PATRICK SCHUEFFEL
NIKOLAJ GROENEWEG
RICO BALDEGGER

THE CRYPTO ENCYCLOPEDIA

COINS, TOKENS AND DIGITAL ASSETS FROM A TO Z

GROWTH-PUBLISHER BERN

This page intentionally left blank

THE
CRYPTO ENCYCLOPEDIA
Coins, Tokens and Digital Assets from A to Z

Patrick Schueffel
Nikolaj Groeneweg
Rico Baldegger

GROWTH
PUBLISHER
Bern

GROWTH
PUBLISHER

In cooperation with
School of Management Fribourg (HEG-FR)
HES-SO // University of Applied Sciences and Arts Western Switzerland
Visit the School of Management Fribourg home page at
http://www.heg-fr.ch/EN

Published in Switzerland

ISBN 978-2-940384-47-1

PREFACE

The subject of cryptocurrencies, tokens and digital assets is an emerging field. It attracts an increasing amount of attention in the world of business as well as academia.

When a new subject is developing, it is important to use one common language, otherwise unavoidably misunderstandings emerge, and communication would become error prone and thus inefficient. Under those circumstances progress would hardly be possible, and the advancement of the field would seriously be hampered.

Throughout many talks at conferences, in sessions with investors, throughout lectures at university, and in further education courses for practitioners, we came across many occasions of misunderstandings. These misunderstandings gave rise to the thought of sharing our point of view when discussing crypto.

In order to help creating a shared terminology we wrote this book. Drawing on a wealth of experience in the field of cryptocurrencies as founders, entrepreneurs, educators, and researchers we intended this book as a single, consolidated and authoritative source on that subject. We hope it will serve this purpose

Patrick Schueffel
Nikolaj Groeneweg
Rico Baldegger

This page intentionally left blank

2FA (two factor authentication, TFA, two step verification)

A two factor authentication is a process of confirming a user's alleged identity by using a combination of two different components, for instance a password and a physical token (e.g. > *PIN* and credit card).

51% attack (fiftyone percent attack)

51% attack is the name for a concerted attack on a > *distributed ledger* system where > *miners* controlling more than 50% of the system's > *hashing power* can manipulate transactions.

accelerator (startup accelerator, seed accelerator, seed accelerators)

An accelerator is a time-limited, cohort-based program, supporting > *startup* companies in their business endeavors. the program typically includes mentorship and educational components and is generally concluded by a public > *pitch* event or > *demo day* for potential investors.

accidental fork

An accidental fork is a specific form of a > *fork* which occurs if due to coding errors newer versions of generated > *blocks* are not truly compatible with older ones.

address

The address is a unique identifier which is created by > *hashing* a > *public key* and describes the digital address where > *coins* or > *tokens* can be transferred to or where coins, tokens or > *smart contracts* can be stored.

Airdrop An airdrop is an allocation process for distributing > *tokens* to a group of token holders after an > *ICO* has been completed or a > *fork* has gone live.

algo trading see > *algorithmic trading*

algorithm An algorithm is a set of rules or a procedure to be followed for solving a mathematical problem.

algorithmic trading Algorithmic trading is a trading method which makes use of automated > *algorithms* and pre-programmed trading instructions, such as time, price, and volume to execute tranches of a larger order over time.

Alt see > *Altcoin*

Altcoin An Altcoin (umbrella term encompassing "alt" for "alternative" and "coin") is a labelling for a cryptocurrency that is alternative to Bitcoin.

alternative coin see > *Altcoin*

Altfi (alternative finance) Altfi is a term describing financial channels, processes and instruments that have developed outside of the conventional finance system comprising regulated banks and capital markets.

AML (anti-money laundering)

AML is a set of measures, laws and/or regulations designed to prohibit the practice of > *money laundering*.

angel investor (business angel)

An angel investor is an affluent or high net worth individual who provides early capital for a business > *startup*, usually in exchange for convertible debt or ownership equity. Oftentimes this individual also provided knowledge and contacts for the start-up.

anonymization (data anonymization)

Anonymization is the process changing data in such a way that identifiers are being encrypted, removed, substituted, distorted, generalised or aggregated so that data privacy is ensured.

API (application programming interface)

An API is a set of functions and protocols for building application software. It defines methods of communication between various software components and provides access to data of an operating system, application, or other service. It facilitates developing computer programs by providing building blocks which can then be assembled by the developer.

ASIC (Application-specific integrated circuit)

An ASIC is an integrated circuit designed for a specific application, rather than one produced for genera purpose.

ASIC Miner

ASIC mining is the process of > *mining* > *cryptocurrencies* using > *ASIC* equipment allowing for a significantly faster production speed than with an ordinary desktop or laptop as these systems are specifically manufactured for this purpose.

bagholder

A bag holder is a term describing an investor who holds a position in an asset that decreases in value, until virtually worthless with only small chances of regaining value, e.g. holding a cryptocurrency beyond a pump and dump crash.

bank book

see > *ledger*

BCH

see > Bitcoin *Cash*

bid-ask spread

see > spread

Bitcoin

Bitcoin is a > blockchain based > cryptocurrency and a > *digital payment* system invented by an unknown with the alias > *Satoshi Nakamoto* in 2008.

Bitcoin cash (BCH)

Bitcoin Cash is a cryptocurrency resulting from a > hard fork of > Bitcoin which took effect on 1 August 2017 in order to increase Bitcoin's block sizes.

Bitcoin halving see > *halving*

Bitcoin mining Bitcoin mining is the process of creating and releasing new > Bitcoin currency. This is done by verifying and adding transactions to the > blockchain as rewards for doing computational work.

block A block is an unalterable set of data making up a pivotal component of the > blockchain by recording the most recent transactions that have not yet been recorded by any previous block.

block height The block height is a metric used to describe the number of sequentially added blocks in the > blockchain between any given block and the > genesis block

block reward The block reward is the compensation that a miner can claim for creating a > block on the > blockchain.

block size Block size is a value providing the amount of data that is stored in any given > block on the > blockchain.

blockchain The blockchain is a publicly accessible > *distributed ledger* that was initially designed and implemented to enable > *Bitcoin* transactions. It is a piece of IT infrastructure that serves as a database which is used to keep a continuously growing list of records, so called > *blocks*.

bonus A bonus is reward for a > *cryptocurrency* investor, typically granted throughout the > *pre-sales* or early > *ICO* stages of a cryptocurrency project and thus awarding early investments.

bot see > *trading bot*

BTC see > *Bitcoin*

burn see > *coin burn*

burn reserve A burn reserve describes the lot of tokens that are not distributed during > *ICO* and which will be burned in order to avoid dilution.

buy wall A buy wall is an expression describing a situation when the amount/size of buy orders for a particular > *coin* or > *token* is significantly larger than the number of sell orders.

