

Marc PAIRON

CRYPTOCURRENCY GLOSSARY & TIPS

words, initial words and pictograms. A rebellious language, without formal spelling rules, it is born out of direct communication. A buzzword or a meme may be invented by a single person and quickly be adopted by the whole crypto community.

Apart from their use as technological terms, a number of these terms and derivative terms refer to historical events, are the result of playful jostling, or were taken from common language or some other jargon and then given a new dimension or meaning. Within the crypto community, a single cheesy word or term may give rise to numerous derivative terms, thereby becoming part of the business folklore. Thus, 'To the moon!', a general battle cry of enthusiastic crypto speculators with which they refer to, or express their hope for, an astronomical rise of a cryptocurrency, has given rise to various new words: moonboy, moongirl, moonkid, moon mission, moon ride, moonshot, etc. Common crypto language is also laced with irony bordering on sarcasm. For example, a historic crisis caused by Mt. Gox, a Japanese bitcoin exchange that went bankrupt in February 2014 as a result of poor security and incompetent management, produced various crypto terms. Goxed means 'suffering from technical glitches' and gox'd is defined as 'being the victim of a cyberattack in which cryptocurrencies were stolen'. Spelling errors and typos are equally embraced by the crypto community and may rapidly attain the status of generally accepted terms.

Crypto is a fascinating language, which is rapidly expanding and constantly evolving on internet forums and in chat boxes. The typical words and often exhilarating terms are illustrative of the exciting period of cryptocurrency development. The virtual crypto market, investing in blockchain projects and related technological developments will contin-

ue to play a major role in the real world's financial news for a long time to come. Some trendy crypto terms will slowly but steadily become mainstream. Just like the launch of the euro produced a new common language, so will the development of cryptocurrencies. Considering the hundreds of millions of people worldwide involved in cryptocurrency, crypto has long ceased to be a niche language. It may, however, take some time before these crypto terms end up in conventional dictionaries, because the language is still in its infancy. For a term to be included in such a lexicon, it must be encountered regularly for at least a number of years in the language used by a community or a specific sector. Such a descriptive dictionary then serves as an arbitrator when there is doubt about the correct spelling, definition or status of a word. In the as-yet unregulated crypto world, there are no arbitrators, at best there is a democratic consensus. In this world, everything is created by and for the participants. This also includes the language, some terms of which may only be short-lived whereas others will survive over generations.

History

A cryptocurrency is a virtual currency that is recorded in a blockchain, a gigantic digital archive. Leaving the technical details aside, a blockchain can be described as a form of public bookkeeping, where all digital transactions are stored from the outset by means of special software. Outsiders think that cryptocurrency refers only to bitcoin, while the brand recognition of the Bitcoin network is currently the signboard of a rapidly growing crypto market that already comprises more than 1500

different digital currencies – only a few of which are relevant.

In 2009, bitcoin was the first virtual currency launched by the software developer or a group of IT professionals under the alias of Satoshi Nakamoto. However, the person who calls himself Nakamoto is not the inventor of the contemporary cryptocurrency, but is indebted to many software experts. The American computer scientist and cryptograph David Chaum is in any case the founder of the idea that a cryptocurrency could be possible, and had documented as much already in 1982. In the beginning of the 1990s, he put the encryption of virtual transaction to practice. Chaum would enable users to obtain digital assets from a bank and to issue them without being traceable by the bank or another party. His ideas rank as the technical roots of the vision of the CypherPunk movement, which was launched in San Francisco (USA) in 1992.

The core of the CypherPunk movement consisted of brilliant computer scientists and ingenious software developers who had started to code privacy-oriented computer programmes a few years earlier, and would develop many concepts independently from each other that are at the center of the Bitcoin blockchain technology. The CypherPunks wanted to provide technological solutions for societal problems. They were people who attached high value to privacy and were thus keen to strengthen democracy. These people were activists and anarchists who, just like David Chaum, wanted to offer alternatives for the online economy and for the Western political system. They provided the building blocks for the current cryptocurrency that would stand for freedom and independence from banking institutions and governments.

