or headed to the Moon.

When using Mooning in conversation, provide liberal amounts of context to avoid any misunderstanding with another practice of a similar name.

Moving Average Convergence Divergence (MACD): a technical indicator used by traders to pick up on market signals and the strength of those signals. The indicator is found by taking the difference in exponential moving averages of an Asset, which creates a line demonstrating its value over a certain period. Traders can create Futures Contracts or make Spot Trades depending on if/when the price is above or below that line. Markets characterized by higher volatility, like the Cryptocurrency market, make use of the MACD more difficult.

MSB: acronym for Money Services Business.

Mt. Gox: a Tokyo-based Cryptocurrency Exchange that operated between 2010 and 2014. Mt. Gox lost more than 850,000 bitcoins and filed for bankruptcy in 2014.

See also Goxxed.

Multilateral Trading Facilities: see Alternative Trading System.

Multipool Mining: when Miners jump between Cryptocurrencies in order to Mine the most profitable Cryptocurrency at any one time (taking into account the reward, fees, difficulty, and their own processing power).

Multi-Sig: short for a transaction that requires multiple Private Keys for authorization.

See also Multi-Signature Wallet.

Multi-Signature Wallet: a Wallet (Software) that requires transactions to be authorized by more than one Private Key before being broadcast to the network.

Nationwide Multistate Licensing System (NMLS): a system mandated by the SAFE Mortgage Licensing Act of 2008 that consolidates the process for all US state mortgage licensing applications and renewals. Since the NMLS' inception, many states have added applications for, and ongoing management of (including annual license renewal), additional license types to the system, including state Money Transmitter licenses and the BitLicense.

Native Token: a Token that is intrinsic to a particular Distributed Ledger and which is used for Validation (e.g., Bitcoin for Blockchain, Ether for Ethereum).

In contrast, see Non-Native Token.

New York State Department of Financial Services (NYSDFS): the agency charged with administering New York's financial services laws and regulations, including those related to banking, Money Transmission, and Virtual Currency (e.g., the BitLicense regime).

NFT: acronym for Non-Fungible Token.

NGMI: acronym for "Not Gonna Make It." The spiritual and financial opposite of WAGMI.

No-Action Letter: a letter written by the staff of a government agency (such as the SEC) indicating that the staff will not recommend that the agency undertake enforcement action against an entity should it engage in a certain course of action. A No-Action Letter is sent in response to a regulated entity's request when the legal status of the activity in question is unclear. A No-Action Letter essentially tells the recipient, "We think you can probably get away with that."

No-Coiner: a person who does not own any Cryptocurrency, ostensibly because they don't believe Cryptocurrency has any actual value.

Node: any computer or other hardware device that connects to a Blockchain network to maintain a copy of the Blockchain, and in some cases, download and verify Blocks.

See also Full Node and Lightweight Node.

Nonce: a random or pseudo-random number added to a hashed Block that, when rehashed, meets a Blockchain's difficulty-level restrictions and allows the Block to be successfully added to the Blockchain. Cycling through solutions in order to guess the Nonce is referred to as POW, and the Miner who is able to find the Nonce is awarded the Block and paid in Cryptocurrency.

Non-Custodial: the Decentralized storage of Private Keys by a user (rather than by an Intermediary Custodian) in relation to Wallets or Exchanges.

See also Self-Custody.

Non-Fungible Token (NFT): a Token that represents something unique and is neither interchangeable (i.e., cannot be replaced with another Token of the same type) nor divisible. NFTs are used to create unique verifiable digital identities, and are employed in applications that require unique digital items (e.g., crypto-collectibles, crypto-gaming, identification, Tokenized tickets, proof of attendance, etc.).

NFTs contain unique information embedded in Smart Contracts and are immutably recorded on their Blockchain. NFTs can be tied to any Digital Asset, but they do not contain the Digital Asset itself (only a link to it). Furthermore, ownership of an NFT does not guarantee ownership of the underlying asset, copyright, or licensing rights.

See also Fungibility, Floor Price, and Rug Pull.

Non-Native Token: a Token that is created on top of a programmable Distributed Ledger (e.g., Ethereum) and is used for non-Validation purposes (e.g., Asset Token, Utility Token).

Noob: a variation of "newbie" that refers to a person who is new to the Cryptocurrency space.

Off-Chain: a transaction in which the value moves outside of a Blockchain for reduced Transaction Fees and shorter transaction times.

See also On-Chain.

Off-Ledger: created and maintained outside of the Blockchain but still relevant within it. When referring to Currency, Off-Ledger is that which is created outside of the Blockchain, but still accepted within it. Off-Ledger can also refer to Cold Storage.

Office of Foreign Assets Control (OFAC): an office of the US Department of the Treasury that administers, investigates, and enforces the economic and trade sanctions implemented by the US government. OFAC publishes a list of sanctioned people and nations that the US government has decided pose a risk to national security, foreign policy, or the US economy.

On-Chain: a transaction that occurs on the records of a Blockchain.

See also Off-Chain.

One Cancels the Other (OCO) Order: a pair of linked orders with built-in tools to ensure that only one order is executed. When one order is executed, canceled, or expires, the other is canceled.

Open Source: any type of technology that is made public and can be seen, changed, and shared by the public.

Open/Close: the price reference at which an Asset (e.g., Cryptocurrency) opens and closes at the beginning and end of a specified timeframe, respectively.

OpenXR: an Open Source, royalty-free API standard for access to Virtual Reality and Augmented Reality Platforms and devices.

Option: a contract giving the holder the right to either buy or sell an Asset at a specific price on or before specific dates. Investors can use Options on Cryptocurrency as part of a hedging strategy to guard against significant movements in the market price of the Cryptocurrency.

See also Futures Contract.

