

51% Attack: Consider this concept as sort of a “hostile takeover” of a cryptocurrency; it's possible in theory, but most industry experts doubt it's very likely. The process of mining blocks of digital currency data often takes considerable computing time and energy. It's conceivable that a miner or mining pool could expend the computing resources necessary to control more than 50% of the total computing power devoted to the currency's network, and once they have majority control, they could “take over” and do some damage. For example, they could reverse current and new transactions, and could keep new data blocks and currency from being created. They would create more of an interruption than anything else, but they would not be able to “steal” currency or hack other investors' accounts. Gaining more than 50% of a digital currency network's computing time would take a lot of energy and computers, which in and of itself would be very expensive. Additionally, that percentage would have to be sustained over a decent period of time in order to do any damage. While it's a potential threat—and since it's dramatic, it makes for good media copy—it's unlikely to happen. The work-to-reward wouldn't be worth it.

Airdrop: The term airdrop is sometimes used to describe the process of distributing tokens to wallets. For example when the network of an ICO or fork goes live the newly created token might be airdropped to wallets of existing coin holders.

Altcoin/Alt: An altcoin (sometimes just called an “alt”). Any coin that isn't Bitcoin.

Alt Season: The part of the overarching cryptocurrency market cycle where many altcoins “moon” (go up quickly in price) against the dollar and Bitcoin at once (for example, late December 2017 – early January 2018).

All Time High (ATH): The highest price a given cryptocurrency has seen so far. Not the ideal place to buy an asset.

Anonymous: Your name is completely obscured. A case where no one could figure out your identity, no matter what.

Application Specific Integrated Circuit (ASIC):

An Application Specific Integrated Circuit (ASIC) is a computer chip created to perform one specific function, and only that function. Since mining of cryptocurrency data blocks can demand a lot of computer space and time, some miners set aside entire devices—or partition off a section of their computers—to do nothing but mining.

ASIC Mining: Out-of-the-box computer systems that you buy at electronics stores usually don't include the processing power that's necessary for the cryptocurrency mining process. As a result, many miners purchase separate computing devices set aside solely for mining. As an alternative, they can also get an Application Specific Integrated Circuit (ASIC); this is a specially-designed computer chip created to perform one specific function, and only that function—in this case, mining calculations. ASICs reduce the processing power and energy required for mining, and can help reduce the overall cost of the process in that way. Whether the ASIC—a term that refers to the specialized chip itself—is integrated into an existing computing system, or functions as a stand-alone device, the term “ASIC” is often used generically to refer to the overall system itself, and not just the chip.

Asymmetric Key Algorithm:

This is the algorithm used to generate public and private keys, the unique codes that are essential to cryptocurrency transactions. In a symmetric key algorithm, both the sender and receiver have the same

key; they can encrypt and exchange information privately, but since both parties have the decoding information, they can't keep information private from one another. With an asymmetric key algorithm, both parties have access to the public key, but only the person with the private key can decode the encryption; this assures that only they can receive the funds.

Asset: Something of value, often held as a store of value or wealth.

Backwards compatible

In accord with previous protocols. In the case of cryptocurrencies, a software update that is backwards compatible will not mess things up by creating a hard fork.

Bart: A chart pattern that looks like the hair of a famous cartoon character.

Bearish / Bullish: A bear market is when the price trend is stagnant or downward. A bull market is when the price trend is upward. Those terms are used in different ways, but as a general rule: bull means “up,” and bear means “down.” A bull charges forward, a bear mauls your face, eats your picnic basket, and then hibernates in a cave for months.

Bear Trap:

This is a manipulation of a stock or commodity by investors. Traders who “set” the bear trap do so by selling stock until it fools other investors into thinking its upward trend in value has stopped, or is dropping. Those who fall into the bear trap will often sell at that time, fearing a further drop in value. At that point, the investors who set the trap will buy at the low price and will release the trap—which is essentially a false bear market. Once the bear trap is released, the value will even out, or even climb.

Bit: The tiniest amount of computer code, defined as a 1 or a 0.

Bitcoin: Bitcoin is decentralized and distributed software that allows for trustless peer-to-peer global financial transactions and record keeping. It can be described as a blockchain based smart contract system with a native cryptocurrency token.

Bitcoin Price Index (BPI): For the first few years of Bitcoin's existence, it was difficult for investors to firmly establish what their accounts were worth; the comparative value of Bitcoins against other currencies would vary from exchange to exchange—and sometimes vary quite wildly. In September 2013, digital currency news organization Coinbase decided to remedy the situation, and they created the Bitcoin Price Index (BPI). The BPI gathers information from the largest and most influential Bitcoin exchanges in the world, and applies the aggregated statistics to reach a more balanced and realistic picture of the currency's market value. The BPI has a set of criteria—best practices guidelines for the exchange industry, if you will and exchanges that don't meet or accept these criteria aren't included in the BPI statistics. The strict adherence to these standards—and the accurate information that results have given the BPI a strong reputation in the cryptocurrency trading industry.

Block: This is a collection of transaction data, one of the fundamental elements of cryptocurrency. As transactions are made, the pertinent information for each one is collected—and when the gathered data

reaches a predetermined size, it's bundled up as a block. As soon as possible after blocks are created, they're processed by investors for transaction verification; this process is known as mining.

BlockChain: Blocks of cryptocurrency transaction data don't stand alone. As they're created and processed, they're interlinked with other blocks into what's known as a block chain. On rare occasion, errors in transaction data are not found immediately, or in the block in which their information is embedded; however, as the processing, or mining, continues, information in the block chain is reviewed repeatedly. Therefore, the further down the chain a transaction is, the more secure and correct its details are.

Block Height: Blocks are added to the blockchain sequentially. The current block number is called the block height.

Block Reward: This is the “payoff” given to a miner who has successfully calculated the hash in a data block during the mining process. Since the verification of this data generates new coins, a portion of those will go to the miner. The block reward can also include a percentage of the transaction fees associated with the processed block. The new coins minted by the mining process, by the way, are called “virgin” coins, since they're brand new and have not yet been used for any transactions.

Block size: describes the amount of data that can be added to a given block on the blockchain. Bigger blocks allow for more transactions to be stored in blocks, but as a trade-off, more hash power is required to mine a block. This makes transactions faster, but one can argue centralizes mining. In crypto, almost everything is “a trade-off,” just like IRL (In Real Life).

Bots: Almost all exchanges let users program or use a pre-programmed software that can interact with crypto platforms via an API. One type of software, a type that can execute trades on exchanges, is called a “trading bot” (often referred to as simply a “bot”). It may seem like cheating, and in certain hands, it can sure feel like it, but bots are important in many ways too. They can help implement strategies like trailing stop losses for you, and they can help “make markets” (all those little buys and sells that prevent wide spreads in a given market are generally “market maker” / “accumulation” bots). Like people, bots aren't good or bad, they are neutral and depend on the ethics of the user.