Equating the privacy that CypherPunks had in mind

with anonymity is a misconception. Privacy means personal freedom, for example the possibility to decide for themselves whether to draw the curtains in the living room or leave them open, but not to go and live in an untraceable address. This is confirmed when we peruse an original CypherPunk's manifesto: *Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know; but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.* (from A CypherPunk's Manifesto, Eric Hughes, 1993)

A cryptocurrency is therefore not about anonymity, as is often supposed, but about how people can still decide for themselves with whom they wish to share information in a digital world. Most crypto network blockchains are for that matter transparent, so that every cryptocurrency transaction is traceable; furthermore, the first financial step always starts from the real world, so that traces are nearly always left behind. It is not cryptocurrencies that constitute a danger for anonymous (and possibly shady) financial transactions, but the traditional cash of physical money or valuable physical goods, such as precious metals and artworks. Cryptocurrency uses no cash, because it is not tangible, but entails verifiable digital transfers, from one cryptocurrency address to the other.

The CypherPunk's privacy statement was not so much about cryptocurrencies, but should be understood in a broader sense, namely to restore and protect the personal freedom of an individual, with the dangers entailed by the still young Internet always in mind. The CypherPunks have warned the world that each time interest is shown or an action taken

Legend

- typical crypto linguistic usage
or basic technological and technical terms
- see referenced term
- 🚩 warning sign, financially dangerous, caveat emptor
- TIP useful information

all-time high: the highest historical price of a specific cryptocurrency. Opposite of *all-time low*. Abbreviation: *ATH*. → all-time low, correction, cryptocurrency, HODL, peak

TIP When the price of a cryptocurrency reaches a historical high, it is usually followed by a correction. It is therefore not advisable to get in as an investor or speculator at this rare price position, unless you are so convinced of the favorable prospects of that cryptocurrency as to opt for a long-term strategy.

all-time low: the lowest historical price of a specific cryptocurrency. Opposite of *all-time high*. Abbreviation: *ATL*. → all-time high, cryptocurrency, DYOR, scamcoin, shitcoin

TIP The lowest historical price of a cryptocurrency could, in principle, be a perfect time to get in as an investor or speculator, were it not for the fact that you have to examine the reasons why that particular currency has fallen to that lowest point. It may be a *shitcoin* or a *scamcoin*. It goes without saying that if this is the case, you should stay far away from such a coin.

alphanumeric: method of information processing systems to create files consisting of letters, numbers and/or special characters. This method is used in Cryptocountry for instance to create digital addresses, to receive and store cryptocurrencies and to send these digital coins. → alphanumeric address, cryptocurrency

alphanumeric address: digital destination or place for receiving, storing and sending cryptocurrencies, which may be composed of letters, numbers and/or special characters. → address, alphanumeric, cryptocurrency

alt: abbreviation of *altcoin*. → altcoin

altcoin: abbreviation of *alternative coin*. Designation for every cryptocurrency, except bitcoin. Abbreviated form: *alt*. → Bitcoin, blockchain technology, cryptocurrency, crypto market, crypto network, dead coin, fiat money

- Many crypto networks of solid alternative coins try to add an extra dimension to Bitcoin's revolutionary technology or to change or improve its applications.
- In the crypto market, the value of an alternative currency is measured by bitcoin, not by traditional currencies. Bitcoin is the reference currency of the crypto market.
- Thousands of alternative coins exist or have existed.

altcoin flipping: trading in several alternative currencies, buying and selling them for bitcoin instead of fiat money. → altcoin, Bitcoin, fiat money, flipping

altcoin volume: 1 Trading volume over the last 24 hours of all listed alternative coins on a specific crypto trading platform. 2 Trading volume over the last 24 hours of all listed alternative coins from a selection of international crypto trading platforms. → altcoin, BTC volume, exchange, market volume, volume

- The volume may also refer to another time span, but is usually about the last 24 hours.

AMA: chat abbreviation for *Ask Me Anything*.

