# Bitcoin – slovník

Při studiu Bitcoinu a ekonomie pravděpodobně narazíte na spoustu cizích termínů/zkratek, kterým bez vyhledání nebudete rozumět. Zde je slovník všech důležitých slovíček z této oblasti, který by Vám mohl pomoci ve studio Bitcoinu a ekonomie. V případě, kdyby Vás napadl důležitý pojem/zkratka, na který jsem při psaní tohoto slovníku zapomněl, kontaktujte mě prosím na email ekonomie-jednoduse@proton.me :)

*51% útok*: Jeden z typů útoku na blockchain. Útok, při kterém má těžař nadpoloviční (respektive v praxi to může být i mnohem méně, jde o to, aby daný pool dokázal uzavřít více bloků za čas *t* než ostatní těžaři) výpočetní výkon (hash rate), pomocí něhož provede reorganizaci blockchainu a potenciálně může provést i double spending útoky.

*Akcie:* Cenný papír vyjadřující podíl na vlastnictví určité společnosti. Držitel akcií, akcionář má různá práva, například právo se podílet na zicích firmy formou dividendy.

*Aktivum*: Aktivum je cokoliv, co přináší jeho vlastníkovi nějaký výnos nebo se očekává, že mu ho v budoucnu přinese.

*Algoritmus*: Předem určený postup, kterým se řeší daná úloha. Algoritmy se nejčastěji používají v programování, ale obecně tento pojem můžete najít i v jakémkoliv jiném vědeckém oboru. Algoritmy v informatice mají tyto základní parametry:

1. Determinovanost
   Determinovanost (jednoznačnost) znamená, že je postup práce předem určený a vždy závisí pouze na popisu algoritmu a na vstupu.
2. Konečnost
   Každý algoritmus z definice musí jednou končit (po konečném počtu provedených kroků).
3. Rezultativnost
   Aby algoritmus mohl být algoritmem, musí vždy vydat určitý výsledek.
4. Jednoduchost popisu
   Každý algoritmus je popsaný počtem s konečným množstvím základních instrukcí. Jedná se tedy o instrukce, o kterých přesně víme, jak se provedou.

*Alokace (zdrojů*): Přidělení omezených zdrojů určitému subjektu (firmě, domácnosti). Vzácné zdroje se alokují za pomocí tržních cen, tedy cen, které určuje poměr nabídky a poptávky.

*Altcoiny:* Alternativní kryptoměny k Bitcoinu. Jedná se o všechny kryptoměny kromě Bitcoinu.

*AML:* Anti Money Loundering je opatření snažící se zabránit praní špinavých peněz a financování terorismu. AML vyžaduje identifikaci klientů u finančních služeb, například kryptoměnových burz.

*Anarchokapitalismus:* Ideologie, která odmítá veškerou existenci centrální moci – státu. Anarchokapitalismus je postaven na volném trhu a svobodě jednotlivce. Mnoho Bitcoinerů se právě za anarchokapitalisty považuje.

*Antifragilita*: Pojem, který proslavil Nassim Nicholas Taleb ve stejnojmenné knize. Antifragilní systémy těží z chaosu a nejistoty, krizemi a tlakem získávají na síle. Antifragilita je zjednodušeně odolnost vůči okolním jevům. Opakem je pak fragilita, křehkost chcete-li. Typickým příkladem fragility je centralizovaná moc, například stát. Někteří lidé se domnívají, že Bitcoin, co by technologie je antifragilní, poněvadž každý útok, který přežije, ho činí silnějším a odolnějším.

*ASIC*: Application-Specific Integrated Circuit je hardware, který je sestrojen k jedné specializované činnosti. U Bitcoinu se k těžbě využívají takzvané ASIC minery, specializované stroje přímo k těžbě.

*Asymetrická kryptografie:* Typ šifrovacích algoritmů, ve kterém se používá klíčový pár, privátní a veřejný klíč. Tento šifrovací algoritmus používá Bitcoin.

*ATH* – All Time High: ATH znamená nejvyšší cena v historii. Často se tento název používá ve spojení s bitcoinem či jinými kryptoměnami. Takže, když se někde řekne, že bitcoin dosáhl nového ATH, znamená to, že je na historicky nejvyšší ceně.

*Bankovnictví částečných rezerv (frakční bankovnictví)*: Období v historii, při kterém komerční banky musely mít určité rezervy k emitenci nových peněz. Rezervami chápeme vklady na bankovních účtech.

*Barter*: Barterový neboli směnný obchod, je ten, při kterém s dalším člověkem přímo směníte své zboží za ním nabízené zboží. V barterové transakci tak

neexistují peníze, ale jedná se přímo o obchod, ve kterém směňujete zboží za jiné zboží či službu.

*Batching:* Transakce s více výstupy (adresami, na které mají být bitcoiny zaslány). Batching umožňuje sloučit více transakcí do jedné, čímž pomáhá snížit transakční poplatek. Bez batchingu by totiž bylo potřeba vytvořit několik on-chain transakcí na to, aby se z jedné adresy odeslaly bitcoiny na více jiných adres. S batchingem stačí pouze jedna transakce na základní vrstvě Bitcoinové sítě.

*Bearish*: Medvědí. „Medvědí" trh znamená, že trh očekává dlouhodobý pád akcií, Bitcoinu či jakéhokoliv jiného investičního instrumentu, větší než 20 %. Pád menší než 20 % se označuje jako korekce.

*Bimetalismus:* Peněžní systém, ve kterém souběžně obíhají dva kovy, což historicky bylo zlato a stříbro. Tyto dva kovy mají stejnou nominální hodnotu, tedy si za ně koupíte stejné množství zboží, a to i přes to, že mají jinou skutečnou hodnotu, což znamená, že je jeden kov vzácnější a tím pádem by měl mít i větší kupní sílu. V takovém případě funguje takzvaný Greshamův zákon. Bimetalismus fungoval například ve Spojených státech, a to v 18. a 19. století.

*BIP*: Bitcoin Improvement Proposal je návrh o změnu, vylepšení Bitcoinové sítě. V BIPu se zpravidla nachází technická specifikace určité úpravy. Pochopitelně zde zároveň naleznete důvod, proč by tento návrh měl být do Bitcoinu implementován, jak by Bitcoinu mohl pomoci. Není pouze jeden typ BIPu, nýbrž jich existuje více.

*Bitcoin*: Bitcoin s velkým B je označení pro celou technologii, zatímco bitcoin s malým počátečním písmenem je pouze účetní jednotka, se kterou se obchoduje.

*Bitcoinizace:* Proces adopce bitcoinu, co by platidla. Tento proces se dělí na tři kroky, podle toho, jakou peněžní funkci již Bitcoin splňuje: prvně uchovatel hodnoty, následně prostředek směny, a nakonec účetní jednotka. Bitcoinizovat se je možné na individuální úrovni – bitcoinizace vlastních úspor, na korporátní (firemní) úrovni, a dokonce i na úrovni států (příkladem je země ve střední Americe jménem El Salvador, u které je bitcoin zákonným platidlem).

*Bitcoinový automat (Bitcoinmat):* ATM na bitcoin. Způsob, kterým lze do určité částky (25.000 Kč) nakoupit bitcoin bez KYC. Nevýhodou bitcoinmatů jsou vysoké poplatky.

*Bitcoinový klient*: Software, který si uživatelé Bitcoinu instalují na svá zařízení, aby mohli provozovat plnohodnotný uzel v Bitcoinové síti.

*Bitcoinový protokol*: Bitcoinový protokol je souhrn pravidel, kterými se síť Bitcoinu a její uživatelé řídí. V Bitcoinovém protokolu je určeno, kolik s kdy mincí bude vytěženo, jakým způsobem se navzájem Bitcoinové uzly spojují, jak lze nové bitcoiny vytvořit a spousta dalších parametrů.

*Bitcointalk:* Nejznámější Bitcoinové fórum, kde svého času zveřejňoval příspěvky i samotný Satoshi Nakamoto.

*Bitcoin Core:* Bitcoinové jádro. Nejoblíbenější software používaný k připojení k Bitcoinové síti a provozování vlastního uzlu.
*Bitcoin maximalismus:* Filosofie, která automaticky zavrhuje veškeré altcoiny. A to jednak kvůli jejich technickým, ale i ekonomickým problémům. Přeci jenom naprostá většina altcoinů je podvod a ten zbytek neřeší tak zásadní problém jako Bitcoin (nutno si uvědomit, že bitcoin je jedinými vzácnými nestátními penězi svého druhu), respektive dle slov Bitcoinových maximalistů altcoiny neřeší vůbec žádné problémy a jsou pro společnost naprosto zbytečné.

*Bleskomat:* ATM (bankomat) na nákup Lightning Network bitcoinu, pomocí technologie LNURL-withdraw.

*Blockchain*: Řetězec bloků. Flexibilní a bezpečný způsob uspořádání dat, který v kombinaci s mechanismem konsenzu může umožnit úspěšné fungování decentralizovaného systému. V případě Bitcoinu se jedná o veřejnou databázi s nezměnitelnou historií, do které se zapisují veškeré transakce.

*Block subsidy*: Množství bitcoinů, které vzniknou uzavřením bloku.