Bot Trading: The majority of investors in digital currency use manual methods when they want to buy or sell their cryptocurrency of choice. However, there are now programs available for investors that have been created to make the process more precise and automatic. They download these programs, which monitor alternative currency exchanges and markets for them. These “bots” will carry out transactions automatically according to the price criteria the investor has set. There are those who argue bot trading is a little too reactionary, and that sales and purchases will be made on a “knee-jerk” level, rather than waiting for the market to stabilize. On the flip side of that coin, bot trading advocates insist the method will work in their favor, since they can't personally monitor the markets 24/7.

Brain wallet: Creating a new set of public and private keys and memorizing them. This creates a system where the only place your crypto to currency is stored is in your mind.

Bull Trap: A bull trap is “set” by investors in a stock or commodity who will buy large amounts in order to artificially drive the value upward, or create a false bull market. Traders who are fooled by the bull trap will often buy shares at the inflated price, in the belief that the upward trend will continue and the shares they're buying will rise in value. Unfortunately, those who fell into the bull trap will often be left holding shares for which they paid too much, since once the trap is released, the market evens out, and sometimes even drops.

Bubble: A bubble occurs when a market is driven upward by investors; this has happened in the dot-com and housing industries in the past decade or so. Factors such as industry popularity, speculation of potential worth, political influence, and many other things can combine to create these spikes in value. If the market is perceived to have “topped out,” or investors believe it will no longer retain its overall worth, the bubble can “burst.” This represents a massive sell-off by investors, which can make market value drop sharply. Depending on your perspective, some cryptocurrency markets may or may not have experienced periodic bubbles. The industry's naysayers insist the market is too volatile, and will continue to roller-coaster up and down, with no real stability in sight. Conversely, industry insiders claim these are the growing pains of a new field, and that digital currency fluctuations will smooth out over time.

Buy Low, Sell High / Buy High, Sell Low: To not lose money, you should aim to Buy Low, Sell High. Try not to Buy High, Sell Low. Remember to set stop losses and when all else fails, HODL.

Buy Order: A buy order is established when an investor approaches an exchange and wants to purchase cryptocurrency. These can range from very simple orders (“I want to spend x amount of dollars on Bitcoins”) to complex ones that include factors such as time frame in which the order should be filled, range of price, and so forth. Most exchanges allow for these to be entered online, but some investors prefer to go over the details directly with an exchange representative. Buy orders don't necessarily guarantee your purchase; if your price is too low, for example, the offer may expire without being filled unless you make adjustments.

Buying the Dip: If you are going to average into a coin, can't do better than buying the dip (especially in a bull market, in a stagnant market, or at what you think might be the end of a bear market). This means buying when the price goes down. For building a long-term position, it works much better than buying when the price goes up. It also helps the market as you are part of the force stopping the dip instead of part of the force causing the run-up.

Candlestick Chart: This is a popular at-a-glance type of chart that is commonly used in stock and commodity exchanges. Some charts use a dot to show where a certain stock or commodity closed on a given day; while this is valuable information, it doesn't show the range of price the commodity experienced during the trading day. With a candlestick chart, a vertical bar is used to show the scope of activity in a trading day; the upper edge of the bar will be the opening price (in a bear market), and the lower edge denotes the closing price (also in a bear market; in a bull market, the two are reversed). Lines extend out of the top and bottom of the bar, showing the highest and lowest trading prices for the commodity for that day (thus forming the “wick” of the candle). Candlestick charts are ideal for showing day-to-day market activity in a concise—but still accurate—way, denoting the full range of activity for that period.

Client: A program that relies on a server to feed it information or complete its task. For example, web browsers are clients in that they require information from a web server.

Cold wallet: A place to store public and private keys that resides offline. Since keys are not connected to the Internet in any way, they are less susceptible to being hacked.

Collateral: Something pledged when taking on a loan which, if the loan is not repayed, will be sold in order to payback the loan.

Collective Mining: The commitment of resources and materials to the process of mining digital currency data blocks often proves to be too expensive for individuals to take part. As a result, many enterprising businesses have worked out a way to make mining more affordable for those miners who would otherwise be left out. These companies invest in the hardware that allows for high-end mining power, and they in turn lease the access to this mining capability to third parties. As an individual miner, this means you can sign a contract that allows you to use a predetermined amount of mining power through cloud computing, without the hassle or expense of buying or maintaining the processing power needed to do so. The block rewards that come with the successful mining of the data block go to the individual miner who purchased the contract from the collective mining company.

Confirmation: When a block of transaction information is successfully processed, or mined, all the transactions within that data block are considered confirmed, or validated. Depending on the type of cryptocurrency, the confirmation time for transactions can vary anywhere from 30 seconds to several minutes; longer validation times—though considered a small inconvenience to those making transactions—are generally considered to be more secure, since a “closer look” is being given to the data as it is mined.

Consensus: Agreement; the necessity for miners to agree on the validity of a blockchain. There are multiple methods by which miners can agree on validity, the most popular of which is called proof of work.

Consortium Blockchain:

A blockchain where the consensus process is controlled by a pre-selected set of nodes. Popular among private organizations but not as useful for digital currencies

Continuation Graph Pattern: When you take a look at a market value graph on a digital currency exchange site, you'll be able to see at a glance the upward (“bull” market) and downward (“bear” market) trend lines. However, on occasion you'll see graph patterns that show fluctuations that go against the flow of the current trend, only for the trend to continue in the same direction afterward. This type of graph pattern is known as a “continuation” type; though there may be momentary up-and-down movement in a currency's value, from a macro view the trend hasn't really changed direction. Continuation graph patterns show that investors have tested the current trend and found it to be sound—therefore, it continues.

Correction: After hitting a high, a coin will likely enter a period of correction where it steadies out at a given price before rising again (ideally it rises again from there, sometimes a correction simply spurs on a long “bear market”). In cryptocurrency coins often hit all-time highs and then enter correction periods. In these correction periods we may see “corrections” of 10% or even “crashes” of 20% or more.

Crowdsourcing: The process of receiving funding from a large number of people. Instead of having a few investors give a lot of money each, companies look for many investors to put in small amounts.

Cryptoassets:The broadest term for a blockchain-based store of value. Cryptocurrencies, tokens, and ICO's could all be considered under the umbrella of cryptoassets.