Options Market: a market where Options are bought and sold.

Oracle: an Interface with a data source external to a Blockchain that provides the input data (e.g., share price information) required for a determination of outcomes under a Smart Contract.

Orphan: a Block that has not been accepted into a Blockchain. Orphan Blocks are created when two Miners create a Block at the same time. One Block is accepted and added to a Blockchain, while the other is deemed to be an Orphan and discarded (heart-wrenching, we know).

OTC Broker: an Intermediary who facilitates an OTC exchange of Assets.

Over the Counter (OTC) Trading: the exchange of Assets between parties away from an Exchange or execution facility, whereby buy and sell orders are not listed on a public order book or requests for quotes are not obtained on an execution facility. In the Cryptocurrency context, this means P2P or Off-Chain trading of Digital Assets. OTC Trading is also known as Decentralized trading.

Overbought: when demand for an Asset or Token pushes the price of the Asset or Token above its fundamental value. Think Beanie Babies or Memecoins.

In contrast, see Oversold.

Oversold: when an Asset is trading at a price below its fundamental value and has the potential for a price bounce.

In contrast, see Overbought.

P2P: acronym for Peer to Peer.

Paper Wallet: a method of Cold Storage. The user literally prints a piece of paper with the Private Key and Bitcoin Addresses on it in the form of QR Codes. On the one hand, a Paper Wallet can be incredibly safe — the piece of paper will not be hacked, and you are not relying on a Wallet (Software) provider for cybersecurity. On the other hand, you can lose a piece of paper pretty easily, and once it's gone, you've lost your Private Key and Addresses.

Payment Token: a Token that operates like a store of value or medium of exchange to enable the purchase and sale of goods or services, or to facilitate other transactions, in a similar manner to Fiat.

Peer to Peer (P2P): the transfer of an Asset from one person to another person. P2P is also a model in which two or more persons share resources and distribute tasks through a Decentralized Network, rather than utilizing a centralized server or network.

Permissioned: a system that uses a layer of access control to dictate the actions that may be taken by the Node users of such systems.

Permissionless: a Blockchain network in which users have equal permission to utilize and interact with the network, and in which users' permission to utilize and interact with the network is not set by the network itself or any central person or institution.

In contrast, see Permissioned.

See also Public Blockchain.

Permissions: allowable user actions (e.g., read, write, execute) that are sometimes implanted on a Blockchain to add an extra level of security.

Platform: a parent Blockchain or Distributed Ledger system used as a base upon which other applications and technologies can be developed. Platform may also refer to an Exchange.

Play-to-Earn (Play2Earn): online games in which players can earn and own NFTs and other Digital Assets that represent in-game items or in-game Currency.

PND: acronym for Pump and Dump.

Ponzi Scheme: a fraudulent investment scheme wherein investors are paid “returns” by taking other investors’ funds, rather than through the success of whatever enterprise they were purportedly investing in. Bernie Madoff was a virtuoso of the art.

POS: acronym for Proof of Stake.

POW: acronym for Proof of Work.

Pre-Mine: a practice in which the developer or development team of a Cryptocurrency Mines or creates Tokens before the Cryptocurrency is officially launched and released to the public.

Pre-Mining can be legitimately used as a means of startup funding, for example by preparing for an ICO or rewarding developers working on the project with Tokens in lieu of stock options.

However, Pre-Mining can be controversial due to its use in scams such as Pump and Dump.

Prepaid Access: a term used in lieu of Stored Value under the BSA. FinCEN defines Prepaid Access as “[a]ccess to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number.”

Reference: 31 C.F.R. § 1010.100(ww).

Pre-Sale: the sale of Coins or Tokens for Fiat at a discounted price by an up-and-coming Administrator before an ICO.

Priority Gas Auction (PGA): see Gas War.

Privacy Coin: a Coin that provides its user community with a higher level of anonymity than is typical for Cryptocurrency. Privacy-related features may include Encryption, the bundling of transactions (so that individual users cannot be linked to individual transactions), and stealth Addresses. Two notable Privacy Coins are Monero and Zcash.

Private Address: a unique identifier of alphanumeric characters that represents a virtual destination for sending Coins or Tokens.

In contrast, see Public Address.

Private Blockchain: a Blockchain to which access is restricted. A Private Blockchain is often controlled by a central person or institution.

In contrast, see Public Blockchain.

See also Permissioned.

Private Key: a string of data that permits access to a Digital Asset in a Wallet (Software) or Wallet (Hardware) and is used to spend or exchange the Digital Asset by unlocking a Digital Signature.

Private Placement: in the US, generally a Reg D-compliant Private Sale of Securities. A Private Placement includes Security Tokens that are Permissioned in such a way so as to require verification by an On-Chain regulatory compliance tool to ensure that the investor and the transaction itself are compliant with applicable SEC rules and regulations.

Private Placement Memorandum (PPM): a disclosure document used by a company hoping to attract outside investment in a Private Placement. A PPM lays out the objectives and risks of a business, as well as the terms of the proposed transaction (e.g., sale price, voting rights). In Security Token ICOs, PPMs are often referred to as White Papers.

Private Sale: a capital-raising event involving the sale of unregistered Securities to a limited pool of investors that is often conducted pursuant to an exemption from the registration requirements of the Securities Act of 1933, as amended.

See also Reg A, Reg D, and Reg S.

Profile Picture NFT (PFP NFT): an NFT used as a social media profile picture to express membership in the Crypto community. The rarer the NFT, the cooler the profile pic, and presumably the person behind it.

See CryptoPunks.

Proof of Activity: a Consensus method whereby Miners attempt to find new Blocks by solving cryptographic problems (e.g., POW). Once a new Block is found, the system randomly selects Validators to sign the Block; the likelihood a Validator is selected equals that person’s proportionate share of the applicable Coins (e.g., POS). Proof of Activity is also known as Hybrid POW/POS.

