BITCOIN A TI DRUZÍ

BORIS KALISKÝ

A JEHO

NEPOSTRADATELNÝ PRŮVODCE
SVĚTEM KRYPTOMĚN

IFP publishing

Poděkování

Autor děkuje Jaroslavu Forštovi a IFP Publishing za nabídku napsat tuhle knihu a trpělivou podporu při jejím vzniku. Dále Kateřině za lásku a trpělivost při psaní a pomoc s korekcemi. Radkovi Blažíkovi a Martinovy Šípovi za připomínky k textu.

Boris Kaliský
KRYPTOMĚNY

Odpovědný redaktor Mgr. Jaroslav Foršt
Sazba a zlom IFP Publishing s.r.o.
Vydalo nakladatelství IFP Publishing s.r.o. v roce 2018 jako svou 80. publikaci.

ISBN 978-80-87383-71-1

Obsah

Úvod

Na konci roku 2017 se cena jednoho bitcoinu dotkla hranice 20 000 dolarů neboli více než 400 000 korun. V roce 2018 prochází korekcí. V běžné řeči se cena vrací na úroveň o desítky procent a tisíce dolarů nižší. Od vzniku Bitcoinu[1] v roce 2009 si trh s bitcoinem podobnou fází růstu a poklesu prošel mnohokrát. Průvodním jevem byly rychlonázorové články o tom, jaká je to bublina, kolik stačilo investovat, abyste dnes byli milionáři, kolik států by šlo zásobovat energií spotřebovanou Bitcoinovou sítí a že bitcoin je mrtvý. Podle statistiky stránky 99bitcoins.com/bitcoinobituaries, která počítá předpovědi o konci bitcoinu od renomovaných ekonomů, institucí či médií, byl Bitcoin v okamžiku psaní těchto vět pohřbíván 249 krát (březen 2018).

To je ale jenom jeden, a ještě k tomu zjednodušený pohled na technologii, která je tady krátce, rychle se mění a tím znesnadňuje uchopení. Informovanější autoři se (naštěstí) posunuli od investičních bublin, měny překupníků drog a matematických cvičení o rychlých milionech k podrobnějšímu informování o fenoménu kryptoměn. Na specializovaných serverech se můžete dozvědět, že cena bitcoinu pravidelně a výrazně koriguje. Bitcoin, vyjádřeno celkovou hodnotou v poměru k ostatním kryptoměnám – sice ztrácí své dominantní postavení, ale bližším pohledem má stále nejvyšší hodnotu. Je mezi kryptoměnami nejznámější, většina obchodování na burzách probíhá přes něj a když ostatním kryptoměnám dojde dech, nebo v nějaké zemi spadne hodnota místní národní měny, spekulanti i běžní lidé se obrací k bitcoinu.

O Bitcoinu se taky dočtete, že zaostává svými technickými parametry. Nárůst zájmu koncem roku 2017 způsobil zahlcení jeho sítě. Cena za transakci narostla k desítkám až stovkám korun, čas potvrzení transakce narostl na hodiny. Bitcoin se na čas stal nepoužitelný na běžné platby. Co se už běžně nedočtete jsou podrobnosti o tom, jak probíhá vývoj Bitcoinu, že už existují řešení pro zrychlení transakcí a testují se další, která mnohonásobně navýší kapacitu sítě.

No a do třetice nadšení z možností mladších kryptoměn, které využitím přesahují prostou alternativu k penězům vede k závěrům, že budoucnost patří komplexním kryptoměnám a technologiím na nich založeným. Tady je vhodné opatrné „možná", doplněné o podmínku, že pro své řešení najdou reálné problémy, přežijí dětské nemoci a alespoň z části naplní často velkolepé vize svých tvůrců.

V konečném důsledku platí, že jestli se bude používat bitcoin, jiné měny nebo jejich kombinace, není dlouhodobě důležité. Bitcoin mění způsob, jakým vlastníme, používáme peníze a jak o nich uvažujeme. Kryptoměny a technologie s nimi spjaté mění způsoby uchovávání dat, způsoby, jak vytváříme a garantujeme smlouvy, nebo do jaké míry potřebujeme nebo nepotřebujeme státní instituce a banky k zajištění finančního systému. Stále je však brzo na zásadní závěry o jejich budoucnosti, o tom kde, a v jaké formě se prosadí, jaký bude jejich vliv na tu kterou oblast našich životů a jak změní naši společnost.

[1]Bitcoin – s velkým B je v knize používán pro název systému, který umožňuje transakce kryptoměny bitcoin (malé b).

Komu je kniha určena:

Navzdory zájmu o Bitcon je k dispozici málo[2] knih v češtině, z nichž by čtenář v získal v uživatelsky přívětivé formě informace o jeho fungování a používání. Jedním z důvodů je rychlost, s jakou se Bitcoin a kryptoměny vyvíjejí. Za dobu několika měsíců, což je doba potřebná na přípravu knihy, může dojít k zásadním změnám a autor riskuje, že píše vstříc neaktuálnosti. Na druhou stranu, kdo se dnes chce zorientovat v této problematice, musí sáhnout po literatuře v cizích jazycích, případně se vydat na časově náročnou cestu studia různých internetových zdrojů, často spojenou se zdlouhavým odhalováním relevantních informací.

