Slovník pojmů

51% útok: Jedná se o typ útoku na blockchainovou síť, při kterém jeden subjekt nebo skupina ovládá většinu výpočetního výkonu sítě, což jim umožňuje manipulovat s transakcemi (utrácet stejné mince vícekrát) a potenciálně narušit síť.

Adresa peněženky: Jedinečný identifikátor používaný k odesílání a přijímání bitcoinů, obvykle reprezentovaný jako řetězec písmen a čísel.

Altcoinová sezóna: Období, kdy alternativní kryptoměny zaznamenávají výrazný nárůst cen, často v důsledku zvýšeného zájmu investorů a jejich adopce.

Altcoiny: Všechny digitální měny, které vznikly po Bitcoinu.

Atomic Swap: Výměna jedné kryptoměny za jinou bez potřeby centralizované burzy nebo zprostředkovatele.

Aukce: Proces, při kterém se zboží nebo majetek prodává tomu, kdo nabídne nejvyšší cenu.

Bitcoin: Digitální měna/systém, který umožňuje lidem posílat si navzájem peníze bez nutnosti použití banky nebo jiné instituce.

Burza/směnárna kryptoměn: Platforma, kde mohou uživatelé nakupovat, prodávat a vyměňovat kryptoměny za jiná aktiva, jako je fiat měna nebo jiné kryptoměny.

Blockchain: Veřejný záznam všech uskutečněných transakcí s bitcoiny.

BTC: Jednotka používaná pro bitcoiny. Digitální měna, kterou lze používat k nákupům nebo k obchodování.

Centrální banka (Fed, ECB, ČNB...): Vládou kontrolovanáa řízená instituce, která řídí měnovou politiku země.

Centralizace: Soustředění moci nebo kontroly v jediném subjektu.

Centralizovaný systém: Systém, v němž je moc nebo kontrola soustředěna v rukou jediného subjektu.

Cold storage: Metoda ukládání bitcoinů v režimu offline, mimo dosah hackerů nebo jiných online hrozeb.

Chytrý kontrakt: Samostatně realizovatelná smlouva, jejíž podmínky jsou zapsány v kódu.

Dluh: Peníze, které jsou dluženy někomu jinému.

Decentralizace: Rozdělení moci a kontroly mezi všechny členy sítě namísto centrální autority.
Decentralizovaná autonomní organizace (DAO): Organizace nebo síť řízená smartkontrakty a provozovaná na blockchainu bez centrální autority nebo řídicí struktury.

Decentralizované finance (DeFi): Hnutí v kryptoměnovém průmyslu, jehož cílem je vytvořit decentralizované finanční produkty a služby, které fungují na blockchainu.

Decentralizovaný systém: Systém, ve kterém je moc nebo kontrola rozdělena mezi více subjektů.

Digitální aktivum: Digitální vyjádření hodnoty, se kterým lze obchodovat nebo které lze použít jako uchovatel hodnoty, například bitcoiny.

Distribuovaná účetní kniha: Databáze, která je rozprostřena v síti počítačů a není uložena na jednom konkrétním místě.

Dovoz: Zboží a služby vyrobené v jiné zemi a prodávané na domácím trhu.

Dvojitá náhoda přání: V barterové ekonomice mají obě strany to, co chce jiná strana, a zároveň chtějí to, co má druhá strana.

Dvojnásobná útrata: Když se člověk pokusí poslat své bitcoiny dvěma různým příjemcům současně.

Dvoufaktorové ověřování (2FA): Pro přístup k účtu nebo dokončení transakce je nutné použít dva způsoby ověření, obvykle heslo a samostatný kód nebo zařízení.

Dust Transaction: Transakce, při níž se posílá velmi malé množství bitcoinů, které je příliš malé na to, aby bylo ekonomicky výhodné.

Etický hacker: Osoba, která využívá své schopnosti k identifikaci a opravě zranitelností v počítačových systémech a sítích.