Proof of Authority: a Consensus model, similar to Proof of Stake, that leverages identity (in the form of set, pre-approved authorities, called Validators) as the form of stake rather than actually Staking Tokens. Each network implements a system to authorize and identify Validators, who will then validate transactions and Blocks within the respective network. This allows Proof of Authority networks to use less computational power and does not require communication between Nodes to reach Consensus. Theoretically, Validators will take their role seriously because their verified identity and reputation are at stake, as well as financial incentives to continue to perform honestly and efficiently.

Proof of Burn: a Consensus model alternative to POS and POW. In a Proof of Burn model, Publishing Nodes Burn a Cryptocurrency, receiving publishing rights in proportion to the Burned Cryptocurrency.

Proof of Developer: a mechanism that provides evidence of the identity of the developer of a Cryptocurrency or Protocol. Proof of Developer is employed in order to provide users of that Cryptocurrency or Protocol a level of accountability from developers who might otherwise remain anonymous or use Pseudonyms, which would more easily allow fraud.

Proof of Stake (POS): an alternative to the POW Consensus model that attributes Mining power to the proportion of Coins held by a Miner such that the more Coins owned by a Miner, the more Mining power they have. A Miner in a system using the POS Consensus model is limited to Mining a percentage of transactions that is reflective of the Miner’s ownership stake.

Proof of Work (POW): a method of deciding who is allowed to publish Blocks to a Blockchain by requiring a certain amount of resources to be expended. It is the mechanism used by Bitcoin to validate transactions and determine which Miners are rewarded.

To use Bitcoin as an example, each Miner competes to find a number that is designed to require significant amounts of computing power in order to be located. After finding the number, the successful Miner is permitted to announce a new Block, which can be independently verified by all the other Miners. The Block is then added to the Blockchain. The successful Miner is in turn rewarded with newly created bitcoins (i.e., a Block Reward).

The system allows the participants to agree on the state of a Ledger without the involvement of a centralized regulating entity, since a malicious attacker would have to control a majority of computing power on the network and expend a large amount of resources in order to manipulate the Blockchain.

A common criticism of the POW system is that it requires Miners to consume large amounts of electrical energy in order to maintain the system.

In contrast, see POS.

Protocol: the procedures, systems, and rules governing a specific network application (e.g., the internet, Blockchains, etc.).

Pseudonym/Pseudonymity: when a participant in an online community or Platform writes, posts, plays, or transacts under an alias or false name.

Public Address: a unique identifier of alphanumeric characters that represents a virtual destination for accepting Coins or Tokens.

In contrast, see Private Address.

See also Public Key.

Public Blockchain: a Blockchain that anyone may access and participate in. The Bitcoin Blockchain is an example of a Public Blockchain.

In contrast, see Private Blockchain.

See also Permissionless.

Public Key: the Public Address you share with others to receive Cryptocurrency. A Public Key can be used to verify Digital Signatures made with a Private Key.

Public Sale: an offer of Cryptocurrency that is open to members of the public. Depending on the nature of the Cryptocurrency, the offering, and the jurisdiction, a Public Sale could be regulated under applicable Securities or Commodities laws.

A Public Sale is also known as a “crowdsale.”

In contrast, see Private Sale.

Publishing Node: a Full Node that also “publishes” (or allows for the creation of) new Blocks on a Blockchain.

Pump and Dump (PND): a scheme whereby a group of Cryptocurrency traders artificially drums up enthusiasm for a Coin or Token in order to instigate a coordinated purchasing frenzy. As the Coin’s price climbs, other traders, unconnected to the Pump and Dump group, latch on to the buying spree, further boosting the Coin’s price.

Then the group proceeds to Dump the Coin by selling at the now-inflated price. While the Pump and Dump group earns a profit, the traders who purchased the Coin based on the artificial enthusiasm are left with losses.

Pumping: when a party promotes a Cryptocurrency that it holds in an effort to increase that Cryptocurrency's market price.

See also Pump and Dump.

QR Code: short for "Quick Response" code. A QR Code is a matrix barcode that you can scan with a smartphone in order to perform a transaction, such as making a purchase, logging into a service, or opening a website, among many others.

Quantitative Easing: traditionally a form of monetary policy used to generate Liquidity whereby a central bank purchases securities from the market. In crypto, Quantitative Easing is a tool used by a developer of a cryptoasset for creating market Liquidity by engaging in market selling.

In contrast, see Quantitative Tightening.

Quantitative Tightening: a monetary policy applied by central banks to decrease the amount of money/Liquidity within an economy, generally by selling government bonds and other financial Assets to financial institutions.

In contrast, see Quantitative Easing.

Race Attack: a malicious act whereby a person creates two conflicting transactions with the intention of spending the same bitcoins twice.

A Race Attack relies on a merchant being willing to accept an Unconfirmed Transaction as payment for goods or services. When the merchant accepts the Unconfirmed Transaction and ships the goods or provides the service, the attacker immediately broadcasts a conflicting transaction to the Bitcoin Blockchain — which transfers the same bitcoins referenced in the Unconfirmed Transaction to another Bitcoin Wallet (Software) controlled by the attacker. If the conflicting transaction is confirmed by the Nodes on the Bitcoin Blockchain before the Unconfirmed Transaction is provided to the merchant, the Unconfirmed Transaction will fail when broadcast to the Bitcoin Blockchain by the merchant, and the merchant will not be able to claim the relevant bitcoins that were purportedly transferred by the attacker.

Raiden Network: technology that allows near-instant and low-fee transactions of Cryptocurrency using Ethereum's technology.

