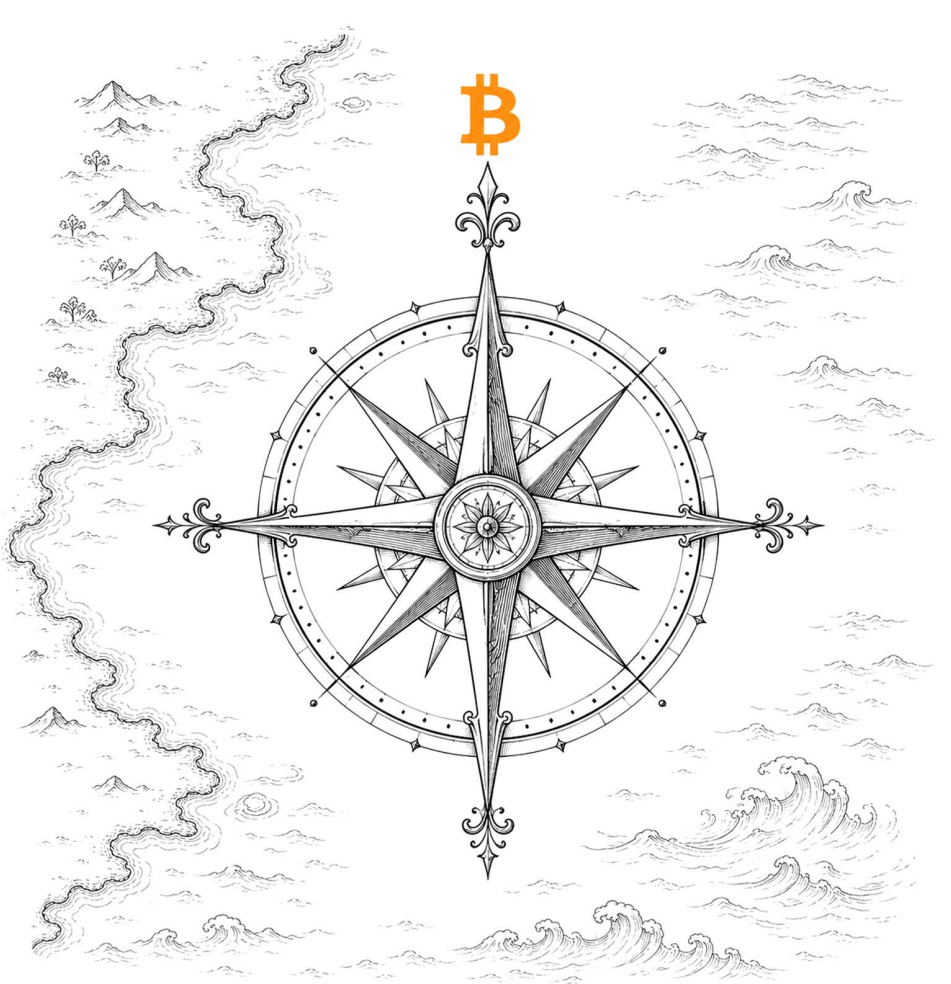
Bitcoin
v kapse

Praktická příručka, kterou bych si přál mít, když jsem začínal



Tomáš Krause

Obsah

Úvod

Poprvé jsem o Bitcoinu slyšel v roce 2012. Vzpomínám si přesně kde a taky vím, jaká byla tehdy moje reakce: *To je nesmysl, kdo by to používal*. A tak jsem ho ignoroval dalších pět let.

Vrátil jsem se v roce 2017, kdy cena letěla až na tehdy závratných 20 000 dolarů a psalo se o něm všude. A tehdy mě napadlo založit i web *bitcoinvkapse.cz* a o Bitcoinu vzdělávat nejen sebe, ale i ostatní.

Tahle kniha vznikla skoro o deset let později proto, že jsem usoudil, že na webu je už tolik materiálu, že by stálo za to ho zhustit do kompaktnější formy a nabídnout těm, kteří se nacházejí teprve na začátku své bitcoinové cesty.

Dozvíte se v ní, jak Bitcoin funguje, kde ho koupit, jak ho bezpečně uložit, jak s ním platit a jak se vyhnout podvodům — všechno v kontextu české reality a s konkrétními nástroji, které vám cestu usnadní.