*Blok (block)*: Soubor v blockchainu, do kterého se zapisují transakce, které byly uskutečněny v době po předchozím bloku (což je zhruba 10 minut), hash předchozího bloku, časové razítko a nonce. Každý blok potvrzuje blok předchozí. Tyto bloky jsou na sebe kryptograficky navázány a tvoří řetězec bloků – blockchain.

*BOLT 11 faktura:* Protokol pro Lightning Network platby.

*Brettonwoodský systém*: Období v historii (1944-1947), kdy byla většina světových měn kryta dolarem, který byl pak navázán na zlato. Za zlato byl však dolar směnitelný pouze státům, který byly součástí tohoto systému, nikoliv podnikům či jednotlivcům.

*BTC*: Zkratka pro bitcoin, podobně jako je CZK zkratka pro Českou korunu nebo USD pro dolar.

*BtcPayServer:* Nejznámější server pro přijímání LN plateb. Tento server se používá v E-shopech i kamenných obchodech, zkrátka (téměř) všude, kde se přijímají Lightning Network platby. Je naprosto zdarma, generuje Vám pokaždé nový LN invoice a funguje bez nutnosti důvěry protistrany, tento server si totiž spravujete Vy sami.

*BTFD:* Buy The Fucking Dip. Fráze, která říká, že se nemáme bát a koupit bitcoin, když jeho cena klesá, v DIPu.

*Bullish*: Býčí. „Býčí“ trh je přesný opak „medvědího“ znamená, že dané aktivum (zde – Bitcoin) dlouhodobě stoupá. Abychom si tyto dva pojmy nepletli, představme si, že medvěd útočí na svoji kořist předními tlapami směrem dolů. Naopak býk útočí zespoda na horu, nabírá kořist na rohy.

*Burza*: Finanční instituce, která organizuje trh s investičními instrumenty. Skrze burzu lze nakupovat či prodávat různé investiční nástroje, jako jsou například cenné papíry, komodity, nebo i bitcoin.

*Buzzword:* Slovo nebo fráze, která se po určitou dobu stane populární. Tyto termíny se pak často používají v případech, které nemají s tímto slovem nic společného. Prostor kryptoměn je plný buzzwordů jako je například blockchain, DeFi, NFT, Metaverse či ICO.

*Byte* (čti bajt) Je základní jednotka kapacity počítačové paměti a objemu počítačových dat. Byte je osm bitů, které tvoří osmiciferné binární číslo v rozmezí 0–255. Jeden byte je obvykle nejmenší objem dat, se kterými dokáže procesor (součást počítače) pracovat. S byty se u Bitcoinu setkáte, když u transakce zadáváte poplatek. U transakcí se totiž zadávají poplatky v jednotce sats za jeden virtuální byte.

*Cantillonův efekt*: Jeden z dopadů tvorby peněz. Proces, při kterém se přerozdělují peníze vznikem nových peněz, a to od držitelů k jejich emitentům.

*CBDC* – Digitální měny centrálních bank. Nový koncept peněz, o kterém se dnes hojně diskutuje, jakožto možné budoucnosti peněz. CBDC by umožnily centrálním bankám nové měnovopolitické nástroje, kterých by však mohly jednoduše zneužít. Především by ale díky CBDC získali absolutní kontrolu nad peněz a celkově nad ekonomikou.

*Celkové náklady:* Veškeré náklady obětované příležitosti k produkci určitých statků.

*Centralizovaný (systém)*: Systém, ve kterém jedna autorita řídí celou strukturu. Opakem je pak decentralizace.

*Centrální banka*: Instituce, jejíž hlavní funkce je ovlivňovat cenovou stabilitu a určovat podmínky pro tvorbu peněz komerčním bankám. Také slouží jako takzvaný věřitel poslední instance.

*Ceteris paribus:* Latinská fráze, která v překladu znamená – za jinak stejných podmínek, za nezměněných okolností. Sousloví ceteris paribus se v ekonomii, co by vědním oboru, hojně používá, a to, protože je v současné ekonomice několik proměnných, přičemž každá z nich může ovlivnit fungování těch dalších. Proto, když se zkoumá jedna neznámá, říká se u ní ceteris paribus, protože se v tu chvíli se nepočítá s ostatními parametry.

*Change output:* Pokud nejsou z adresy během transakce utraceny všechny UTXOs (zjednodušeně všechny btc), zbylé bitcoiny se vrátí na nově vygenerovanou adresu. Tomuto výstupu transakce říkáme change, proto change output. Bitcoin totiž vždy pracuje s nulovým zůstatkem, tedy vždy utrácí všechny mince, jež jsou na dané adrese.

*Cross-Input Signature Aggregation:* Možný budoucí soft fork, který by umožnil agregovat více digitálních podpisů v Bitcoinové transakci do jednoho, čímž by výrazně zlevnil transakce utrácející více UTXOs. CISA by dokázala snížit i velikost běžné transakce (s jedním vstupem a výstupem), tudíž by byli i běžní lidí incentivizováni používat tuto technologii. CISA by umožnila ekonomicky výhodný CoinJoin, který by výrazně zvýšil soukromí jednotlivých Bitcoinových transakcí a ztížil analýzu blockchainu.

*Coinbase transakce:* Generující transakce. Vůbec první transakce s novými bitcoiny, kde Bitcoinový protokol odmění těžaře náležitým množstvím bitcoinů. Pozor, neplést se směnárnou Coinbase.

*CoinJoin*: Anonymizační technologie, která zamíchá několik různých vstupů v několik různých výstupů tak, aby nebylo možné zjistit, který vstup patří, kterému výstupu. Touto technologií se výrazně ztěžuje analýza dat v blockchainu.

*Cold storage/wallet:* Peněženka (respektive klíčenka), která není připojena k internetu a uchovává tak prostředky ve větším bezpečí. Cold storage jsou hardwarové peněženky, například Trezor.

*CPI*: Consumer Price Index je index spotřebitelských cen, kterým se měří cenová inflace.

*CryptoNote:* Protokol, jehož součástí je „mixér“, který náhodně míchá veškeré transakce tak, aby se dosáhlo plné anonymity.

*Custodial peněženka*: Peněženka, u které k Vašim adresám nevlastníte privátní klíče (tudíž „své“ bitcoiny v podstatě nevlastníte), avšak tyto klíče spravuje určitá autorita – Vaše peněženka. Mezi custodial peněženky patří například LN peněženky BlueWallet a Wallet of Satoshi.

*Cypherpunk*: Osoba, která se zabývá a pomáhá k rozšiřování silného šifrování, díky kterému se snaží pomoci sociální a politické změně. Skupina Cypherpunks má již delší historii, první zmínky o Cypherpunks jsou již v 80. letech minulého století.

*DAO:* Decentralizovaná autonomní organizace. Organizace reprezentovaná pravidly zakódovanými jako počítačový program, který je transparentní, kontrolovaný členy organizace a neovlivňován centrální vládou. Často se jedná o decentralizovaný bankovní systém založený na blockchainu.

*DApps:* Decentralizované aplikace. DApps jsou aplikace, které mohou fungovat autonomně, obvykle pomocí inteligentních smluv. DApps mají oproti standardním aplikacím výhodu v tom, že nemají jeden centrální bod správy, nýbrž jsou rozmístěny mezi jednotlivé uživatele sítě.

*DCA*: Pravidelné investování do bitcoinu. DCA je investiční strategie, při které pravidelně nakupujete bitcoin bez ohledu na jeho cenu. Tato strategie je považována, jakožto ta vůbec nejlepší pro investici do bitcoinu, ale i jiných aktiv, protože si díky pravidelnému investování průměrujete svoji nákupní cenu a nečasujete trh, čímž snižujete pravděpodobnost špatného nákupu a případné ztráty.

*Decentralizace*: Opak centralizace. V decentralizovaném systému nemá kontrolu jedna autorita, které musí ostatní důvěřovat, avšak decentralizovaná síť je rozmístěna mezi několika jejich uživateli, kteří ji spravují. Například Bitcoinovou síť spravují uzly a těžaři.

*DeFi:* Nahrazení standardních finančních nástrojů (jako jsou půjčky, deriváty, hedging) pomocí smart kontraktů. DeFi fungují především na blockchainu Etherea, ale i jiných platform. Nejvýznamnějším DeFi projektem je MakerDao, který prakticky definoval celé toto odvětví.

*Deflace*: Snižování měnové zásoby, zánik peněz, jež jsou v oběhu. Druhá definice deflace je pokles cen spotřebních statků.

*Depreciace:* Znehodnocení domácí měny vůči zahraničním měnám ve flexibilním (plovoucím) měnovém kurzu. Některé státy (například Čína) úmyslně snižují hodnotu své měny za účelem zvýšení exportu.

*Devalvace:* Oslabení domácí měny vůči zahraničním měnám v systému fixních kurzů. Příkladem devalvace měny je například, roku 1934, 41% devalvace amerického dolaru, kdy se po Executive Order 6102 jednostranně snížil kurz dolaru se zlatem z původních 20.67 USD na 35 USD za jednu troyskou unci zlata (31,1 g).

*DExs*: Decentralizované burzy jsou postaveny na smart kontraktech a fungují na P2P směně prostředků, tedy směně od jednoho uživatele druhému uživateli. Nejznámější decentralizovanou burzou je Uniswap, kde jednotliví uživatelé mezi sebou směňují ERC-20 tokeny za Ether anebo přímo za jiný ERC-20 token.