Rank: the Market Capitalization of one Cryptocurrency in relation to other Cryptocurrencies.

Realverse: physical reality (aka, the universe) as opposed to Virtual Reality or the Metaverse.

Regulation A (Reg A): a statutory exemption from SEC registration requirements that permits sales to non-accredited investors. Reg A applies to public Securities offerings up to US$50 million in any one-year period that have satisfied certain regulatory filing requirements. Reg A is sometimes referred to as Reg A+.

Regulation A+ (Reg A+): a colloquial name for Regulation A.

Regulation CF (Reg CF): Title III of the US JOBS Act. Signed into legislation in 2018, Reg CF allows private companies to raise up to US$1 million via a crowdfunding platform.

Regulation D (Reg D): a statutory exemption from SEC registration requirements that permits Private Placements of Securities to accredited investors (who must meet certain requirements, including a minimum net worth).

Regulation S (Reg S): a statutory exemption from SEC registration requirements that permits offers and sales of Securities that are deemed to be conducted outside of the United States.

REKT: a play of the term “wrecked” that is used to indicate that a Cryptocurrency trader has suffered large trading losses. For example: Alice reminded Bob that he should have checked himself before he REKT himself, trading in what clearly was a PND.

Relative Strength Index (RSI): a form of Technical Analysis that serves as a momentum oscillator, measuring the speed and change of price movements. Relative Strength Index fluctuates between 0 and 100, where a Cryptocurrency is considered Overbought when the indicator is above 70 and Oversold when the indicator is below 30.

Replicated Ledger: a copy of a Blockchain network’s Distributed Ledger that is distributed to all of the participants in that network.

Resistance: a term for pricing pressures that prevent the value of a Cryptocurrency from rising to a new level. For example, traders selling their Tokens or closing Short Positions may act as a “ceiling” on the price of a Cryptocurrency.

Correspondingly, a “resistance level” indicates the maximum value that an analyst or the market believes a Cryptocurrency’s price will reach, due to Resistance.

See also Technical Analysis.

Reverse Indicator: a person, organization, or community that is usually incorrect in their predictions of Cryptocurrency price movements; their actions or statements indicate the reverse of what is likely to happen.

A Reverse Indicator is sometimes referred to as a “contrarian indicator.”

Reward System: a means of providing incentives to Blockchain Network Users for activities within the network (e.g., processing transactions and maintaining the network).

Ring Signature: a Digital Signature created by an individual and attributable to a defined group of persons who each have their own Public Keys and Private Keys. Just one member of the group creates the Digital Signature, but the Ring Signature makes it impossible to tell who that person is. The Ring Signature allows for protection and Anonymity, while keeping information and access within a smaller group.

Roadmap: a strategic planning tool used to plan the development of a project.

Round Robin Consensus Model: a Consensus model for Private Blockchains in which Nodes take turns at creating Blocks. The Round Robin Consensus Model ensures that no single participant can create a majority of Blocks, thereby generating a fair, non-monopolized Blockchain network.

Royalties: income accrued by an NFT creator through the NFT’s resale on the secondary market. Royalty standards must be coded into the NFT’s Smart Contract. Royalties are also known as “creator earnings.”

Rug Pull: in the context of Exchanges, Digital Asset projects, and NFT collections, synonymous with Exit Scam.

In the context of NFTs, also the removal or switching of an NFT’s linked Digital Asset. One clever artist proved the point by altering the underlying linked images in a collection of NFTs to JPEGs of Persian rugs.

See also InterPlanetary File System.

satoshi (sat): the smallest unit of measurement of Bitcoin. There are 100 million satoshis in one bitcoin. Named in honor of Satoshi Nakamoto. Bitcoin enthusiasts and investors often speak of “stacking sats” (i.e., accumulating bitcoin).

Satoshi Nakamoto: it’s a bird … it’s a plane … it’s … a Pseudonym used by the unknown person(s) or entity(ies) who developed Bitcoin, authored the Bitcoin White Paper, and created and deployed Bitcoin's original reference implementation, including the first Blockchain database. As of 2012, Nakamoto's P2P Foundation profile claimed to be a 37-year-old male living in Japan, however the identity of this person, group of people, entity, or group of entities is the subject of rampant speculation and conspiracy theories and has never been confirmed.

Scalability: the ability of a Cryptocurrency network to process an increased number of transactions.

Scale/Scaling: as any investor on Shark Tank would say, you need to be able to Scale your business — or grow it without too many problems — if you want the business to be viable. Blockchain has run into Scalability issues as it grows in popularity. Developers are working on solutions to address those issues, as well as the Scalability issues of the Ethereum Platform.

Scamcoin: a Coin that is a scam used by its creator to enrich themselves at the expense of other holders. Scamcoins are often pre-Mined by the developer with a scheme to Pump and Dump.

Scrypt: a type of Algorithm used in the POW Consensus model adopted by certain Cryptocurrencies (e.g., Litecoin). The Scrypt Algorithm differs from SHA-256.

Second-Layer Solutions: a set of solutions built on top of a public Blockchain to extend its Scalability and efficiency. Second-Layer Solutions are often used for micro-transactions or actions. Examples of Second-Layer Solutions include Ethereum Plasma and Bitcoin Lightning Network.

Secure Hash Algorithm 256 (SHA-256): a standardized Hash Function published by the US Commerce Department's National Institute of Standards and Technology with an output size of 256 bits. SHA-256 is the Hash Function used by the Bitcoin Blockchain.

Securities and Exchange Commission (SEC): the US federal agency that regulates transactions in Securities to protect investors and keep order in markets. Cryptocurrencies that are Securities are thus subject to SEC jurisdiction and oversight.