Cryptocurrency:Crypto is a word root that comes from the Greek for “hidden” or to hide;” for example, cryptography is the process of coding written messages. Cryptocurrency is a financial tool that takes the form of long blocks of alphanumeric code, and this alternative currency is traded between investors and used as a form of payment for goods and services to merchants who accept it. Unlike traditional bill-and-coin currency such as the US dollar, cryptocurrency is not directly tied in to any government, corporation or bank, and is therefore not susceptible to inflation, regulations or charges and fees that affect traditional legal tender. Cryptocurrencies are relatively new; the first to be publicly introduced was Bitcoin in 2009. Cryptocurrency is also known by the terms “digital currency” and “alternative currency.

NOTE: Sometimes the term token is used to specifically refer to tokens that are created on distributed platforms like Ethereum. ERC-20 tokens exist on the Ethereum network alongside the native token, Ether. Despite the term token sometimes being used to refer to ERC-20 tokens (and other tokens of this sort), all cryptocurrencies are technically tokens in that they are “value tokens” and in that transaction can be represented by a string of encrypted data called a “token.”

Cryptography:The process of making something secret or hidden.

Cryptotokens:A cryptoasset that is redeemable for something or usable in some way.

Cybersphere:Unnecessarily fancy word for the Internet.

Cypherpunks:A group of digital pioneers first active in the 1980's who sought to defend digital privacy through various cryptographic measures. First spoke of a need for digital currency.

Cup and Handle Pattern:This is a pattern that appears on market value graphs when investors want to test the validity of an upward, or “bullish,” trend in a commodity market.

The upward trend, due to investor buying and selling, will gradually slope downward, then back up again, in a gently-sloping “Letter U” shape. After this “cup” is formed, the market will be tested again briefly, making a quick downward slope that's considerably smaller (and shorter in duration) than the

“cup” preceding it; this forms the “handle” to the teacup shape. The cup and handle is considered a “continuation” pattern, in that, once the handle is formed, the upward trend will continue.

DAO:Short for Decentralized, Autonomous Organization. Large mechanisms that can self manage and perform various functions, often including smart contracts as a component. Often built on blockchain platforms such as Ethereum.

DCA: Dollar cost averaging. Instead of going all in at once, one might want to dollar cost average into a volatile asset like a cryptocurrency to buy the average price over time to create a long position. There are a number of forms of “averaging,” dollar cost averaging is one of the more popular.

Decentralized:This is a term you'll hear often when cryptocurrency is being discussed. In this context, it means the currency isn't issued or controlled by a centralized authority, such as a bank or government. While this means cryptocurrency isn't directly affected by inflation or governmental regulations—which its advocates insist makes for a more level international playing field—it also means its investors carry more responsibility for its well-being. They should be aware of the risks

inherent with cryptocurrency, such as value fluctuation and the lack of institutional protections against theft and fraud. There's no FDIC for digital currency—as there is in the centralized US banking system—so once it's stolen, it's gone forever.

Decentralized app (dApp):

An application that has back-end code running on a decentralized network instead of a central server.

Demurrage: This is a charge levied against the accounts of investors who don't use their digital currency for transactions, but just leave it sitting as a long-term investment. Some cryptocurrencies use this as a way to keep their currency in circulation, and to prevent hoarding. After all, it's in the issuer's best interest to keep their currency active; it makes it more stable and supports its value. If you're looking to invest in cryptocurrency—and not necessarily use it for purchases—you'll want to shop around to see which ones carry demurrage fees.

: A Decentralized EXchange (a peer-to-peer exchange with no middleman). Many DEX exchanges exist on the Ethereum platform as Dapps. One example is EtherDelta.

Difficulty: The term “difficulty” here refers to how easily a data block of transaction information can be mined successfully. Each type of cryptocurrency has algorithms (such as SHA-256 and Scrypt) that determine the mining difficulty for their corresponding coins—and adjust those difficulties as circumstances warrant. Setting the difficulty for cryptocurrency mining is a challenge, one that needs to strike a delicate balance. Make the process too easy, and miners will flood the market with too many new coins created by the mining process. Make it too difficult, and miners will lose interest in taking part. The latter has become an issue with more popular digital currencies like Bitcoin; its difficulty has risen to the point that most individual miners can't justify the added cost of specialized mining machinery. Collective mining (where miners can contract mining power from third parties) has eased this somewhat, but many prospective miners are looking for newer and “easier” currencies to mine.

Digital Asset: Not every cryptocurrency is meant to be a currency. If it is a digital store of value, it can be called a digital asset (both Cryptokitties and Ether are digital assets, but only Ether is a cryptocurrency token). Digital assets can be fungible or non-fungible. Cryptokitties are represented by non-fungible tokens (meaning unique tokens that can't be replaced and still retain value; sort of like hand crafted one-off artworks) unlike Ether which is fungible tokens (all Ethers are equally valuable, there is no specific unique Ether that is worth more or less than other Ethers; like how dollars work).

Distributed Denial of Service (DdoS): To anyone who maintains any kind of online presence, this term represents a potential nightmare. The letters DDoS are almost always followed by the word “attack,” because that's exactly what it is. A DDoS attack begins when the attacker rounds up hundreds, if not thousands, of “zombie” computers; this is achieved by downloading trojans or viruses onto remote computers without the owner knowing. Once the zombie network is in place, the attacker targets one website, email server or network, and directs all the zombie computers to flood the victim with tasks or requests. This coordinated attack can bring a website or network to its knees; DDoS attacks commonly crash servers and make websites temporarily disappear until the attack can be traced and halted. Several cryptocurrency exchanges have been the targets of DDoS attacks, which are often politically or personally motivated. Webmasters and server owners can avoid DDoS attacks with powerful security measures such as firewalls, but the main issue remains in the hands of individual computer owners. Since the “zombie” trojans and viruses tend to work invisibly in the background, the members of a zombie computer network never know they're part of it. In order to avoid such an

infestation, computer owners should download a current (and easily updated) security program that searches their systems for malware and spyware.

Distributed: Something split into many pieces and separated out. Mining power in blockchain systems is said to be distributed.

Double spending: the practice in which a coin holder applies the same currency to two different transactions—is a concern with zero confirmation transactions. Since cryptocurrency is not “attached” to the person spending it in any way, by the time their double spending is discovered through the mining process, they are long gone and untraceable. With the demand for zero confirmation transactions on the upswing, entrepreneurs in the cryptocurrency industry are looking at ways to instantly verify—or deny—transactions without having to wait for mining to take place. In the meantime, many businesses levy fees to offset the financial risk of zero confirmation transactions, and yet others are refusing to accept them until the technology catches up.

Due diligence: Research conducted before making any kind of investment. Even if someone recommends an investment to you, smart investors will always conduct independent research.

