21 lekcí

Co mě naučil pád do bitcoinové králičí nory

BRAINS Publishing

21 lekcí

Co mě naučil pád do bitcoinové králičí nory

Gigi

Věnováno mé ženě, mému dítěti a všem dětem na tomto světě. Nechť vám bitcoin dobře slouží a přináší vizi budoucnosti, za kterou stojí za to bojovat.

BRAIINS

Česká firma působící na globální úrovni, která svými produkty posouvá bitcoin dopředu. Od operačního systému Braiins OS+ pro ASIC minery, nástroje Farm Proxy k agregaci jejich těžebního výkonu přes Braiins Pool – první těžební pool na světě – až po protokol Stratum V2, který zásadním způsobem vylepšuje infrastrukturu těžby bitcoinu.

PROJEKTY BRAIINS

BRAIINS OS+

FARM Proxy

STRATUM V2

BRAIINS POOL

Formerly **Slush Pool**

21 Lessons

What I've Learned From Falling Down the Bitcoin Rabbit Hole

První vydání verze 0.3.11 git commit 6a933bb

[α] https://creativecommons.org/licenses/by-sa/4.0/

„Řekla bys mi prosím, kudy se dostanu odtud?“
„Záleží na tom, kam se chceš dostat.“
„To je mi jedno kam…“
„Pak je jedno, kudy půjdeš.“

– Lewis Carroll, *Alenka v kraji divů*

Obsah

O této knize
(... a jejím autorovi)

Tato kniha je krapet neobvyklá. Ale co, bitcoin je krapet neobvyklá technologie, takže neobvyklá kniha o bitcoinu by mohla být na místě. Nejsem si jistý, jestli jsem i já neobvyklým člověkem (rád se považuji za obyčejného chlápka), ale příběh o tom, jak tato kniha vznikla a jak jsem se stal jejím autorem, stojí za to odvyprávět.

Zaprvé, nejsem spisovatel. Jsem inženýr. Nestudoval jsem psaní. Studoval jsem kód a programování. Zadruhé, nikdy jsem neměl v úmyslu napsat knihu, natož knihu o bitcoinu. Sakra, nejsem ani rodilý mluvčí.[1] Jsem jen člověk, který se zapálil pro bitcoin. A to hodně.

Kdo jsem, abych psal knihu o bitcoinu? To je dobrá otázka. Krátká odpověď je snadná: jsem Gigi a jsem bitcoiner.

Dlouhá odpověď je trochu složitější.

Mým oborem je informatika a vývoj softwaru. V předchozím životě jsem byl členem výzkumné skupiny, která se mimo jiné snažila přimět počítače myslet a uvažovat. V dalším životě jsem psal software pro automatické zpracování pasů a další věci s tím spojené, což je ještě děsivější. O počítačích a našem zasíťovaném světě něco vím, takže mám asi menší náskok, abych dokázal pochopit technickou stránku bitcoinu. Nicméně, jak se snažím nastínit v této knize, technická stránka věci je jen malou částí té bestie, kterou bitcoin je. A každý z těchto střípků je důležitý.

[1] Důvod, proč píšu tato slova v angličtině, je ten, že můj mozek pracuje záhadným způsobem. Kdykoli se objeví něco technického, přepne se do anglického režimu.

Tato kniha vznikla na základě jedné jednoduché otázky: „Co vás bitcoin naučil?“ Na tuto otázku jsem se pokusil odpovědět v jediném tweetu.

Pak se z tweetu stala tweetová bouře. Tweetstorm se změnil v článek. Z článku se staly tři články. Tři články se proměnily v 21 lekcí.

A z 21 lekcí vznikla tato kniha. Tak se mi zdá, že kondenzovat své myšlenky do jednoho tweetu není zrovna moje nejsilnější stránka.

Možná se ptáte: „Proč vůbec psát tuto knihu?“. Opět existuje kratší a delší odpověď. Krátká odpověď zní, že jsem prostě musel. Byl jsem (a stále jsem) bitcoinem posedlý. Považuji ho za nekonečně fascinující. Nemohu o něm, ani o dopadech, které bude mít na naši globální společnost, přestat přemýšlet. Dlouhá odpověď je taková, že věřím, že bitcoin je nejdůležitějším vynálezem naší doby a že je třeba, aby více lidí pochopilo jeho podstatu. Bitcoin je stále jedním z nejvíce nepochopených fenoménů našeho moderního světa a trvalo mi léta, než jsem si plně uvědomil závažnost této mimozemské technologie. Zjišťování, co bitcoin je a jak změní naši společnost, je hluboký zážitek. Doufám, že se mi podaří zasít do vaší hlavy semínka, z nichž by toto uvědomění mohlo vyklíčit.

Ačkoliv se tato část nazývá „O této knize (… a jejím autorovi)“, celkově vzato na této knize, na tom, kdo jsem a co jsem udělal, vlastně vůbec nezáleží. Jsem jen uzel v síti – a to doslova i obrazně. Navíc byste stejně neměli věřit tomu, co tvrdím. Jak my bitcoineři rádi říkáme: udělejte si vlastní výzkum a hlavně: nevěřte, ale ověřujte.