Security: a financial instrument that is tradeable and holds some form of monetary value. Typical examples of Securities include equity stocks, bonds, and Options. If a Token has the characteristics of a Security, it is likely to be regulated by the Securities laws of the relevant country.

See also Howey Test and Security Token.

Security Token: a Token that is structured as a Security or is deemed to be an investment contract. Security Tokens can represent an underlying real Asset and pay dividends, share profits, pay interest, or invest in other Tokens or Assets to generate profits for the Security Token holders.

Security Token Offering (STO): an initial offering of a Token that is structured as a Security to potential investors. In the US, STOs must be either registered with the SEC or exempt from such registration.

See also Security Token.

Seed Phrase: a list of words that stores all the information needed to recover a Cryptocurrency Wallet (Software) or Wallet (Hardware). A Seed Phrase is also known as a Mnemonic Phrase.

Segregated Witness (SegWit): a Protocol activated in 2017 that changed the way data is stored. SegWit increases transaction speed by moving signature (or witness) information outside a Block, allowing more transactions to be processed. SegWit also supports Second-Layer Solutions and Protocols, such as the Lightning Network, which boosts Bitcoin's transaction capacity by taking small, frequent transactions Off-Chain and setting such transactions in the Blockchain only when users are ready.

Self-Custody: when Assets are held in Custody by the owner, rather than by an Intermediary such as a Custodian or Exchange.

See also Non-Custodial, Wallet (Hardware), and Wallet (Software).

Selfish Mining: first discussed in a 2013 paper published by Cornell researchers, Selfish Mining is an attack in which a Miner generates a Block but does not publish it to the Blockchain and instead keeps working on the same Block. Other Miners work on Blocks that are not part of the longest chain and are therefore leading to a dead end. Once the Selfish Miner's Block is worth enough, they publish it and then are in the best position to Mine the next Block.

Sell Wall: a situation in which a large limit order has been placed to sell when a Cryptocurrency reaches a certain value.

In contrast, see Buy Wall.

Settlement: the process of transferring an Asset (e.g., Cryptocurrency) into the account or Wallet of a buyer and the corresponding counterparty Asset (e.g., cash or another Cryptocurrency) into the account or Wallet of the seller following a trade of the relevant Asset(s) in order to satisfy contractual obligations arising under the trade.

SHA-256: acronym for Secure Hash Algorithm 256.

Sharding: a solution meant to address Scalability issues encountered by large Blockchain networks that have grown to the point at which power consumption and long transaction confirmation times have become problematic.

Sharding involves grouping certain Nodes in a Blockchain into “shards” that in turn process specific transactions. A Blockchain that employs Sharding will have some Nodes contain partial copies of the complete Blockchain, rather than have every Node contain a complete copy, in order to increase overall network performance.

Shilling: the act of using propaganda or false information to create excitement in a Cryptocurrency to influence its price. Not a synonym for the former British coin and monetary unit equal to 12 pence.

See also Pump and Dump, Pumping.

Short/Short Position: a position taken by an investor who expects the price of an investment to go down over time. The investor opens a Short Position with a brokerage firm by borrowing shares in investment “X” from a broker, and immediately selling the shares of X on the market for the current market price. The Short Position remains open until the investor buys the same number of shares of X and returns them to the broker. The profit (or loss) associated with the Short Position at closure is the decline (or increase) in the value of X times the applicable number of shares of X, minus any Transaction Fees assessed by the broker and/or any interest charges assessed by the broker for the period that the Short Position was open.

Short Squeeze: when the price of a stock or cryptoasset rises sharply, which then forces (or “squeezes”) short sellers to buy the stock or cryptoasset in order to limit their losses, which in turn pushes the price further upward.

See also Short/Short Position.

Side Chain: a Blockchain that is interoperable with one or more other Blockchains or Platforms and which allows Cryptocurrency or Digital Assets to be transferred across, or used between, those Blockchains or Platforms.

For example, a Side Chain might interoperate with both the Bitcoin Blockchain and the Ethereum Blockchain in order to allow a person to transfer bitcoins to a Bitcoin Wallet (Software) on the Side Chain, with the Side Chain issuing a confirmation that allows the person to obtain an equivalent amount of Ether, which can be used in the Ethereum network.

Simple Agreement for Future Tokens (SAFT): a form of investment contract that Cryptocurrency entrepreneurs can sell to accredited investors (as defined under SEC regulation). Much like a SAFE (simple agreement for future equity) contract, SAFTs allow investors to convert their investment into the proposed Token at a later date (once the Token or Cryptocurrency is launched).

Simplified Payment Verification (SPV): a method of verifying that a transaction has been included in a Block without downloading a copy of the entire Blockchain. Discussed in section 8 of the Bitcoin White Paper, SPV is the method of verification typically used by Lightweight Nodes.

Smart Contract: an Immutable Protocol that follows pre-defined rules to enforce or self-execute agreed-upon obligations automatically and without the involvement of third parties.

Soft Cap: a fund-raising goal in an ICO that refers to the minimum amount of funds that a developer team aims to raise.

If a Soft Cap is not reached after an ICO, the project may be terminated and the raised capital returned to investors, though this outcome differs from case to case.

In contrast, see Hard Cap.

Soft Fork: a change in the software Protocol on which a Blockchain operates that does not require Nodes to upgrade to maintain Consensus. A Soft Fork is considered backward-compatible because the new Protocol accepts a subset of Blocks validated under the old Protocol, which causes all Blocks validated by the new Protocol to also be valid under the old protocol. Once 51% of the Hashing Power upgrades to the new Protocol, the new software Protocol will become recognized as a main Blockchain.

See also Accidental Fork and Hard Fork.

Solidity: a contract-oriented programming language used for writing Smart Contracts. Solidity is the primary language on Ethereum.

