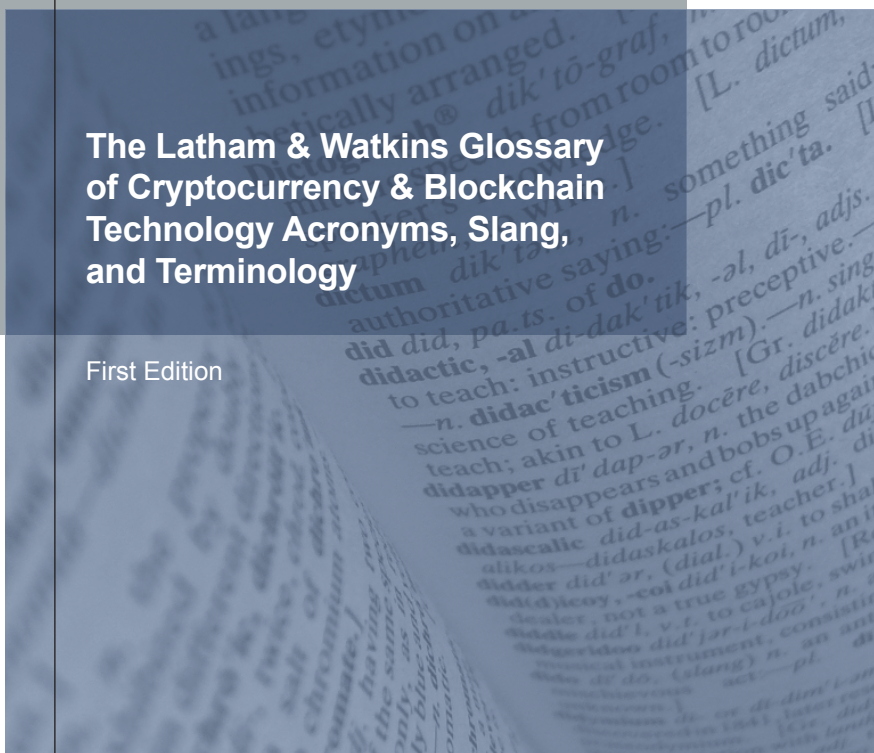
LATHAM & WATKINS LLP

# *The* BOOK *of* JARGON®

## Cryptocurrency & Blockchain Technology

**The Latham & Watkins Glossary of Cryptocurrency & Blockchain Technology Acronyms, Slang, and Terminology**

First Edition



The Book of Jargon®: Cryptocurrency & Blockchain Technology *is one of a series of practice area-specific glossaries published by Latham & Watkins.*

*The definitions contained in* The Book of Jargon® *are designed to provide an introduction to nearly 300 terms developed for the business, academic, and legal community.*

*If you have suggestions for additional terms or expanded or clarified definitions for the current terms, email fintechglossary@lw.com.*

*Additional* Books of Jargon®, *including*

Emerging Companies
European Capital Markets and Bank Finance
Global Mergers & Acquisitions
Global Restructuring
Healthcare & Life Sciences
Hedge Funds
International Arbitration
Master Limited Partnerships (MLPs)
Oil & Gas
Patent Trial & Appeal Board (PTAB)
Project Finance
US Corporate and Bank Finance

*are available at LW.com.*

*51% Attack:* when one or more persons collectively controls more than 50% of a network's computing power and maliciously uses their Hashing power to reverse Confirmed Transactions, interferes with the process of recording new Blocks, prevents new transactions from gaining Consensus, allows Double Spending of the local currency, or takes 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.

*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.

*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.

*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.

*API:* acronym for Application Program Interface

*Application Program Interface:* 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):* computer hardware that is designed for one particular function, such as running the Hash Algorithms used to Mine a specific cryptocurrency like Bitcoin or Litecoin.

*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.

*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 …

*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.

*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.

*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 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. 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-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.

*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).

*BSA:* acronym for Bank Secrecy Act.

*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.

*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).

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

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

In contrast, see Decentralized Exchange.

*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.

See also Private Blockchain. In contrast, see Decentralized Network.

*CFTC:* acronym for Commodity Futures Trading Commission.

*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:* originated by Tim Swanson (former director of market research for Blockchain consortium R3), the term Chainwashing refers to the widespread use of the word "Blockchain" among vendors as a marketing buzzword, even though many such vendors lack an economically viable Blockchain-based product.

*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 Crytpocurrency 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.

*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.

*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 would include 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.

*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.

*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).

*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.

*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.

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

*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: 1) it is deterministic, meaning the Hash Function always produces the same result; 2) it is fast, meaning it returns the Hash of an input very quickly); 3) it is pre-image resistant, which basically means that it is virtually impossible to determine the original input data from its Hash value; and 4) 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:* the writing or cracking of codes.

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

*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.

*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.

*Dapp:* acronym for Decentralized Application.

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

*Decentralized Application (Dapp):* 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.

*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.

See also Public Blockchain. In contrast, see Centralized Network.

*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).

*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.