Snažil jsem se poctivě odvést svou práci a poskytnout vám, laskaví čtenáři, spoustu zdrojů, do nichž se můžete ponořit. Kromě poznámek pod čarou a citací v této knize se snažím udržovat aktualizovaný seznam zdrojů na: 21lessons.com/rabbithole a na bitcoin-resources com, kde je také uveden seznam spousty dalších pečlivě vybraných zdrojů, knih a podcastů, které vám pomohou pochopit, co je to bitcoin.

Stručně řečeno – je to prostě kniha o bitcoinu, napsaná bitcoinerem. Bitcoin tuto knihu nepotřebuje a vy ji pravděpodobně nebudete potřebovat k tomu, abyste bitcoin pochopili. Věřím, že mu porozumíte,

jakmile budete připraveni, a také věřím, že první střípky bitcoinu si vás najdou, až budete připraveni je přijmout.

V podstatě každý pochopí i získá bitcoin přesně ve správný čas. Do té doby bitcoin prostě je, a to stačí.[2]

[2] Beautyon: *„Bitcoin je. A to stačí.“* [8]

Předmluva

Pád do bitcoinové králičí nory je zvláštní zážitek. Stejně jako mnozí jiní, mám i já pocit, že jsem se během posledních pár let studia bitcoinu naučil víc než za dvě desetiletí formálního vzdělávání.

Následující lekce jsou destilátem toho, co jsem se dozvěděl. Poprvé jsem je publikoval jako sérii článků s názvem „Co mě bitcoin naučil", a následující řádky lze považovat za třetí vydání původní série.

Stejně jako bitcoin, ani tyto lekce nejsou statickou záležitostí. Plánuji na nich pravidelně pracovat a v budoucnu vydávat aktualizované verze a další materiály.

Na rozdíl od bitcoinu však budoucí verze tohoto projektu nemusí být zpětně kompatibilní. Některé lekce mohou být rozšířeny, jiné přepracovány nebo nahrazeny.

Bitcoin je nevyčerpatelný učitel, a proto netvrdím, že tyto lekce jsou všezahrnující nebo úplné. Jsou odrazem mé osobní cesty králičí norou. Lekcí existuje mnohem více a každý člověk se po vstupu do světa bitcoinu naučí něco jiného.

Doufám, že pro vás budou tyto lekce užitečné a že proces poznávání prostřednictvím jejich čtení nebude tak namáhavý a bolestivý jako učení se z první ruky.

Gigi

twitter.com/dergigi

Předmluva k českému vydání

„Pokud mi nevěříte nebo to nechápete, nemám čas vás přesvědčovat, promiňte.“

– Satoshi Nakamoto

Bitcoin přitahuje zajímavou sortu lidí. Nejenom ty z technologického odvětví, jako jsou programátoři, a podnikatele, jako jsem já, ale lidi všech možných povolání. Mezi bitcoinery najdete manažery, elektrikáře, policisty nebo prodavače vánočních stromků, kteří díky bitcoinu objevili úplně nový svět. Svět, který mají všichni přímo před očima, ale přitom je pro většinu lidí stále neviditelný. A pokud jej už objeví, zůstává pro ně velmi neuchopitelný. Tento bitcoinový svět tu však je a pouze čeká na váš okamžik. Až otevřete oči, začnete ho vnímat, snažit se ho pochopit a vydáte se na svou vlastní cestu bitcoinovou králičí norou. Jakmile se dostanete do této fáze, tak vaše důvody, díky nimž vás bitcoin[1] pohltil, bude velmi těžké vysvětlit někomu dalšímu. A stejně vám nebude věřit, protože si ty své jedinečné důvody musí najít sám.

Možná by se zdálo, že kvůli výše uvedenému nemá smysl věnovat vzdělávání zvláštní úsilí. Opak je ale pravdou, celý bitcoinový ekosystém se točí okolo hesla *Udělejte si vlastní výzkum* (Do Your Own Research). Nováčci nemusí nutně opakovat chyby, jež v minulosti nespočetněkrát vytrestaly jejich předchůdce. Přístup k hodnotnému, ověřenému a komunitou posvěcenému obsahu může zásadně usnadnit jejich

[1] Ačkoliv se v literatuře stále rozlišuje mezi Bitcoinem (série technologií tvořících bitcoinový ekosystém) a bitcoinem (peněžní jednotkou, vypořádávací vrstvou sítě), rozhodli jsme se v této a dalších knihách používat variantu s malým písmenem. Následujeme tím obecný jazykový trend, kdy se často skloňované technologie či produkty používáním zobecňují a začínají se psát s malým písmenem. Příkladem budiž slovo internet, jehož zápis nás už dnes ani nepřekvapí. Jednotný zápis bitcoinu s malým písmenem tak kromě větší srozumitelnosti pro čtenáře znamená i vykročení k širšímu přijetí bitcoinu. (pozn. red.)