FOMO: Fear of missing out (strach z promeškání příležitosti) je termín používaný k popisu pocitu úzkosti nebo lítosti, že člověk může propásnout ziskovou příležitost na trhu.

FUD: Fear, uncertainty and doubt, termín používaný k popisu negativních zvěstí nebo informací, které mohou způsobit paniku nebo pokles trhu.

HDP: Hrubý domácí produkt neboli celková hodnota zboží a služeb vyprodukovaných v dané zemi za určité období.

Hard Fork: Změna protokolu, která vytvoří novou verzi blockchainu, která není kompatibilní s předchozí verzí (např. Bitcoin Cash).

Hardwarová peněženka: Fyzické zařízení používané k ukládání soukromých klíčů a správě kryptoměn, které poskytuje vyšší bezpečnost než softwarové peněženky.

Hashovací funkce: Matematická funkce, která přijímá vstupní data libovolné velikosti a na jejímž výstupu je řetězec znaků pevné velikosti. Běžně používaná v kryptografii a blockchainové technologii.

Slovník pojmů

Hash Rate (rychlost hašování): Je to způsob měření výpočetního výkonu bitcoinové sítě.

HODL: : Termín používaný v kryptoměnové komunitě pro označení dlouhodobého držení kryptoměny namísto jejího prodeje nebo obchodování s ní.

Hodnota peněz v čase: princip, podle kterého mají peníze větší hodnotu v současnosti než v budoucnosti.

Hot Wallet: Peněženka, která je připojena k internetu a umožňuje snadný přístup k bitcoinům.

ID transakce: Řetězec čísel a písmen, který v bitcoinovém blockchainu zobrazuje podrobnosti o bitcoinovém převodu (například odeslanou částku, adresy odesílatele a příjemce a datum převodu).

Inflace: Zvýšení obecné cenové hladiny zboží a služeb v ekonomice. Jinými slovy zvýšení peněžní zásoby v oběhu, které zvyšuje poptávku a tím tak tlačí ceny nahoru.

Komoditní peníze: Předměty, které mají hodnotu samy o sobě a používají se jako prostředek směny, v historii například zlato nebo stříbro.

Kontrola kapitálu (peněz): Omezení pohybu peněz přes hranice.

Kryptoměnová peněženka: Softwarový program, který uchovává soukromé klíče a umožňuje uživatelům posílat, přijímat a spravovat kryptoměny.

Kryptografie: Obor matematiky, který pomáhá vytvářet bezpečné systémy.

Kupní síla: Určuje cenu peněz peněz, za které lze nakupovat zboží a služby.

Lightning Network: Platební protokol druhé vrstvy, který umožňuje rychlejší a levnější bitcoinové transakce pomocí otevřených kanálů mimo hlavní řetězec. Slouží pro malé a každodenní transakce.

Mechanismus Konsensu: Zároveň je to metoda používaná v blockchainové technologii k ověřování transakcí a zajištění integrity blockchainu.

Merkle Tree: Datová struktura používaná v bitcoinovém blockchainu k efektivnímu ověřování integrity velkých souborů dat.

Mempool: V tomto nástroji si uživatelé mohou prohlížet jednotlivé bloky, transakce a adresy peněženek.

Měnová a fiskální politika: Politika centrální banky a vlády, která ovlivňuje nabídku peněz a úrokové sazby v ekonomice.

Multi-Signature: Je bezpečnostní funkce, která vyžaduje více než jeden soukromý klíč k autorizaci bitcointové transakce.

Nabídka a poptávka: Ekonomický princip, podle kterého je cena zboží nebo služeb určena vzájemným působením množství dodávaného zboží nebo služeb a poptávky.

Non-Fungible Token (NFT): Z překladu „nezaměnitelný token" je typ digitálního aktiva, které představuje jedinečný nebo unikátní předmět, často používaný k reprezentaci uměleckých děl, sběratelských předmětů nebo jiných předmětů.

Nonce: Náhodné číslo přidané do hlavičky bloku za účelem vytvoření hashe, který odpovídá cíli obtížnosti.