Tato knížka je psána s cílem poskytnout počáteční informace o kryptoměnách, jejich fungování, používání a možnostech. Najdete v ní převážně informace o Bitcoinu jeho historii, vlastnostech a možnostech. Dále postupy, jak se nakupuje/prodává a jak jej bezpečně používat. Autorův názor je, že ještě nějakou dobu bude Bitcoin klíčovou kryptoměnou na trhu. Také pochopení jeho základů a možností usnadňuje pochopení vývoje, který v oblasti kryptoměn probíhá a jehož důsledkem je dalších více než 1400 obchodovaných kryptoměn. Proto v knize najdete také informace o tom, kam směřuje vývoj v oblasti, jaké možnosti nabízejí nové kryptoměny a technologie s nimi spojené, a kde lze nalézt aktuální informace v případě, že se čtenář rozhodnete do těchto technologií investovat svůj čas a peníze.

Boris Kaliský

srpen 2018

[2] Na českém trhu průlomová je kniha Dominika Stroukala a Jana Skalického; Bitcoin: Peníze budoucnosti, která Bitcoin nahlíží pohledem ekonomického liberalizmu a jako alternativy centralizovaným státním měnám. Autor z jejího prvního vydání čerpal hlavně při psaní první kapitoly této knihy. Více na: www.penize-budoucnosti.cz.

Stručné dějiny bitcoinu (a kryptoměn)

Peníze a technologie

Co jsou peníze? Co to je hodnota? Co je hodnota peněz? Klíčové otázky, pokud chceme pochopit cenu a hodnotu bitcoinu a ostatních kryptoměn.

Od 20. století funguje peněžní systém na tzv. fiat penězích, které jsou definované jako „peníze s nuceným oběhem[1]". Pro jeho pochopení se musíme vrátit do doby zlatého standardu a k dnes stále rozšířené víře, že peníze jsou kryté, nebo že mají vnitřní hodnotu. Zlatý standard čili ukotvení hodnoty papírových peněz hodnotou zlata (a směnitelnost peněz za dané množství zlata) se v průběhu dvacátého století ukázal jako nefunkční. Projevilo se to jeho neschopností reagovat na následky první světové války a následné hospodářské krize. Jeho poslední zbytky skončily v roce 1971, kdy prezident Nixon zrušil směnitelnost dolaru za zlato.

V Čechách tento systém fungoval nepřímo. Rakousko-uherská banka nikdy neměla povinnost směnit bankovky za zlato. Bylo ale možné měnit je například za dolary nebo libry, které směnitelnost za zlato umožňovaly. Československá koruna měla zákonem z roku 1927 deklarovanou hodnotu 44,58 miligramu zlata. To však za účelem měnové a kurzové politiky, nikoliv směnitelnosti.

Informace o krytí přetrvávala na bankovkách a její hodnota byla průběžně upravována. Naposledy v roce 1953 po měnové reformě, která kromě znehodnocení vkladů obyvatel (např. kdo měl 5 000 Kč na účtu, dostal 1 000 nových korun, kdo měl 25 000, dostal také 1 000) stanovila obsah zlata v koruně na 0,123426 gramu. Tento obsah nijak nesouvisel s hodnotou koruny a přetrval do konce 80. let.[2] Bankovky stále obsahovaly text: „Bankovky jsou kryté zlatem a ostatními aktivy Státní banky Československé". Z této věty nejspíš pramení přetrvávající dojem, že i současné peníze jsou kryty zlatem. Dnešní peníze jsou kryty, respektive čerpají svou hodnotu **z víry a důvěry**. Konkrétně v schopnosti národní banky dohlížet na emisi (lidově – tisk) peněz a na dodržování pravidel finančního systému. Jedním z nich je například tzv. kapitálová přiměřenost bank. Ta vyjadřuje, kolik peněz má banka na účtu ve srovnání

[1] Moderní ekonomiky současnosti používají tzv. peníze s nuceným oběhem (z lat. slova fiat – překládaného jako „ať se stane" nebo „budiž", které se v ang. užívá jako „z nařízení"), které nejsou navázány na žádnou komoditu. O vynucení se starají právní normy (zákony), které orgány státu zavádí a řídí konkrétní soustavu peněz a upravují aspekty jejího oběhu a ochrany. Ustanovení měny je vždy právním aktem a měna je jedním z atributů suverenity státu. Nebo ještě jinak – fiat měny jsou dnes národní měny jako Česká koruna. Jejich vznik a oběh se řídí zákony, které schvaluje parlament a spravuje je kompetentní úřad – v ČR je to Česká národní banka.