*Dezinflace:* Zpomalující inflace. Jedná se o pokles tempa růstu cen spotřebních statků. Pozor, neplést s deflací, deflace je snižování měnové zásoby, zatímco dezinflace je snižování růstu inflace.

*Diamond hands*: Diamantové ruce je slangový termín pro investora, který navzdory poklesu ceny, neprodá svoji investici, ale bude ji stále držet.

*Difficulty alorhitm*: Algoritmus, který každých 2016 bloků mění náročnost těžby. Díky tomuto algoritmu se uzavírá nový blok průměrně každých 10 minut.

*Digitální podpis:* Kryptografická technologie, pomocí níž je možné zajistit „identifikaci" v digitálním světě, a to právě pomocí asymetrické kryptografie. Digitální podpisy používá k transakcím Bitcoin.

*DINO: Decentralized In Name Only:* Decentralizovaný pouze ve jméně. Fráze, která naráží na to, že je slovo *decentralizovaný* buzzword a často se používá i v projektech, které nemají s decentralizací vůbec nic společného (viz některé kryptoměny).

*DIP*: Krátkodobý pokles ceny, který je často způsoben negativními zprávami, v důsledku, nichž tradeři prodávají bitcoin. V tento moment bývá dobré bitcoin naopak nakupovat než se ho zbavovat. Tyto DIPy jsou totiž často vykoupeny velrybou, která využije toho, že může bitcoin nakoupit levněji, v důsledku čehož cena opět vyletí. Trh bitcoinu je však nepředvídatelný a na základě minulosti nelze předpokládat stejné vyvíjení ceny.

*Distributed Ledger*: Distribuovaná účetní kniha, typ datové struktury, která je rozmístěna mezi více uživateli. Jednou z takovýchto struktur je blockchain, který je součást fungování Bitcoinu. Ledger a blockchain jsou u Bitcoinu synonymy.

*Dividenda:* Částka, kterou akciová společnost vyplácí svým vlastníkům, akcionářům.

*Don't trust, verify*: „Nedůvěřuj, ale ověřuj" je pojem, který říká, že nemáme slepě důvěřovat, avšak si věci ověřovat. Tato fráze je často spojovaná právě s Bitcoinem, u kterého nemusíte věřit, že ho nebude více a že nad ním nikdy nikdo nebude mít kontrolu, stačí se totiž podívat do zdrojového kódu Bitcoinu, což třeba u amerického dolaru není možné. Bitcoin je totiž systém, u kterého nemusíte nikomu věřit.

*DoS útok:* Typ útoku na internetové služby nebo stránky, jehož cílem je cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům.

*DDoS útok:* Podtp útoku DoS, při kterém je pro zahlcení cílové služby požadavky využito velké množství počítačů z různých geografických lokalit.

*Dust UTXO*: Neutratitelné UTXO.

*Dluhopis:* Dluhopis neboli obligace je cenný papír vyjadřující vztah mezi věřitelem (člověkem, který půjčuje peníze) a dlužníkem (člověkem, který si od věřitele půjčuje peníze).

*Dvojí útrata* (angl. double spend): Situace, kdy utratíte tytéž mince vícekrát. Před tím, než vznikl Bitcoin, byl tento problém v digitálním světě bez centrální autority, neřešitelným.

*DYOR:* Do Your Own Research. Udělejte si vlastní průzkum. Tato fráze nám říká, že nemáme pouze věřit a například slepě následovat investiční rozhodnutí určitého člověka, ale že si máme nejprve danou věc sami nastudovat (například makroekonomickou situaci k lepším investičním rozhodnutí).

*ECDSA:* Algoritmus pro tvorbu digitálních podpisů s využitím eliptických křivek, který Bitcoin používal před tím, než přešel na úspornější Schnorr.

*Ekonomie*: Vědní obor, který zkoumá alokování vzácných zdrojů mezi alternativními užitími (zjednodušeně, ekonomie popisuje, jak lidé a společnost rozhodují o využití svých zdrojů – času, prostoru a kapitálu, mezi veškerými statky, které na celém světě existují).

*Ekonomika*: souhrn hospodaření daného subjektu – stát, jednotlivec, organizace, kdy si každý hospodařící subjekt klade následující otázky:

1. Co a kolik se bude vyrábět?
2. Jakým způsobem a za jakou cenu se bude vyrábět?
3. Pro koho se bude vyrábět?

*Elasticita (pružnost) nabídky*: Rychlost změny nabízeného množství na trhu, vzhledem k změně cen nabízeného statku.

*Elasticita (pružnost) poptávky*: Rychlost změny poptávaného množství na trhu, vzhledem k změně cen poptávaného statku.

*ERC-20 token:* Nejčastěji používaný druh tokenu. Jedná se o tokeny, které mohou zastupovat teoreticky cokoliv. K vytvoření ERC-20 tokenů je zapotřebí sestrojit smart kontrakt. ERC-20 token je například Tether (USDT) nebo Dogecoin (DOGE).

*ERC-721 token:* Nezaměnitelný token. ERC-721 token, na rozdíl od ERC-20 tokenu není zaměnitelný, každý token je unikátní. Všechny NFT jsou ERC-721 tokenami.

*Ethereum:* Platforma, na které je možné vytvářet smart contracts nebo sestrojit DApps. Její peněžní jednotkou je Ether a dnes se jedná o 2. největší kryptoměnu.

*Ethereum 2.0:* Aktualizace Ethereového blockchainu, která se snaží (respektive bude snažit) o to, zvýšit škálovatelnost, rychlost a zároveň výrazně snížit transakční poplatky u Ethereových transakcí. Tento přechod se už pár let odkládá a je otázkou, zda se vůbec někdy uskuteční.

*Executive Order 6102:* Příkaz, který roku 1933 nutil tehdejší občany USA odevzdat veškeré zlaté mince a certifikáty, které tehdy cirkulovaly v oběhu. Při neuposlechnutí tohoto rozkazu hrozila pokuta 10.000 USD a trest odnětí svobody až na pět let.

*Exit scam:* Podvod, při kterém instuce přestane odesílat objednávky, zatímco přijíma platby za nové objednávky. Tento podvod se často používal u ICO, kdy vývojáři kryptoměny zmizeli s penězi investorů během nebo po počáteční nabídce nových mincí.

*Export*: Vývoz. Objem zboží a služeb, které stát vyrábí a vyváží do zahraničí.

*Fee ra*te: Ukazatel, který nám říká, kolik satoshi musíme zaplatit za jeden virtuální byte, aby naše transakce byla brzy potvrzena.
Fiat: Nejen italská automobilka, ale i peníze s nuceným oběhem, zákonné platidlo; spadají sem všechny národní/státní měny (z latinského fiat, budiž, staniž se). Fiat jsou zároveň ničím nekryté měny, tedy označení měny zde není úplně vhodné.

*Fiat*: Nejen italská automobilka, ale i peníze s nuceným oběhem, zákonné platidlo; spadají sem všechny národní/státní měny (z latinského fiat, budiž, staniž se). Fiat jsou zároveň ničím nekryté měny, tedy označení měny zde není úplně vhodné.

*Fixní náklady:* Náklady, které se nijak nezvyšují s vyšším objemem výroby. Fixním nákladem mohou být pro těžaře například ASIC minery, s množstvím nově vytěžených bitcoinů totiž nerostou náklady na správu těchto hardwarových zařízení.

*FOMO*: Fear Of Missing Out je strach z toho, že vám „ujíždí vlak". Jedná se o paniku, při které rychle nakupujete bitcoin, protože se bojíte, že už půjde jen nahoru a vy nestihnete nakoupit levně.

*Fork*: Větvení sítě. Stav, kdy více různých těžařů vytěží blok ve stejnou chvíli. To je ale problém, protože je více validních blockchainů se stejně velkým důkazem o vykonané práci. Jaké je tedy řešení, když u Bitcoinu není žádná centrální autorita, která by mohla o pravdě rozhodnout? Prostě se těží dál a uvidíme, nadcházející bloky určí, který blokchain je nejsilnější (má nejvíce bloků) a ten slabší řetězec s osiřelým blokem, dle Nakamotova konsenzu, přestane být validní a síť jej přestane akceptovat. Přirozený Fork je důvod, proč těžaři nemohou se svými nově vytěženými bitcoiny provádět transakce okamžitě, ale až po určité době – maturation time. Fork je zároveň označení pro implementaci nových pravidel do Bitcoinové sítě. Ten pak dělíme na Soft Fork a Hard Fork.

*FUD*: Fear, Uncertainty, and Doubt (strach, nejistota, pochyby). Šíření negativních, nepodložených a často lživých informací s cílem snížení ceny daného aktiva (Bitcoinu).

*Genesis block:* Vůbec první blok, který byl kdy vytěžen, a to samotným Satoshi Nakamotem. Součástí tohoto bloku byla i zpráva: „The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". Tato zpráva odkazovala na článek v časopise The Times, ve kterém bylo psáno: „Kancléř na pokraji druhého záchranného balíčku pro banky". Satoshi tím zřejmě chtěl poukázat na křehkost a neudržitelnost současného finančního systému postaveného pouze na důvěře.