Byzantine fault (error avalanche)

The Byzantine fault is a condition of a distributed computing system where components may fail, yet imperfect information exists on whether a component has failed and if so which one(s)

Byzantine fault tolerance

Byzantine fault tolerance is the ability of a computing system to cope with the questionable reliability of data caused by the > Byzantine fault.

CCI30 Crypto Currencies Index

The CCI30 Crypto Currencies Index is an index tracking the 30 largest > *cryptocurrencies* by > *market capitalization*.

central ledger (centralized ledger, general ledger)

A central ledger is a single principal repository that keeps records of transactions of an entity and is typically controlled by a single person or a narrowly defined group of individuals.

circulating supply

The circulating supply is the amount of coins that are circulating in the market, i.e. which are in the general public's hand; if tokens are > pre-mined the circulating supply will equal to the hard cap after > *ICO*.

coin

Coin is commonly used alternative expression for > *cryptocurrencies*.

coin burn

A coin burn describes the irreversible process of sending > *tokens* of > *cryptocurrency* to a > *public address* from they can never be retrieved as the > *private keys* of such the public address is unobtainable.

cold storage

A cold storage is an electronic device that can store > *cryptocurrencies* independent of having an online connection to the Internet and thus reduces the likelihood of unauthorized access, hacking attacks, and other vulnerabilities that an online system is otherwise susceptible to.

cold wallet

A cold wallet is a > *digital wallet* employing > *cold storage* technology.

collectables (collectable tokens)

see > *NFT*

Colored Coin

A Colored Coin is an expression describing a set of methods for representing and managing real world assets using the > Bitcoin > blockchain infrastructure.

commit

A commit is a command used in > *Github* to save changes in a code or project to a local repository.

comparison site

A comparison site is a Website that compares the scope and price of a particular product or service across different providers.

complementary currency

A complementary currency is a currency which is not a legal tender, but complementing national currencies, i.e. > *Fiat money*.

computationally universal

see > *Turing complete*

consensus mechanism
A consensus mechanism describes the actions necessary to achieve agreement on data in distributed systems.

consensus process
see > consensus mechanism

Cosmos Network
The Cosmos Network is a decentralized network of independent, scalable, and interoperable > blockchain*s*.

crowd sale
see > ICO

crowdfunding
Crowdfunding is one specific form of > *crowdsourcing* where funding for a project or business is raised from a number of people, oftentimes via campaigns launched via the Internet.

crypto exchange
see > *cryptocurrency exchange*

crypto index (CRIX)
Cryptocurrency Index (CRIX) is an index comprising 20 constituents from the crypto currency markets.

crypto protocol
A crypto protocol is the underlying set of rules upon which > *Dapps* are built; prominent crypto protocols are > *Ethereum*, NEO, Stellar, Lisk, QTUM etc.

cryptocurrency (math based currency)

A cryptocurrency is a > digital currency in which > *encryption* techniques are used to control the generation of units of currency and verify the transfer of funds, operating independently of one single central unit. Cryptocurrency businesses oftentimes raise money through > ICO*s*.

cryptocurrency exchange (crypto exchange, digital currency exchange)

A cryptocurrency exchange is a platform that provides users with the possibility to trade > *cryptocurrencies* for other cryptocurrencies and/or > *Fiat money*.

cryptographic nonce

see > *nonce*

Custodian

A custodian is a person or entity who has responsibility for taking care of assets.

cybersecurity

Cybersecurity are the measures, technologies, processes, and practices taken to protect a computer or computer system against unauthorized access or attack or damage.

Cypherpunk

A cypherpunk is a person that actively advocates the widespread usage of cryptography and privacy-enhancing technologies as a means to social and political change.

DAG (directed acyclic graph)

A DAG is a > *directed graph* such that staring at any node and following the vertices along their direction, there is no way to return to the original starting node; DAGs are being used as an alternative > *DLT* to > *blockchain* technology.

DAICO (Decentralized Autonomous Initial Coin Offering)

The DAICO (umbrella term encompassing “> *DAO”* and “> *ICO”*) is a process of decentralized capital investment: investors retain the control of the capital requested by the project team by approving certain milestones, so called > *TAPs*

DAO

The DAO (Decentralized Autonomous Organization) was an organization setup to pool funds to develop technologies supporting new decentralized business models; after being hacked in June 2016 it ceased to exist in late 2016.

DAPP (decentralized application)

A dapp is an application that runs on a decentralized > *P2P* network, such as > *Ethereum*.

data anonymization

see > *anonymization*

database shard

see > *sharding*

deanonymization

Deanonymization is the process of changing data in such a way that it becomes identifiable; it is the reverse process of > *anonymization*.

decryption

Decryption is the process of decoding an incomprehensible message or information into another form which can be easily understood by third parties; it is the reverse process of > *encryption*.

demo day

A demo day is a day on which > *startup* companies present their businesses to potential investors and other partners. Oftentimes it is seen as the “graduation” date for a cohort of firms participating in a > *incubator* or > *accelerator* program.

democratization of finance

Democratization of finance is a term describing the process by which financial services and products become more accessible to more people.

DEX (distributed exchange)

A DEX is a > *cryptocurrency exchange* that operates on a > *P2P* principle, i.e. in a decentralized fashion, permitting users to retain their > *cryptocurrencies* in their > *digital wallet* instead of handing them over to a central authority.