Nemusíte rozumět kryptografii ani ekonomii. Nemusíte být programátor. Stačí být zvědavý a věnovat pár hodin jejímu přečtení. Výhodou této knihy je, že se dá číst i na přeskáčku. Nemusíte číst všechny kapitoly, vyberte si jen to, co vás zajímá právě teď. A pokud budete mít nějaký dotaz nebo vám něco nebude jasné, neváhejte mi napsat.

PS: v knize píšu Bitcoin i bitcoin. Ten s velkým B je síť, protokol, prostě ten vynález. S malým b je to měna, mince.

Tomáš, *bitcoinvkapse.cz*

Věnováné mé ženě, která byla prvním čtenářem této knihy a přežila to :)

Část I: Úvod do Bitcoinu

Kapitola 1: Co je Bitcoin a proč vznikl

V říjnu 2008, uprostřed největší finanční krize za poslední desetiletí, zveřejnil někdo pod přezdívkou Satoshi Nakamoto dokument popisující digitální měnu, která nepotřebuje banky – Bitcoin. A 3. ledna 2009 ho spustil a vytěžil první blok. V jeho datech schoval citaci titulku z britských novin The Times z toho dne: „Chancellor on brink of second bailout for banks" – Ministr financí na pokraji druhé záchranné půjčky pro banky. Jasný vzkaz proč Bitcoin vzniká a taky důkaz, že žádné bitcoiny nebyly vytěženy před tímto datem.

Mě osobně Bitcoin zaujal, protože jako první v historii řeší problém, který se zdál neřešitelný – jak si dva lidé na opačných koncích světa pošlou peníze bez toho, aby museli věřit nějaké třetí straně. Žádná banka, žádný PayPal, žádný prostředník. Jen matematika.

Co je Bitcoin

Bitcoin (zkratka BTC) je první a nejznámější kryptoměna a stejnojmenná síť, která funguje od roku 2009, kdy ji popsal a vytvořil člověk nebo skupina lidí podepsaná jako Satoshi Nakamoto. Zhruba od roku 2021 razí bitcoineři čím dál hlasitěji heslo, že Bitcoin není krypto. Chtějí se tím distancovat od „kryptoměn", které často řeší neexistující problémy, případně jsou rovnou podvodem. S Bitcoinem není spjat žádný skandál ani krach, což se o mnoha jiných kryptoměnách říct nedá.

Bitcoin neexistuje v žádné fyzické podobě. Neexistují mince ani bankovky, veškeré mince jsou pouze virtuální, tedy jen změť jedniček a nul. O fungování měny se stará decentralizovaná síť na sobě nezávislých počítačů. Neexistuje žádný centrální bod, který by šel vypnout a Bitcoin tak zničit. Neexistuje ani žádný člověk, který by měl hlavní slovo a mohl Bitcoin ovládat. Síť funguje na principu konsenzu a vždy se musí dohodnout většina.

Konečné množství bitcoinů je předem známo a do oběhu se uvolňují postupně. Bitcoinů bude existovat 21 milionů a ani o jeden více. Všechny bitcoiny budou vytěženy v roce 2140. Drtivá většina však už okolo roku 2030.

Kupovat lze i zlomky bitcoinu. V současnosti je bitcoin dělitelný na 8 desetinných míst, ale toto číslo lze v budoucnu navýšit. Nejmenší jednotkou je jeden *satoshi* (na počest zakladatele), což je 0,00000001 bitcoinu.

Rozdíl proti klasickým (FIAT) měnám

Podívejte se na klíčové rozdíly mezi Bitcoinem a klasickými FIAT měnami (koruny, dolary, eura...).

	Bitcoin	FIAT měny
Omezené množství	Ano, nikdy nebude existovat více jak 21 milionů bitcoinů	Ne, státy si peníze mohou tisknout – a také je tisknou, jak je napadne
Lze peníze zabavit?	Při správném používání ne	Ano, bez problémů
Anonymita	Pseudonymní — všechny transakce jsou veřejné, identita za adresou ne (pokud ji sami neprozradíte)	V případě bankovních převodů ne, v případě platby v hotovosti ano
Odolnost proti falšování	Ano, bitcoin nelze zfalšovat	Ne
Centralizace	Ne, neexistuje žádná centrální správa, osoba ani místo, kde by šlo Bitcoin vypnout	Ano, státní měny ovládají státy prostřednictvím centrálních bank