Spatial Computing: the integration of Virtual Reality and Augmented Reality with the real world. Physical space becomes a computer interface, and people can simultaneously interact with both the virtual and the physical world.

Spot Market: a market where traders can buy and sell Digital Assets for immediate exchange.

Spot Trade: the act of buying or selling a Commodity (like a Coin or Token) immediately. Almost all Cryptocurrency trading is Spot Trading.

As Ariana Grande might say, “You see it, you like it, you want it, you got it.”

In contrast, see Futures Contracts.

Stablecoin: a Cryptocurrency that is pegged to a specific underlying Asset and that is designed to have low volatility and consistently reflect the value of the underlying Asset (e.g., Tether, Gemini Dollar, and USD Coin).

Stake/Staking: (i) a way of earning fees or other rewards by putting certain Cryptocurrencies at Stake to help verify transactions on the related Proof of Stake network. Depending on the network, Staking may represent direct participation in the Consensus mechanism (e.g., serving as a Validator) or delegation to others who participate in the Consensus mechanism.

(ii) a way of incentivizing participation in DeFi Protocols by providing additional rewards to Protocol participants who Stake into a Smart Contract. Rewards help to make Protocol participation “stickier” by encouraging participants to remain Staked. For example, a Decentralized Exchange may provide additional Staking rewards (often in the form of Governance Tokens) to Liquidity Providers who Stake their Liquidity Pool Tokens into a Smart Contract.

See also POS.

Stale Block: a Block that has been successfully Mined but not included on the current longest Blockchain, usually because another Block at the same Block Height had its chain extended first. Fortunately, a Stale Block does not smell like that old meatloaf long forgotten in the fridge.

Not to be confused with Orphan.

State Channel: Off-Chain transactions made by Blockchain users. The transaction is initiated in the Blockchain, then the State Channel is opened and the transaction occurs Off-Chain, at which point the State Channel is closed and the transaction is submitted to the Blockchain. This is presented as a solution to Blockchain Scalability issues, because it reduces the number of transactions that need to be conducted On-Chain.

Stored Value: monetary value that represents a legal claim against the issuer that is stored on an electronic record or other digital medium and is evidenced by an electronic or digital record. Stored Value may be used to redeem money or monetary value, or as payment for goods or services.

SubDAO: a DAO that is controlled by, spun out of, or functionally a subsidiary to another DAO.

Swap: a financial contract to exchange one cash flow for another. In the US, Swaps usually refer to Derivatives subject to regulation by the CFTC under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.

Sweep the Floor: when a collector of NFTs buys the lowest priced items in a collection, raising the Floor Price and fomenting interest in the collection.

Sybil Attack: a cybersecurity risk to networks (e.g., Blockchains) that involves a single actor attempting to overtake the network through the use of an overwhelming number of accounts, computers, or Nodes. Named after a woman known in the field of Psychology to have suffered from multiple personality disorder.

Symbol: a unique series of characters (typically letters) that an Exchange assigns to an Asset.

See also Ticker.

Szabo: a Hungarian computer programmer and Cryptocurrency expert, Nick Szabo is a leading candidate to be Satoshi Nakamoto (or at least part of the team that created Bitcoin). Szabo has denied being Nakamoto, but many people don't believe him.

See also Finney.

Taint: the percentage of Cryptocurrency in one account that can be traced back to another account. Taint is often used to measure how many Coins in a user's Wallet are related to negative or illicit activities (e.g., stolen or fake Coins).

Tamper Evident: the concept that any edit to a Block on a Blockchain will leave a clear, Immutable sign that the Block has been altered or tampered with, which is critical to maintaining auditability and transparency on the Blockchain.

Tamper Resistant: a system designed to effectively ensure that altering agreed-upon data is difficult, expensive, or both.

Tangle: the Blockchain transaction storing and processing mechanism developed by IOTA.

Technical Analysis (TA): the practice of analyzing data, patterns, and trends in the Cryptocurrency market to predict future price movements, and to serve as a basis for investment decisions.

See also Fundamental Analysis.

Telepresence: technology that allows actions such as communication and collaboration to be performed at a distance or virtually, as if physically present in that location.

Testnet: a testing network that uses similar software to that of Cryptocurrency, but with a Coin that is not intended to have any value or be traded on an Exchange.

As its name suggests, a Testnet is a testing environment used by developers to experiment with new code and features, or to perform specific tests without disturbing a Blockchain network.

In contrast, see Mainnet.

Think Long Term (TLT): basically an affirmation to repeat when you watch the value of your Bag decline precipitously. Those investing in the Cryptocurrency market deal with a lot of price volatility, but are encouraged to TLT and HODL; stick with your Coins and Tokens and the market will trend up in the long term.

This Is Gentlemen: a meme in the Crypto world indicating positive news.

Ticker: the Symbol or acronym for a Token or Coin (e.g., BTC or ETH).

Timelock/Locktime: a type of Smart Contract mechanism that restricts a transaction from being processed until a specific time or Block Height on the Blockchain.

Timestamp: a form of identification given for when a transaction occurred. Timestamps usually contain the date and time of day accurate to fractions of a second.

TLDR: acronym for “Too Long Didn’t Read.” The TLDR is the summary of the key aspects of a longer publication. TLDR is often used in White Papers to indicate the gist of a Token project.

Token: a type of Fungible and tradeable Cryptocurrency that can be used for payment on, access to, or to otherwise facilitate operations on, a particular Blockchain, and that requires another Blockchain to exist and operate. In contrast to Coins, which operate in a manner similar to E-Currency on their own separate Blockchain, a Token runs on top of another Blockchain and is used to access the features and functionality of applications on that Blockchain.