DYOR: Do Your Own Research. Listening to the person on the internet is step 1, step 2 is doing your own research and making your own investment choices. A Reddit thread is not your fiduciary. For example, I have no specific certification that qualifies me to write a list of crypto acronyms. If you did your DD (Due Diligence), you would know that.

EMA: Exponential Moving Average. A line based on price action over time that helps traders to spot trends.

EW: Elliot Wave. A pattern that the price movement of assets tends to make. Used in technical analysis.

F.U.D.: Fear, Uncertainty and Doubt. This is usually disseminated by people and/or companies to put others at a disadvantage.

Faucet: If you're a business owner, and you want to generate publicity for your product or service, what's the best way to do that? Well, free stuff, of course! People will line up around the block for a chance to pick up something for nothing. This lesson hasn't been lost on the cryptocurrency industry, and there are many places online where those interested can stop by and request some shiny virtual coins for free. The sites that offer free digital currency are called “faucets.” Of course, those running the faucets aren't just doing it out of the kindness of their sainted hearts. The amounts of currency given away on faucet sites are quite small, and they offer just enough of a taste to get potential investors interested in picking up more—and not for free this time around. Faucet owners also tend to offer advertising on their sites as another way to offset the cost of giving away some of their currency for nothing. On occasion, either lack of investor interest or shortage of funding will cause a faucet site to shut down; when that happens—in keeping with the terminology—that faucet is said to have “gone dry.”

Fiat Currency: “Fiat” is the Latin word for “it shall be,” so that translation isn't of much help to us here. In a nutshell, a fiat currency is a financial tool that is not backed up by any physical commodity or goods; essentially, it exists and flourishes simply because the people who use it believe in it. While that

might sound like a somewhat shaky proposition, it should be pointed out that the majority of currencies in the world including cryptocurrencies—are fiat currency systems. They can be used for transactions—and are viable for trade in their own markets—because those who use them—be they governments, banks, or individual investors—have faith in their validity as a financial entity. Should that faith be lost—the Confederate States of America currency, or the “Dixie Dollar,” is a prime example—the currency loses its value. In theory, all fiat currencies have the potential to become worthless—banks can fail, governments can fall—so they rely very heavily on that faith.

In contrast, a lot of people don't realize the United States dollar wasn't always a fiat currency. All currency issued in the US used to be backed by a proportional amount of silver or gold; if you hear the terms “gold standard” or “silver standard,” that is what they used to mean. However, due to economic factors, by 1973 the US dropped both the gold and silver standards, making the dollar a full fiat currency.

Fibonacci: Fibonacci brought modern mathematics to the west in many ways. He also popularized a set of ratios that are commonly used in trading to find support and resistance levels (Fibonacci retracement levels); they pair nicely with EW.

Fill or Kill: This is a simple type of buy order made with a cryptocurrency exchange. The investor dictates how much currency they want, and at what price, and establishes a cutoff date for the order. The exchange will then do their best to fill the order according to those criteria. If the exchange hasn't found an appropriate match for the order by the cutoff date, the order is canceled and left unfilled. In other words, fill this order according to these guidelines and within this time frame. If you can't, kill it.

FOMO: The Fear Of Missing Out. The emotional response that makes people impulse buy tokens at their all-time high. Try to not react to FOMO.

Fontas: This isn't so much a “what” as it is a “who.” Fontas is a mysterious investor or group of investors who has been using pump and dump schemes to manipulate the value of various digital currencies. That is to say, he/she/they have been buying large amounts of currency at low prices, then they've used misleading information to get other investors to buy, falsely inflating the currency's price. At that point, Fontas sells a large chunk of their cryptocurrency investment for a sizable profit. Thus far, Fontas' focus has been on Bitcoin, but they are trying to do the same with Litecoin and Namecoin; however, investors are on to the scheme. Needless to say, Fontas is not exactly the most popular investor in the alternative currency industry. However, even savvy investors who weren't taken in by Fontas' scheme have to grudgingly admit its effectiveness.

Fork (Cryptocurrency Forks): Like a “save as” for software. When an update is made to the software, a new version and old version are created. Soft forks are meant to be updates to the existing software (generally a blockchain or software that interacts with the blockchain in cryptocurrency). Hard forks are meant to create two identical versions of the software which can both change after the hard fork occurs. Anyone who owns tokens on one blockchain owns tokens on the new one in most cases when a fork occurs. There are other types of forks, but that is the gist. Bitcoin forks have names like Lightning, Segwit, Bitcoin Cash, etc. I can't get into every funky name here, but they are all either soft forks or hard forks meant to upgrade the chain or create a new one.

Forging: The process of adding blocks (and validating transactions) in a proof of stake consensus system.

FUD: Fear, Uncertainty, and Doubt. The emotion that people try to invoke in others when they want to bring the price of a coin down or drum up headlines. It can be smart to react to FUD, as one can't stop widespread FUD from spurring on a correction, especially after a coin just hit an All Time High. FUD is what causes economic depressions. It is what makes bubbles burst. FUD can be warranted or not.

Gas: The Ethereum network requires one to pay "gas" to send a transaction or otherwise execute a smart contract. Gas can be paid in ether (but it is calculated in GWEI, where a GWEI is 1/1000000000th of an Ether).

Genesis Block: In the cryptocurrency mining process, blocks of data are processed and validated one by one, and each of these blocks are linked in chronological order, forming what is called a block chain. But every chain has to start somewhere, and the very first block of data mined in order to launch an alternate currency is known, appropriately enough, as a "Genesis block." The main way in which a Genesis block differs from all the other blocks on the chain following it is that the Genesis block will have its "previous hash" data set to all zeroes. This indicates that no other data was processed before the block in question; all other blocks will have other numbers in this data field.

The most famous Genesis block generated was Block 0 of the Bitcoin chain, created by the currency's founder, Satoshi Nakamoto, in January 2009. Genesis blocks are almost always mined by the creator of a given digital currency—and sometimes several other subsequent blocks, as well—to establish the coin before it's released to the general public. In comparison, for cryptocurrency types that have failed and no longer exist, the final block of data mined for such a currency is referred to as the "Omega block."

Graph Gaps: On occasion, gaps will appear in trend lines on market value graphs. These gaps indicate a visible drop or rise in a commodity's value that hasn't necessarily happened due to trading. These can be the result of closed markets, statistical adjustments by analysts, or by strong news about the commodity. There are three types of gaps:

- 1. Breakaway Gap.** These appear at the beginning of a strong upward or downward trend, and represent very high-volume trading.
- 2. Runaway Gap.** These occur during an upward or downward trend, and represent a quick momentary intensification of that trend.
- 3. Exhaustion Gap.** This occurs toward the end of an upward or downward trend, and tends to indicate a small trend in the opposite direction.