[2] Více k tématu např.: stránky České národní banky - Čím je kryta měna? www.cnb.cz/cs/faq/cim_je_kryta_mena.html

s penězi, které investovala nebo půjčila klientům. Minimum je 8 %. Na každých 8 korun, které banka reálně má, může teoreticky půjčit a tím vytvořit 82 korun v podobě úvěru. Když příliš mnoho bank půjčí hodně peněz klientům, kteří nezvládají splácet, může to skončit například ekonomickou krizí let 2007-2010. Pro spravedlnost vůči českým bankám a uklidnění čtenáře – v době psaní knihy uvádí ČNB solidní průměr nad 50 %. Vysoká kapitálová přiměřenost umožňuje bankám vyplácet vklady i v případě, že utrpí ztráty v důsledku špatných investic – když jejich klienti přestanou být schopni splácet půjčky. Pro hodnotu peněz to znamená, že každá koruna, která je v oběhu, je zčásti „krytá" dluhem věřitelů.

Ale to je stále jen část příběhu hodnoty. Aby mohli věřitelé splácet, musí mít možnost peníze vydělat. Potřebují právní jistotu, vzdělání, infrastrukturu, rozumné zdanění (ať už je to cokoli) a další služby v současnosti zajišťované převážně státním aparátem a politickým vedením státu. Prosperita z toho vyplývající se projevuje v hodnotě měny státu. Bohužel to pro její stabilitu nestačí. Žijeme v globalizovaném světě. Pokud bychom v Česku měli ideálně fungující národní banku, perfektně vyladěné státní instituce pod maximálně kompetentním politickým vedením, stále budeme součástí světa, kde si některé vlády bezhlavě půjčují (Řecko od osmdesátých let), banky jsou ochotny půjčit na paláce nezaměstnaným (hypoteční krize v USA 2007–2009) nebo politické elity ignorující vlastní zákony, bídu a životy svých obyvatel jménem ideologického blouznění (dnešní Venezuela).

Tím se dostáváme zpět k hodnotě bitcoinu a kryptoměn. Jsou odpovědí na svět, kde je část obyvatel mobilní, jejich identita je rozprostřena napříč různými místy, přičemž žijí v digitálním světě okamžitého přenosu informací, kde se potřebují pohybovat (a platit) bezpečně.

Hlavní otázka pro 21. století a svět peněz a internetu může znít následovně: Můžeme dál žít v globální, digitalizované ekonomice a používat kusy kovu a papíru omezené čarami na mapách, které ztrácejí hodnotu inflací, složitě se přesouvají a stále na ně dohlíží nějaký úřad nebo banka? A čím je můžeme nahradit?

Dlouho předtím, než na otázku odpověděl Satoshi Nakamoto bitcoinem, vzniklo několik jiných projektů, které ukázaly, kde jsou slepé uličky nestátních digitálních peněz.

Jeden z pokusů představil Američan David Chaun v roce 1989 v podobě systému a firmy DigiCash, která provozovala měnu eCash. Chaun se věnoval šifrování s použitím veřejných a soukromých klíčů, které jsou dodneška jednou ze základních technologií kryptoměn. Aplikace těchto poznatků v systému DigiCash umožnila uživatelům zašifrované bankovní převody, které nemohla sledovat třetí strana, včetně bank nebo vlády. Systém používalo několik bank, ale nerozšířil se a společnost zkrachovala. Jedním z důvodů byl Chaunův důraz na bezpečnost hraničící s paranoií a série nešťastných manažerských rozhodnutí, které vyústily do vzpoury jeho pracovníků. Každopádně jeden ze základních principů kryptoměn – asymetrické šifrování[3] - byl v praxi použit a pro další vývoj bylo podstatné, že ve společnosti pracovali lidé, kteří principy kryptoměn posunuli dál (např. jistý Nick Szabo; to ale předbíháme). V roce 1998 přichází Adam Back se systémem Hashcash. Pro upřesnění: Jeho princip již dříve

[3]Asymetrické šifrování používá k utajení posílaného obsahu dva tzv. klíče: veřejný a soukromý. Jsou to řetězy písmen, čísel a znaků, které pomocí šifrovacího algoritmu zašifrují obsah. Veřejný klíč je odvozen od soukromého, ale není možné (přesněji statisticky extrémně málo pravděpodobné) zpětně odvodit soukromý klíč ze znalosti veřejného. Veřejný klíč lze volně distribuovat. Bez znalosti soukromého klíče neumožňuje dešifrování zprávy. Zjednodušeně si subjekty používající asymetrické šifrování vymění veřejné klíče. Při komunikací své zprávy zašifrují veřejným klíčem druhé strany, která ho rozšifruje svým soukromým klíčem.

vypracovali Cynthia Dwork a Moni Naor v roce 1992. Moni Naor spolupracoval s Davidem Chaunem na konceptech eCashu a když půjdeme v příběhu dál, zjistíme, že rybníček krypto--odborníků je docela malý, přesto ale dokázal utajit jednoho klíčového.

Ale zpět k Hashcash-u. Tento systém bojoval proti emailovému spamu pomocí tzv. proof of work, nebo ověřením vykonané práce. Při zaslání emailu musel odesílatel, respektive jeho počítač, věnovat čas a výkon na nalezení systémem určeného čísla. Systém byl navrž žen tak, aby na nalezení toho správného čísla potřeboval počítač přibližně sekundu. Tím potvrdil, že odesílatel posílá jeden nebo jen několik málo emailů a nespamuje reklamami o řešení erektivních dysfunkcí. Pokud by to přece jen zkusil, systém by náročnost hledání čísla s přibývajícím počtem spamů exponenciálně zvyšoval, až by počítač zahltil a spammerovi by se jeho „obchodní model" přestal vyplácet.