Token Generation Event (TGE): the creation of Tokens by a Blockchain. A TGE may coincide with an ICO, a distribution (e.g., an Airdrop, equity compensation), or a Generation Transaction.

Token Velocity: the number of times a Token changes hands during a period of time.

Tokenization: the process of replacing a primary account number (usually a credit card) with a surrogate number (or token — different from a Token) that is randomly generated and not otherwise associated with a payment device. Tokenization is supposed to provide account holders with additional security, especially at point-of-sale terminals, so that their credit card numbers are not vulnerable to hacking.

Tokenization can also describe the process whereby traditional Assets (such as stocks and real estate) are digitized into tradeable, Blockchain-based Tokens that represent whole or Fractionalized ownership of the underlying Asset, and can take the form of Fungible or Non-Fungible Tokens. Regulators have not looked kindly on this form of Tokenization, and often view it as an unregistered securities offering.

Tokenless Ledger: a distributed Blockchain ledger that does not require a Token or other Cryptocurrency to function.

Tokenomics: a new subset of economics that studies the Token economy. Tokenomics examines how people interact with Tokens (from creation to destruction) and how Tokens work within and affect the broader economy and society. The term "token economy" was first coined by a Harvard psychologist in 1972; his token economy involved rewarding good behavior with valueless tokens, which could be exchanged for something of value, as a method of managing behavior.

Tor: free software for enabling anonymous communications.

Total Value Locked (TVL): the aggregate value of funds in a Liquidity Pool, or the underlying supply of funds available to a specific DeFi Protocol for trading or lending. At its most basic level, the TVL is the amount of funds locked in a given Smart Contract associated with a DeFi Protocol.

Transaction Fee: an amount of Cryptocurrency charged to process a transaction and paid to a Miner.

Transaction Pool: a set of transactions that are ready to be processed and included in a Block on a Distributed Ledger. A Transaction Pool is also known as a Pending Transaction Pool.

Travel Rule: a Bank Secrecy Act rule that requires financial institutions to collect, retain, and share certain information on the originators and beneficiaries in connection with transfers of US$3,000 or more. In 2019 interpretative guidance, FinCEN confirmed that MSBs facilitating transmittal of funds involving Convertible Virtual Currency above the US$3,000 threshold are subject to compliance with Travel Rule requirements.

Trustless: a system that enables a user to deal with others without relying on a counterparty's trustworthiness.

Tumbler: a service to mix Cryptocurrency funds with others, with the purpose of obscuring the original source of the funds. Tumblers are controversial due to their potential to facilitate money laundering.

See also AML and Mixer.

Turing Complete: any system or programming language that is capable of computing any computable function with enough time and resources.

Two-Factor Authentication (2FA): the kind of annoying authentication process that you become very grateful for when someone tries to steal your identity.

2FA requires more information from the user than simply a username and password. The user's identity is confirmed by combining two of the following three factors: (i) something they know; (ii) something they have; or (iii) something they are. Thus, for example, a user can access their data with a username, password, and code texted to a mobile phone associated with the account. NYSDFS now requires any financial institution subject to its regulations to implement either 2FA or another multi-factor authentication process to access non-public information.

Unconfirmed Transaction: a transaction that is not included in a Block and, thus, is not executed. Most Blockchains require at least one Confirmation in order for a transaction to be completed, so Unconfirmed Transactions are usually synonymous with incomplete transactions. If a user pays a higher Transaction Fee, that can encourage Miners to confirm (and therefore complete) transactions.

In contrast, see Confirmed Transaction.

Unspent Transaction Output (UTXO): unspent output, or leftover Cryptocurrency change, from Cryptocurrency transactions that can be used as input in a new transaction.

Utility Token: a Token designed for use by consumers on a Platform and not intended to constitute a Security.

See also Consumer Token and Security Token.

Validation: the act by a Miner of confirming that a transaction on a Blockchain is legitimate prior to creating a Block.

Validator: a Blockchain Network User who performs the function of validating transactions sent to the Blockchain network. In the Bitcoin Blockchain, Validators are known as Miners.

Validity Proof: see Zero Knowledge Proof.

Vampire Attack: when a DeFi or NFT Platform attempts to lure users and liquidity from a competing Platform by offering better incentives for use (e.g., higher interest rates, Token rewards, etc.).

Vanity Address: an Address that includes a readable message within the traditional string of numbers and letters, e.g., 3LathamisaGr8lawfirm1988713CjWTWBltH202dc.

Vaporware: a Cryptocurrency project that does not come to fruition.

VASP: acronym for Virtual Asset Service Provider.

Vector76 Attack: a method to compromise a Blockchain network. An attacker deposits a large amount of Cryptocurrency with a target, and then Pre-Mines and withholds a Block that contains the deposit. When the network announces a new Block, the attacker simultaneously releases the Pre-Mined Block to the target, submitting a transaction withdrawing the deposited funds.

The purpose is to create a Fork so that some Nodes accept that the Pre-Mined Block with the deposit is valid, while others accept the other Block. An attack is successful if the network accepts the other Block as valid instead of the attacker's Pre-Mined Block. The target will send Coins to the attacker for the withdrawal, even though the Ledger does not show that the attacker has made a deposit, and the target is out of pocket for that amount.

A Vector76 Attack demonstrates why it is important to wait for several Confirmations from a Blockchain network before considering a transaction to be valid.

"Vector76" refers to the username of the person who first described the attack's potential use in an online forum.

Venture Capital: a form of private equity (usually institutional investors) focused on investing in startups and small companies. Venture Capital firms invest early in a company's growth, with a focus on long-term Gains and fostering growth in order to get a big return down the road. Basically all Virtual Currency and Blockchain companies have been reliant on Venture Capital to achieve success and growth.