DG (Directed Graph)

A directed graph is a graph made up of a set of vertices (or > *nodes*) connected by edges (or lines) that have a direction associated with them, such that one can only transition between vertices along the direction of the edge connecting them.

diaas (digital identity as a service)

Diaas is a service which provides an entity with a > *digital identity*.

digest

see > *hash*

digital asset

A digital asset is an asset securitized in a digital manner, e.g. by a > *token*.

digital asset array (DAA)

A digital asset array is a bundle of > *digital assets*, such as > *token baskets.*

digital currency (electronic money, digital money)

A digital currency is a type of currency that is non-physical (i.e. no banknotes and coins exist thereof) and which can only be transmitted via electronic means, typically allowing for instantaneous transactions and borderless transfer of ownership.

digital currency exchanges see > *cryptocurrency exchange*

digital identity A digital identity is a set of information representing an external entity on a computer system.

digital money see > digital currency

digital payment A digital payment is a computer-based transaction of money authorized electronically on an electronic device.

digital security A digital security is a digital representation of a security for which ownership is verified and recorded using > *DLT*.

digital security offering see > *DSO*

digital signature see > *signature*

digital token

see > *token*

digital wallet (mobile wallet, mWallet)

A digital wallet is an electronic device that stores payment and authentication information and thus permits an individual to make > *electronic payments* and/or > mobile payments. By using digital wallets users can purchase items on-line with a computer or use smartphones to purchase something at a store. Some digital wallets also permit money transfers among users.

distributed ledger

A distributed ledger is a digital system recording and storing data and which is consensually shared and synchronized across a geographically spread network across multiple sites, institutions and/or geographies.

DLT (distributed ledger technology)

DLT is a technology based on the principle > *distributed ledgers*.

double spending

Double spending is a process that exploits a flaw in a > *cryptocurrency* system which allows a user to spend a single > *coin* twice.

double-spending attack

A double-spending attack is an attack on a cryptocurrency system aiming to conduct > *double-spending* e.g. by conducting a > *51% attack*.

DSO (digital security offering)

A DSO is a security offering executed, recorded and verified using > *DLT*; DSOs are used to issue > *digital securities*.

ecosystem (business ecosystem)

An ecosystem is a network of interacting individuals and organizations such as suppliers, producers, competitors, and other stakeholders that produces goods and services of value to customers, who are themselves members of the ecosystem.

EEA (Enterprise Ethereum Alliance)

The EEA is an alliance of organizations developing standards allowing for harmonization and standardization of > *Ethereum* applications.

electronic money

see > digital currency

electronic payment (e-payment, Epayment, electronic funds transfer)

An electronic payment is a payment made from one party to another via electronic means without the direct intervention of human staff and instead of using cash or check, in person or by mail.

EMV (Europay, Mastercard and Visa)

EMV is a global technical standard set forth by Europay, MasterCard, and Visa for credit and debit cards as well as for payment terminals and automated teller machines that can accept them.

encryption

Encryption is the process of encoding a message or information into another form which cannot be easily understood by anyone except authorized parties.

Enterprise Ethereum Alliance

see > *EEA*

ERC

ERC is an abbreviation for Ethereum Request for Comment; answers proposed to ERCs can serve as new > *token* standards

ERC-1400

ERC-1400 is a suggested standard for > security tokens so that issuers, investors, > *KYC* providers, > *digital wallets*, > *cryptocurrency exchanges*, regulators and developers can work together using the identical framework.

ERC-20

ERC-20 is a quasi standard comprising a list of rules set forth for all > *Ethereum* > *tokens*, so that developers can accurately predict how new tokens will function within the Ethereum system.

ERC-721

ERC-721 is a quasi standard for non-fungible tokens comprising a list of rules set forth for > *non-fungible* > *Ethereum* > *tokens*, so that developers can accurately predict how tokens will function within the > *Ethereum* system that bear unique information.

error avalanche

see > *Byzantine fault*

Ether

Ether is a > *cryptocurrency* > *token* which can be transferred between accounts and used to compensate > Ethereum > *nodes* for computations performed.

Ethereum

Ethereum is a public > *blockchain* based decentralized computing platform for applications that run > *smart contracts*.

Ethereum Classic

Ethereum Classic is a decentralized computing platform that runs > *smart contracts*; it came into existence as a > *hard fork* from > *Ethereum* in 2017 but is not backwards compatible with > *Ethereum*.

exchange

see > *crypto exchange*

Fabric

see > *Hyperledger Fabric*

Fiat money

Fiat money is unredeemable money that has no intrinsic value and which is made a currency by a resolution (from Latin,"fiat" meaning "let it be done").

Fiat ramp

A Fiat ramp is a > *payment gateway* that permits the user to send > *fiat money* to an account and use these funds to purchase > *cryptocurrencies*.

fiftyone percent attack

see > *51% attack*

financial inclusion

Financial inclusion is the process of making financial products and services - transactions, payments, savings, credit, investments and insurance - affordable to disadvantaged and low-income segments of society in a fair and transparent fashion. The objective of financial inclusion is to decrease those segments of society which are > *underbanked* or even entirely > *unbanked*.

Finney

Finney is a denomination of > *Ether* and a popular measurement unit of > *Gas*. 1 Ether = 1'000'000'000'000'000 Finney

first-mover advantage (FMA)

A first-mover advantage is the advantage a business gains by being the first significant player to enter a new market or market segment, leading to higher revenues and profits over time.

Flappening

The Flappening is the name of a potential future event when Litecoin reclaims its leadership of > *Bitcoin Cash* in terms of > market capitalization.

Flippening

The Flippening is the name of a potential future event when > *Bitcoin* is overtaken by another > *cryptocurrency* in terms of > market capitalization.

FOMO

FOMO is an acronym for "Fear Of Missing Out" and describes the anxiety that a value creating event may currently be happening and that one misses out on it; it regularly describes the buying behaviour when cryptocurrencies are suddenly gaining in value and more buyers appear to enter the market all of a sudden.

foreign exchange

Foreign exchange is the process by which one national currency (> *Fiat money*) is exchanged for another national currency.

Forex (foreign exchange market, FX, currency market)

Forex is the market where > *foreign exchange* takes place.

fork

A fork is a split in a > *blockchain* resulting in two individual blockchains; forks can be caused by > *51% attack*, errors in the program code, or a new set of rules for the > *consensus process*.

forking

Forking is the process of creating two alternative pieces of code, resulting in a > *fork*.

FPGA (Field Programmable Gate Array)

A FPGA is an integrated circuit that can be configured after manufacturing, allowing it to be adapted to a variety of tasks; FPGAs were used in > *cryptocurrency* > *mining* in the early 2010s, before the more price-competitive > *ASICS* came to the market; compared to CPUs, FPGAs offer higher > *hashrates* at a fraction of the electricity expenditure. FPGAs offer greater flexibility than > *ASICS*, as they can be reconfigured to mine for any > *coin*.

fraud

see > *scam*

Frontier, Homestead, Metropolis, Serenity

Frontier, Homestead, Metropolis, Serenity are the names of the four planned stages of the > *Ethereum* development roadmap.