*Get of zero*: Fráze, která znamená mít alespoň část svých peněz v bitcoinu. Bitcoin je totiž stále ještě velmi malé (co se tržní kapitalizace týče) investiční aktivum, co se tržní kapitalizace týče, tudíž je u něj stále ještě velký potenciál k nemalému růstu ceny, proto je v něm dobré mít alespoň určitou část svého portfolia a být tak vystaven možnému růstu ceny bitcoinu. Svým způsobem je vyšší riziko žádný bitcoin nemít než určitou část skutečně vlastnit.

*Gold bug:* Člověk, který je zastánce drahých kovů, zejména zlata. Tito lidé se domnívají, že budoucností peněz je právě ono zlato. Nejznámějším Gold bugem a zároveň velkým kritikem Bitcoinu je Peter Schiff.

*Gradually, then suddenly:* Fráze popisující adopci Bitcoinu. Dle této fráze by měl být Bitcoin zprvu adoptován postupně a v určité fázi najednou.

*Greshamův zákon*: Zákon, který nám říká, že ve chvíli, kdy paralelně obíhají dvě různá platidla, horší peníze vždy vytlačí ty lepší. A to, protože lidé mají tendenci šetřit si ty peníze, které se jim postupem času zhodnocují, a naopak utrácet ty peníze, které neslouží jako uchovatel hodnoty, nýbrž pouze jako prostředek směny (často vynucený).

*Hard Fork:* Zpětně nekompatibilní změna Bitcoinového protokolu. Hard Fork může způsobit split (rozdělení) blockchainu. Hard Fork byl například SegWit2x, který Bitcoinová síť nakonec neimplementovala.

*Halving:* Proces, při kterém se půlí odměna těžařům. Každých 210 000 bloků (cca 4 roky) se sníží odměna těžařů přesně o polovinu. V roce 2024 přichází další halving, po němž bude odměna pro těžaře od Bitcoinového protokolu činit 3,125 BTC.

*Hardware:* Veškeré fyzicky existující technické vybavení počítače.

*Hash*: Otisk Hashovací funkce. Převod vstupních dat do relativně malého čísla. Výstup hashovací funkce se označuje otisk či hash.

*Hashcash*: Systém založený na Proof of Work, který omezuje spam a chrání před DoS útoky. Tento systém se používá i u Bitcoinu.

*Hashovací funkce:* Matematická funkce, jež převádí zprávu nebo jakákoliv jiní vstupní data na otisk, hash, nečitelnou kombinaci písmen a čísel. Drobná změna ve zprávě na vstupu vede k velké změně ve výstupu. Bitcoin využívá hashovací funkci SHA-256.

*Hashrat*e: Používá se k měření celkového výpočetního výkonu využitého k těžbě. Zároveň se jedná o ukazatel bezpečnosti krytoměn. Čím větší má daná kryptoměna hashrate, tím je bezpečnější a odolnější, například k 51% útokům.

*Hedging:* Strategie řízení rizik používaná k snížení rizika ztráty v investicích zaujímáním opačné pozice v souvisejícím aktivu.

*Helicopter Money:* Helikoptérové peníze. Termín známého ekonoma Miltona Friedmana, jenž popisuje nástroj monetární/fiskální politiky, při kterém se vytvoří nové peníze a ty se přímo rozdistribuují mezi běžné lidi. Této formy stimulace ekonomiky se dočkaly Spojené státy v roce 2020 (viz stimulus check), kdy vláda za cílem zvýšení zaměstnanosti, posílala lidem přímé platby až ve výši 1.400 dolarů. Zajímavostí je, že ačkoliv měly tyto peníze proudit do spotřebních statků, velká část z nich skončila v investicích, jako byly akcie nebo třeba i bitcoin.

*Hierarchistická determinovaná peněženka (HD wallet)*: Typ kryptografické peněženky generující zdroje privátních a veřejných klíčů (XPriv a Xpub) z Recovery seedu. Recovery seed (24 anglických slov) → XPriv + Xpub → privátní + veřejné klíče → (z veřejného klíče) veřejné adresy.

*HODL*: Fráze, která se používá, jakožto označení pro dlouhodobé držení kryptoměn. Tato legendární fráze vznikla v roce 2013 překlepem na Bitcoinovém fóru, Bitcointalk.

*Hodnota*: Subjektivní ocenění statků. Nic nemá hodnotu samo o sobě, tu skutečnou hodnotu statků dávají lidé, na základě toho, jak dobře daná věc uspokojuje jejich individuální potřeby.

*Hot storage/wallet*: Kryptoměnová peněženka (respektive klíčenka), která je vždy připojena k internetu. Z hlediska bezpečí nejsou Hot wallets vůbec ideální. Hot storages jsou softwarové peněženky, například Coinomi.

*Honey badger:* Medojed. O Bitcoinu se často říká, že je honey badger, a to, protože je odolný, a stejně jako medojedovi, je mu všechno jedno.

*Honeypot*: Anglicky „hrnec medu“ je informační systém, který vybízí útočníky k útoku na něj. Honeypoty jsou převážně centralizované služby, u kterých stačí vypnout jedno místo provozu a celá služba zanikne.

*Hyperbitcoinizace:* Masivní adopce bitcoinu, jakožto peněz.

*Hyperinflace:* Extrémní cenová inflace (v řádech vyšších desítek, stovek nebo i více % ročně). Hyperinflací si v historii prošla Výmarská republika (meziválečné Německo) a dnes si jí prochází například Zimbabwe nebo Venezuela.

*ICO:* Počáteční nabídka mince. Jedná se o možnost nákupu kryptoměny ještě před zahájením jejího veřejného obchodování na burzách

*Import:* Dovoz. Celkový objem produktů a služeb dovezený ze zahraničí. Opakem je pak export.

*Inflace*: Nárůst měnové zásoby, „nafouknutí" množství peněz v oběhu. Novější a více používaná definice inflace je, že se jedná o meziroční nárůst cen spotřebních statků.

*Inflační cílování*: Snaha centrálních bank dosáhnout určité míry růstu ceny spotřebních statků.

*Integer Overflow:* Chyba ve špatné validitě transakce. Této chyby si ale bohužel (nebo možná bohudík) někdo všimnul a zneužil ji k sestavení transakce generující 184 miliard BTC! Této chyby útočník zneužil v říjnu roku 2010 a do 5 hodin od tohoto incidentu byla téhož dne opravena pomocí Soft Forku. Bitcoin byl ve svých začátcích (a částečně i dodnes) zkrátka divoký západ...

*Investice:* Obětování zdrojů za účelem jejich zhodnocení do budoucna.

*IPO:* První veřejná nabídka akcie. Jde o proces, při kterém daná společnost poprvé vstupuje na burzu, a tím se její akcie stávají přístupné široké veřejnosti.

*Kapitalizace*: Toto slovo má několik významů, avšak nás zajímá kapitalzace u Bitcoinu. Součinu veškerých mincí a jejich ceny se říká tržní kapitalizace. Tento údaj nám ukazuje, jak moc je určité aktivum, včetně kryptoměn, velké.

*Konsenzuální algoritmus*: Konsenzus je v decentralizovaném systému způsob, jak dosáhnout vzájemné dohody, bez toho, aby si účastníci museli navzájem důvěřovat. Je totiž podstatné, aby se v takovémto systému komunita vzájemně dohodla na tom, co je pravda. Mezi nejznámější konsenzuální mechanismy patří třeba Proof of Work nebo Proof of Stake. O obou těchto algoritmech konsenzu si povíme více v technologické části.
Komerční banka: Komerční banka s malým „k" je instituce, která má legislativní pravomoc emitovat peníze.

*Kryptoanarchie:* Filosofie spočívající v používání silné kryptografie (asymetrického šifrování) k dosažení větší osobní i ekonomické svobody.

*Kryptografie:* Šifrování. Utajování smyslu zpráv převodem do podoby, která je čitelná pouze se speciální znalostí.

*Kryptoměna*: Ačkoliv pojem kryptoměna považuji za chybný, protože Bitcoiny jsou spíše penězi, nežli měnou a měly by se proto nazývat kryptopenězi, tak tento výraz budu v této knize pro lepší srozumitelnost používat. Tento pojem je totiž veřejnosti známý a velmi často ve spojení s Bitcoinem používaný.

*Kupní síla*: Ekonomický termín, který označuje sílu peněz či měn. Čím větší má určité platidlo svoji kupní sílu, tím více zboží či služeb si za něj koupíte. A naopak, čím menší kupní sílu má jisté platidlo, tím méně statků si za něj obstaráte.
*KYC*: Know your customer, nutnost prokázání totožnosti při nákupu bitcoinu na směnárnách.

*Kurzový závazek:* Nestandardní nástroj měnové politiky ČNB. Od roku 2013 do roku 2017 Česká Národní Banka na devizovém trhu uměle oslabovala kurz české koruny. Česká koruna byla v těchto letech navázána na euro, a to v kurzu 27 Kč za euro (což byl netržní kurz, skutečná parita eura a koruny hrála v prospěch koruny, tedy euro stálo méně než 27 Kč). Devalvací koruny se zvyšovala zahraniční poptávka po tuzemských statcích. A to, protože bylo pro cizince české zboží levnější. Kvůli tomu se do ČR investovalo spousta zahraničního kapitálu. Tedy tím, že se ČNB snažila dosáhnout svého vysněného cíle cenové stability, 2% inflace, nekonvenčím měnovopolitickým nástrojem v podobě devalvace kurzu, zapříčinila vyšší export, tedy zahraniční poptávku.