Princip proof of work je dnes použit pri miningu, nebo jak se říká těžbě bitcoinu a některých dalších kryptoměn. Těžicí zařízení při něm soutěží o to, kdo nalezne číslo dané sítí a získá nové bitcoiny. Podrobněji si to vysvětlíme v příslušné části knihy.

Dalším a velmi důležitým posunem ve směru dnešních kryptoměn byl koncept B-money, který zveřejnil programátor Wei Dai (v roce 1998). Návrh formuloval systém pro anonymní transakce bez zapojení třetí strany a vyžadoval vklad počítačového výkonu (tj. Proof of work). Výsledky by ověřovala celá komunita zapojena v síti a zápis transakcí by se uchovával ve veřejném záznamu. Účastníci sítě by pro její potřeby dedikovali výkon a za tuhle práci by byli odměňováni. Transakce uchovávané ve veřejném účetním záznamu by byly verifikovatelné kryptografickým hashem4. Dohody/transakce měly být platné po odeslání do sítě s digitálním podpisem (nám již známé asymetrické šifrování). No a k Nickovi Szabovi. V roce 1998 navrhl „Bit gold" mechanismus pro decentralizovanou měnu, kde by účastníci řešili kryptografické úkoly a řešení by zveřejňovali na otevřeném záznamu. Důležitým prvkem bylo rozdělení procesu na dílčí úkoly označené časovým údajem. Tyto dílčí úkoly dnes najdeme v podobě bloků v blockchainu - databáze transakcí bitcoinu.

[4] Hashovací funkce má několik vlastností:

- Jednosměrnost. Z výstupu je (extrémně) náročné zjistit předlohu.
- Odolnost vůči získání jiné předlohy. Je náročné vypočítat jakoukoliv jinou předlohu y, která by dala stejný výstup jako jiná předloha (nazveme ji x).
- Odolnost vůči nalezení kolize. Je obtížné systematicky najít dvojici vstupů/předloh (x, y), pro které h (x) = h (y).

No a když používám slovo extrémně náročné, tak to znamená mnoho milionů let práce všech počítačů, které v současnosti máme na planetě. Bitcoin používá hashovací funkci k tvorbě a zajištění záznamu o transakcích. Tím, že jsou „zahashované", a tak je (extrémně) náročné je změnit.

Hashování si můžete zkusit: www.xorbin.com/tools/sha256-hash-calculator:

Příklad hashování na větě (vstupu): Vím, kdo je Satoshi Nakamoto.

Tuto větu podrobíme hashovací funkci (SHA256), tj. její znaky přepočítá algoritmus a zobrazí následující výstup: 174b383a038eb637e337b355f53d673c185d6aa17656e7afb07916a23410e49c

Při textu: **Ne**vím, kdo je Satoshi Nakamoto (přidali jsme 2 písmena) dostaneme:

aa244315f61eef8c17ff5d97e6a4a42a4ff2f9f9a196519f9ed8ad1582585b07

Malá změna docílí úplně jiný výstup, v tomto případě vždy dlouhý 64 znaků. Kdybychom zadali jedno písmeno nebo celou knihu – vždy dostaneme výstup o stejné délce.

Ve stručnosti můžeme rok 1998 uzavřít s tím, že matematici a programátoři, kteří se označovali jako „cypherpunks" (nezaměňovat s Cyberpunks)[5] neboli kryptopankáči, sdružení kolem komunikačního portálu Cypherpunks Mailinglist, popsali principy bitcoinového protokolu.[6] Jeho základem byla síť, ve které si navzájem neznámí účastníci mohou důvěryhodně posílat transakce, které podepíšou klíči asymetrického šifrování a zabezpečí zahashováním. Zápis (účetní kniha) bude veřejný, účastníci v síti ho budou průběžně (po označených částech) ověřovat, při tom budou pomocí počítačů řešit kryptografické úkoly a budou odměňováni za výpočetní výkon, který síti věnují pro její fungování. Teorii bychom měli. Jak jsme ale viděli u projektu DigiCash Davida Chauny, ani dobrý plán nemusí přežít setkání s realitou.

V následující části si ukážeme příklady projektů, které z velké části doplatily na to, že byly centralizované (jejich vedení tvořilo několik veřejně známých osob), nebyly připraveny na hrozby rodícího se digitálního světa, a hlavně narazily na zákon a státní instituce chránící dolar.