FUD

FUD is an acronym for Fear, Uncertainty, and Doubt, describing the negative sentiment oftentimes intentionally induced by someone or of a group of individuals who want the price of coin or token to drop.

FUDster

A FUDster is an individual who spreads > *FUD*.

full node

A full node is a component of a network built on > *DLT* that fully validates every transaction and > *block* presented to it through the network by verifying them against the network's > *consensus mechanisms*.

fungible

fungible is a quality of an asset denoting that the asset can be exchanged for another asset of a similar or identical type without any significant loss occurring to the holder; to be fungible > *tokens* must not bear any unique information.

Gas

Gas is a measurement of how much processing is required by the > *Ethereum* network to process a transaction; transactions with higher Gas prices are prioritized by the network.

Gas limit

The Gas limit is the maximum amount of > *Gas* a user is willing to spend for a particular transaction on the > *Ethereum* network.

Gas price

Gas price is the price of a Gas unit denominated in > *Ether* .

general ledger

see > *central ledger*

genesis block

The genesis block is the very first > *block* of any > *blockchain*.

Git

Git is an > *open source* version control system that was developed by Linus Torvalds; it chronologically records changes to a file or set of files so that developers can recall any earlier versions of the code at a later point in time.

Git commit

see > *commit*

Github

GitHub is an online hosting service for version control using > *Git*; GitHub is Web-based and offers distributed version control and source code management functionality.

Gwei

Gwei is a denomination of > *Ether* and a popular measurement unit of > *Gas*.
1 Ether = 1000000000 Gwei.

halving

Halving is the process of reducing the rewards per mined block in order to maintain the total supply of a coin or token; it was first applied to > *Bitcoin* where the reward is halved after the first 210,000 > *blocks* are mined and then every 210,000 thereafter.

hard cap

The hard cap is the maximum number of coins that will ever be created (e.g. 21mn. for Bitcoin); not all cryptocurrencies have a hard cap (e.g. > *Ether*).

hard fork

A hard fork is a specific form of a > *fork* which occurs when the developers of a > *blockchain* decide that changes must be made to the code so that it will create lasting incompatibilities between the older and newer version; contrary to a > *soft fork* a hard fork requires that all > *nodes* upgrade to the new version of the code; as all nodes will only recognize the new blocks as valid, a softfork is backward-compatible.

hardware wallet

see > *cold wallet*

hash

A hash is the result of executing a > *hash function*.

hash code

see > *hash*

hash function

A hash function is a one-way > *algorithm* used to map data of arbitrary size onto data of a fixed size.

hash value

see > *hash*

hashed

Hashed is an attribute of a data set which has been transformed using a > *hash function*.

Hashgraph

Hashgraph is a > *DLT* and alternative to > *blockchain* which achieves superior performance by using a > *consensus mechanism* based on a virtual voting > *algorithm* combined with the gossip protocol.

hashing

Hashing describes the process of executing a > *hash function*.

hashrate

The Hashrate denotes the speed at which > *hash functions* are executed.

HFT (high frequency trading)

HFT is a form of trading using sophisticated systems to transact a large number of orders at extremely high speeds.

HODL

HODL is slang term used in the cryptocurrency community for holding a cryptocurrency rather than selling it; it can also be interpreted as an acronym for "Hold On for Dear Life".

hot storage

A hot storage is an electronic device that stores > *cryptocurrencies* and which is connected to the Internet; it is typically easier to setup, access, scale than > *cold storage* but more susceptible to unauthorized access, hacking attacks, and other vulnerabilities.

hot wallet

A hot wallet is a > digital wallet *employing* > hot storage technology

Hyperledger

see > *Hyperledger Fabric*

Hyperledger Fabric

Hyperledger Fabric is an > *open source* modular platform based on > *blockchain* technology designed for enterprise contexts.

IaaS (ICO as a Service)

see > *IEO*

ICO Advisor

An ICO Advisor is a person who advises a project on the various facets of an > *ICO*, such as legal, business modeling, > *tokenomics*, technology, marketing and industry.

ICO Rating

see > *rating*

IEO (initial exchange offering, ICO as a service)

An initial exchange offering (IEO) - or ICO as a service (IaaS) - is a process in which > *cryptocurrencies* are sold via a > *crypto exchange*: The exchange takes the position of the issuing project in the offering process and after the project has provided the newly mined cryptocurrencies to the exchange, the exchange collects funds (e.g. > *Ether* , > *Bitcoin,* > *Fiat money* etc.) from contributors and allots the newly mined > *coins* or > *tokens* to the contributors.

immutability

Immutability is a feature of data stored on the > *blockchain*. Hence, the blockchain contains a history of transactions which is typically permanent, inerasable, and unalterable history of transactions. Immutability can be threatened by extraordinary events, such as > *51% attacks*.

Incubator

An incubator is an organization that accelerates the development of new and > *startup* companies by providing entrepreneurs with an array of targeted resources and services such as office infrastructure and management training. Through their network of contacts incubators often provide new paths to funding from > *Angel Investors*, > venture capital firms and other investors. The services provided by incubators are usually developed and orchestrated by the incubator management.

initial coin offering (ICO)

An initial coin offering is an unregulated means of > *crowdfunding* applied by > cryptocurrency businesses as an alternative to the rigorous and regulated capital-raising process required by venture capitalists, banks, or stock exchanges. In an ICO a percentage of the newly issued > *cryptocurrency* is sold to investors in exchange for legal tender or other cryptocurrencies such as Bitcoin.

Initial Token Offering (ITO)

An Initial Token Offering is largely identical to an > *Initial Coin Offering*, yet it typically pertains to projects built on the > *Ethereum* > *blockchain*.

IPO (initial public offering)

An initial public offering is the process by which a private company is offered for the first time to the general public on a securities exchange. IPOs are typically conducted by small and young firms seeking capital to expand, but they can also be done by large privately-owned companies looking to become publicly traded.

know your customer (KYC)

KYC is a set of principles for identifying and verifying the identity of banking clients to adhere to anti-money laundering regulations, but also to ensures that the bank has detailed information on the clients' risk tolerance, investment knowledge and financial standing.

lambo

lambo is an abbreviation for Lamborghini; owning one appears to be the objective of many participants in the crypto > *ecosystem*.

ledger

A ledger is record-keeping system for recording and totaling economic transactions; in banking the ledger was the principle book or "bank book", containing all debit and credit account records of the bank.