bitcoinovou pouť, či přinejmenším její počátek. A že sám Satoshi ve výše uvedeném citátu odmítá trávit čas přesvědčováním? Vždyť ani nás Gigi v knize o ničem nepřesvědčuje, pouze nás zve do své soukromé králičí nory. Satoshiho rolí navíc nebylo nikoho přesvědčovat, přivedl na svět geniální vynález, bitcoinovou síť. Jako podnikatel zcela chápu, že jeho priority ležely úplně jinde. Proto zůstává úkol edukace na nás, Satoshiho následovnících. Gigiho kniha není určena pouze nově příchozím do bitcoinového světa. Své si odnese každý, kdo má otevřenou mysl. Ten, kdo už do světa bitcoinu nahlédnul a dokázal proniknout vrstvami šumu k čistému signálu, hlavu otevřenou rozhodně má. Ale málokdo bude mistrem všech tří hlavních aspektů, jež 21 lekcí projednává – filozofie, ekonomiky i technologie. Pevně věřím, že si zde na své přijdou jak dosud nepolíbení nováčci, tak ostřílení matadoři. Navíc v knize naleznete nepřeberné množství odkazů, jež vám vystačí na několik let dalšího studia.

Má vlastní bitcoinová cesta začala v roce 2014. Tehdy pro mě byl bitcoin prostředkem, jak umožnit lidem z jakéhokoliv koutu planety využívat služby mé logistické firmy. To, co v západním světě bereme za samozřejmost – mít bankovní účet a platební kartu – bylo, a stále je, pro většinu lidí na Zemi nedostupná věc. Z tohoto pohledu je bitcoin doslova zázračným řešením. Žádná třetí strana nebo prostředník nestojí v cestě. Tohle moje vlastní praktické využití jsem považoval za začátek obrovské revoluce.

V dalších letech jsem bitcoin bral jako zajímavou technologii, fascinovala mě ta komunita lidí kolem a jejich silné přesvědčení. K výraznému posunu v mém myšlení došlo během covidové krize a následného tisknutí peněz. Jak může fungovat současný systém, kdy politici vytvářejí a rozdávají peníze bez jakýchkoliv zábran a s přesvědčením, že snad i bez následků? Měl jsem za to, že důsledky zmíněné měnové politiky musí odhadnout každý, kdo přemýšlí selským rozumem. Teď, po pár letech, vidíme její následky na vlastní oči. Inflace je skrytá daň, a pokud jste jedním z těch zodpovědných lidí, kteří celý život spoří a nedělají zbytečné dluhy, nemůžete se jí bránit.

Ve světle těchto událostí pak myšlenka bitcoinu s jeho omezenou nabídkou 21 milionů jednotek působí i v západním světě jako stabilní alternativa současného finančního systému. Jako záchranný kruh nebo ultimátní pojištění. Rozmarní politici, nenažrané banky a celý fiat systém stojí na hliněných nohách. Alternativa existuje v nové cestě vedoucí k osobní svobodě a osobní zodpovědnosti, jež jdou vždy ruku v ruce. Stačí se do ní probudit, podobně jako v Matrixu.

To je ta cesta králičí norou, jak ji popisuje Gigi. A každý jeden z nás si ji zažije po svém. Já jsem se jen snažil ukázat, co mě samého dovedlo jak k tomuto přesvědčení, tak k dalším krokům, kdy teď už aktivně bitcoinovou síť podporuji vlastní činností v oblasti těžby. Pro mě už cesta zpět neexistuje.

Oproti lživému a manipulativnímu světu politiky bitcoin šíří optimismus a znamená šanci na lepší svět pravdy a jasných pravidel. Řekněte, není úžasné mít možnost být součástí této historické příležitosti a spoluvytvářet ji?

Podržte si ony pověstné kapesní hodinky a vydejte se na svou vlastní neopakovatelnou cestu bitcoinovou králičí norou. Říká se, že je prý bezedná, ale na to už budete muset přijít sami. Přeji vám šťastnou cestu plnou poznání a rozšiřování obzorů. Gigiho kniha vám bude dobrým průvodcem...

John Vanhara

5. srpna 2022, Los Angeles, USA

„Ty hloupá Alenko,“ odpovídala si. „Jak se chceš
tady učit? Stěží se sem sama vejdeš,
jakpak by se sem vešly učebnice!“

– Lewis Carroll*, Alenka v kraji divů*

Úvod

> *„Ale já nechci mezi potrhlíky,“ bránila se Alenka. „Málo platné,“ řekla kočka, „tady jsme všichni potrhlí. Já jsem potrhlá, ty jsi taky potrhlá.“„Jak to víš, že jsem potrhlá?“ zeptala se Alenka. „To je jisté, jinak bys sem nechodila.“*
>
> – Lewis Carroll, *Alenka v kraji divů*[1]

V říjnu 2018 položil Arjun Balaji nevinnou otázku: „Co vás bitcoin naučil?“ Poté, co jsem se pokusil na tuto otázku odpovědět (žalostně neúspěšně) v krátkém tweetu, uvědomil jsem si, že věcí, které jsem se naučil, je příliš mnoho na to, abych na ně mohl odpovědět rychle. Pokud vůbec.