*Laser e*yes: Někteří lidé, kteří podpotují Bitcoin, mají na svých profilech laserové oči, jaký je však jejich význam? Laserové oči máte, pokud věříte, že cena bitcoinu bude jednou vyšší než 100 000 USD, avšak do té doby si je nemůžete ze své profilové fotky odstranit.

*Lightning Invoice:* Platební požadavek, faktura, pomocí které můžete přijímat LN bitcoin. Tato faktura obsahuje částku k zaplacení, metadata, adresu příjemce, čas exiprace tohoto platebního požadavku a vlastní volitelnou zpráva. Pro délku této zprávy se používají QR kódy.

*Lightning Network*: Jedno z řešení problému škálovatelnosti bitcoinových transakcí, které se nám zatím jeví, jako to nejúspěšnější. Pomocí Lightning Network můžete posílat levné a okamžité transakce. Je to nadstavba nad základní Bitcoinovou sítí, vrstva chcete-li.

*LNURL pay:* Způsob placení a přijímání LN plateb. LNURL si klade za cíl zjednodušit mnoho technicky složitějších LN akcí tak, aby vyžadovaly pouze kliknutí nebo skenování QR kódu. Díky LNURL pay můžete trvale používat jednu a tu samou adresu pro přijímání LN bitcoinu a navíc tato adresa nemusí být pořád online, což je obrovská výhoda, oproti LN fakturám. To je způsobeno tím, že LNURL pay je odkaz na vygenerování Lightning příkazu v danou chvíli. Pro vyzkoušení LNURL pay můžete vyzkoušet tento odkaz, čímž zároveň podpoříte moji tvorbu:

LNURL1DP68GURN8GHJ7AMPD3KX2APWWPSHYCTVV4KXU6TSDAKXJUEWVDA
Z7MRWW4EXCUP0V9CXJTMKXYHKCMN4WFKZ7VFSX5USE22VHN :)

*LNURL withdraw*: Způsob, pomocí kterého lze přijímat LN bitcoin. Kdokoliv Vám může vytvořit odkaz nebo QR kód, pomocí kterého je možné jednoduše přijmout platbu v LN. Tuto technologii využívá například Bleskomat.

*MAHF:* Miner Activated Hard Fork je zpětně nekompatibilní změna Bitcoinového protokolu, o jejíž aktivaci rozhodují Bitcoinoví těžaři.

*MASF:* Miner Activated Soft Fork je zpětně kompatibilní změna Bitcoinového protokolu, o jejíž aktivaci rozhodují Bitcoinoví těžaři.

*Maturation time*: Doba, kdy nově vytěžené bitcoiny ještě nelze utratit. Maturation time je v Bitcoinu implementován kvůli tomu, že občas přirozeně dochází k rozštěpení blockchainu, Forku, vlivem vytěžení bloku různými těžaři ve stejnou chvíli.

*Měn*a: Poukázka na peníze. Měna je kryta penězi a za peníze je také směnitelná.

*Melting ice cube:* Tající kostka ledu. Označení, které použil Michael Saylor, CEO MicroStrategy (firma vlastnící více než 100.000 bitcoinů) pro státní měny, jejichž ztráta kupní síly vypadá podobně jako když taje kostka ledu.

*Mempool*: Databáze, ve které jsou validní transakce, které však ještě nejsou zařazeny do bloku, nejsou potvrzené těžařem.

*Merkle tree*: Merkleův strom, nebo také hashový strom je datová struktura používaná v kryptografii a informatice. Jedná se o strom, který má

v listech data a ve všech ostatních vrcholech má hodnotu odpovídající výsledku kryptografické hashovací funkce.

*Mezní náklady:* Náklady na dodatečnou jednotku výstupu.

*Monero:* Kryptoměna postavena na technologii CryptoNote, která je absolutně anonymní. Této anonymity dosahuje pomocí kryptografických technologií, jako jsou Ring Signatures.

*Merkle root*: Konečný otisk, výsledek hashování podle Merkle tree.

*Metaverse*: Síť 3D virtuálních světů zaměřených na sociální spojení. Poprvé se tento pojem objevil v dystopickém kyberpunkovém románu Sníh z roku 1992.

*Monopol*: Privilegium, kvůli němuž je povoleno pouze jednomu subjektu provádět svoji činnost. Všechny ostatní subjekty mají zakázáno vstoupit do tohoto odvětví. Druhá definice monopolu je, že se jedná o formu nedokonalé konkurence, při které je na straně nabídky pouze jeden subjekt.

*Multisig*: Multi Signature (vícepodpisová) adresa je taková, která má více než jeden privátní klíč. Používá se k tomu, aby mělo k jedné peněžence přístup více rozdílných uživatelů. K odeslání transakce z této adresy, je pak potřeba podepsat zprávu (kterou vám vygeneruje peněženka) více privátními klíčemi. Tím se snižuje riziko zpronevěry bitcoinů.

*Nakamoto-Greshamův zákon:* Teorie vycházející z Greshamova zákona, které nám říká, že je racionální používat bitcoin jako uchovatel hodnoty, a naopak fiat jakožto prostředek směny, a to kvůli jejich odlišným monetárním politikám.

*Nakamotův konsenzus:* Pravidlo Bitcoinové sítě, které nutí nody vždy považovat ten nejdelší řetězec důkazu vykonané práce (blockchain s nejvíce platnými bloky) za jediný validní.

*Náklady obětované příležitosti:* Všechno, co obětujeme k získání námi poptávaného statku (peníze, čas, prostor...).

*New York Agreement:* Dohoda, jejímž obsahem byly dva body: aktivace SegWitu (oddělení svědka, digitálního podpisu, od ostatních dat v bloku) a zvýšení velikosti bloku na dvojnásobek, tedy 2 MB. Proto onen Hard Fork nese název

SegWit2x = SegWit + 2x zvětšení bloku. Součástí této kontroverzní dohody byly i technické chyby (například Replay Protection), kvůli čemuž nedošlo k aktivaci tohoto Hard Forku.

*NFT*: Nezaměnitelný token je takový dokument, který má pouze jeden originál, jenhož hash je zapsán na blockchainu.

*Node*: anglický termín pro Bitcoinový uzel.

*Non-custodial peněženka:* Non-custodial, taktéž Self-custodial peněženka je taková peněženka, u které Vy vlastníte privátní klíče k Vaší peněžence. Tudíž taková peněženka, u které si Vaše bitcoiny spravujete Vy sami, nikoliv jistý (ne)důvěryhodný prostředník. Jedná se o jediné bezpečné uchování si vlastních bitcoinů. Mezi Non-custodial peněženky patří například Trezor, Ledger, Exodus a u LN peněženek je to například Phoenix.

*Nonce:* označení pro náhodné číslo, které lze použít pouze jednou. U Bitcoinu se těžaři snaží naleznout nonce, pomocí které by mohli uzavřít blok a dostat náležitou odměnu.

*Not your keys, not your coin*: Tato fráze se vztahuje k nutnosti mít svůj privátní klíč k bitcoinům. Pokud nemáte privátní klíče ke svým kryptoměnám, jednoduše je nevlastníte a pouze důvěřujete protistraně (směnárně), že o ně nepřijdete, což se bohužel děje velmi často.

*Number go up:* Termín odkazující na funkci úpravy obtížnosti těžby a fixní zásobu bitcoinu. Vzhledem k extrémní vzácnosti bitcoinu a nemožnosti jej zkopírovat to může mít za následek, že cena bitcoinu poroste.

*Obskurantismus (obscurantism):* Komunikační strategie, u které se popisují věci tak složitě, že jim nikdo není schopen porozumět, tedy ani nemůže vyvrátit relevantnost daných argumentů. Někteří kritici Etherea se domnívají, že je to právě tato strategie, která způsobuje takové nadšení okolo této kryptoměny.

*Off-chain:* Procesy v Bitcoinu mimo základní vrstvu. Nejznámějším příkladem off-chain transakce je Lightning network.

*On-chai*n: Základní vrstva Bitcoinové sítě. On-chain transakce jsou pak standartní transakce bitcoinů z adres/y na adresu/y, nikoliv například otevírání platebních kanálů.

*On-chain analýza*: On-chain analýza je analýza dat v určitém blockchainu. Mezi tyto data může nepaříklad patřit množství bitcoinů na jednotlivých adresách.
Open source software: Takový software, který má svůj zdrojový kód veřejně přístupný. Tento zdrojový kód může kdokoliv upravovat, nebo navrhovat úpravy tohoto softwaru.
*Orphan block:* Osiřelý blok. Důsledek přirozeného rozštěpení sítě, kvůli vytěžení bloku více různými těžaři ve stejnou chvíli. Jedná se o zamítnutý blok, jehož těžař nezíská odměnu v podobě nových bitcoinů. Osiřelý blok je blok, který je součástí kratšího řetězce důkazu vykonané práce, tedy není dle Nakamotova konsenzu validní.