Ledger Nano

Ledger Nano is a popular USB > *cold wallet* to store > *cryptocurrencies*.

Lightning Network

The Lightning Network is a payment protocol that was created on top of > *blockchain*-based > *cryptocurrencies* such as example > *Bitcoin*. It reduces the number of interactions on the blockchain and thus enables faster transactions and thus higher levels of scalability.

Lightweight Node

A Lightweight Node is a component of a network built on > *DLT* that performs basic and limited functions contributing to authenticating and validating the transactions on the network.

Litecoin

Litecoin is a > *blockchain* based > *cryptocurrency* following the > *P2P* principle and resulting from an open-source software project that was published on Gibthub in 2011. The intervals between > *mining* > *blocks* is shorter than with > *Bitcoin* and due to the usage of different > *algorithms* > *FPGA* and > *ASIC* devices are harder to deploy for Litecoin mining than for Bitcoin mining.

majority attack see > *51% attack*

maker fee Maker fees are charges due when a market participant places a limit buy order below market price or a limit sell order above market price; as this action adds liquidity to the market, the maker fee is on crypto currency exchanges oftentimes lower than the opposite, the > *taker fee*.

market capitalization (market cap.) Market capitalization traditionally refers to the total market value of a company's outstanding shares; in the context of cryptocurrencies it denotes the total value of a project's > *tokens* or > *coins* in circulation.

Master Node A master nodes is a > *full node* in a network built on > *DLT* which keeps the complete copy of the > *distributed ledger* in real-time and is online 24/7; master nodes may also support the network by governing voting events, executing protocol operations, enforcing the laws of the corresponding network etc.

math based currency see > cryptocurrency

maximum supply

see > *hard cap*

Meta Mask

MetaMask is a browser extension for accessing > *dapps*; as such it can also serve as a > *digital wallet*.

MEW (My Ether Wallet)

MEW is a free, > *open source* > *software wallet* for usage in the > *Ethereum* network.

Miner

A miner is a person that engages in > *mining*.

Minimum viable product (MVP)

A minimum viable product is an early version of a product with just sufficient features to satisfy early adopters, and to collect feedback for future product development.

Mining (to mine)

Mining describes the process of creating new block on a > *DLT* system such as the > *blockchain* by validating transactions and demonstrating > *PoW* and as a result being rewarded with newly created > *coins* > *tokens* as a result.

mining rig

A mining rig is a computer system especially designed for carrying out > *mining* tasks and is thus typically using > *ASIC* technology.

mobile payment

A mobile payment is a > *digital payment* via a mobile device so that the transaction can be conducted independently of the geographic location of the person conducting the transaction.

mobile wallet

see > *digital wallet*

money laundering

Money laundering is the process of transforming monetary proceeds of crimes into apparently "legitimate" assets.

mooning

Mooning is the process of a > *token* or > *coin* undergoing an extreme price hike, it's "going to the moon". The price goes up to astronomical levels. It may be the first phase of a > *pump and dump* scheme.

mPOS

Describes a mobile > *POS*. It is the place where sales are made in case mobile business is conducted.

multichain

A multichain is a platform that bridges different > *blockchain* technologies. As such it makes different > *DLTs* compatible.

multisig (multisignature)

Multisig is a process that requires more than one signature to approve a transaction before it can be transmitted to the > *blockchain* and thus increases security for > *cryptocurrency* transactions.

mWallet

see > digital wallet

NFT (non-fungible token)

An NFT is a > *non-fungible* > *token*, i.e. a token that bears some unique information; NFTs are therefore oftentimes considered collectable tokens

node

A node is device on a network that represents a piece of a > *DLT* and carries out certain tasks such as maintaining a copy of a > *ledger* or parts thereof, processing transactions etc.

nonce

A nonce is an arbitrary number or string that can be used only once in a cryptographic communication.

non-fungible

non-fungible is a quality of an asset denoting that the asset cannot be exchanged for another asset of a similar or identical type without any significant loss occurring to the holder; to be non-fungible > *tokens* must bear some unique information.

off chain

Off chain is a property of a transaction denoting that it does not occurs on a > *distributed ledger* such as the > *blockchain.* An off chain transaction does not have to validated it is typically faster than an > *on chain* transaction.

on chain

On chain is a property of a transaction denoting that it occurs on a > *distributed ledger* such as the > *blockchain*, and thus that it is reflected there as soon as its state has been validated. An on-chain transaction is therefore regularly slower than an > *off chain* transaction.

Onboarding (client onboarding)

Onboarding is the process of adding a new client to the existing group of clients or members of an organization and familiarizing the client or member with services, products, and processes. In the case of financial services, onboarding regularly involves > *AML* as well as > *KYC* procedures.

Online Wallet see > *digital wallet*

open API An open API is a publicly available > *API* that provides third-party developers with the necessary information to access a proprietary system in order to build applications communicating with this system.

open source Open source is a principle according to which the source code of software is made available to anyone and for any purpose, such as inspection, modifying, and distribution by the copyright holder.

P2P (peer to peer) P2P is a quality of decentralised system describing the fact that all participants (peers) are equally privileged and equipotent participants; in the context of the > *blockchain*, P2P describes a network of equally privileged and equally potent > *nodes*.

paper wallet A paper wallet is a printout of the wallet > *address* and > *private key* and thus a specific form of > *cold storage*.

Parachain (parallelizable chain)

A parachain is a simpler form of > *blockchain*, which builds on the security features provided by a > *relay chain* rather than providing its own. One key feature of a parachain is that the computations it performs is inherently independent of the relay chain.

payment gateway

A payment gateway is a merchant service that authorizes payment processing (credit card, debit card, Paypal, > *cryptocurrencies* etc.) for retailers of any kind, e.g. online businesses, physical stores, restaurants etc.

PayTech

PayTech is a subset of > *Fintech* and a new domain within the financial industry that applies technology to improve payments. It builds on technologies such as the > digital wallet,> *DLT* and > *NFC* and strives to advance > *electronic payments* and/or > mobile payments, both at > *POS* and > *mPOS.*

PIN

A PIN is a numeric or alphanumeric password or code used in many electronic financial transactions for authenticating or identifying a user to a system and/or a system to a user.