Předtím si ještě připomeneme několik fenoménů internetového boomu na přelomu milénia. Kolem společností, které podnikaly, chtěly podnikat, případně jen předstíraly podnikání na internetu, se vytvořila vlna přehnaných očekávání. Společnosti si zakládaly webové stránky a měnily názvy s příponou .com (v ang. vyslovované jako dot-com), aby profitovaly z nákupní horečky a prodaly své akcie za přemrštěné částky, které nereflektovaly jejich hodnotu. Dot-com bublina nakonec splaskla. Nezkušení investoři, často lidé bez základních znalostí akciového trhu zlákáni vidinou rychlých peněz, přišli o peníze. Zkušení spekulanti a šťastlivci naopak vydělali a množství společností zaniklo. Zároveň tento boom přinesl na trh s inter-

Když se řekne dot.com bublina. Zdroj: www.tradingview.com

[5] Cypherpunk-áči se věnovali programování, bezpečnosti a hlavně zabezpečení komunikace na internetu. Cyberpunk je subkultura a subžánr science fiction, kde vyspělá technologie, umělá inteligence, často undergroundoví hackeři naráží na distopickou realitu rozpadlé společnosti pod kontrolou velkých korporací.
[6] Komunikační protokol či protokol je soubor pravidel, které používají programy anebo operační systémy na komunikaci mezi koncovými body komunikačního systému (v telekomunikacích či výpočetní technice).

netovými technologiemi kapitál. Vznikly společnosti jako Amazon, Google či Ebay. Začalo pomalé budování rychlejší infrastruktury, hledání obchodních modelů, bezpečnostních standardů, zákazníků...

V této době, v roce 1998, vzniká služba PayPal. V roce 2000 ji koupil Elon Musk a vznikl první platební systém, který propojil kreditní karty, emailové účty a přes internet obchodníky se zákazníky v pohodlí domova a internetového prohlížeče. Jeho úspěch ukázal na obrovský trh s elektronickými platbami, v němž chtěli vydělat i poskytovatelé anonymních transakcí s pomocí alternativních peněz.

E-gold

Ještě před PayPal, v roce 1996, vznikla společnost E-gold. Nabízela online platby a mobilní platby pro jednotlivce a obchody pomocí vlastní měny, která byla krytá fyzickým zlatem uloženým u společnosti. Systémy společnosti měly tu smůlu, že se staly obětí prvních phishingových útoků a zneužití nedostatků tehdejších operačních systémů a prohlížečů na získávání údajů od jejich uživatelů. Tyto útoky společnost ještě ustála. Její konec nastal s teroristickými útoky z 11. září a následným zpřísněním legislativy proti praní peněz a financování terorismu - tzv. Patriot act. Společnost se dostala do sporu s vládou a přes spolupráci a snahu vyhovět novým legislativním požadavkům ji opatření soudů, negativní publicita a následná ztráta důvěry klientů přinutily ukončit činnost. Přesto do roku 2009 dokázala firma přilákat a obsloužit 5 milionů účtů.

Bernard von NotHaus a Liberty Dollar

Mimo to, že založil Svobodnou marihuanovou církev v Honolulu, byl i tvůrcem měny „Liberty Dollar". V praxi se jednalo o stvrzenky za uskladnění zlata a stříbra, které měly podobu papírových a kovových mincí, případně byly elektronické. Ideologický záměr vyjadřuje název organizace, která měnu provozovala: Národní organizace pro zrušení Federálního rezervního systému a Zákonu o vnitřních příjmech. Americké úřady se chvíli neuměly vyjádřit, nakolik je to legální, ale nakonec von NotHouse obvinili a odsoudili za výrobu a distribuci mincí „podobných mincím Spojených států amerických".

Goldfinger Coin & Bullion group

Digitální měnu e-Bullion vázanou na zlato začala v roce 2000 poskytovat také firma Goldfinger Coin & Bullion group. Služby zahrnovaly nákup digitální měny kryté zlatem pomocí standardních bankovních účtů, debetní kartu umožňující platbu a výběr v amerických dolarech a tzv. CRYPTOkartu, která umožňovala účinné dvoufázové zabezpečení účtu. Jenomže v létě roku 2008 se zakladatel Jim Fayed ocitl ve vězení za nelicencované převody peněz a později byl odsouzen za přípravu vraždy své bývalé manželky. Dnes čeká na trest smrti. Jeho společnosti ukončily činnost a jejich zdroje byly zabaveny vládou USA bez náhrady klientům.

Arthur Budovsky

Problémy s licencí, dokonce dvakrát, měl i Arthur Budovsky. Mezi lety 2002 až 2006 provozoval službu Golden Age. Po prvním soudu za poskytování ilegálních finančních služeb vyvázl

s podmínkou. Za dalším podnikáním se přesunul do Kostariky a spustil Liberty Reserve. Služba umožňovala nákup digitální měny kryté zlatem, dolarem či eurem bez nutnosti ověření totožnosti majitele účtu. Budovsky byl zatčen v roce 2013 a obviněn z praní peněz. V roce 2016 byl odsouzen na 20 let ve vězení.

Uvedené příběhy mají mnoho společného. Ukázaly potenciál nestátních/digitálních peněz. Pro úplnost ale dodejme, že jak na straně legitimního podnikání, tak i pro účely praní, nebo odklonění peněz. Každá ze společností bruslila na tenkém právním ledě, a i v případě upřímné snahy o legální podnikání se časem dostaly do „spárů" justice. To bylo usnadněno tím, že všechny byly provozované skrze centralizované v registrech zapsané společnosti identifikovatelnými osobami, na které mohla být vznesena obvinění a měly odstavitelné účty. Uvedené projekty kryly své měny pomocí cenných kovů, to jim sice dávalo velkou míru důvěry – víra v krytí zlatem je zakořeněná celosvětově - ale zároveň to vyžadovalo těžkopádné skladování a umožňovalo odstavení firmy od podkladových aktiv (úřady mohly zlato snadno zabavit). Digitální měna potřebovala jiné základy.