View Key: one of the two pairs of Private Keys and Public Keys associated with each Address, with the private View Key required to view all transactions related to the account. The other pair is called the “spend key,” with the private spend key used to spend any funds in the account.

Virgin Bitcoin: a freshly Minted Bitcoin that has not been transferred or otherwise part of any transactions.

Virtual Asset Service Provider (VASP): per FATF guidance, “any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual assets and fiat currencies; (ii) exchange between one or more forms of virtual assets; (iii) transfer of virtual assets; (iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and (v) participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.”

Reference: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

Virtual Currency: “a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.”

Thanks to El Salvador’s adoption of Bitcoin as legal tender in 2021, FinCEN’s definition is now partially obsolete.

Reference: FATF Report Virtual Currencies: Key Definitions and Potential AML/CFT Risks (June 2014).

Virtual Reality (VR): an immersive experience in a fully simulated digital environment, often through the use of a head-mounted display.

In contrast, see Augmented Reality.

See also Spatial Computing.

Volatility: a mathematical tool that measures price movements — specifically, the rate at which value fluctuates — for an Asset over time. Volatility is traditionally denoted by the “σ” symbol.

WAGMI: acronym for “We’re All Gonna Make It.” Words of encouragement and optimism in Crypto circles, especially in Bear markets.

See also NGMI.

Wallet: a means for storing the Private Keys to access and transfer Cryptocurrency Assets.

See also HD Wallet, Multi-Signature Wallet, Paper Wallet, Wallet (Hardware), and Wallet (Software).

Wallet (Hardware): a physical device similar to an external drive used to secure Cryptocurrency by storing a person's Private Keys offline. Since a Wallet (Hardware) is not connected to the internet, it is viewed as more secure than a Wallet (Software).

Wallet (Software): a non-physical storage device for Cryptocurrency that a person downloads as a software file and that remains connected to the internet. A Wallet (Software) can be downloaded and installed on a computer, run online via the cloud, or run on a smart device via a mobile application.

Wash Trade: a form of market manipulation in which investors create artificial volume and value in the marketplace by simultaneously selling and buying Cryptocurrencies or NFTs.

Web2 (Web 2.0): the current phase of the internet defined by accessing content and creating content. Web2 is dominated by centralized companies that provide services in exchange for accessing and monetizing users' personal data, while users monetize their hobbies and talents in the Web2 Creator Economy.

Web3 (Web 3.0): the next phase of the internet, built on Decentralized Peer-to-Peer networks, Artificial Intelligence, the Creator Economy, and distributed ownership of Protocols. Web3 allows for the ownership and transfer of value and information.

Wei: the smallest denomination of Ether, equal to 1/1,000,000,000,000,000,000 (or 10-^{18}) of an ether.

Whale: Moby Dick, Shamu, or any person or entity that owns a significantly large amount of, or has a significantly large investment in, a particular Cryptocurrency.

Whale Club: a chat room where Whales coordinate investment syndicates.

White Paper: a document published by a new project informing investors about and promoting the project's Token, Protocol, and/or Dapp.

Whitelist: a list of approved or allowed items/participants. Whitelist is often used in the context of approved participants in an Initial Coin Offering.

Wrapped Token: a Token that represents a Cryptocurrency from another Blockchain (or in some cases the same Blockchain) and which aims to track the value of the original Cryptocurrency. Wrapped Tokens are often used on DeFi Platforms to transact in Tokens from otherwise non-compatible Blockchains or to facilitate use of Native Tokens in Smart Contracts and DeFi. For example, wrapped Bitcoin (wBTC) is an ERC-20 version of Bitcoin that can be used on the Ethereum network, and wrapped Ether (wETH) is an ERC-20 version of Ether that can be used in Smart Contracts and DeFi Platforms on the Ethereum network.

See also Native Token and Non-Native Token.

Wrench Attack: a decidedly analog method of stealing someone's Crypto hoard, via threats or actual physical violence, to obtain their Digital Asset Private Key. As someone with knowledge of the matter once said, "You can do all the Cryptography you want, but you can't beat a $5 wrench."

Yellow Paper: a document that presents the technical specification of a proposed Protocol. A Yellow Paper is often seen as a more detailed supplement to a White Paper.

Yield Farming: Staking or lending Cryptocurrency to third parties in order to generate returns. Liquidity Providers transfer their Cryptocurrency to a Lending Pool, which incentivizes this activity with rewards (e.g., a set annual percentage yield, usually dependent on the type of Cryptocurrency, or Governance Tokens).

Zero Confirmation Transaction: a transaction that has not been recorded and verified on a Blockchain.

See also Unconfirmed Transaction.

Zero Knowledge Proof: a method by which one party can verify their knowledge of certain information without revealing how they know such information. Zero Knowledge Proof may be used to verify the occurrence of a transaction on a Blockchain without revealing the sender, recipient, Asset, or amount.

To qualify as Zero Knowledge Proof, a Protocol must satisfy three requirements: (i) Completeness: If the statement is true, an honest verifier will be convinced by an honest prover; (ii) Soundness: If the statement is false, no cheating prover can convince an honest verifier that it is true; and (iii) Zero-Knowledge: If the statement is true, no cheating verifier learns anything other than the fact that the statement is true.

Also known as Validity Proof.

Austin
Beijing
Boston
Brussels
Century City
Chicago
Dubai
Düsseldorf
Frankfurt
Hamburg
Hong Kong
Houston
London
Los Angeles
Madrid
Milan
Munich
New York
Orange County
Paris
Riyadh*
San Diego
San Francisco
Seoul
Shanghai
Silicon Valley
Singapore
Tel Aviv
Tokyo
Washington, D.C.

LW.com

* In cooperation with the Law Firm of Salman M. Al-Sudairi LLC