Pitch

A pitch is a business plan delivered verbally by an entrepreneur to potentials investors or other parties.

plasma

Plasma is a combination of different methods to make the > *blockchain* more scalable.

platform

see > *crypto protocol*

POC (proof of concept), also PoC (proof of concept)

In project management a PoC is a significant accomplishment which demonstrates that the realization of a certain method, concept or idea is feasible.

POP (proof of principle)

see > *PoC (Proof of Concept)*

PoS (Proof of Stake)

Proof-of-stake is a > *consensus process* that requires network participants to ‘lock up’, resp. 'stake', specific quantities of > *tokens* used in the network for a short amount of time in order to ‘vote’ and generate network consensus; the participant can > *mine* or validate > *block* transactions corresponding to the quantity of > *coins* or > *tokens* he or she holds: the more coins or tokens are held by the miner, the more mining power he or she has.

PoW (proof of work)

Proof of work is a > *consensus process* that requires a datum that is very costly to produce in terms of time and/or resources, yet which can be very simply verified by another party; PoW for > *Bitcoin* is referred to as a > *nonce*.

pre-mined

Pre-mined is an attribute describing the process throughout which > *coins* or > *tokens* are being put in circulation: if pre-mined all tokens will be put in circulation upon > *ICO*.

pre-sale

A pre-sale is a phase that can occur during an > *ICO* and which is held in advance of the regular sale; select investors can then typically buy > *coins* or > *tokens* at a significant discount.

private key

A private key is a confidentially kept string of code that - when paired with a > *public key* - sets off > *decryption* > *algorithms*, for instance permitting users to access their > *cryptocurrencies*.

private sale

Private sale is a sales process where tokens or > *cryptocurrencies* are tendered to a clearly defined group of investors, rather than being sold to the broader public.

proof of work

see > PoW

Proof of address

A proof of address serves as evidence for the registered domicile of a user and is typically obtained during a > *KYC* process (e.g. a bank statement mentioning the address of a client, a utility bill etc.)

Proof of burn

Proof of burn is a method used in the context of > *coin burn* to proof that a specific number of coins or tokens were irrevocably burnt by sending them to an address from which they cannot be retrieved.

Proof of identity

A proof of identity serves as evidence for the true identity of a user and is typically obtained during a > *KYC* process (e.g. a copy of a passport, official ID etc.).

proof-of-keys

The proof of keys is a movement, rallying for investors to remove all their > coins and > *tokens* from third-party > *crypto exchanges* and other third-party service providers on a specific date. The event compels the service providers to evidence that they hold the crypto funds they claim to store for the client and that they are thus in possession of the users' > *private keys*.

protocol

see > *crypto protocol*

PSD2 (Payment Services Directive 2)

PSD2 is the second Payment Services Directive, set forth by the European Union which aims at improving consumer protection with regards to online payments, promoting the development and use of innovative online and > *mobile payments*, and making European cross-border payments more secure.

PSP (payment service provider)

A PSP is a firm that offers other business services for accepting > *electronic payments* and thus establishes a connection between shops and financial institutions such as banks and credit card firms, but also > *cryptocurrency* > *payment* gateways.

public address

A public address is a > *hashed* version of the > *public key*.

public key

A public key is a publicly known string of code that is related to a > *private key* and used in algorithms to encrypt data, for instance to send > *cryptocurrencies* to a user’s > *address*.

pump and dump (P&D)

Pump and dump is a type of > *scam* in which the fraudster buys a > coin or > token and then artificially inflates its price using false and misleading positive statements in order to sell it thereafter at a higher price.

pumping

see > *shilling*

race attack

A race attack is a specific type of a > *double-spending attack* exploiting information asymmetries: the attacker (payer) supplies a payment transaction to the victim (vendor) as well as to the network. If the victim sees the unconfirmed transaction first, before the network rejects the transaction as a > *double spending*, there is a large likelihood that the victim will never get paid.

Raiden Network

The Raiden Network is a complementary extension to the > *Ethereum* network intended to allow for near-instant, low-fee and scalable transactions with any > *ERC20* compatible token.

rating

A rating is a relative estimate or evaluation; > *ICO* ratings are regularly used to advertise the alleged quality of an ICOs.

reddit

Reddit is a US-American social news aggregation, web content > *rating*, and discussion website; the user community can submit as well as vote on content as diverse as links, text posts, images etc.

RegTech

RegTech is a new domain within the financial industry that applies technology to improve regulatory processes, especially with regards to > KYC and > AML.

regulatory sandbox

A regulatory sandbox is a supervised space, open to both authorized and unauthorized firms, that provides a set of rules that allows innovators to test their products and services in a live environment without following some or all legal requirements, subject to predefined restrictions.

relay chain

The relay chain is a > *blockchain* that lends security to attached > *parachains* and ensures secure message-passing between them.

restricted countries

Restricted countries is a list of countries in which specific > *coins* and > *tokens* are not offered for sale throughout an > *ICO* process.

ROI (Return on Investment)

The ROI is a performance measure used to evaluate the efficiency of an investment in terms of the amount of return an investment yields relative to the investment's costs; ROI = (Investment Payoff - Investment Cost) / Investment Cost.

SAFT (Simple Agreement for Future Tokens)

The SAFT is an agreement conveying rights in > *tokens* prior to the development of the tokens' functionality; it ensures the delivery of > *tokens* to the investors once a functioning application has been developed for that token.

Sandbox

see > *regulatory sandbox*

Satoshi Nakamoto (SATS)

Satoshi Nakamoto is a pseudonym used by an individual or a group of individuals who developed > *Bitcoin*, devised the Bitcoin > *white paper*, and developed the first > *blockchain*.

SATS

see > *Satoshi Nakamoto*

scam (fraud)

A scam is an intentional deception to deprive another person of his or her right and to secure an unlawful gain and thus a dishonest scheme, resp. fraud; in the world of > *cryptocurrencies* various types of scam exist, varying from deceptive > *ICOs* where the company has little more to offer than a > *white paper*, to unjustified fees and costs charged by unregulated > *crypto exchanges* and malware using devices *to* > *mine* > *Bitcoin* without the user's consent.

secret key

see > *private key*

security token

A security token is an investment vehicle which has the character of a security, i.e. it is bought in anticipation of future profits in form of dividends, revenue share, or price appreciation.