[1] Všechny citace v úvodech lekcí pochází z překladu Aloyse a Hany Skoumalových *Alenka v kraji divů a za zrcadlem*, vydaného nakladatelstvím Slovart v roce 2005. (pozn. překl.)

To, co jsem se naučil, se samozřejmě týká bitcoinu – nebo to s ním alespoň souvisí. Nicméně, i když jsou zde některé z vnitřních mechanismů bitcoinu objasněny, následující lekce nejsou vysvětlením toho, co bitcoin je a jak funguje. Mohly by však pomoci prozkoumat některé záležitosti, jichž se bitcoin dotýká: filozofické otázky, ekonomické skutečnosti a technologické inovace.

Jednadvacet lekcí je rozděleno do bloků po sedmi, což dohromady dává tři kapitoly. Každá kapitola se na bitcoin dívá jinou optikou a extrahuje z něj poučení, která lze získat při zkoumání této podivuhodné sítě z různých úhlů pohledu.

Kapitola I zkoumá filozofické základy bitcoinu. Souhru mezi neměnností a změnou, koncept absolutní vzácnosti, neposkvrněné početí bitcoinu, problém identity, rozpor mezi replikací a lokací, sílu svobody slova a hranice poznání.

Kapitola II se zabývá ekonomickým poznáním bitcoinu. Dává nám lekci o finanční negramotnosti, inflaci, hodnotě, penězích a jejich historii, bankovnictví částečných rezerv a o tom, jak bitcoin mazaně a oklikou znovu zavádí zdravé peníze.

Kapitola III se věnuje některým poznatkům získaným při zkoumání bitcoinové technologie. Po pojednání o síle čísel následují úvahy o důvěře, proč určování času vyžaduje práci, jak je pomalý vývoj a nenarušování systému předností, a nikoliv chybou, co nám může vznik bitcoinu říci o soukromí, proč cypherpunkeři píší kód (a ne zákony) a jaké metafory by mohly být užitečné pro zkoumání budoucnosti bitcoinu.

Každá lekce obsahuje v textu několik citátů a odkazů. Pokud nějaká myšlenka stojí za podrobnější prozkoumání, v poznámkách pod čarou nebo v bibliografii najdete odkazy k souvisejícím pracem.

Přestože jsou určité předchozí znalosti o bitcoinu výhodou, doufám, že tyto lekce zvládne strávit každý zvídavý čtenář. I když některé z lekcí spolu souvisejí, každá by měla být schopna obstát sama o sobě a lze

je číst samostatně. Technickému žargonu jsem se snažil maximálně vyhýbat, avšak bez některých termínů, specifických pro danou oblast, se zcela obejít nelze.

Doufám, že můj text poslouží ostatním jako inspirace, aby se ponořili pod povrch a prozkoumali některé z hlubších otázek, které bitcoin vyvolává. Mě samotného inspirovala mnohá díla jiných autorů a jim všem jsem neskonale vděčný.

V neposlední řadě: cílem mého psaní není vás o čemkoliv přesvědčovat. Mým cílem je přimět vás k zamyšlení a ukázat vám, že bitcoin skýtá mnohem víc, než se na první pohled zdá. Nemohu vám ani říct, co bitcoin je, nebo co vás naučí. To si budete muset zjistit sami pro sebe.

> „Z týhle cesty se nemůžeš vrátit. S modrou kapslí všechno skončí, probudíš se doma a budeš věřit, čemu budeš chtít. Ale s tou červenou[2] – zůstaneš v říši divů a já ti ukážu, jak hluboko králičí nora vede."
>
> – Morfeus

„Pamatuj si, já ti nabízím jen pravdu, nic víc."

[2] s *oranžovou* kapslí

Kapitola I.

Filozofie

Filozofie

> *Myš se na ni podívala zvědavě a jako by na ni jedním očkem mrkla, ale nic neříkala.*
>
> – Lewis Carroll*, Alenka v kraji divů*

Podíváme-li se na bitcoin jen zběžně, můžeme dojít k závěru, že je pomalý, nehospodárný, nepotřebný a příliš paranoidní. Při zvídavém pohledu však člověk může zjistit, že bitcoin není takový, jaký se na první pohled zdá.

Bitcoin umí vzít vaše předpoklady a postavit je na hlavu. Po nějaké době, zrovna když už jste si zase připadali silní v kramflecích, bitcoin znovu přiletí jako neřízená střela a vaše domněnky opět rozbije.

0.1 Slepí mniši zkoumající bitcoinového býka

Bitcoin je plodem mnoha oborů. Stejně jako když slepí mniši zkoumají slona, každý, kdo přistupuje k této nové technologii, tak činí z jiného úhlu. A každý dojde k odlišným závěrům o povaze tohoto zvířete.

Následující lekce se týkají některých mých předpokladů, které bitcoin zbořil, a závěrů, k nimž jsem dospěl. V prvních čtyřech lekcích se věnuji filozofickým otázkám neměnnosti, vzácnosti, lokality a identity.