Odměna za blok: Množství nových bitcoinů, které jsou těžařům přiděleny za přidání nového bloku do blockchainu.

Osiřelý blok: Blok, který nebyl zařazen do hlavního řetězce blockchainu, protože byl zneplatněn předchozím konkurenčním řetězcem.

Obnovovací fráze/seed: Série 12, 18, 20 nebo 24 slov, která lze použít k vygenerování několika párů soukromých a veřejných klíčů. Ty lze použít k obnovení bitcoinové peněženky.

Obchodní pár: Sada dvou měn nebo aktiv, která lze vzájemně obchodovat na kryptoměnové burze.

Potvrzení: Proces, při kterém je transakce zpracována sítí a je velmi nepravděpodobné, že by byla zrušena. Metoda „těžařů", která slouží k ověřování pravosti transakcí pomocí jejich počítačového hardwaru a softwaru. Doporučuje se počkat na nejméně šest potvrzení, aby se zabránilo dvojímu utracení.

Počáteční nabídka mincí (ICO): Způsob získávání finančních prostředků, při kterém se investorům prodává nová kryptoměna výměnou za fiat nebo za zavedenější kryptoměnu, jako je například Bitcoin.

Protokol na první vrstvě: Základní vrstva blockchainové sítě, která se stará o základní aspekty konsensu, ověřování transakcí a ukládání dat.

Protokol na druhé vrstvě: Sekundární vrstva postavená nad blockchainovou sítí první vrstvy, která se často používá ke zvýšení škálovatelnosti, rychlosti a funkčnosti.

Prostředky směny: Jakýkoliv předmět/prostředek, který je všeobecně přijímán výměnou za zboží a služby.

Peněžní zásoba: celkové množství peněz v oběhu.

Papírová peněženka: Vytištěná kopie soukromých a veřejných klíčů uživatele, která slouží k ukládání a správě kryptoměn off-line.

Peer-to-Peer (P2P): Decentralizovaná síť, ve které účastníci komunikují přímo mezi sebou, nikoli prostřednictvím centrální autority.

Slovník pojmů

Peg: Pevný směnný kurz mezi dvěma měnami, kdy je jedna měna navázána na hodnotu druhé měny.

Proof-of-Stake (PoS): Mechanismus konsensu používaný v některých blockchainových sítích, který vyžaduje, aby uživatelé drželi určité množství kryptoměny, aby se mohli podílet na ověřování transakcí.

Proof-of-Work (Důkaz o vykonané práci): V tomto případě se jedná o mechanismus konsensu, který vyžaduje, aby uživatelé provedli určité množství výpočetní práce, aby se mohli podílet na ověřování a zabezpečování sítě.

Poměr rezerv: Podíl vkladů, které musí banka držet jako rezervy.

Podpis: Digitální matematický mechanismus, který někomu umožňuje prokázat vlastnictví.

Peněženka: Virtuální schránka na bitcoiny, která obsahuje soukromý klíč (klíče) umožňující odesílat, přijímat a spravovat bitcoiny.

Restriktivní bankovnictví: Omezení bankovních služeb nebo přístupu k bankovním službám.

Síť: Skupina vzájemně propojených subjektů.

Síť uzlů: Síť propojených počítačů nebo zařízení, které podporují a udržují bitcoinovou síť.

Soukromý blockchain: Blockchain, který je kontrolován jednou organizací, není tedy decentralizovaný.

Soukromý klíč: Tajný klíč, který prokazuje právo osoby utrácet bitcoiny z konkrétní peněženky prostřednictvím kryptografického podpisu.

Satoshi Nakamoto: Pseudonym, který používá anonymní tvůrce Bitcoinu.

Satoshi: Nejmenší jednotka bitcoinu, která se rovná 1/100 000 000 bitcoinu. Je pojmenována po tvůrci Bitcoinu, Satoshi Nakamotovi.

Satoshi na bajt (sat/b): Jednotka používaná k měření výše poplatku za bitcoinovou transakci zaplaceného za jeden bajt transakčních dat.