Hard fork:

A hard fork is a protocol change that results in an entirely new blockchain with an entirely new currency. Before the change, all transactions are valid, and after the fork two blockchains will exist with two currencies. Example: Bitcoin and Bitcoin Cash hard fork.

Hash: This is a random and complex mathematical formula used in the verification of blocks of transaction data in the process known as mining. Once a miner calculates the proper hash in a block, they're rewarded with coins and a percentage of the transaction fees embedded in that block. Achieving the right hash in a given block can take several tries and calculation adjustments—and some blocks, even though properly processed, may not "pay out." The difficulty of calculating the hash in a block is set fairly high, so the rewards aren't distributed at too fast a rate; after all, mining also helps create new coins, and the mathematics are set so this doesn't happen too quickly—that could destabilize the currency.

Hash Rate: The hash rate is the speed at which complex mathematical calculations are performed in the mining of cryptocurrency data blocks. What this measurement boils down to is: the higher the hash rate of a mining system, the more data blocks can be successfully mined—which in turn means more block rewards for the miner or miners involved. As some types of digital currency become more popular—and the mining as a result becomes more competitive—the hash rates required for successful mining can increase as a result. Higher hash rates often require specialized computing equipment, and the use of more energy. Also, more complex mining algorithms such as SHA-256 require higher hash rates than simplified systems like Script.

The following terms are used for mining hash rate measurement:

KH/s: Kilohashes per second, or one thousand hash computations per second

MH/s: Megahashes per second, or one million hash computations per second

GH/s: Gigahashes per second, or one billion hash computations per second

TH/s: Terrahashes per second, or one trillion hash computations per second

PH/s: Petahashes per second, or one quadrillion hash computations per second

Hash Power: The rate at which a given piece of hardware can mine a coin (mining is the cracking of cryptographic codes). It is like horsepower but refers to how fast hardware can decrypt hashes.

HODL: A misspelling of “hold” pronounced “HOD-L” based on a forum post from 2014 that some in the crypto community have decided now means “Hold On for Dear Life.” This is what you have to do when coins enter their common 20% – 80% corrections if you want to come out the other end still owning coins.

ICO: Initial Coin Offering. A new way of crowdfunding where a company creates a token and sells it. People buy tokens in the hopes that they will rise in value as the company does. Many think ICO's might be classified as securities in the near future.

Keys (Cryptographic Keys): Cryptocurrency is largely based on public-key cryptography. The concept is that one key can be known publicly (the public key) and the other can't (the private key). The public key is encrypted from and linked to a private key that can't be known. In cryptocurrency, your public address is a hash of your public key. It lets people send you crypto. Meanwhile, your public key is a hash of your private key. Your private key lets you access the crypto associated with a public address. To resume, a public address is the public account number people can send coins to; it has a public key, which is a hash of a private key. Meanwhile, the private key is like a unique personal password that lets you access an associated address in your wallet and send coins from it by creating a signature (a signature essentially an encrypted version of your private key). Never share your private keys, as they are the root of all the information needed to access one's crypto!

Key Pair: A public and private key associated with a cryptocurrency address. When an "account" on a blockchain is created, the account consists of a public key and a private key.

Inflation: In financial terms, inflation indicates the general trend of rising prices for consumer goods and services. As a result—unless consumers' income matches the rate of inflation—it means consumers have a lower level of purchasing power as prices go up. Banks and governments often do whatever they can to stop long periods of excessive inflation, just as they do the same for its opposite, deflation—or a sustained drop in prices. Though inflation is a natural financial process, most countries try to keep the rate of inflation at a more manageable level of 2-3%; the majority of consumers are able to adapt more readily to these rates. Inflation can also apply to assets, such as a home or an investment portfolio. In the spirit of “buy low, sell high,” many savvy investors will wait until a given commodity has shown

a long and sustained period of asset inflation before selling (at a substantially higher price than they initially paid), and will often then turn around and buy a commodity that shows indications of an oncoming inflationary trend. Like most commodity trading, this concept applies to cryptocurrency investing.

Issuer

We admit openly that we use this as a term of convenience when we talk about cryptocurrency. With traditional currency, the issuer would be the US Treasury for American bills and coins, for example. Technically, digital currency coins aren't issued, they're created by the mining process. There's no central bank, no government deciding when new cryptocurrency comes into being; it's "minted" when investors mine the data blocks. There's really no one owner of Bitcoin, and no corporate board making the decisions; all of its investors have a vested interest and a share in it. As such, when we use the term "issuer," we mean the investors in a type of cryptocurrency; we use it conceptually and not literally.

Laddering: Setting incremental buy or sell orders.

Lambo: Lambo is short for Lamborghini. A Lambo is sort of a status symbol, goal post, and/or meme. Somehow everyone's cognitive dissonance kicks in and there is this assumption that everyone who owns any amount of any tokens will somehow be driving a Lamborghini within the next 6 months. While it isn't impossible, the only real bit of insanity here is trading in your coins for a physical object like a car [even a very cool car]. SAD!

Ledger: Something used to record transactions, an itemized list of transactions.

Leverage: A measure of how much money is borrowed during margin trading. A ratio of how much money is borrowed compared with how much money is put down as collateral. 1:1 leverage means not borrowing anything. 1:100 leverage means borrowing 100 times more than is offered as collateral.

Light client: Most wallets; accesses only the most recent information on the blockchain that's relevant to your particular account at the time, rather than storing the entirety of the massive file that is the blockchain.

Liquidity: The ease and quickness with which an asset can be bought and sold at the actual market price. Higher market volume often denotes higher liquidity. The most liquid asset is money itself and an example of an illiquid asset might be real estate.

Long / Short: Going long means betting on the price going up, going short means betting on the price going down.

MA / EMA / MACD: Moving Averages (MA) track help people understand the trend of a coin over time. Moving Average Convergence Divergence (MACD) shows the relationship between two moving averages of prices. The MACD is calculated by subtracting the 26-day Exponential Moving Average (EMA) from the 12-day EMA. When these lines cross, they can tell us about the general trend of the asset. We would be looking for Death Crosses and Golden Crosses. Feel free to Google those terms, specifically check out Investopedia.

Main Net: The main network a cryptocurrency and its blockchain live on, as opposed to the Test Net (test network where developers and users can test transactions).

Maker/Taker: Maker fees are fees associated with limit orders. Taker fees are fees associated with market orders. This only applies to exchanges that use a Maker/Taker model and is only relevant when one fee type is lower than the other. GDAX is an example of an exchange where this matters. On GDAX maker orders have no fees, but taker orders do.