*Overflow Bug 2106*: Chyba v Bitcoinovém protokolu, kvůli které nebude možné tvořit další bloky po roce 2106, a to kvůli tomu, že timestamp (časové razítko) má pouze určitou možnou číselnou velikost. Tato chyba vyžaduje k jejímu řešení pouze a jedině Hard Fork.

*P2P*: Peer-to-Peer, rovný s rovným, klient s klientem. Označení počítačové sítě, ve které není prostředník. Například Bitcoin je P2P, protože posíláte své bitcoiny přímo dané osobě, a ne přes prostředníka, jako tomu je u fiatu (banky).

*P2PK:* První, původní způsob přijímání bitcoinu, pomocí veřejného klíče (nikoliv veřejné adresy). Tento typ adresy se používal pouze v úplných začátcích fungování Bitcoinu, dnes se již dávno nepoužívá.

*P2PKH:* Druhý typ adresy, začínající číslem *1*. Způsob, kterým se bitcoiny odesílají na hash veřejného klíče – veřejnou adresu.

*P2SH:* Třetí typ adresy, začínající číslem *3*. Typ transakce, která umožňuje utrácet bitcoiny na základě jakéhokoli skriptu poskytnutého odesílatelem.

*P2WPKH:* Nejnovější typ bitcoinové adresy se začátkem *bc1.* Tento typ adresy má nejmenší transakční poplatky. Jedná se o typ ScriptPubKey, který se používá k uzamčení bitcoinů na adresu SegWit.

*Paralelní Polis:* Nezisková organizace, spojující vědu, moderní technologie a umění, která funguje paralelně, nezávisle na státu. Paralelní Polis funguje pouze na kryptoměnách, nikoliv fiatu, její součástí je Bitcoin Coffee, kde si můžete dát skvělou kávu za bitcoin, LN či altcoiny. Jedná se o jednu z prvních institucí na světě, která začala za své služby přijímat bitcoin a jiné kryptoměny, a

to již v roce 2014. Paralelní Polis každoročně pořádá Hackers Congress (HCPP), kde se scházejí ty největší kapacity v tomto oboru.

*Passphrase*: Zálohovací fráze, pomocí níž dosáhnete ještě většího zabezpečení vaší kryptoměnové peněženky. Jedná se v podstatě o 13./25. vámi vybrané slovo k recovery seedu. Bez znalosti této fráze se útočník nemůže dostat k vaší skryté peněžence.

*Pending:* Čekající. Stav Bitcoinové transakce, kdy transakce teprve čeká na zařazení do bloku anebo má, pro danou peněženku, nedostatek potvrzení (většinou je minimum 6).

*Peníze*: Nástroj k přesouvání hodnoty v čase a prostoru. Peníze musí splňovat určité funkce. Zároveň by peníze měli splňovat 6 peněžních vlastností. Peněžní funkce i vlastnosti si v této knize více probereme.

*Peněženka*: Kryptoměnová peněženka je software či hardware, který vám uchovává v bezpečí vaše klíče (veřejný a soukromý), proto je lepším pojmem klíčenka. Na tyto peněženky si ukládáte vaše kryptoměny.

*Pizza day:* 22. 5. 2010. V tento den byla poprvé realizována transakce s bitcoiny za hmotné zboží. Laszlo Haneycz si koupil 2 pizzy za 10.000 btc. Od tohoto roku se vždy počítá, kolik by ony pizzy stály v dnešních penězích a stal se z toho komunitní vtip. Někteří lidé se domnívají, že se jednalo o ten nejhloupější nákup v historii. Ovšem Laszlo na to odpovída, že nakoupené dvě pizzy byly opravdu chutné a že to kvůli tomu za to stálo. Ačkoliv to může znít zvláštně a iracionálně, utrácet bitcoiny může být rozumné, i když se časem zhodnocují. Pokud totiž chceme vybudovat Bitcoinvou ekonomiku, musí lidé bitcoinem platit, přestože to může být ekonomicky iracionální. Takže pokud chcete vybudovat nový monetární systém postavený na bitcoinu, jděte a nakupte si za něj zboží, zároveň tím podpoříte odvážné producenti, kteří se rozhodli btc přijímat.

*Plasma:* Stejně, jak je Lightning Network řešením škálovatelnosti druhé vrstvy pro Bitcoin, je Plasma něco velmi podobného pro Ethereum. Plasma by měla být společně s dalšími koncepty do Etherea implementována při přechodu na Ethereum 2.0.

*Platební kanál (payment channel):* Na platebních kanálech je postaven celý koncept Lightning Network. Platební kanál je specifická, multisig transakce mezi dvěma uživateli, ve které je možné provést neomezené množství dalších

transakcí, tedy pokud nedojde jedné ze stran likvidita. Přičemž do blockchainu se zapíše pouze otevření a zavření onoho platebního kanálu.

*Ponziho schéma*: Investiční podvod, kdy provozovatel fondu peníze neinvestuje a nezúročuje, ale místo toho vyplácí prostředky fondu těm investorům, kteří investovali dříve.

*Potvrzení transakce:* Většina peněženek považuje transakci za úspěšnou pouze tehdy, kdy má určité množství (většinou minimálně 6) potvrzení. Potvrzením je chápáno umístění transakce v hloubi blockchainu. Jinými slovy, pokud po zařazení Vaší transakce do bloku proběhne vytěžení 6 bloků, transakce má právě tolik potvrzení.

*Privátní klíč*: Jeden z dvojice klíčů v asymetrické kryptografii. Jedině vlastník privátního klíče může s bitcoiny na svých adresách nakládat.

*Proof of Stake:* Konsenzuální algoritmus, u nějž transakce validují (potvrzují) pouze uživatelé s určitým množstvím mincí z ekosystému dané sítě, tedy se nejedná o žádný náklad ze skutečného, fyzického světa. PoS je často (právem) kritizován pro jeho centralizaci, špatné zabezpečení a náchylnost k různým typům útoků. Na Proof of Stake by měla přejít kryptoměna Ethereum ve svém několik let odkládaném přechodu na Ethereum 2.0.

*Proof of Work:* Nejznámější, nejbezpečnější a časem nejprověřenější algoritmus konsenzu. Tento konsenzuální algoritmus je postaven na těžbě, tedy na potvrzování transakcí pomocí výpočetního výkonu – nákladu z fyzického světa. Bitcoin používá k zabezpečení fungování sítě právě PoW.

*Průměrné náklady:* Náklady na jednu jednotku výstupu. Průměrné náklady jsou podíl celkových nákladů a veškerých jednotek výstupu. Pozor, neplést s mezními náklady!

*Quantitative Easing (QE):* Kvantitativní uvolňování. Nekonvenční nástroj monetární politiky, při kterém centrální banky na sekundárním trhu nakupují aktiva s cílem stimulace růstu cen aktiv finančního trhu. Pozor, QE není tištění peněz! Nové „peníze“ od centrální banky se dostanou pouze do mezibankovního sektoru a je až na samotných obchodních bankách, aby tyto peníze lidem půjčovaly, jinak se nedostanou do měnové zásoby a běžné lidi bez přístupu k finančním trhům nijak přímo neovlivní. To je naprosto zásadní rozdíl mezi QE a helikoptér money.

*QR kód*: QR je zkratka dvou anglických slov, Quick Response, tedy se jedná o kód rychlé (identifikační, informační) reakce, obdoba čárového kódu, ale s větším množstvím informací. QR kód se u Bitcoinu používá u veřejných adres. Tyto adresy jsou dlouhé, a kdybyste je měli všechny znaky do vaší peněženky sami vepisovat, zabralo by vám to zbytečně dlouhou dobu, navíc je zde možnost, že byste v napsání adresy udělali chybu, poslali byste tak bitcoiny někomu úplně jinému. Řešení tohoto problému je právě QR kód. Když byste někomu chtěli poslat bitcoiny, vaše peněženka vám umožní skenovat QR kód, což je v tomto případě, digitální ztvárnění adresy, na kterou chcete odeslat bitcoiny. Po naskenování jednoduše podepíšete vašim privátním klíčem zprávu, kterou vám vaše peněženka vytvořila. Chvíli poté přijdou příjemci bitcoiny. Tímto způsobem jste ušetřili spoustu času, a navíc zde neriskujete, že byste se omylem přepsali v popisu adresy, na kterou chcete odeslate vaše bitcoiny.

*Rakouská (ekonomická) škola:* Škola ekonomického myšlení, která klade důraz na volný trh bez státních zásahů. Od ostatních ekonomických škol myšlení se odlišuje převážně svojí metodologií, jejíž podstatou je analýza lidského jednání – praxeologie. Většina rakouských ekonomů zastává názor, že by peníze měly být vzácné, tudíž nemalá část Bitcoinerů se právě k této škole přiklání.

*Recovery Seed*: Obnovovací fráze. 24 nebo 12 anglických slov, které jsou vygenerovány při tvorbě nové bitcoinové peněženky pro účely obnovy peněženky v případě její ztráty.

*Reorg (reorganizace bloku)*: Proces, který nastává v nadcházejícím bloku takového bloku, který vytěžili rozdílní těžaři v jednu a tu samou chvíli a síti byly tyto bloky rovněž rozdistribuovány ve stejný čas. Reorganizace řetězce nastane ve chvíli, kdy Váš uzel obdrží bloky, které jsou součástí nového nejdelšího řetězce. Váš uzel deaktivuje bloky ve svém starém nejdelším řetězci ve prospěch bloků, které staví nový nejdelší řetězec.