Kapitola I – Filozofie

- **Lekce 1:** Neměnnost a změna
- **Lekce 2:** Vzácnost vzácnosti
- **Lekce 3:** Replikace a lokace
- **Lekce 4:** Problém identity
- **Lekce 5:** Neposkvrněné početí
- **Lekce 6:** Síla svobody slova
- **Lekce 7**: Hranice poznání

Pátá lekce zkoumá, jak je příběh vzniku bitcoinu nejen fascinující, ale pro tento systém bez centrální autority naprosto zásadní. Poslední dvě lekce této kapitoly zkoumají sílu svobody slova a hranice našeho individuálního poznání, odrážející se v překvapivé hloubce bitcoinové králičí nory.

Doufám, že svět bitcoinu pro vás bude stejně poučný, fascinující a zábavný, jako byl a stále je pro mě. Zvu vás, abyste následovali bílého králíka a prozkoumali hlubiny této králičí nory. Takže si podržte kapesní hodinky, skočte dolů a užijte si pád.

1. Neměnnost a změna

> *„Copak se se mnou v noci stala nějaká změna? Počkat: byla jsem to já, když jsem ráno vstávala? Tak se mi zdá, že mi bylo nějak divně. Ale jestli to nejsem já, ptám se dál, kdo tedy jsem? To je ta záhada!“*
>
> – Alenka

Bitcoin je už z podstaty těžké popsat. Je to nová věc, a ať už jej nazveme digitálním zlatem, nebo internetem peněz, jakýkoliv pokus o srovnání s předchozími koncepty se nutně mine účinkem. Nehledě na to, jaké analogii dáváte přednost, dva aspekty bitcoinu jsou naprosto zásadní: decentralizace a nezměnitelnost.

Jedním ze způsobů, jak o bitcoinu přemýšlet, je nahlížet na něj jako na automatizovanou společenskou smlouvu.[1] Software je jen jedním z dílků skládačky a doufat, že změníte bitcoin změnou softwaru, je marná snaha. Člověk by musel přesvědčit zbytek sítě, aby takové změny přijal, což je mnohem více psychologická záležitost než věc softwarového inženýrství.

> „Bitcoin nás změní víc než my jeho.“
>
> – Marty Bent[2]

[1] Hasu, *Unpacking Bitcoin's Social Contract* [32]
[2] Tales From the Crypt [10]

Trvalo mi dlouho, než jsem si uvědomil hloubku tohoto tvrzení. Jestliže bitcoin je jen software, který je celý open-source, můžete v něm jednoduše měnit věci podle libosti, ne? Omyl. Velmi špatně. Nepřekvapí nás, že tvůrce bitcoinu tohle věděl až příliš dobře.

> „Podstata bitcoinu spočívá v tom, že vydáním verze 0.1 byla již natrvalo určena jeho základní koncepce."
>
> – Satoshi Nakamoto[3]

Mnoho lidí se pokoušelo povahu bitcoinu změnit. Doposud nikdo z nich neuspěl. Zatímco existuje nepřeberná řada forků a altcoinů, bitcoinová síť stále funguje stejně jako v době, kdy byl spuštěn první uzel. Na altcoinech z dlouhodobého hlediska nezáleží. Forky nakonec vyhladoví k smrti. Důležitý je bitcoin. Dokud se nezmění naše základní chápání matematiky a/nebo fyziky, bude bitcoinovému medojedovi i nadále všechno jedno.

> „Bitcoin je prvním příkladem nové formy života. Žije a dýchá na internetu. Je naživu, protože dokáže lidem zaplatit, aby jej udrželi naživu. [...] Nelze jej změnit. Nelze jej zpochybnit. Nelze s ním manipulovat. Nelze jej poškodit. Nelze jej zastavit. [...] Kdyby náš svět zničila jaderná válka, přežil by bez poškození a fungoval by dál."
>
> – Ralph Merkle[4]

Tlukot srdce bitcoinové sítě přežije nás všechny.

[3] Příspěvek na BitcoinTalk fóru: Re: Transactions and Scripts [56]
[4] DAOs, Democracy and Governance [44]

Uvědomění si výše uvedeného mě změnilo mnohem víc, než se kdy mohou změnit uplynulé bloky bitcoinového blockchainu. Změnilo to mé časové preference, mé chápání ekonomie, mé politické názory a mnoho dalšího. K čertu, dokonce to mění i lidský jídelníček.[5] Pokud vám to všechno zní šíleně, jste v dobré společnosti. Všechno je to šílené, a přesto se to děje.

Bitcoin mě naučil, že se nezmění. Já ano.

[5] Inside the World of the Bitcoin Carnivores [58]

2. Vzácnost vzácnosti

„To úplně stačí – doufám, že už víc neporostu...“

– Alenka

Obecně se zdá, že s rozvojem technologií se věci stávají dostupnějšími. Stále více lidí si tak může dopřát to, co dříve bylo luxusním zbožím. Brzy budeme všichni žít jako králové. Většina z nás už tak žije. Jak napsal Peter Diamandis v knize Hojnost[1]: „Technologie je mechanismus, který uvolňuje zdroje. Může učinit z toho, co bylo dříve nedostatkové, věc naprosto hojnou.“

Bitcoin, sám o sobě pokročilá technologie, tento trend překonává a vytváří novou komoditu, která je skutečně vzácná. Někteří dokonce tvrdí, že je jednou z nejvzácnějších věcí ve vesmíru. Jeho nabídku nelze nafouknout, a to bez ohledu na to, kolik úsilí se člověk na vytvoření většího množství rozhodne vynaložit.