Masternode: A network overlaying a traditional consensus mechanism that allows for additional features. First shown in the Dash system. Masternodes are nodes that have voting rights. Masternodes generally get a cut of mining rewards and require locking up a large amount of a given crypto while running the node.

Margin call: When trading with borrowed money, an exchange can margin call you and sell off collateral if your position reaches a critical point where it must be closed. Margin called = you have to pay up.

Margin trade: To trade using a loan. The act of borrowing money in order to make an investment.

Mining: Cryptocurrency transactions are bundled together in packets of data that are called blocks. The timely processing of these blocks is essential to the health of cryptocurrency, and since there's no one central entity that can carry out all this processing on their own, it's done by the currency's investors. This is called mining, and the miners are offered incentives to take on the task. When a block of data is properly mined, and specific predetermined algorithmic and mathematical criteria (known collectively as “hash”) have been met, the miners collect a reward of coins and a percentage of the transaction fees from the block they've processed. It should be noted mining is more a perk than a requirement; you can invest in cryptocurrency without mining, if you wish.

Mining serves a dual purpose; not only does it validate transactions, but it results in the generation of new cryptocurrency. For currencies that carry mintage caps, the mining reward of coins will eventually disappear when the cap is met; by that time, it's projected—and hoped—that transaction volume will be high enough to provide adequate incentive for miners to take part in the process for their share of transaction fees alone.

Mining Pools: In many cases, the process of mining can be a resource hog; it can eat up a lot of processing time and space on computers. Since most individual miners don't have the computing power or the hardware to dedicate one or more machines strictly to mining, they'll join with other miners to distribute the processing burden. When more than one miner is involved in the processing of data blocks, this is called a mining pool. Once the mining is completed and verified, the pool's members divide the coin and transaction fee rewards evenly.

Moon: Where you want your coin to pass by on its way to Mars. Mooning is when a coin goes on a “run” (AKA bull run). That is when the price goes up quick. The opposite is a crash, correction, or dip. Can't get a Lambo without mooning, can't see the moon if you don't HODL. NOTE: You'll make old school more virtuous crypto nerds cry if you say “Lambo, moon, and HODL” in the same sentence. So try to be polite and say “Tesla, Stratosphere, and Laddering” when appropriate.

Multisignature wallet: A wallet that is only accessible using more than one private key. More safe from hacking than a single signature wallet.

Node: Any computer that is connected to a blockchain network. Full nodes can verify the validity of transactions.

Nonce: A special number added to the end of a block that, when hashed with the entire block as well as the hash of the previous block, produces a new hash with a certain number of leading zeroes. When miners are creating a block, they are racing to find the nonce.

Noob Trap: “Noob” is an abbreviation for the term “new blood,” and is also sometimes expressed as “newb” or “newbie.” It applies to anyone who is a newcomer to a given community—in this case, investing in digital currency. Most alternative currency investors are good folks, and are willing to lend a helping hand and advice to those who are new to the game. However, there are also folks who see noobs as an easy mark, and these unscrupulous investors often use market manipulation methods to take advantage of those who may not yet know any better. Luckily, some judicious studying of these methods can help new investors protect themselves from falling into market manipulation traps. For better understanding of the types of noob traps there are in the digital currency world, see the terms Bear Trap, Bull Trap and Pump and Dump.

Offline Storage: This concept relates to how your cryptocurrency is stored. If your currency is online—on an active drive on a computer that's turned on, or accessible through cloud computing-- that means it's also accessible by other computer users. Sometimes that access takes place without your knowledge. This can lead to hacking and theft, since cryptocurrency—by design—isn't connected directly to any one person. As such, it's important to keep your unique currency information offline as often as possible; it's best to do so unless the currency is directly in use for a transaction. Two of the best ways to keep your investment info offline is to store it on an external drive that can be disconnected from your computer when it's not needed, or to print it out and store it in a paper wallet. If you decide to take advantage of a wallet service from a cryptocurrency exchange, one of the first questions you should ask them should be about offline information storage, since digital currency theft is usually untraceable and irreversible.

Oracle: Something that feeds information to a blockchain. Smart contracts can use oracles to know when the terms of an agreement have been met.

Paper Wallet

In the most specific sense, a paper wallet is a document containing all of the data necessary to generate any number of Bitcoin private keys, forming a wallet of keys. However, people often use the term to mean any way of storing bitcoins offline as a physical document.

Panic Selling: Selling in a panic at a low because the price is going down and one fears it might go lower.

Peer-to-Peer: Also abbreviated as P2P, this is a concept that's central to cryptocurrency. Transactions are made between individuals (peers), with no interruption or dictation from a centralized authority. On the plus side, all those invested in a type of cryptocurrency have a say in its well-being, without having to answer to a bank or government. On the minus side, this means people of less-than-ideal reputations are able to invest, just like anyone else. Cryptocurrency systems tend to be self-policing, but in the young industry's growing pains there have been conflicts between keeping the riffraff out and keeping the environment as free and accessible as possible.

Pennant Pattern: This pattern forms on market value charts when investors want to test a current trend in a commodity's value. The buying and selling that takes place during this testing period—which generally last one to three weeks—forms fluctuations that can be bracketed by converging diagonal lines, forming a “pennant” shape. These pennant patterns can occur during both upward-trending

(“bear”) and downward-trending(“bull”) markets. Since they don't signify the current trend is going to reverse, the pennant pattern is considered one of the “continuation” pattern types. Once the pattern is formed, the trend will continue moving in the direction it had been beforehand.

Platform Exchange:This is a digital currency exchange that limits the role they play in transactions made between investors. The majority of exchanges are there to facilitate these transactions, and make them easier to carry out. The exchange will sort through buy and sell orders, and will then match up investors who meet the criteria of the order in question. Their algorithms are designed so the trades being made are both secure and fair to both parties involved. Beyond that, however, the exchange does not play any“middleman” or mediating role. This is in contrast to exchanges that will hold the transaction funds in escrow, or will discuss the details of the trade with both investors before moving forward.

PoS: A proof-of-stake system (Pos). It is where mining is done by those who hold coins. The result is a bit like getting paid interest for holding coins.

PoW: A proof-of-work system (PoW). It is where mining is done by those who have the hash power, time, and energy. The result is that time and energy is traded for rewards.

Private Key:This unique identifier code is issued to investors to be used as a digital signature during transactions.Compared to public keys—which are openly listed in the directories of many cryptocurrencyexchanges—private keys are to be just that: closely guarded and not given out. Your private key is what you use when you receive a transfer—from an investor who encrypts it with your public key—to “sign”your approval of the transaction. Private keys should be treated just as you would your credit card or Social Security numbers.