AML: abbreviation of *Anti-Money-Laundering Directive*. Regulation with which financial institutions must comply. → CTF (2nd meaning), KYC

- Customers of a financial institution need to be screened in order to prevent or detect possible money laundering, and in order to prevent illegally acquired funds from entering the legal circuit.

bear trap: temporary drop in the price, after which it rises again. Opposite of *bull trap*. → bull trap, cryptocurrency, holding, noob trap

TIP When the value of a strong cryptocurrency suddenly drops significantly, the advice is to keep that cryptocurrency. Anyone who does sell – if the price recovers – has fallen into the 'bear trap'.

bear trend: synonym of *bear market*, a declining price trend. Opposite of *bull trend*. → bear market, bull trend

bearwhale: combination of a bear and a whale. Someone who has an enormous amount of cryptocurrency and is therefore able to manipulate the market, can cause the price of a cryptocurrency to collapse temporarily. A bearwhale can also behave as a bullwhale, i.e. is also able to push the price higher. → bear, Bitcoin, bullwhale, cryptocurrency, exchange, panic selling, sell wall, whale

- In October 2014, a bearwhale on the Slovenian crypto trading platform Bitstamp suddenly put 30,000 bitcoins up for sale. At that time, these were worth about \$9 million. The highest bid price was then set at \$350, but because of the oversupply, the price fell immediately to \$300 and collapsed even further as a result of a general panic selling brought about by the huge bearwhale's sell wall.
- Different categories named after a sea creature are based on the size of one's cryptocapital.

believer or **cryptobeliever:** someone who buys one or more cryptocurrencies because he/she trusts in the future prospects of these technological projects. → bitliever, cryptocurrency, crypto market, crypto network, community, development team, OG HODLer

- A cryptobeliever invests in cryptocurrency because of his confidence in the project and the development team. Such believers are at the heart of the crypto community, inspiring and supporting the development team and showing understanding and patience during the development.
- Cryptobelievers are often experienced investors and analysts who monitor and verify all messages and references to their cryptocurrency.
- For a cryptobeliever, a rise in price is a pleasant side effect, not an end in itself.
- The hard core of cryptobelievers may never leave the crypto market or at least hold their cryptocurrency for a long time to come.

bet the farm: risk everything you own as an investment or bet everything on a single cryptocoin. → AFI, all-in, altcoin, Bitcoin, cryptocurrency, don't put all your eggs in one basket, speculator

- It has happened on several occasions that someone or a family has literally *bet the farm*, that they sold everything they have to invest in bitcoin and other cryptocurrencies.
- Because there are countless small crypto investors and speculators within the crypto community, 'betting the farm' can just as easily be a tough statement about an equivalent of only a few hundred dollars.

BFA: initialism for *Brute Force Attack*. → brute force attack

bid or **bid price:** the price one offers for cryptocurrencies, which is usually expressed in satoshi. Opposite of *ask*. → ask, cryptocurrency, hit the bit, satoshi

big blocker: person who believes that increasing the block size of the Bitcoin network would improve scalability – the ability to

forks, testnet launches, the rebranding of a crypto network, airdrops, delistings, coin burnings, white paper launches and much more. → airdrop, announcement, cryptocurrency, crypto network, delisting, hard fork, proof of burn, rebranding, testnet, white paper

CoinDesk: important and reliable American crypto news website (coindesk.com). → BPI, Cointelegraph, Consensus

- CoinDesk was founded in May 2013 and organizes, among other things, the large-scale annual blockchain conference Consensus.
- In September 2013, CoinDesk created the Bitcoin price index.

coinexchange: other designation for *exchange*. → exchange

CoinMarketCap: American website (coinmarketcap.com) with trading volumes, market capitalizations and other data from listed cryptocurrencies. Initialism: *CMC*. → cryptocurrency, market cap, real-time, volume, WorldCoinIndex

- The prices on CoinMarketCap are not in real-time but are displayed with a delay. For real-time market values see world-coinindex.com.