„Jen dvě věci jsou skutečně vzácné: čas a bitcoin.“

– Saifedean Ammous[2]

[1] Peter Diamandis. *Hojnost*, v českém vydání na s. 15 [23]
[2] V prezentaci o *Bitcoinovém standardu* [2]

Paradoxně toho bitcoin dosahuje pomocí mechanismu kopírování. Transakce se vysílají, bloky jsou šířeny, distribuovaná účetní kniha je – ano, hádáte správně – distribuovaná. To všechno jsou jen vznešená slova pro kopírování. Bitcoin dokonce kopíruje sám sebe na co nejvíce počítačů tím, že motivuje jednotlivé lidi, aby provozovali síťové uzly a těžili nové bloky.

Všechna tato duplikace úžasně funguje v koordinovaném úsilí o vytvoření vzácnosti.

V době hojnosti mě bitcoin naučil, co je to opravdová vzácnost.

3. Replikace a lokace

> *Někdo se zlostně rozkřikl – byl to Králík – „Anton! Anton! Kde jsi?“*
>
> – Lewis Carroll*, Alenka v kraji divů*

Když pomineme kvantovou mechaniku, lokace je ve fyzikálním světě bezproblémová. Na otázku: „Kde je X?“ lze smysluplně odpovědět bez ohledu na to, zda je X osoba, nebo předmět. V digitálním světě je již otázka polohy záludná, ale není nemožné na ni odpovědět. Kde jsou vlastně vaše e-maily? Špatná odpověď by byla „v cloudu“, což je jen počítač někoho jiného. Přesto, pokud byste chtěli vystopovat každé úložné zařízení, na kterém se vaše e-maily nacházejí, mohli byste je teoreticky najít.

U bitcoinu je otázka „kde“ *vskutku* ošemetná. Kde přesně jsou vaše bitcoiny?

> „Otevřel jsem oči, rozhlédl se kolem sebe a položil nevyhnutelnou, tradiční, žalostně otřepanou pooperační otázku: Kde to jsem?“
>
> – Daniel Dennet[1]

[1] Daniel Dennett, *Where Am I* [22]

Problém je dvojí: Zaprvé, distribuovaná účetní kniha je distribuována pomocí úplné replikace, což znamená, že je všude. Za druhé, neexistují žádné bitcoiny. Nejen fyzicky, ale ani *technicky*.

Bitcoin (protokol) eviduje soubor neutracených transakčních výstupů, aniž by se vůbec musel odkazovat na nějakou entitu, která by představovala bitcoin (peníze). Existence bitcoinu se odvozuje z toho, že se podíváme na množinu neutracených transakčních výstupů a každou položku se 100 miliony základních jednotek nazveme bitcoinem.

> „Kdepak je? Právě v tuto chvíli – na cestě? [...] Za prvé, žádné bitcoiny nejsou. Prostě nejsou. Neexistují. Existují záznamy v účetní knize, která je sdílená [...] Neexistují na žádném fyzickém místě. Účetní kniha však existuje v podstatě na každém fyzickém místě. Geografie zde nemá smysl – s určováním pravidel vám zde nepomůže."
>
> – Peter Van Valkenburgh[2]

Co tedy skutečně vlastníte, řeknete-li: „Mám bitcoin", když žádné bitcoiny neexistují? No, vzpomínáte si na všechna ta podivná slova, která vás peněženka během založení nutila zapsat? Tak tedy právě tato magická slova jsou tím, co vlastníte: kouzelné zaklínadlo, pomocí něhož lze do veřejné účetní knihy přidat několik záznamů – klíče k „přesunu" některých bitcoinů. A právě proto jsou vaše privátní klíče v praxi vašimi bitcoiny. Pokud si myslíte, že si tohle celé vymýšlím, můžete mi své privátní klíče směle poslat.

Bitcoin mě naučil, že lokace je ošemetná záležitost.

[2] Peter Van Valkenburgh v podcastu *What Bitcoin Did*, epizoda 49 [73]

4. Problém identity

„Kdopak jsi?“ řekl Houseňák.

– Lewis Carroll*, Alenka v kraji divů*

Nic Carter napsal, jako poctu Thomasovi Nagelovi za pojednání o stejné otázce v souvislosti s netopýrem, skvělý článek, který se zabývá otázkou: Jaké to je být bitcoinem? Vynikajícím způsobem ukazuje, že otevřené, veřejné blockchainy obecně, a bitcoin zvláště, trpí stejným problémem jako Théseova loď: který bitcoin je skutečný bitcoin?