Než se objevil Satoshi Nakamoto, udály se dvě důležité věci. Té první jste si možná nevšimli, protože se udála někde v Africe. Zato ta druhá chvíli vypadala jako konec světa.

Začneme tou v Africe. Oproti tzv. globálnímu severu, do kterého patří i Česká republika, čelí obyvatelé zemí třetího světa (neboli globálního jihu) ve vztahu k finančním službám mnoha problémům. Jejich státy mají nestabilní měny, špatnou dopravní a komunikační infrastrukturu při velkých vzdálenostech mezi relativně malými sídly. Pro banky je náročné vybudovat tam své pobočky a poskytovat finanční služby. Pobočka ve vísce s pár desítkami obyvatel je nerentabilní. Kromě dopravní nedostupnosti komplikuje situaci také nízká finanční gramotnost (a vůbec gramotnost), nedostatky v právní ochraně věřitelů (a vymáhání dluhů), neschopnost státní správy evidovat a legitimovat obyvatele, případně nemožnost doložit svou adresu (základní podmínky pro zřízení osobního účtu). V roce 2014 bylo v zemích OECD na 1 000 obyvatel 1 450 bankovních účtů, v některých částech Afriky toto číslo klesalo pod 300.[7] U bankomatů byl poměr jen 5,8 zařízení (subsaharská Afrika) vůči 75 (na 100 000 obyvatel)[8] v OECD: Dostupnost bankomatů dále omezují vzdálenosti, nedostatek dopravních prostředků, výpadky bankomatů z důvodů výpadků elektřiny, servisu a doplňování penězi. Tento stav má na prosperitu afrických zemí zásadní vliv. Obyvatelé mají ztížený přístup k hotovosti a musí ji kompenzovat výměnným obchodem. Úvěry jsou, za předpokladu, že se k nim obyvatelé vůbec dostanou, drahé, což omezuje možnosti investovat do rozvoje, a ještě snižuje konkurenceschopnost kontinentu.

Naštěstí dostupnost mobilních služeb překonává malé pokrytí bankami a bankomaty. V roce 2002 si britská organizace Gamos všimla, že obyvatelé Ugandy, Ghany a Botswany používají kredit (předplacených karet do mobilních telefonů) jako náhradu za peníze a bankovní převody. Místo posílání peněz si posílali kredit do telefonů a ten prodávali dál. Pokročilejší verzi představila firma mCel v Mosambiku (2004) a v roce 2007 vznikla M-Pesa (M - mobilní, pesa - svahilsky peníze) v Keni. Služba se do roku 2018 rozšířila do 10 zemí k 29 milionům zákazníků, pro které zajišťuje vklady, převody a výběr peněz, platby účtů, nákup kreditu, převody mezi bankovním účtem a omezeně úvěry a pojištění. Kromě pozitiv pro rozvoj chudých zemí má tato forma digitálních peněz a bankovnictví další implikace. Jednou z nich je po-

[7] Data – African Development Bank, The Banking System in Africa: www.afdb.org/fileadmin/uploads/afdb/Documents/Knowledge/AEB_Vol_6_Issue_5_2015_The_Banking_System_in_Africa__Main_Facts_and_Challenges-10_2015.pdf

[8] Zdroj viz: data.worldbank.org/indicator/FB.ATM.TOTL.P5?view=map

znatek, že nepotřebujeme banky k tomu, aby existovaly bankovní služby. Respektive na to, abychom mohli přesouvat nějakou formu hodnoty rychle a bezpečně, stačí primárně vhodný komunikační protokol a spojení. Banka přestává být institucí a stává se službou.

V době, kdy se v Africe rozvíjela malá revoluce, začaly si americké banky uvědomovat, že půjčily příliš mnoho peněz příliš mnoha lidem, kteří příliš často nemají na to, aby své půjčky splatili. Tyto rizikové půjčky byly navíc sofistikovaně transformovány a prodány dalším bankám a investorům, často s nesprávným ratingem, podle kterého se jednalo o bezpečné produkty, u nichž nehrozí ztráta hodnoty. Nakoupili je banky a jejich klienti po celém světě, čímž se problém rozšířil do podoby světové ekonomické krize.

Ve stručnosti

2007 - Začíná krize na trhu s nemovitostmi, věřitelé v USA nedokáží splácet bankám rizikové hypotéky, krize zasahuje velké banky v USA a EU, kterým chybí peníze.

2008 - Krize naplno zasahuje světovou ekonomiku. Krachuje banka Lehman Brothers, americká vláda plánuje záchranné balíčky pro stabilizaci soukromých bank. K záchraně bank přistupuje i Velká Británie. V eurozóně dochází k ekonomické recesi.

2009 - Vlády USA a EU pokračují v podpoře svých ekonomik pomocí garancí a poskytnutí financí (záchranných balíčků). Klesají mzdy, investice, HDP..., roste nezaměstnanost.