coinmine: a location where cryptocurrency is extracted with a great deal of hash power. Synonym: *mining farm*. → cryptocurrency, hash power, mining, mining farm

coinmining: synonym of *mining*. → mining

Cointelegraph: important and reliable American crypto news website (cointelegraph.com), launched in 2013. → CoinDesk

Coin Traded Fund: investment product that closely follows the index of a cryptocurrency and from which crypto investors can

buy shares. Initialism: *CTF*. → cryptocurrency, GBTC

cold storage: digital data stored without being connected to the internet. Synonym: *offline storage*. → cold wallet, cracking, hot storage, malware, man in the middle attack, private key, wallet

- A cold wallet is an offline digital cryptowallet that is hard to crack and is barely susceptible to malware.
- *Hot storage* is the opposite of *cold storage*.

TIP The safest way to use cold storage is to lock digital data into a device that has never been connected to the internet before.

cold wallet or cold storage wallet: offline digital cryptowallet, with which transactions can only be executed when the wallet is connected to the internet. Opposite of *hot wallet*. → cold storage, cryptocurrency, hot wallet, transaction, wallet

- A cold wallet is used to store cryptocurrency for a longer period of time.

colored coin: protocol built on top of a blockchain. For example, bitcoins can be colored to represent different assets, such as certain financial instruments, gold or property. → Bitcoin, blockchain, colored coins protocol, protocol

colored coins protocol, the: although originally designed as a digital currency, the Bitcoin network supports a limited scripting language that can be used to store metadata on the blockchain. → Bitcoin, blockchain, colored coin, cryptocurrency

- The 'colored coins protocol' allows metadata to be linked to Bitcoin transactions and to use Bitcoin's infrastructure to send and trade unchanging digital assets that represent a real-world value, such as securities, shares, commodities, new currencies, home or car property deeds, etc.

collective mining: association of individual crypto miners using a company's resources and materials to extract digital currency blocks from a crypto network. → block, crypto network, miner, mining, mining pool

- The use of resources for the crypto mining process has often become too expensive for individuals to be able to participate independently. In collective mining, a company invests in the hardware and provides the necessary mining energy, facilities that can be rented by miners.

collusion: within the blockchain technology, 'collusion' means that a number of users of a blockchain are playing the protocol rules to their advantage. In this way, a conspiracy can arise to try, for example, to achieve a hostile takeover, such as a 51% attack, of the blockchain of that crypto network. → blockchain, blockchain technology, crypto network, protocol, 51% attack 🚩

commodity: physical asset, often used as a raw material for the production of goods or services.

community or **crypto community:** 1 Collection of participants and supporters of a specific crypto network. 2 Group of people who share a common interest in cryptocurrency and its technology, who unite in internet forums or in real associations. 3 Anyone who is – in any way – involved worldwide in the technological evolution of cryptocurrency and other related applications. → blockchain technology, cryptocurrency, crypto network, red flag

- The size and activity of the crypto community of a specific-cryptocurrency is a very important fact. After all, it is this group of supporters that morally and financially support the digital project and gives it the opportunity to prove itself in the future.

- When the crypto community of a particular cryptocurrency is too small, barely growing or does not communicate seriously on internet forums, it is a red flag – a warning sign. 🚩

compiler: software program that translates bits of code written in high-level programming languages into a code at a low level.

completed order: order placed on a crypto exchange that is fully executed. Opposite of *open order*. → exchange, order

conditional order: order placed on a crypto exchange to buy or sell cryptocurrency at a certain price or after certain other conditions have been met. → cryptocurrency, exchange, order

confirmation: means that a transaction has been verified one or more times by the crypto network, i.e. the successful action of hashing a transaction and adding it to a blockchain. → blockchain, crypto network, hashing, long confirmation, miner, mining, transaction, transaction fee

- Confirmation of the digital transactions is done by the crypto miners.
- After confirmation, a transaction can almost never be undone.
- The higher the transaction fee one is prepared to pay, the faster the transaction will be executed.

confirmation time: time interval between the sending of a cryptocurrency and the confirmation of the digital transaction. → confirmation, cryptocurrency, long confirmation, transaction