> „Uvědomte si, jak málo odolné jednotlivé komponenty bitcoinu jsou. Celý zdrojový kód byl přepracován, pozměněn a rozšířen tak, že se sotva podobá své původní verzi. [...] Registr toho, co kdo vlastní, tedy samotná účetní kniha, je prakticky jediným trvalým rysem sítě [...]. Abychom mohli tento systém považovat za skutečně nezávislý, musíme se vzdát snadného řešení spočívajícího v tom, že existuje subjekt, který může jeden konkrétní řetězec označit za legitimní.“
>
> – Nic Carter[1]

[1] Nic Carter, *What is it like to be a bitcoin?* [19]

Zdá se, že rozvoj technologií nás neustále nutí brát takové filozofické otázky vážně. Dříve nebo později budou samořiditelná auta čelit reálným verzím tramvajového dilematu a budou nucena činit etická rozhodnutí, na kterých životech záleží a na kterých ne.

Kryptoměny, zejména od prvního sporného hard forku, nás nutí přemýšlet o metafyzice identity a dospět ohledně ní ke shodě. Je zajímavé, že dva nejdůležitější příklady, které jsme dosud zažili, vedly k rozdílným odpovědím. Dne 1. srpna 2017 se bitcoin rozdělil na dva tábory. Trh rozhodl, že nezměněným řetězcem zůstává původní bitcoin. O rok dříve, 25. října 2016, se na dva tábory rozdělilo Ethereum. Trh rozhodl, že originálním Ethereem bude naopak *pozměněný* řetězec.

Za předpokladu, že sítě pro přenos hodnoty budou řádně decentralizované, budou muset na otázky vyvolané paradoxem Théseovy lodi odpovídat, dokud budou existovat.

Bitcoin mě naučil, že decentralizace je v rozporu s identitou.

5. Neposkvrněné početí

„Už mají hlavy pryč,“ zahulákali v odpověď vojáci.

– Lewis Carroll*, Alenka v kraji divů*

Každý má rád dobré příběhy o původu. Příběh vzniku bitcoinu je fascinující a jeho detaily jsou důležitější, než by se na první pohled mohlo zdát. Kdo je Satoshi Nakamoto? Byl to jeden člověk, nebo skupina lidí? Byla to žena? Mimozemšťan cestující v čase, nebo pokročilá umělá inteligence? Odhlédneme-li od obskurních teorií, odpověď se pravděpodobně nikdy nedozvíme. A to je důležité.

Satoshi se rozhodl zůstat v anonymitě. Zasadil semínko bitcoinu a zůstal tu dostatečně dlouho na to, aby se ujistil, že síť nezahyne ještě v plenkách. A pak zmizel.

To, co může vypadat jako hra na schovávanou, je ve skutečnosti pro opravdu decentralizovaný systém klíčové. Žádná centrální kontrola. Žádná ústřední autorita. Žádný vynálezce. Nikdo, kdo by mohl být trestně stíhán, mučen, vydírán nebo jinak šikanován. Neposkvrněné početí technologie.

„Jednou z nejlepších věcí, které Satoshi udělal, bylo, že zmizel.“

– Jimmy Song[1]

[1] Jimmy Song, *Why Bitcoin is Different* [67]

Od stvoření bitcoinu vznikly tisíce dalších kryptoměn. Žádný z těchto klonů s ním však nesdílí stejnou historii původu. Pokud chcete bitcoin zastínit, budete muset překonat příběh o jeho vzniku. Ve válce idejí rozhodují o přežití narativy.

> „Zlato se poprvé začalo zpracovávat do šperků a používat pro směnný obchod před více než 7 000 lety. Podmanivý lesk zlata vedl k tomu, že bylo považováno za dar bohů."
>
> – Rakouská mincovna[1]

Stejně jako zlato v dávných dobách, by i bitcoin mohl být považován za dar bohů. Na rozdíl od zlata je však původ bitcoinu až příliš lidský. A tentokrát víme, kdo jsou bohové jeho vývoje a správy: lidé po celém světě, ať už anonymní, nebo ne.

Bitcoin mě naučil, že příběhy jsou důležité.

[1] The Austrian Mint, *Gold: The Extraordinary Metal* [46]

6. Síla svobody slova

„Prosím?“ zeptala se Myš zamračeně, ale zdvořile. „Říkal jsi něco?“

– Lewis Carroll*, Alenka v kraji divů*

Bitcoin je myšlenka. Myšlenka, která je ve své současné podobě projevem mechanismu poháněného čistě textem. Každý aspekt bitcoinu je text – whitepaper je text. Software, který běží v jeho uzlech, je text. Účetní kniha i jednotlivé transakce jsou všechno texty. Veřejné a soukromé klíče jsou textem. Každý aspekt bitcoinu je text, a proto je rovnocenný slovu.