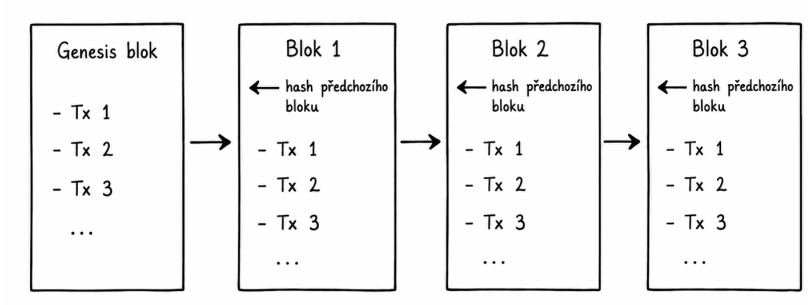
Blockchain

V souvislosti s Bitcoinem pravděpodobně narazíte na slovo *blockchain*. Co to je a proč je pro Bitcoin klíčový?

Formální definici z učebnice si odpustím. Laicky řečeno: Bitcoin používá blockchain jako obrovskou účetní knihu, kde je navždy zapsaná jakákoliv transakce v síti. Když vám někdo pošle bitcoin, navěky už bude v této databázi zapsáno, že se tak stalo a že bitcoin je teď váš. A nejlepší na tom je, že nikdo tento záznam nedokáže změnit a tvrdit, že bitcoin poslal někomu jinému nebo neposlal vůbec.

Jak je to možné? Bitcoinový blockchain existuje v nekonečně kopiích po celém světě, stáhnout si ho můžete i vy. Veškeré transakce s bitcoiny musí ověřit na sobě nezávislé uzly a není možné, aby si jeden uzel do blockchainu zapsal transakci po svém. Uzly se navzájem kontrolují a jakoukoliv anomálii by okamžitě odhalily a odmítly.

Představte si blockchain jako vlak, do kterého se připojuje nekonečné množství vagónů. Vagón = blok, do kterého se volně sypou všechny transakce, které se po celém světě s bitcoiny dělají. Jakmile je vagón plný, těžaři hádají číslo (odborně hash), které celý vagón reprezentuje. Když ho někdo najde a většina se shodne na tom, že je to správně, vagón se tímto číslem zaplombuje, transakce v něm se potvrdí (proběhnou) a začne se plnit další vagón. Fígl je v tom, že kdyby se někdo pokusil změnit jeden jediný znak v již zapečetěném vagónu, okamžitě se změní ona pečeť a celý vlak se rozpojí a havaruje. Proto je nemožné změnit cokoliv v již proběhlých transakcích.



Blockchain jako řetěz bloků

Blockchainu ještě věnujeme celou samostatnou kapitolu.

Těžaři

V předchozím odstavci jsem zmínil těžaře a asi se ptáte, kdo to vlastně je.

Bitcoin je navržen tak, že mince se uvolňují do oběhu postupně a těžaři zajišťují, že nové mince vznikají. Počítají matematické operace, kterými se zamyká „vagón". Jakmile je vagón spočten a uzamčen, dostává těžař, který udělal správný výpočet jako první, odměnu v bitcoinech. Tato odměna se po potvrzení každých 210 000 bloků (vagónů) půlí a tím se přísun nových bitcoinů do systému zpomaluje. Protože se jeden nový blok potvrzuje zhruba každých deset minut, dochází k půlení jednou za 4 roky.

Možná vás teď napadá otázka, co se stane, až odměna klesne tolik, že už se těžení nevyplatí. Dobrá otázka. Kromě odměny za vytěžený blok dostávají těžaři i odměnu za zpracované transakce – bitcoiny nelze poslat zadarmo, vždy musíte zaplatit drobný poplatek za provedení platby. Těžaři by tak měli mít vždy motivaci síť provozovat.

Pokud si teď říkáte, že jdete také těžit bitcoiny, tak na to zapomeňte. Mělo vás to napadnout před mnoha lety, dnes je už pozdě. Na úplném začátku Bitcoinu mohl být těžařem kdokoliv, kdo měl počítač a připojení k internetu. Dnes už je nemožné těžit bitcoiny na běžných počítačích a používají se k tomu speciální jednoúčelové počítače, tzv. ASIC minery.