*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: 1) contracts to buy or sell something for future delivery, such as forwards and Futures Contracts; 2) 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; 3) contracts to exchange one cash flow for another, such as Swaps; and 4) many combinations of the foregoing.

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

*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.

*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.

*DLT:* acronym for Distributed Ledger Technology.

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

*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.

*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.

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

*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 key exchange.

*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

*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").

*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 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.

*EVM:* acronym for Ethereum Virtual Machine.

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

*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).

*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.

*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.

*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 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.

*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, Soft Fork.

*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.

*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.

*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: 1) a standardization of terms; 2) the opportunity to offset; 3) the right to liquidate rather than take physical delivery; and 4) no specified right to any particular lot of Commodity.

*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.

*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.

*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.

*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.

*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, 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 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, 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.

*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.

*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."

*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.

*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.

*ICO:* acronym for Initial Coin Offering; pronounced "eye-see-oh."

*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.)

*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.

*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.

*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.

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

See also OTC Broker.

*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.

*Irreversible Transaction:* a transaction that can not 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 deciding 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.

*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.

*KYC:* acronym for Know Your Customer.

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

*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.

*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.

See also Limit Buy, Limit Sell. In contrast, see Market Order.

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

See also Limit Buy, 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.

*Long / Long Position:* a position taken by an investor that 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.

*Market Capitalization:* 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.

*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 absolutely nothing to do with German Chancellor Angela Merkel or Duchess of Sussex Meghan Markle.

*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 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.

*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.

See also Staking, 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.

*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: 1) dealer in foreign exchange; 2) check casher; 3) issuer of traveler's checks or money orders; 4) provider of Prepaid Access; 5) Money Transmitter; and 6) US Postal Service; and 7) 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.

*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.

*MSB:* acronym for Money Services Business

*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).

*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, Lightweight Node.

*Nonce:* a random or pseudo-random number added to a hashed Block that, when rehashed, meets a Blockhain'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-Fungible Token:* a Token that represents something unique and which is neither interchangeable (*i.e.*, cannot be replaced with another Token of the same type) nor divisible. Non-Fungible Tokens are used to create unique verifiable digital identities, and are employed in applications that require unique digital items (*e.g.*, crypto-collectibles, crypto-gaming).

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

*NYSDFS:* acronym for the New York State Department of Financial Services.

*OFAC:* acronym for Office of Foreign Assets Control.

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

*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.

*Oracle:* an interface with a data source external to a Blockchain that provides 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:* acronym for Over the Counter.

*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.

*P2P:* acronym for Peer to Peer.

*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.

See also Public Blockchain. In contrast, see Permissioned.

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

*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.

*POS Consensus Model:* 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 he or she has. 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.

*POW:* acronym for Proof of Work.

*POW Consensus Model:* a Consensus model in which the Publishing Nodes in a Blockchain network compete against each other to complete each Blockchain transaction. In this model, each transaction is completed when a Publishing Node solves a complex mathematical puzzle (resulting in a Block Reward for the Publishing Node).

*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.

*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.

See also Permissioned. In contrast, see Public Blockchain.

*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, Reg S.

*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 POS/POW.

*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 pseudonymous, which would more easily allow fraud.

*Proof of Stake (POS):* a method that allows users to Mine Blocks according to the stake they hold (*i.e.*, the more Coins a user holds, the more Mining power a user has).

*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 application of a Blockchain.

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

See also Public Key. In contrast, see Private Address.

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

See also Permissionless. In contrast, see Private Blockchain.

*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:* 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.

*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.

*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. The amended Reg A is sometimes referred to as Reg A+.

*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.

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

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

*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.

*Satoshi:* a unit of measurement of 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.

*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.

*SEC:* acronym for Securities and Exchange Commission.

*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, 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 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.

*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.

*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.

*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, Hard Fork.

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

*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).

*Staking:* the purchase and holding of a quantity of Cryptocurrency for a defined period of time.

See also POS.

*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.

*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.

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

*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.

*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.

*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.

*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.

*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, 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: 1) something they know; 2) something they have; or 3) something they are. Thus, for example, a user can access his or her data with a username, password, and a 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.

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

See also Consumer Token, Security Token.

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

*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.

*Virtual Currency:* "a medium of exchange that operates like a currency in some environments but does not have all of the attributes of real currency … [and] does not have legal tender status in any jurisdiction." Reference: FinCEN, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (March 18, 2013).

*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.

*Wallet (Hardware):* a physical device similar to an external drive used to secure Cryptocurrency by storing a person's Private Keys offline. As 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.

*Wei:* the smallest denomination of Ether, equal to 1/1,000,000,000,000,000,000 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.

*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.

*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. A 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 a Zero Knowledge Proof, a protocol must satisfy three requirements: 1) Completeness: If the statement is true, an honest verifier will be convinced by an honest prover; 2) Soundness: If the statement is false, no cheating prover can convince an honest verifier that it is true; and 3) Zero-knowledge: If the statement is true, no cheating verifier learns anything other than the fact that the statement is true.

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

**LW.com**

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