SegWit (Segregated Witness): V případě Bitcoinu se jedná o upgrade protokolu, který mění způsob ukládání dat v blockchainu, což umožňuje zvýšit kapacitu a snížit transakční poplatky.

Sidechain: V tomto případě se jedná o blockchain, který je připojen k jinému blockchainu a umožňuje přenos aktiv nebo informací mezi oběma řetězci.

Soft Fork: Změna protokolu Bitcoinu, která je zpětně kompatibilní se staršími verzemi softwaru.

Stablecoin: Typ kryptoměny navržený tak, aby si udržoval stabilní hodnotu často tím, že je vázán na fiat měnu nebo jiné aktivum.

Směnný kurz: Hodnota jedné měny ve vztahu k jiné měně.

Směnný obchod: Výměna zboží a služeb bez použití peněz.

Spotřební koš: Soubor zboží nebo služeb, který se používá k měření změn životních nákladů (často k měření inflace).

Těžební pool (Mining Pool): skupina těžařů, kteří spolupracují, aby zvýšili své šance na nalezení nových bloků a získání bitcoinů. Odměny jsou následně rozdělovány podle výpočetního výkonu.

Těžba: Proces, při kterém se pomocí počítačového hardwaru provádějí matematické výpočty, aby se potvrdily transakce a zvýšila bezpečnost sítě.

Token: Hodnotová jednotka vytvořená na blockchainu, která často reprezentuje konkrétní aktivum nebo užitek v rámci určitého ekosystému.

Tokenizace: Proces vytvoření digitální reprezentace aktiva nebo třídy aktiv na blockchainu, který umožňuje částečné vlastnictví a převoditelnost.

Transakční poplatek: Malá částka, kterou platí odesílatel transakce a která motivuje těžaře, aby transakci zařadili do bloku a přidali ji do blockchainu.

Transakce: Převod bitcoinů z jedné adresy na druhou v bitcoinové síti.

Unbanked („Bez bankovního účtu"): Jednotlivci nebo komunity bez přístupu k tradičním bankovním službám.

Uzel: Počítač nebo zařízení, které je připojeno k bitcoinové síti a podílí se na ověřování, přenosu transakcí. Dále zabezpečují, že pravidla v síti jsou dodržována.

Účetní kniha: Záznam o finančních transakcích.

Účetní jednotka: Standardní měrná jednotka používaná k vyjádření hodnoty zboží a služeb.

Vícepodpisová peněženka (Multisig): peněženka, která vyžaduje více podpisů nebo schválení před provedením transakce, což poskytuje dodatečné zabezpečení a kontrolu.

Veřejný blockchain: Blockchain je otevřený komukoli, kdo se může účastnit a ověřovat transakce, čímž se stává decentralizovaným.

Veřejný klíč: Jedinečný identifikátor používaný pro příjem bitcoinů odvozený ze soukromého klíče uživatele pomocí matematického procesu.

Slovník pojmů

Veřejný klíč/adresa bitcoinu: Jednoduše řečeno adresa používaná k přijímání bitcoinů.

Veřejná účetní kniha: Veškeré transakce v bitcoinové síti se zaznamenávají do decentralizované databáze.

Volatilita: Míra kolísání ceny aktiva v čase.

Velryba: Jednotlivec nebo organizace, která drží značné množství bitcoinů a je schopna ovlivňovat ceny na trhu prostřednictvím velkých obchodů.

Whitepaper: Dokument, který vysvětluje problém a řešení, které se blockchainový projekt nebo kryptoměna snaží řešit.

XBT a BTC: Zkratky pro označení bitcoinu. XBT se dnes již nepoužívá.

Záloha peněženky: Kopie soukromých klíčů pro obnovení bitcoinové peněženky, kterou lze použít k opětovnému získání přístupu k peněžence v případě ztráty nebo krádeže originálu.

Znehodnocení: Snížení hodnoty dané měny, často snížením množství drahého kovu v minci (v historii příměs levnějších kovů, ořezávání, děrování mincí).