Běžní uživatelé

Jako běžný uživatel nemusíte nic těžit a dokonce nemusíte ani chápat všechny technické detaily fungování Bitcoinu. Můžete si ho koupit a platit s ním, nebo si ho nechat jako investici či spoření. Většina lidí si bitcoiny pořizuje spíše jako to druhé, zejména proto, že cena bitcoinu se proti státním měnám dlouhodobě zvyšuje.

Bitcoin je první forma peněz v historii lidstva, kterou stát neumí ani vytisknout, ani zabavit, ani vypnout. To je celé jádro toho, proč existuje a proč o něm má smysl mluvit dál.

V následujících kapitolách se podíváme podrobněji na to, kdo je nebo není Satoshi Nakamoto, proč Bitcoin a ne altcoiny, a zejména jak si Bitcoin pořídit a bezpečně uložit.

Rozcestník pro další studium: bitcoinvkapse.cz/kniha/kapitola-1

Kapitola 2: Kdo je (nebo není) Satoshi Nakamoto

Bitcoinu je jedno, kdo ho stvořil. Fungoval by úplně stejně, i kdyby ho vymyslel kdokoliv jiný. A přesto je příběh Satoshiho Nakamota fascinující. Člověk (nebo skupina lidí?) vytvoří systém, který dnes přesouvá miliardy dolarů, a pak jednoduše zmizí. Záměrně smaže všechny stopy. Nechce slávu, nezpeněží pozici zakladatele, nepřijme žádnou cenu. Podle mě je tahle anonymita zakladatele jednou z nejsilnějších věcí, které Bitcoin má. Díky ní nikdo nemůže říct „zavolám Satoshimu a on to změní."

Zpráva, která změnila svět peněz

Prvního listopadu 2008 obdrželi čtenáři newsletteru The Cryptography Mailing List krátkou zprávu. Jejím autorem byl neznámý člověk, který se podepsal jako Satoshi Nakamoto. Text zprávy byl stručný: *„Pracuji na novém systému elektronických peněz, který je plně založen na peer-to-peer modelu, bez potřeby důvěryhodného prostředníka."*

K e-mailu byl přiložen odkaz na stručný dokument – Bitcoin white paper. Teoretický návrh platebního systému, který funguje bez bank, bez centrální autority, bez někoho, komu by bylo potřeba důvěřovat.

O sobě Satoshi sdělil jen naprosté minimum: rok narození 1975 a původ z Japonska. Nic víc.

Komunikace a zmizení

Po zveřejnění white paperu Satoshi jen neteoretizoval, ale aktivně pracoval na kódu a s dalšími vývojáři komunikoval přes e-mail a na fóru Bitcointalk. Byl všem k dispozici, odpovídal na dotazy, řešil problémy.

Pak, v roce 2011, předal vývoj komunitě se slovy *„projekt je v dobrých rukou"* a vypařil se. Doslova. Žádné rozloučení, žádné vysvětlení, žádný comeback.

A od té doby je ticho.

Desítky teorií, žádná jistota

Anonymita autora Bitcoinu přitahuje spekulace jako med včely. V průběhu let se objevily desítky teorií o tom, kdo se za jménem Satoshi Nakamoto skrývá.

V roce 2014 zveřejnil magazín Newsweek fotografii staršího pána jménem Dorian Satoshi Nakamoto – shoda jmen plus povolání matematika a IT specialisty se zdála příliš nápadná. Dorian to razantně popřel.

Podnikatel Craig Wright se propojení s Bitcoinem nebránil – naopak, sám se několikrát pokoušel dokázat, že Satoshi je on. V březnu 2024 ale soud rozhodl, že není Satoshi.

Hodně lidí si myslí, že za jménem Satoshi Nakamoto stojí Nick Szabo – Američan maďarského původu, který ještě před Bitcoinem vymyslel koncept digitální měny Bit Gold. Myšlenka je nápadně podobná Bitcoinu. Lingvistická analýza textů od Szaba a Nakamota navíc ukázala podezřelou shodu ve stylu psaní. Szabo to popírá.

Hal Finney – zvláštní případ

Zvláštní místo mezi „podezřelými" zaujímá Hal Finney – jeden z prvních lidí, kteří se Satoshim komunikovali, a příjemce vůbec první bitcoinové transakce v historii.