*Replay Protection:* Odolnost Bitcoinové sítě po Hard Forku vůči tomu, aby nebylo možné zaměnit transakce původní sítě s odvětveným blockchainem.

*Retail*: Maloobchod. Retailoví investoři jsou běžní investoři, kteří nedisponují milionovým, či ještě větším kapitálem.

*Satoshi* (sats): Nejmenší část Bitcoinu, jedna stamiliontina – 0,00000001. Bitcoin si nemusíte koupit celý, můžete si klidně koupit jedno satoshi - 0,0075 Kč (ve

chvíli čtení může být cena jiná). Tato nejmenší část je pojmenována po tajemném tvůrci Bitcoinu – Satoshi Nakamotovi.

*Script* (skript): Skript je u Bitcoinu seznam instrukcí, za jakých podmínek může být použito určité UTXO, co by vstup transakce. Skript následně slouží k odemykání a zamykání bitcoinů na adresách.

*ScriptPubKey:* Skript, který určuje, jak lze bitcoiny utratit.

*Security budget*: Odměna, kterou dostávají těžaři za vytěžení nového bloku. Security budget je dvojfázový, protože bitcoinoví těžaři dostávají, co by odměnu, jak bitcoiny od samotného protokolu, tak i transakční poplatky od uživatelů Bitcoinové sítě.

*SegWit:* Soft Fork, který z bloku oddělil digitální podpisy od ostatních prvků transakce, čímž snížil velikost transakce. SegWit vyřešil problém s transaction melleability a umožnil fungování technologie Lightning Network.

*SegWit2x:* Hard Fork, jehož cílem bylo implementovat SegWit a zároveň 2x zvětšit místo v bloku. Tento návrh Bitcoinová síť neimplementovala.

*SHA*: Secure Hash Algorithm. Rozšířená hashovací funkce, která vytváří z libovolně velkých vstupních dat otisk (hash) s fixní délkou. Druhů těchto algoritmů je několik, a jmenují se podle toho, jakou délku má následný otisk. Algoritmus SHA-256 vychází z SHA-2, který vyvinula národní americká bezpečnostní agentura (NSA) a má otisk s 32 bytů. Tento algoritmus je extrémně bezpečný, používá jej nejen Bitcoin, ale i vláda USA k ochraně citlivých informací. Pomocí otisku SHA-256 má těžař možnost uzavřít blok a dostat od sítě odměnu. SHA-256 má u Bitcoinu i jiná uplatnění, například vytváří bitcoinovou adresu, kdy je veřejná bitcoinová adresa dvakrát zahashovaný veřejný klíč.

*Sharding (Shard Chains):* Součást konceptu Ethereum 2.0. Jedná se o rozštěpení blockchainu Etherea na 64 menších „střepů“, které mezi sebou vzájemně komunikují. Tento koncept by měl být implementován za účelem zlepšení škálovatelnosti.

*Shitcoin*: Vulgární (přesto velmi přesné) označení pro altcoin, který nemá žádné využití. Čím více nabýval Bitcoin na popularitě, tím více lidí se ho snažilo napodobit a tvořili altcoiny, které k ničemu nesloužily, neměly žádnou hodnotu. A právě pro tyto altcoiny se ujal termín shitcoin.

*Schnorrovy podpisy*: Alternativa k algoritmu ECDSA pro tvorbu digitálních podpisů, která úsporněji pracuje se vstupy a digitálními podpisy transakcí, umožňující jejich agregaci.

*Single point of failure:* Jediný bod selhání. Chyba v návrhu, která představuje potenciální riziko, protože by, byť malá chyba, mohla způsobit zkázu celého celku. Centralizované systémy trpí tímto problémem.

*Skin In The Game*: Mít „kůži ve hře" znamená podstoupit riziko zapojením se do dosažení určitého cíle. U Bitcoinu to znamená, mít v něm alespoň část svých peněz, být součástí hry, ve které se automaticky podstupuje riziku zisku či ztráty.

*Smart contract (smart kontrakt)*: Smart kontrakt, chcete-li chytrá smlouva je typ protokolu, který zajišťuje, ověřuje anebo vynucuje vyjednání či provedení kontraktu.

*Směnárna:* místo, kde lze nakupovat a prodávat různá aktiva podle stanovených kurzů. Směnárna má většinou větší poplatky nežli burza a je příjemcem směnných kurzů, nikoliv jejich tvůrcem (to je totiž burza).

*Soft Fork*: Zpětně kompatibilní změna v Bitcoinovém protokolu. Soft Fork byl například SegWit a Taproot.

*Software:* Sada všech počítačových programů, které provádějí nějakou činnost.

*Sound Money:* Zvučné peníze. Peníze, jejichž zásoba není elastická a mají vysoké stock to flow. Mezi sound money patří i bitcoin.

*Split (blockchainu):* Rozdělení, rozvětvení blockchainu z důvodu neúplné akceptace Hard Forku sítí, respektive jednotlivými uživateli – nody. Splitem byl například Bitcoin Cash, když síť neimplementovala Hard Fork, který měl 8x zvětšit Bitcoinové bloky + zavést SegWit. Část uživatelů Bitcoinu přešla na toto jeho odvětvení.

*Spoření:* Odkládání spotřeby peněz za účelem jejich použití v budoucnu. Spořením pak vznikají úspory.

*Stablecoin*: Stabilní mince. Stablecoiny jsou kryptoměny, jejichž cena se moc nemění (není volatilní). Většinou jsou Stablecoiny kryté nějakou fiat měnou, například Tether (USDT) je krytý americkým dolarem v poměru 1

*Stacking sats*: Tuto frázi bychom mohli přeložit jako „štosovat saty“. Jedná se o spoření si do bitcoinu, postupné získávání satů.

*Statek* (ekonomický): Cokoliv, co lidem zvyšuje užitek (kromě takzvaného nežádoucího statku). Statek nemusí být pouze fyzický objekt, tedy nějaké zboží, avšak může se jednat i o službu.

*Stát:* Systém politických motivací. Mocenské uspořádání, ve kterém mohou privilegovaní jednotlivci žít na úkor ostatních (například pomocí daní, dotací či Cantillonově efektu) a využívat svůj monopol na násilí k získání větší moci nebo majetku. Anebo, jak by řekl Frédéric Bastiat: „Stát je velká fikce, pomocí níž se každý snaží žít na úkor všech ostatních.“

*Stock to flow:* Vztah mezi tvorbou a aktuální zásobou peněz. Z tohoto vztahu pak vzešel stejnojmenný statistický model (ignorující základní ekonomické principy, například fakt, že poptávka není neměnná), predikující cenu bitcoinu pouze na základě jeho nabídky. Dle tohoto modelu by díky halvingu mělo každé 4 roky dojít k výraznému růstu cen bitcoinu.

*Svícový graf*: Graf, který se používá k popisu cenových pohybů aktiv. Jedná se o soubor takzvaných svíček. Zelená svíčka značí cenový růst, a naopak svíce červená nám ukazuje, že se cena propadla.

*Symetrická kryptografie:* Symetrická neboli konvenční šifra je kryptografický algoritmus, který používá k šifrování i následnému dešifrování tentýž klíč.

*Taproot:* Soft Fork, který přináší zlepšení ochrany soukromí Bitcoinových transakcí a do budoucna může umožnit spoustu různých zajímavých technologických a anonymizačních vylepšení. Funguje na principu skrytí spendovacího skriptu transakce, čímž může být třeba multisig transakce nebo otevření platebního kanálu nerozeznatelný od běžné transakce.

*Těžba*: Proces zabezpečení Bitcoinové sítě. Těžař za uzavření bloku, ve kterém jsou transakce, dostává odměnu v podobě bitcoinů. Tuto odměnu získá, pokud nalezne zlatou nonce.

*The Blocksize war:* Hádka (chvílemi velmi vyhrocená) o velikosti Bitcoinových bloků. Problém se škálovatelností bitcoinových transakcí byl dlouhotrvající a někteří „Bitcoineři“ (respektive, časem spíše Bcashisté) se domnívali, že jeho řešením je zvětšení velikosti bloku, čímž by se do něj mohlo vlézt více transakcí. Tento spor nakonec vyvrcholil v Hard Fork, čímž vznikla nová kryptoměna – Bitcoin Cash.

*The DAO hack:* Nalezení chyby ve smart kontraktu DAO, pomocí níž byl z tohoto projektu vykraden veškerý investovaný kapitál. Nepopulární reakcí vývojářského týmu Etherea na The Dao hack byl Hard Fork, který rozdělil Ethereum na Ethereum Classic (původní verze, ta, ve které byla nalezena chyba ve smart kontraktu) a Ethereum (verze blockchainu Etherea, ve které byla ona chyba opravena).

*Timelock:* Primitivní forma smart kontraktu ve skriptu Bitcoinové transakce, která umožňuje utrácet bitcoiny z adresy (UTXOs) po specifikované době (určené číslem bloku). Timelocku využívá například coinbase transakce u maturation time.