Proof-of-Stake Mining:Rewards for this type of mining are based upon the amount you've already invested in the cryptocurrency in question. The more currency you hold, the higher your potential rewards for mining will be. Proof-of-stake mining, as of yet, is not used as a stand-alone method, but is used by some cryptocurrency issuers in combination with proof-of-work Mining. Peercoin and Novacoin are two major cryptocurrencies that use this combination mining method.

Proof-of-Work Mining:The rewards for this type of mining are straightforward: you receive coins and transaction fee rewards in direct correlation to the actual mining work you do. As such, the more mining you do, the more you can make. With some major cryptocurrencies such as Bitcoin and Litecoin, this is the only type of mining option available; however, some use a combination of proof-of-work and proof-of-stake mining.

Protocol:A set of rules, applicable across different operating systems and coding languages.

Pseudonym:A fake name or identifier. In a pseudonymous system, if a connection is made between the pseudonym and the person it corresponds to its power to hide identity is compromised.

Public Key:

This is a unique encrypted code issued to an investor. When they want to make a transaction with their cryptocurrency, they give their public key out—many cryptocurrency exchanges have a directory of

these for their investors—so the transfer can be made. The public key is a way to positively identify someone making a transaction, even though their actual name or personal information is not embedded in the key itself. Contrast this with a private key—which is not publicly known, and should be closely guarded—which is used to accept and validate a transaction.

Pump and Dump: This is a market strategy that's strongly frowned upon by conscientious investors. An individual or group will invest heavily in a stock or commodity when its price is low, and will then publicize it aggressively, often using misleading or outright false statements. This is the “pump” part of the term, and it's designed to get other investors interested and to drive the price upward. Once that happens, the individual or group will sell off their shares at a higher price; this often results in a profit for them, but it also creates a drop in the commodity's value. This is the “dump” part, and needless to say, does not please the other investors.

Cryptocurrency markets are just as susceptible to pump and dump strategies as other markets are. To help guard against it, heavy and aggressive over-investment is discouraged, and digital currency investors learn quickly how to sort the truth from false information

QR Code: These are a lot like the rectangular bar codes you'll find on just about anything you buy, except QR codes are square in shape and can hold more information than bar codes. Below is an example of a QR code

Rekt: A state of having lost money on an investment. Losing money = getting rekt.

ROI: A return on investment. What you would ideally like to happen.

RSI: The relative strength index (RSI) is a momentum indicator that compares the magnitude of recent gains and losses over a specified period to measure speed and change of price movements. It is smart to enter a coin when it has a low RSI.

Satoshi: Currently, this is the smallest possible fraction of cryptocurrency available for transactions. It refers to 0.00000001 Bitcoin, and is named after Satoshi Nakamoto, the enigmatic creator of the first publicly-available digital currency. Nakamoto wrote the white paper in 2008 that evolved into the creation of Bitcoin—and until March 2014, no one had been able to pin down the true identity of the person or persons operating under the pseudonym. An expose in Newsweek Magazine at that time revealed that Satoshi Nakamoto was, indeed, the creator of Bitcoin's real name.

Satoshi Nakamoto: A persona created by the person or people who created Bitcoin. Satoshi may or may not exist and may or may not be alive. He/She sacrificed fame (and potentially a fortune) to remain anonymous.

Scaling: The process of expanding a network to properly accommodate an increase in users.

Script: Script is a type of mining algorithm, and it's used by major cryptocurrencies such as Litecoin and Novacoin. It has the one major advantage over other algorithms such as SHA-256 in that it's quicker and easier to use. It doesn't use up as much computer processing space or time, so individual miners can more readily process blocks of data with it.

Seed phrase:

A string of words associated via an encrypted algorithm to a private key, allowing the retrieval of said

key if the words are known.

Sell Order:This takes place when an investor approaches an exchange with the intent to sell some or all of their cryptocurrency investment. Sometimes sell orders are simple and straight to the point (“Just sell what I have at the best price you can find”), or the investor can set criteria that have to be met before the sale can be made. This can include, price, time frame, percentage of holdings being sold, and so forth. Most exchanges have sell order forms that can be filled out, but if investors have specific questions or concerns, they can talk directly to an exchange representative before activating their order.

SHA-256:This is a mining algorithm protocol used by cryptocurrencies such as Bitcoin and Peercoin. While a popular algorithm, SHA-256 tends to use a lot more computing power and processing time than others,so it can be more difficult for individual miners to use. As a result, the majority of SHA-256 mining is performed by mining pools or individual miners who have separate computers they can devote solely to mining.

Shilling:Talking up a product because you are covertly paid to do so.

Shit Coin:This is what people call altcoins they don't like.

Silk Road:This was the notorious online black marketplace where drug deals and money laundering occurred on a regular basis. Many of the transactions on Silk Road used cryptocurrencies, which gave the entire industry a black eye for a while. After a long FBI investigation, Silk Road's owner was arrested inOctober of 2013, and the entire operation was shut down.

Smart contract:A digital agreement that has the power to auto-execute and the ability to transfer funds between parties.The combination of a contract and an escrow account in one piece of code that runs on a blockchain.Digitally signed by all parties involved.

Snapshot Block: Forks occur at specific block heights. The block height you have to be in a coin by to qualify for a fork is called a snapshot block. It is the block at which a snapshot of the ledger will be taken to determine the balances of the ledger of the fork.

Soft fork:A protocol change that is backwards compatible, allowing unupgraded nodes to interact with upgraded ones normally. A soft fork does not necessitate the creation of an entirely new cryptoasset.

Solidity:The coding language of the Ethereum blockchain.

Spoofing; When a person or people with a lot of money and coins buy and sell to themselves in a set range to create the illusion of volume.

Stale Block:When a block of cryptocurrency data has been successfully processed by a miner or mining pool, that block of data is considered stale. Experienced miners know to skip stale blocks, for it would be a waste of their time to try to mine them again.

Stop-Loss Order:This is a standing “get me out of here!” sell order that investors in stocks or commodities (such ascryptocurrency) use to, well...stop their losses. Or at least minimize them.Investors often establish a stop-loss order the minute they make a purchase. This is a sell order that specifies the price at which the currency should be sold. For example, if you buy shares of something at \$100 each, you might decide to issue a stop-loss order at \$60. As long as the share price

remains above that number, all is well—and nothing will happen unless you contact the exchange personally. However, the second the price hits \$60, all or part of your currency (whichever you specify) will be sold at your stop-loss order price. Different exchanges treat this differently; some sell immediately, and some wait to see if it's just a momentary “hiccup” on the market; if the price falls below your stop-loss limit, you'll get the latter amount for your shares.