Consensus: large-scale cryptoconference, organized by the American crypto news website CoinDesk, that has been held annually in New York (USA) since 2015. → CoinDesk

cryptocurrency is hyped. → cryptocurrency, hyping, market manipulation, scam, suspicion

TIP If particularly good news does not form the basis of a striking rise in the price of a cryptocurrency, there is a good chance that a hype has been artificially created by some form of manipulation and/or scam.

don't put all your eggs in one basket: conventional wisdom from the traditional stock exchange that certainly applies to the crypto market and refers to an investment method that spreads the risks. → ashdraked, cryptocurrency, cryptofolio, crypto market

TIP If all the eggs are stored in one basket and that basket falls, then they are all broken or in this case one is ruined as a crypto investor. That is why it is advisable to build a cryptofolio from different investment angles and cryptocurrencies.

DoS: initialism for *Denial of Service*. → denial of service

double bottom: term from the technical analysis that indicates a pattern in which the price of a cryptocurrency touches the support level twice and then rises again. Opposite of *double top*. → cryptocurrency, support, technical analysis

double fork: irreversible split resulting from two different blockchains, creating a new blockchain and its associated currency. → blockchain, cryptocurrency, hard fork

• In March 2018, Zclassic (ticker symbol: ZCL) was the first external cryptocurrency to fork with Bitcoin's blockchain (BTC). This fork yielded the new digital currency Bitcoin Private (BTCP).

double-spending or **double-spend:** the successful operation or the ability to spend the same cryptocurrency twice. → confirmation,

cryptocurrency, miner, transaction

- A *double-spend* does not create new cryptocurrencies, but is a fraudulent method of trying to recover cryptocurrencies that have been sent (previously spend).
- Since cryptocurrency is made up of digital currencies, the electronic files associated with a transaction can be copied and used several times. This is, of course, an illegal practice within the crypto community.
- An attempt at fraud by 'double-spending' must be prevented by the control of the crypto miners. Transactions without confirmation are therefore risky.

double top: term from the technical analysis that indicates a pattern in which the price of a cryptocurrency reaches the resistance level twice and then drops further. Opposite of *double bottom*. → cryptocurrency, resistance, technical analysis

downtrend: declining price trend. Opposite of *uptrend*. → uptrend

DPoS: initialism for *Delegated Proof of Stake*. Derivative form of 'proof of stake', a method to mint new cryptocurrencies. → cryptocurrency, proof of stake

drain: mass sale of a cryptocurrency caused by panic. → cryptocurrency, panic selling

drop: slight to sharp decline in the value of a cryptocurrency. → correction, cryptocurrency, dip

dual-mining: mining two cryptocurrencies, which use different algorithms, simultaneously on a single mining system. → algorithm, cryptocurrency, mining

hold on for dear life: within the crypto community, this means keeping a cryptocurrency at all costs – even during a sharp fall in price – as if your life depended on it. Derived acronym: *HODL*. → cryptocurrency, HODL

honeynet: 1 Network to which several honeypots, counterfeit computer systems to catch cybercriminals, are connected. 2 Website set up by scammers to attract inexperienced crypto speculators with the intention of deceiving them. Synonym: *watering hole*. → cracker, honeypot, noob, scam

honeypot: computer system set up as a trap to capture cybercriminals or detect new methods of cracking. → cracker, honeynet

hopping: short for *pool hopping*. → pool hopping

hosted wallet: software cryptowallet managed by a third party, such as a crypto trading platform. Synonyms: *web wallet* and *online wallet*. → exchange, wallet

hot storage: the storage of cryptocurrency in a location connected to the internet. *Cold storage* is the opposite of *hot storage*. Synonym: *online storage*. → attack, cold storage, cryptocurrency, malware

- A *hot storage wallet* is an online digital wallet, which, by its connection to the internet, is also accessible to other computer users and is therefore susceptible to cybercrime and malware. The safety of a hot wallet depends on the procedures and methods used by its operators.
- A hot wallet is used to keep cryptocurrency on hand, so that it can be quickly and easily traded or spend.