Segregated Witness (Segwit)

SegWit is the label used for a > *soft fork* implemented on some > *blockchain* protocols, such as > *Bitcoin*, which changes the transaction format so that it transfers parts of the transaction data out of the main > *block*, thus reducing the effective size of transaction and thus allowing more transactions to fit into a single block without increasing the > block size.

sell wall

A sell wall is an expression describing a situation when the amount/size of sell orders for a particular > *coin* or > *token* is significantly larger than the number of sell orders.

shard

see > *sharding*

sharding

Sharding is a specifying type of database partitioning: it divides large databases, such as the > *blockchain* the into smaller, faster, more easily manageable parts called database shards or shards.

Shilling (pumping)

Shilling is the process of someone heavily advertising a > *cryptocurrency*; it is the first part of > *pump and dump* schemes.

Shitcoin

A shitcoin is a > *token* or > *coin* which has no value or utility (any longer).

side chains

A sidechain is a separate > *blockchain* that is attached to its parent blockchain (mainchain) using a two-way peg.

Signature

A signature is the mathematical operation for verifying the authenticity of a transaction or a document and can for instance be used to prove someone's ownership over his/her > *digital wallet*, > *coins* or data.

smart contract

A smart contract is an online contractual agreement based on the > *Ethereum* > *blockchain* that runs exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

soft cap

In the context of an > *ICO* or an > *ITO*, a soft cap is the minimum amount of money a project intends to raise. If this minimum amount is reached, the ICO or ITO is considered a success; although normally the project is expected to return the funds if the soft cap is not reached, there have been cases of projects keeping the funds despite the > *ICO* or > *ITO* not being successful which may be considered a > *scam*.

soft fork

A soft fork is a specific form of a > *fork* which occurs when the developers of a > *blockchain* decide that changes must be made to the code so that previously valid blocks are made invalid; contrary to a > *hard fork* a soft fork requires that only a majority of > *nodes* upgrade to the new version of the code; as old nodes will continue to recognize the new blocks as valid, a soft fork is backward-compatible.

software wallet

A software wallet is a > *digital wallet* existing as an application on a computer and typically employs > *hot storage* technology.

Solidity

Solidity is an object-oriented programming language that smart contracts can be written in; it can be used on various > *DLT* platforms.

spoofing

Spoofing is a form of market manipulation, resp. > *scam*, in which a market participant places a large buy or sell order with no intention of executing it. By doing so he or she creates an artificial impression of high or low demand for a traded asset and thus oftentimes induces price changes.

spread

A spread is the difference between the highest bid and the lowest ask price of an asset. Low spreads are a sign of a liquid markets.

stable coin

Stable coins are > *coins* that correlate relatively little with overall cryptocurrency markets. Oftentimes stablecoins are pegged to single > *fiat monies* or to exchange traded commodities.

staking

Staking is part of the > *proof of stake* > *consensus process* which requires network participants to ‘lock up’, specific quantities of tokens used in the network for a short amount of time in order to ‘vote’ and generate network consensus; typically staking is rewarded depending on the size of the stake provided.

startup (start-up, startup company) .

A startup is a business that is in the process of being setup or one that has just recently begun operation.

state channels

State channels are secure transactions among > *DLT* users that occur off the blockchain and thus minimize the use of on-chain operations; they are used, for instance, in the > *Raiden Network* or > *Lightning Network*.

STO (security token offering)

An STO is an event at which a > *security token* is offered at a set price before being offered on an exchange, similarly to an > *IPO* in traditional finance; discounts may apply at this time; STOs are subject to country-specific regulations.

Szabo

Szabo is a denomination of > *Ether* and a popular measurement unit of > *Gas*. 1 Ether = 1000000000000 Szabo.

taker fee

Taker fees are charges due when a market participant places a market or limit order that executes immediately against a limit order already on the orderbook; as this action removes liquidity from the market, the taker fee is on > *cryptocurrency exchanges* oftentimes higher than the opposite, the > *maker fee*.

Tangle

Tangle is a > *DLT* that requires the user to approve of two previous transactions if he/she wants to carry out a new one; by doing so the initiator of a new transaction indirectly confirms that a subsection of the Tangle is valid and that it conforms to the protocol rules; it thus represents Tangle’s > *proof of work*; Tangle therefore merges the transaction making process with the > *consensus mechanism*.

tap

A tap is a poll among the investors in the > *DAICO* process aimed at securing capital for certain tasks in the course of the project.

Telegram

Telegram is a cloud-bases instant messaging application, similar to WhatsApp, Line and Facebook Messenger. One of Telegram's defining features are its "supergroups", that can group up to 100.000 users in a single group-chat. This feature makes Telegram the platform of choice for mass-communication. The application has become very popular in the crypto world, where it is routinely used by companies, investors and other parties to communicate investing opportunities.

TFA (two factor authentication)

see > *2FA*

This is it, gentlemen

“This is it, gentlemen” is used in the crypto community to point out positive things that are currently happening.

timestamp

A timestamp is a set of information identifying the time at which an event is recorded by a computer; on the > *blockchain* timestamps show the chronological order of the > *blocks* and marks the exact time of each transaction; timestamps prove what has happened when on the blockchain.

timestamping

Timestamping is the process of proving that a certain event occurred priori to a certain point in time; timestamping based on > *blockchain* > *timestamps* is particularly trustworthy, since timestamps on the blockchain are subject to > *immutability*.

Token

Tokens are > *cryptocurrencies* that are created and accounted for in > *DLT* systems and represent an asset, a usage right or a unit of value issued by a organization and are typically emitted throughout an > *ICO*, > *ITOs*, or > *private sale*; oftentimes, > *tokens* do not run on proprietary DLT systems, but use other > *cryptocurrencies'* > *blockchains*, most typically > *Ethereum*.

token basket (token set)

A token basket is a composite collection of > *tokens* that has been created using an > *Ethereum* **>** *smart contract*; token baskets allow for investing in a collection of > *digital assets* rather than investing in each of those assets individually.

token contract

A token contract is a > *smart contract* on the > *Ethereum* network.

token contract address

A token contract address is the location of the actual > *token contrac*t that manages the logic for tokens.

token gravity

Token gravity is a concept describing how > tokens are expected to move within a digital ecosystem

token sales

Token sales is the process of tendering newly mined > *tokens* or > *coins*, oftentimes in the context of an > *ICO* or > *STO*.

token set

see > *token basket*

tokenization

Tokenization is a method of protecting sensitive information by substituting a critical data element with a non-sensitive unique alphanumeric identifier, referred to as a token, that has no exploitable meaning or value to third parties. E.g. tokenization can be used to create a representation of a real-world asset by a digital token.