Store of value: One of the three functions of currency. Refers to the ability of a currency to be saved, stored, and exchanged for goods or services at a later time.

Technical Analysis (TA): Technical Analysis is the art/science of trying to predict future trends from historic price and volume data. You don't need TA as a casual investor, but you should learn the basics if you trade. See tradingview.com. That said, even though crypto can be speculative and see a lot of emotional trading, and thus TA tends to help, it is vital to do some Fundamental Analysis (FA) and other analysis types as well. A chart can only tell you so much; you also need to understand factors like demand, supply, tech, upcoming upgrades, the news, etc. Don't make the mistake of thinking a coin “has to” go to X support level just “because TA,” sometimes good news, bad news, or a software update can be the main driver of a coin's price (and that won't always be clear from a chart).

The DAO: A decentralized venture fund, built on Ethereum. A major hack of the DAO early on forced Vitalik Buterin to fork Ethereum to return stolen funds.

Ticker Symbols: Every coin has a trading symbol or ticker symbol. For Ripple, it is XRP, for Bitcoin BTC, for Litecoin LTC, for Ether (ETH), etc. People often refer to coins by their ticker symbol and not their name.

Timestamp: A sequence confirming the exact time at which an event occurred. Used for recordkeeping and auditing purposes.

Tokenized: When an asset is split into many small pieces and distributed using a blockchain.

Tokenization: If you just sent unencrypted data across the internet it would not be secure. So instead of doing that information is tokenized. It is encrypted and turned into a string of data. That string can then be sent and stored. Data sent between wallets and stored on the blockchain is tokenized. This is why the term cryptocurrency tokens are used.

Trading Walls: Generally speaking, the trend line on a chart (such as those offered by digital currency exchanges) will move more or less diagonally as trades are made. However, once in a while there is a buy or sell order that comes in which will make the trend line move directly up and down, creating a vertical line that resembles a wall. These “walls” represent a temporary high demand in interest, either in buying or selling a certain type of digital currency. If a wall is created by a large buy order, it's called a “buy wall,” and if it represents a sizable sell order, it's called a “sell wall.” Generically speaking, these walls are called “trading walls” or “bid walls.” Once the orders have been filled—or are ignored by the market in general—the wall disappears, and the diagonal trend line continues.

Transaction Fee: To send a transaction a fee must be paid (with most cryptos). This fee is a reward for miners. In Ethereum it is called “Gas,” it might have a unique name for a given cryptocurrency.

Triangle Pattern: Generally speaking, triangle patterns form on market value charts when investors buy and sell to test a current trend. The highs and lows of these fluctuations can be bracketed by

straight lines that define the highs and lows during that testing period; these lines form an open-ended triangular shape. There are three types of triangle patterns:

1. Descending Triangle. This is formed when the lower line of the triangle is a horizontal line, and the upper line tilts downward from left to right. The descending triangle represents a downward-trending, or “bear,” market.

2. Ascending Triangle. This is the inverse of the descending triangle, with an upward left-to-right tilted line at the bottom, and a horizontal line at the top. Ascending triangle patterns indicate an upcoming “bull,” or upward-trending, market.

3. Symmetrical Triangle. The symmetrical triangle stands out because both lines forming the triangle are tilted. It's also a more tricky pattern to predict, because it can continue in either an upward (“bullish”) or downward (“bearish”) direction

TX: A transaction number. This allows you to track a transaction. If you are freaking out because your transaction is taking too long, you probably just have to wait longer. Try tracking the TX.

Unit of account: One of the three functions of currency. Refers to the use of currency as a concrete measure of how much things are worth, so that they can be compared to each other.

Virtual machine: A virtual machine is able to run an operating system without the machinery of a host. A method for running a decentralized network where computing power needed to run an operating system is distributed among many machines, creating a computer that only exists virtually, or a virtual machine.

Wallet: Just like a bill-and-coin wallet, this is a place to keep your digital currency. There are four types of cryptocurrency wallets:

1. Software Wallet. These are programs you load onto your desktop or laptop computer.

2. Mobile Wallet: These come in the form of applications you install on your smartphone or tablet computer. They usually include QR code scanning and phone-to-phone transfers for on-the-go transactions.

3. Web Wallet: These are usually gotten through exchanges, and stored on third-party servers via cloud computing. They can be accessed by any computing device.

4. Paper Wallet: Your digital currency can be printed out—usually in the form of QR codes—and these hard-copy cryptocurrency “bills” can be kept in a physical wallet just like traditional money.

Weak Hands: When too many new investors (in a given coin) invest in a coin the coin can be said to be “in weak hands.” Long-term investors who have built a position in a coin they love tend to HODL when the going gets rough (and thus they have “strong hands”), new investors with weak hands tend to get “weak knees,” and “panic sell” in a correction.

Wedge Pattern: These are a type of “continuation” pattern you'll see on market value graphs; that means they represent a momentary shift against the current trend, but the trend tends to continue in the direction it was going once the pattern is fully formed. Wedge patterns can be spotted by two diagonal, but non-converging, lines that bracket the up-and-down fluctuations that occur while investors test the current trend. There are three types of wedge patterns:

1. Rising Wedge. This wedge shape is tilted upward; thus the name. However, a rising wedge occurs during a downward trend, or “bear” market. It's a momentary upward shift, but the bear market continued afterward.

2. Falling Wedge. The falling wedge is tilted downward. It represents just the opposite of the rising wedge, in that it denotes a brief downward movement during a “bull” market, which continues once the

wedge is formed.

3. Level Wedge. These appear to move in more or less a horizontal direction on a graph. Just like the rising and falling wedges, the level wedge shows a brief respite in a trend, which will continue once the wedge pattern is complete

Whales: Whales are cryptocurrency investors with many coins or dollars. These investors can help move markets, or they can help stop markets from moving. When you see a 250 BTC buy wall or sell wall, that is a Whale. When the price goes down quickly and it makes you sad, or it shoots up and liquidates your short position, you can curse your semi-mythic nemeses “whales.”

White paper:

A summary of the goals, timelines, policies and niche of a company. Includes the value proposition.

Yellow paper:

A technical, research style paper explaining the computer science, math, and economics behind a proposed blockchain technology application.

Zero Confirmation Transaction:

The processing of data for cryptocurrency transactions can take anywhere from half a minute upward to over ten minutes in some cases. Though this is necessary in order to validate transactions—and guards against fraudulent activity such as double spending—the waiting period can be inconvenient for those involved in the transactions. As a result, some exchanges and businesses that deal with digital currency are offering “zero confirmation” transactions, which are almost immediately verified without waiting for the mining process to confirm the data block.