hot wallet: cryptowallet with internet access where the user can store virtual currency online. Opposite of *cold wallet*. Synonym:

software wallet. → cold wallet, cryptocurrency, software wallet, wallet

H&S: abbreviation of *Head and Shoulders pattern*. → head and shoulders pattern

human intelligence: the intellectual capacity of human beings or their mental ability with many different functions. Opposite of *artificial intelligence*. Initialism: *HI*. → artificial intelligence

humpback whale or **crypto humpback whale:** super-rich crypto investor (or organization) that has a crypto fortune of more than 5,000 bitcoins, or an equivalent in alternative cryptocurrencies. → altcoin, Bitcoin, crypto ocean

hydro mining: a method of crypto mining based on hydroelectric power stations and water cooling systems, in order to achieve an energy-efficient and profitable mining activity. → mining

HYIP: initialism for *High-Yield Investment Program*, an investment method that promises a high return, but usually involves fraud.

hyperbitcoinization: term that describes that, due to the increasing value of bitcoin, funds flow from the traditional stock market to the crypto market. → Bitcoin, crypto market

hying: 1 The standard meaning of hying is 'making something a fashion phenomenon through the media'. 2 In the crypto community, hying, through social media and internet platforms, means making efforts to get a particular cryptocurrency to catch on with a particular audience in order to bring about price increases. → cryptocurrency, don't believe the hype, overhyped



IANAL: initialism for *I Am Not A Lawyer*. A statement that indicates that one has no knowledge of any legal consequences of some act or construction.

iceberg order: large buy or sell orders on a crypto exchange, only part of which (the tip of the iceberg) is visible. → cryptocurrency, exchange, hidden order, order

- After the execution of the visible part of an iceberg order, a subsequent phase becomes visible each time until it has been fully executed. The purpose of an iceberg order is not to disclose the size of the order, so that it cannot have an impact on the price development of the cryptocurrency in question.

ICO: initialism for *Initial Coin Offering*. → altcoin, crowdfunding, cryptocurrency, DAICO, DICO, distribution date, Ethereum, hard cap, hidden cap, ICO scam, initial coin offering gold rush, IPCO, ISO, ITO, maximum contribution, minimum contribution, pre-ICO, private presale, private sale, public presale, simple agreement for future tokens, soft cap, token, utility token offer, whitelist

- An *ICO* is used by start-ups or projects that want to launch their own cryptocurrency and raise funds for this purpose, as a form of crowdfunding. During this first offer, a limited number of coins is offered at a much reduced price.
- Although the *ICO* now has a dubious reputation due to misuse of the concept, there are many popular alternative coins that have been launched in this way. For example, the Ethereum project launched a particularly successful *ICO* in the summer of 2014. They raised \$16 million at an issue price of only \$0.311 per cryptocoin. Given the current market value, the Ethereum project alone has produced a large number of

cryptomillionaires.

TIP In the past, the launched coins were often already much more expensive when they appear on the market after an *ICO* than initially, and they can still significantly increase in value in a short period of time. However, you must be particularly vigilant and perform thorough research, as many *ICOs* have proven to be the subject of fraud. Anyone in the unregulated cryptoworld can organize an inflated *ICO*. Participation in an *ICO* is thus more a matter for the experienced investor. 🚩

ICO scam: the presale of worthless digital coins or coins that will never be released, thus making only the promoters richer. → initial scam offering, shitcoin 🚩

IIRC: chat initialism for *If I Recall Correctly*.

IMAO: common chat acronym for *In My Arrogant Opinion*. → IMHO, IMO

IMHO: common chat acronym for *In My Humble Opinion*. → IMAO, IMO

immediate-or-canceled order: type of order placed on a crypto trading platform and automatically canceled if it is not executed in full or in part immediately after it is placed. Initialism: *IOC*. → exchange, good-till-canceled order, order

immutability: refers to the fact that once a block has been verified and added to a blockchain, its contents – including transaction data – can no longer be edited or modified. → block, blockchain, transaction

IMO: common chat acronym for *In My Opinion*. → IMAO, IMHO