Tokenomics

Tokenomics (umbrella term that encompasses > *token* and economics) is the economics underlying a token: it sets forth when, which quantity of tokens are issued and burned and for which purposes they can be used and when; it thus determines the framework for supply and demand.

total supply

The total supply is the total amount of > *tokens* or > *coins* in existence at the present; it is equal to the total amount of coins/tokens mined minus any that have been verifiably > *burned*.

TPS (transactions per second)

TPS is the rate at which a system can process transactions, i.e. at which rate blocks can be created on the > *blockchain*.

trading bot

A trading bot is an application that is directly linked to > *crypto exchanges* oftentimes via an > *API* and, programmed to trade > crypto currencies following pre-defined > *algorithms*.

transaction fee

A per transaction fee is an expense a user must pay to an intermediary for conduction a transaction on a specific system. On > *cryptocurrency exchanges* fees are typically calculated based on a percentage of the notional order value for a matched trade; the fees typically differ between > *maker fee* and > *taker fee*.

transactions per second

see > *TPS*

Trezor

Trezor is a popular USB > *cold wallet* to store > *cryptocurrencies*.

Turing complete

Turing complete is a term given to a system that is able to recognize or decide specific other data-manipulation rule sets (the ones used by Turing Machines); Turing complete is a label used to express the power of such a data-manipulation rule set; the large majority of modern programming languages are Turing complete.

unbanked

Unbanked is a characteristic describing people who do not use banks or financial institutions oftentimes because they do not have access to banking services or because they prefer cash transactions outside the banking system.

underbanked

Underbanked is a characteristic describing people who do not have sufficient access to mainstream financial services and products typically offered by retail banks and thus regularly rely on cash and checks as a mean of funding rather than bank related methods such as credit cards or loans.

utility token

A utility token is > *token* issued in order to fund the development of an IT systems and/or business model and can typically be used to later on purchase goods or services created by the issuer of that token and can thus oftentimes be seen as usage rights.

vesting

Vesting is a term characterising the fact that an asset is wholly owned by an investor; crypto projects oftentimes implement long-lasting token release vesting schedules for their token sale investors, locking them into those tokens for a considerable period of time.

virtual currency

see > *digital currency*

Vitalik Buterin

Vitalik Buterin is a Russian-Canadian developer best known as a co-founder of > *Ethereum*.

wallet

see > *digital wallet*

Wash Trade

A wash trade is a trade on an exchange used to manipulate the market: An investor

simultaneously sells and buys the identical financial instruments in order to create exaggerated and potentially misleading activity in the marketplace. Wash trades are often used by
> cryptocurrency exchanges to inflate trading volumes.

Weak Hands Weak hands is a term used to describe investors selling their assets during a negative market sentiment, similar to a card players who folds their cards at the first sign that they are going to lose; typically weak hands will sell during lows.

Wei Wei is the smallest denomination of
> *Ether* and a measurement unit of > *Gas*.
1 Ether = 1'000'000'000'000'000'000 Wei

Whale Whale is a term used to describe participants in the cryptocurrency market that are large enough to influence it; in this context the ocean serves as a metaphor for the entire market as it is home to large and small fish and waves can be understood as market movements.

White Paper A white paper is an in-depth report that aims to educate the reader on a particular issue, or explain a particular methodology or solution; in the crypto-world white paper often refers to the document issued by companies priori to their > *ICO* or > *STO* informing the reader of the purpose of the > *ICO* or > *STO* and the technology behind it, in which case the white paper could be argued to be a tool to help the company sell the > *cryptocurrencies*.

whitelisting

Whitelisting is the process of explicitly allowing specific identified investors to participate in a token sale.

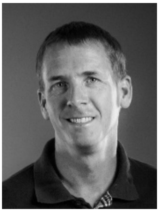
This page intentionally left blank

POSTFACE

This book is far from being complete. As an emerging field the topic of cryptocurrencies, tokens and digitalassests is constantly evolving. Hence, should you be missing one particular term or expression which you believe ought to be included in this booklet, do send us an e-mail: patrick.schueffel@hefr.ch
We look forward to hearing from you!

Patrick Schueffel
Nikolaj Groeneweg
Rico Baldegger

About the authors



Patrick Schueffel is professor at the School of Management Fribourg, Switzerland, and the institution's Liaison Officer in Singapore. His research focus is on Banking, Finance and Entrepreneurship. After a long-time banking career in Zurich, he is now also active as a founder, investor and advisor in the Singaporean and Swiss Crypto scene alike and enthusiastically connecting the dots between Europe and Asia.

Nikolaj Groeneweg is an entrepreneur and A.I. engineer with a decade of experience on the intersection of business and technology - growing startups and helping corporates bring to market new initiatives. He is currently based in Singapore, where he is a founder in the Crypto scene and an advisor to companies looking to do business in Asia Pacific.

Rico Baldegger is the Rector of the School of Management Fribourg, Switzerland, and teaches and researches at this institution as a professor. His research focus is on Business Administration, Innovation, Entrepreneurial Economics and International Economics. As a serial entrepreneur he has helped creating numerous companies active in Switzerland and abroad.

What is the blockchain? What is a distributed ledger? What do people mean when they talk about ERC-20? What is the difference between a hard and soft fork? And between hot and cold storage?

Containing over 300 entries on all aspects of crypto, tokens and digital assets, this encyclopedia incorporates the latest information available from academia and practice on these topics. Loaded with clear, concise, and authoritative information, it is the most comprehensive single-volume A-Z reference work of its kind.

Our aim in preparing this dictionary is to share the vocabulary of a newly emerging field of business and research endeavour. We are convinced that this will make a major contribution to our mutual understanding. It thus is essential for all practitioners, students and educators in the field of crypto who want to ensure that we use a common language throughout the ecosystem.

GROWTH-PUBLISHER BERN

ISBN 978-2-940384-47-1

9 782940 384471 >