Argument je jednoduchý: kdybyste sami vymysleli a spustili něco jako Bitcoin, neposlali byste první transakci sami sobě? Protiargument: bylo by strašně náročné a náchylné na chyby povídat si sám se sebou a hrát, že jste dva.

Hal Finney zemřel v roce 2014 po dlouhém boji s ALS. Svou případnou větší roli v příběhu Bitcoinu nikdy nepotvrdil.

Proč to možná nikdy nezjistíme

Odhaduje se, že skutečný Satoshi Nakamoto vlastní přes jeden milion bitcoinů, kterými za celou dobu nepohnul. Pokud je naživu, tak dobře ví, co dělá a má silný důvod zůstat v anonymitě – nejen kvůli obrovským penězům, ale i kvůli své bezpečnosti.

Každý, kdo byl v minulosti veřejně označen jako Satoshi, čelil obtěžování a mediálnímu tlaku. Anonymita je v tomhle případě nejlepší ochrana.

To, že identitu zakladatele Bitcoinu neznáme je lepší a správné. Bitcoin funguje bez ohledu na to, kdo ho stvořil. Jeho pravidla jsou zapsaná v kódu, ne v osobě zakladatele. A žádný jiný velký finanční systém na světě tohle o sobě říct nemůže.

Rozcestník pro další studium: bitcoinvkapse.cz/kniha/kapitola-2

Kapitola 3: Proč Bitcoin a ne altcoiny

Nebyl jsem vždy Bitcoin maximalista. Chvíli jsem si hrál i s tzv. altcoiny, sledoval jsem desítky projektů a říkal si, že třeba tohle bude další velká věc. Výsledek? Měřeno v bitcoinech jsem byl skoro vždy v minusu. Altcoiny rostly, ale Bitcoin rostl víc. Altcoiny padaly, ale Bitcoin padal méně. Po roce nebo dvou jsem si řekl dost a přestal jsem jiné kryptoměny řešit.

Ale to je jen můj osobní příběh. Důležitější je princip.

Bitcoin vznikl jako řešení konkrétního problému: jak mít peníze, které nikdo nemůže znehodnotit, zabavit nebo vypnout. Tohle je velký problém a Bitcoin ho elegantně vyřešil pomocí decentralizace, omezeného množství a pravidel zapsaných v kódu, která nikdo nemůže změnit bez souhlasu většiny.

Altcoiny většinou tvrdí, že jsou „rychlejší" nebo „levnější" nebo „chytřejší". Možná jsou. Ale skoro vždy za cenu toho, že mají centrálního šéfa, neomezenou emisi nebo mince předtěžené pro své zakladatele. A často také řeší problémy, které neexistují, nebo je lze řešit pomocí dnešních fiat peněz.

Bezmála dvě dekády provozu bez výpadku, bez centrálního šéfa, bez skandálu. To je to, co nemá žádná jiná kryptoměna.

Dvě kategorie altcoinů: podvody a zbytečnosti

Zjednodušeně řečeno existují dva druhy altcoinů. První jsou otevřené podvody – projekty, které vznikly jen proto, aby jejich zakladatel zbohatl na úkor nakupujících. Druhé jsou projekty, které sice nejsou záměrně podvodné, ale řeší problémy, které buď neexistují, nebo je řeší Bitcoin.

Dobrý příklad první kategorie jsou různé „lepší Bitcoiny", které se i v Česku čas od času šíří přes síť „poradců" a youtubových influencerů. Ti vám vysvětlí, že právě tahle nová kryptoměna je naprostá bomba a vy na její koupi pohádkově

Líbila se vám ukázka?

Tohle byly první dvě kapitoly z knihy **Bitcoin v kapse** – *Praktická příručka, kterou bych si přál mít, když jsem začínal*.

Zbývá dalších 29 kapitol nabitých informacemi z praxe: jak Bitcoin funguje, kde ho koupit, jak ho bezpečně uložit nebo jak se vyhnout podvodům – podívejte se na začátek na obsah.

Budu rád, když si koupíte celou knihu na bitcoinvkapse.cz/kniha. A pokud vám po jejím přečtení nebude něco jasné, můžete mi napsat a probereme to spolu.