2010 - Ekonomika USA se začíná pomalu zotavovat, EU řeší problémy Řecka, Irska, Španělska...

Kde přesně byla příčina krize? Nezodpovědné banky? Státy, které nedostatečně nastavily pravidla? Občané a podniky si nezodpovědně půjčovali? Z důsledků nám zbylo několik ponaučení, které mají význam pro hodnotu kryptoměn.

- Banky jsou „too big to fail" (příliš velké, aby zkrachovaly), a vláda je proto zachrání z daní občanů. Zároveň jsou příliš silné – finančně a lobbisticky, takže dokážou ovlivnit zákony a možnosti státní kontroly svého podnikání. Zisky tučných let jsou privatizovány (inkasují je akcionáři a vrcholový management). Ztráty socializovány (záchrana bank, rekapitalizace, dokonce i tzv. zlaté padáky často financuje stát z daní).
- Stát není schopen průběžně reagovat. Jeho aparát nedokáže včas rozeznat krizi, protože jeho mechanismy jsou pomalé a pod vlivem zájmových skupin. Řešení na poslední chvíli pocítí všichni občané (nárůst zadlužení, pokles kvality státních služeb, nárůst daní).
- Občan nemá alternativu ke státním penězům, které spravují banky. V podstatě je až třetí v pořadí. Opatření státu rozhodují o ceně jeho peněz. Banky mají moc nad jeho účtem a nad informacemi o jeho ekonomické aktivitě a navíc mu (občanovi) oba subjekty mohou omezit přístup k penězům. Alternativy (např. výměnný obchod, pěstování vlastního jídla, výroba energie z vlastních zdrojů, použití drahých kovů) jsou ekonomicky neefektivní, hlavně při koncentraci obyvatel do měst.

Stručná historie bitcoinu

2008-2009

Dějiny bitcoinu „oficiálně" začaly v roce 2008. 18. srpna byla registrována doména bitcoin.org. Stále funguje a je rozcestníkem k informačním zdrojům o bitcoinu. 31. října uveřejnil Satoshi Nakamoto článek (nebo také White paper): Bitcoin: A Peer-to-Peer Electronic Cash System9, v němž popsal, proč je podobný systém důležitý (aby dvě strany mohly spolu obchodovat bez nutnosti, aby někdo třetí transakci garantoval a vstupoval do ní), a jak bude fungovat (podrobně si popíšeme později). V lednu 2009 Nakamoto zveřejnil bitcoinového klienta, tj. program, který umožňuje zapojení do bitcoinové sítě, těžbu bitcoinu a transakce. Ve stejnou dobu Nakamoto těží prvních 50 bitcoinů, které vznikly spolu s tzv. „blokem genesis" neboli prvním blokem blockchainu – účetní knihy, která bude od tohoto momentu evidovat všechny transakce bitcoinu. V prvním bloku byla zpráva: The Times 03 / Jan / 2009 Chancellor on Brink of Second Bailout for Banks. Odkazovala k článku britského deníku The Times daného data, ve kterém se píše o dalším balíku finanční pomoci bankám zasaženým finanční krizí. Kromě důkazu o datu vzniku Bitcoinu poukazuje tato zpráva na finanční marasmus, pro který by mohl být bitcoin alternativou. Po zveřejnění kódu se přidávali nadšenci, kteří začali novou měnu a technologii testovat, posílali si transakce a navrhovali úpravy. V roce 2010 Satoshi Nakamoto prodal své přístupy k doménám bitcoinu a úložištím kódu Gavinu Andersenovi – jednomu z klíčových členů komunity a přestal zasahovat do vývoje.

2010

Kromě prvních verzí bitcoinového protokolu po Nakamotovi zůstaly statisíce bitcoinů, které stihl vytěžit v jeho nejrannějších dobách, kdy se těžbě věnoval jen on. Po svém stažení do ústraní je nepřesunul a tyto bitcoiny pravděpodobně již nikdy nezmění majitele.

Jedním z důvodů je, že by to okamžitě vyvolalo novou vlnu pátrání po skutečné identitě Satoshiho Nakamota. Tomu už se věnovala velká média, zástupy nadšenců a podle některých tvrzení i americké tajné služby. Prý ze strachu, že by bitcoin mohl být zbraní Číny nebo Ruska. Postupně byla rozebrána veškerá komunikace a texty, které Nakamoto napsal, a stejně tak informace, které o své identitě zanechal (například že je Japonec narozený 5. dubna 1975). Analyzoval se jeho jazyk a slovosled z doby, kdy své příspěvky (maily, diskuze na fórech) publikoval. Zkoumaly se vědomosti, které byly potřebné k vytvoření Bitcoinu. Kromě konspirační roviny, komplexních analytických technik, příběhů pátrání i osudů jednotlivých podezřelých, je příběh hledání identity tvůrce Bitcoinu i konstatováním, že je stále možné se digitálně ztratit.