*Timestamp*: Časové razítko je jedním z údajů, které naleznete v Bitcoinových blocích. Každý blok obsahuje časový údaj, který nám říká, kdy byl vytěžen

*Token:* Mince, která nemá svoji vlastní transakční databázi, nýbrž běží na blockchainu určité kryptoměny, nejčastěji Ethereu. Hlavní rozdíl mezi Kryptoměnou a tokenem je právě v tom, že zatímco kryptoměna má svůj vlastní blockchain, token nikoliv.

*To the moon!* : Raketově rostoucí cena. Tuto větu používají lidé, kteří věří v takový růst, že se ani do grafu nevlezou zelené svíce Je však důležité mírnit nadšení, protože se i historicky stávalo, že když jsou lidé na trhu nejpozitivnější, co se týče vývoje ceny, a všude píšou – to the moon! bývá často naopak správný čas na prodej nežli na nákup, protože je trh moc přehřátý a bublina je již přefouknuta a brzy praskne. Ačkoliv cena bitcoinu, s pár výjimkami, prakticky dlouhodobě pouze roste, neznamená to, že bitcoin musí růst věčně. U ceny bitcoinu je, na základě zkušeností z historie, dobré být spíše pozitivní, ale všeho s mírou.

*TPS:* Transakce za sekundu. TPS označuje počet transakcí, které je síť schopna zpracovat každou sekundu.

*Transaction malleability*: Pozměnitelnost, tvárnost, kujnost ID transakce.

*Transakce*: Přesun hodnoty z bodu A do bodu B.

*Transakční poplatky*: U každé Bitcoinové transakce se nastavují poplatky, které motivují těžaře, aby právě Vaši transakci zařadili do bloku a tím ji potvrdili.

*Trezor*: První, stále existující, a dokonce i jedna z nejlepších, ne-li ta úplně nejlepší hardwarová peněženka, která mimo jiné vznikla v Česku.

*Trh*: Prostředí, ve kterém se vyskytují nakupující a prodávající určitých statků.

*Turbo kanál:* Koncept, který umožňuje okamžitě používat platební kanál, a to bez toho, aby byla transakce, která tento kanál otevřela, zapsána na blockchain, což výrazně zvyšuje uživatelskou přívětivost LN. Tento koncept vynalezl Martin Habovštiak ze slovenské Paralelnej Polis.

*Turingův stroj*: Teoretický model počítače popsaný matematikem Alanem Turingem. Skládá se z procesorové jednotky, tvořené konečným automatem, programu ve tvaru pravidel přechodové funkce a pravostranně nekonečné pásky pro zápis mezivýsledků.

*Turingovsky úplný*: Výpočetní stroj nebo programovací jazyk tak univerzální, jak je jen možné. Má stejnou výpočetní sílu jako Turingův stroj.

*TxID:* ID transakce neboli hash transakce je změť znaků přiřazený ke každé transakci, který se následně ověří a přidá do blockchainu. Každá transakce má svoje jedinečné ID („identifikační číslo“).

*UAHF:* User Activated Hard Fork je zpětně nekompatibilní změna Bitcoinového protokolu, o jejíž aktivaci rozhodují uživatelé Bitcoinové sítě.

*UASF*: User Activated Soft Fork je zpětně kompatibilní změna Bitcoinového protokolu, o jejíž aktivaci rozhodují uživatelé Bitcoinové sítě.

*UTXO:* Jediná podoba, ve které Bitcoin existuje. Jedná se o neutracený výstup předchozí transakce, který se použije jako vstup nové transakce. Každý konec je nový začátek, Bitcoin je krásný.

*Uzel*: Ověřuje transakce, které ukládá do mempoolu. Z mempoolu pak těžař vybírá transakce k potvrzení. Zjišťuje, zda uživatel neutrácí již utracené UTXO. Tímto uzlem se může stát kdokoliv.

*Variabilní náklady:* Náklady, které se mění v souvislosti s objemem výroby. Variabilním nákladem je například spotřeba elektrické energie k těžbě bitcoinů, její spotřeba totiž závisí na rozhodnutí těžařů zabezpečovat Bitcoinovou síť (a toto rozhodnutí zase závisí na finanční motivaci, tj. odměně od sítě + transakčních poplatků).

*Veksl:* Směna. Jeden ze způsobů, jak koupit bitcoin (většinou levně a anonymně!) je veksl, tj. směna fiatu za bitcoin s určitým člověkem, bez jakéhokoliv prostředníka. K vekslu slouží skupiny převážně na šifrovaných messangerech, například aplikaci Signal.

*Velryby*: U Bitcoinu není velryba kytovec, ale právě opak retailu. Velryby jsou lidé, co mají velký kapitál a nakupují či prodávají velké množství bitcoinu. Tito lidé jsou schopni zamávat s cenou bitcoinu, kvůli jeho nízké tržní kapitalizaci. Velké cenové pohyby však nemusí být způsobeny pouze nákupem velryb, ale také tím, kolik retailových investorů na trhu je velká a známá velryba schopna ovlivnit.

*Veřejná adresa:* Adresa pro přijímání bitcoinů, která je odvozena od veřejného klíče.

*Veřejný klíč*: Jeden z klíčových párů, pomocí kterého lze zjistit, zda vlastník privátního klíče podepsal zprávu. Avšak z veřejného klíče není možné zjistit klíč soukromý neboli privátní. Veřejný klíč generuje Bitcoinové adresy.

*Volatilita*: Kolísání ceny aktiv. Kryptoměny patří k nejvolatilnějším aktivům, s tímto pojmem se často střetnete právě v souvislosti s nimi.

*Volný trh*: Systém obchodu, ve kterém se ceny určují dohodou mezi nakupujícím a prodávajícím. Na tomto trhu nejsou žádné státní intervence či regulace, které by omezovaly fungování tržních mechanismů.

*Wall Street:* Ulice v jižní části ostrova Manhattan v New Yorku. Tato ulice je slavná tím, že se v ní nachází Newyorská burza a další velmi významné finanční instituce (největší banky, akciové burzy...). Pro některé je Wall Street symbolem kapitalismu.

*Weak hands:* Slabé ruce. Tento termín označuje investora, které své aktivum (třeba bitcoin) dlouhodobě nedrží a v panice prodá.

*When in doubt, zoom out*: Jedná se o frázi, která nám říká, že se nemáme bát, když cena bitcoinu padá, a že si máme oddálit graf, abychom viděli, že dlouhodobě roste.

*White pape*r: Určitý průvodce, který čtenáře stručně informuje o složitějším převážně technickém problému. U Bitcoinu byl white paper prvním představením této unikátní. technologie

*Zlatá nonce*: Golden nonce je jediné číslo, pomocí kterého může těžař uzavřít blok. K nalezení zlaté nonce musí těžař zkoušet několik miliard různých nonce.
Zlatý standard: Období v historii, kdy se platilo buď samotným zlatem anebo poukázkami na něj – peněžními substituty (měnou).

*Zlehčování (peněz)*: Proces, při kterém se snižuje kvalita (v jejímž důsledku i kupní síla) peněz (například u zlata ryzost tohoto kovu).

*ASIC* – Application-Specific Integrated Circuit
*ATH* – All Time High
*BIP* – Bitcoin Improvement Proposal
*BOLT* – Basis of Lightning Technology
*BTC* – Bitcoin
*BTFD* – Buy The Fucking Dip
*CBDC* – Central Banks Digital Currencies
*CE* – Cantillon effect
*CISA* – Cross-Input Signature Aggregation
*CPI* – Consumer Price Index
*DAO* – Decentralized Autonomous Organization
*DApps* – Decentralized Applications
*DDoS* – Distributed Denial of service
*DeFi* – Decentralized Finance
*DExs* – Decentralized Exchanges
*DINO:* Decentralized In Name Only
*DoS* – Denial of Service
*DYOR* – Do Your Own Research
*ECDSA* – The Elliptic Curve Digital Signature Algorithm
*EIP* – Ethereum Improvement proposal
*ERC* – Ethereum Request for Comments

*ETH* – Ether
*ETH2* – Ethereum 2.*0*
*FUD* – Fear, Uncertainty, Doubt
*HD* – Hierarchical Deterministic Wallet
*HW* – Hardware
*ICO* – Initial Coin Offering
*IPO* – Initial Public Offering
*KYC* – Know Your Customer
*LN* – Lightning Network
*LNURL* – Lightning Network Uniform Resource Locator
*MAHF* – Miner Activated Hard Fork
*MASF* – Miner Activated Soft Fork
*NFT* – Non-fungible token
*Nonce* – Number Only Used Once
*NYA* – New York Agreement
*P2P* – Peer to Peer
*P2PK* – Pay To Public Key
*P2PKH – Pay to Public Key Hash*
*P2SH* – Pay to Script Hash
*PoS* – Proof of Stake
*PoW* – Proof of Work
*PubKey* – Public Key
*P2WPKH* – Pay to Witness Public Key Hash
*QE* – Quantitative Easing
*QR* – Quick Response
*SHA* – Secure Hash Algorithm
*SW* – Software
*TPS* – Transaction Per Second
*TxID* – ID transakce
*UASF* – User Activated Soft Fork
*UAHF* – User Activated Hard Fork
*UTXO* – Unspent Transaction Output
*XMR* – Monero