Co dnes můžeme říci, je, že to nemusí být jednotlivec, ale skupina. Určitě s pokročilými znalostmi z programování, kryptografie, počítačových sítí. V podezření se tím pádem ocitli jako jednotlivci i jako skupina členové komunity kryptopankáčů, které jsme zmínili v úvodní kapitole (například Wei Dai, Nick Szabo) a další ze skupiny Hal Finney, který rozvíjel koncept proof of work. Stejně tak byli v podezření první členové bitcoinové komunity jako třeba Gavin Andersen. Postupně se objevovala další jména, včetně například irského studenta Michaela

[9] Překlad například tu: jakfungujebitcoin.blogspot.com/2015/06/slovo-vynalezce-bitcoinu_14.html, v ang.: bitcoin.org/bitcoin.pdf

Cleara, japonského matematika Shinichi Mochizukiho, či samotné americké vlády. Chvíli byl nejvážnějším kandidátem jistý Dorian Nakamoto, ale tak jako všichni před ním, i on popřel, že by byl tvůrcem Bitcoinu a na jeho ne-podporu se z digitálního záhrobí naposledy ozval i Satoshi Nakamoto tweetem - „Nejsem Dorian Nakamoto".

Jedním z podezřelých byl i jistý Craig Wright – programátor, podnikatel a raný člen bitcoinové komunity. Wright se jako jediný vážný kandidát k aliasu veřejně hlásí a pokusil se to dokázat pomocí kryptografických klíčů, které patřily k prvním vytěženým blokům bitcoinu. Jeho důkazy se po podrobném rozboru ukázaly jako neprůkazné a Wright za přivlastnění Nakamotovy identity sklidil příval kritiky. Zajímavou spekulací je, že Wright opravdu je Satoshi Nakamoto a jako další projev své geniality se to pokusil nešikovně dokázat právě proto, aby ho to nadobro vyloučilo z budoucího pátrání po pravém Satoshim.

Pro kohokoliv za jménem Satoshi Nakomoto je rozumné zůstat v utajení. Dnes by mohl být multimilionářskou celebritou, nebo klidně sedět v některém z amerických vězení a bitcoin by se vyvíjel úplně jinak. Připomeňme si osudy podnikatelů VonNothause, Fayeda a Budovskeho a jak čelili americkým zákonům a justici. Nakamotovým odstoupením z projektu se bitcoin mohl vyvíjet svobodně a jako decentralizovaný systém, v němž nezáleží na tom, co si myslí Nakamoto, ale na čem se shodne komunita. Že to bylo dobré rozhodnutí, potvrdí i příklady podnikatele Charlieho Shrema nebo zakladatele ilegálního online tržiště Rossa Ulbrichta – oba byli (mimo jiné) obviněni z praní peněz na základě toho, že někdo nakoupil drogy pomocí bitcoinů, které získal od nich. Bylo by nejspíš otázkou času, než by se nějaký aktivní prokurátor pokusil Nakamotovi „přišít" všechny ilegální nákupy, nebo alespoň provozování nelicencovaných finančních služeb.

Vraťme se do roku 2010. Kromě zmizení Satoshi Nakamota byly důležité tyto čtyři události:

Laszlo Hanyecz v květnu koupil dvě pizzy v hodnotě 41 USD, za které zaplatil 10 000 bitcoinů. Ty nezaplatil pizzerii, ale členovi bitcoinové komunity, který po několika dnech zareagoval na jeho výzvu zveřejněnů na fóru, a pizzu Laszlovi objednal do Kalifornie. Zprávy se chytila média a z události se stala formativní legenda bitcoinu a nejznámější z prvních nákupů za bitcoin. Dnes si událost připomínáme jako tzv. Bitcoin pizza day a pomocí bitcoin pizza indexu novináři přepočítávají, kolik milionů to Laszlo při aktuální ceně bitcoinu zaplatil. Laszlo a mnozí další, co použili své bitcoiny, když měli minimální hodnotu, to samozřejmě nemohli tušit. Každopádně bez jejich pokusů by bitcoin nikdy nemusel prorazit jako matka kryptoměn.

V červenci 2010 jistý Jed McCaleb oživil svůj starý projekt, původně burzu na obchodování s kartami elektronické hry Magic: The Gathering Online (zkráceně: Mt.Gox) a přepracoval ho na online burzu bitcoinu a brzy prodal v Japonsku žijícímu Francouzovi Markovi Karpelesovi. Burza měla brzy vládnout obchodu s bitcoiny.

Třetí událost: V srpnu 2010 se v kódu Bitcoinu našla chyba, která umožnila vytvořit bitcoin mimo pravidla jejich těžby. Někdo se o to opravdu pokusil a vytvořil rovnou 184 miliard bitcoinů. Naštěstí si uživatelé chyby i transakcí všimli a během hodin byla chyba opravena a pomocí nové verze klienta a tzv. forku, čili rozdělení Blockchainu, se síť vrátila do stavu, ve kterém byla dodržena všechna pravidla emise.

Čtvrtou událostí roku byl vznik prvního bitcoinového těžebního poolu. Čech Marek Palatinus založil Slush Pool – první svého druhu. Do té doby těžil každý za sebe. Umožňovalo to jednorázové velké odměny. S růstem počtu těžařů se prodlužovala i doba, kdy se jednotlivci povedlo vytěžení nového bloku. Bitcoinový pool umožnil sdružit výpočetní výkon. Těžaři spo-