„Kongres nesmí vydávat zákony zavádějící nějaké náboženství nebo zákony, které by zakazovaly svobodné vyznávání nějakého náboženství; právě tak nesmí vydávat zákony omezující svobodu slova nebo tisku, právo lidu pokojně se shromažďovat a právo podávat státním orgánům žádosti o nápravu křivd.“

– první dodatek Ústavy Spojených států amerických

Ačkoliv finální bitva kryptografických válek[1] ještě nebyla vybojována, bude velmi obtížné kriminalizovat myšlenku. Natož myšlenku, která je založena na výměně textových zpráv. Pokaždé, když se vláda pokusí postavit text nebo slovo mimo zákon, sklouzneme na cestu absurdity, která nevyhnutelně vede k takovým nehoráznostem, jako jsou ilegální čísla[2] nebo ilegální prvočísla[3].

Dokud existuje část světa, kde je svoboda slova skutečnou svobodou, je bitcoin nezastavitelný.

> „V žádné fázi bitcoinové transakce neexistuje místo, kde by bitcoin přestal být textem. Bitcoin je celý textem, za všech okolností. [...] Bitcoin je text. Bitcoin je slovo. Ve svobodné zemi, jako jsou USA, se zaručenými nezcizitelnými právy a prvním dodatkem, který výslovně zapovídá vládní dohled nad svobodným publikováním, jej nelze regulovat."
>
> – Beautyon[4]

Bitcoin mě naučil, že ve svobodné společnosti jsou svoboda slova a svobodný software nezastavitelné.

[1] *Kryptografické války* je neoficiální název pro snahu USA a spřízněných vlád podkopávat šifrování [26] [78]
[2] Ilegální číslo je číslo reprezentující informaci, kterou je v určitých právních jurisdikcích nelegální držet, vyslovit, propagovat nebo jinak předávat [84]
[3] Ilegální prvočíslo je prvočíslo reprezentující informaci, jejíž přechovávání nebo šíření je v určitých jurisdikcích zakázáno. Jedno z prvních takových prvočísel bylo objeveno v roce 2001. Pokud bylo interpretováno určitým způsobem, pak popisovalo počítačový program, který obcházel systém digitálních manažerských práv na DVD. Šíření takového prvočísla bylo v USA postaveno mimo zákon skrze tzv. Digital Milennium Copyright Act. Ilegální prvočíslo je tedy podtypem ilegálního čísla [85]
[4] Beautyon, *Why America Can't Regulate Bitcoin* [7]

7. Hranice poznání

> *Stále hloub a hloub a hloub. Což tomu padání nikdy nebude konec?*
>
> – Lewis Carroll*, Alenka v kraji divů*

Pronikání do bitcoinu je zkouškou z pokory. Myslel jsem si, že něco vím. Myslel jsem si, že jsem vzdělaný. Myslel jsem si, že se vyznám přinejmenším v informatice. Studoval jsem ji roky, takže musím vědět všechno o digitálních podpisech, hashování, šifrování, provozní bezpečnosti a sítích, ne?

Omyl.

Naučit se všechny základní principy, na kterých bitcoin funguje, je těžké. Pochopit je všechny do hloubky je na hranici nemožného.

> „Nikdo ještě nenašel dno bitcoinové králičí nory."
>
> – Jameson Lopp[1]

Můj seznam knih k přečtení se rozšiřuje mnohem rychleji, než je stíhám přečíst. Seznam studií a článků je prakticky nekonečný. Podcastů na všechna tato témata je víc, než bych kdy mohl naposlouchat. Je to

[1] Jameson Lopp, tweet z 11. listopadu 2018 [41]

opravdu pokořující. Navíc, bitcoin se vyvíjí a je téměř nemožné držet krok se zrychlujícím se tempem inovací. Ještě se ani neusadil prach na první vrstvě a lidé už vybudovali druhou a pracují na třetí.

7.1 Bitcoinová králičí nora je bezedná

Bitcoin mě naučil, že vím velmi málo téměř o čemkoliv. Ukázal mi, že tahle králičí nora je bezedná.

Kapitola II.

Ekonomika

Ekonomika

> *U vchodu do zahrady stál velký růžový štěp. Rostly na něm bílé růže, ale tři zahradníci je usilovně přetírali na červeno. Alence to bylo velmi divné…*
>
> – Lewis Carroll*, Alenka v kraji divů*

Peníze nerostou na stromech. Věřit, že rostou, je pošetilé a naši rodiče dbají, abychom to věděli. Proto nám tohle rčení opakují jako mantru. Nabádají nás, abychom s penězi nakládali moudře, neutráceli je lehkomyslně a v dobrých časech si je šetřili, aby nám pomohly přečkat časy zlé. Vždyť přece peníze nerostou na stromech.

Bitcoin mě naučil o penězích víc, než jsem si kdy vůbec myslel, že budu potřebovat vědět. Díky němu jsem byl nucen probádat historii peněz, bankovnictví, různé školy ekonomického myšlení a mnoho dalších témat. Snaha pochopit bitcoin mě vedla mnohými cestami, z nichž některé se snažím prozkoumat v této knize.

V prvních sedmi lekcích jsme prozkoumali některé filozofické otázky, kterých se bitcoin dotýká. V dalších sedmi lekcích se blíže podíváme na problematiku peněz a ekonomiky.

Kapitola II – Ekonomika

- **Lekce 8:** Finanční negramotnost
- **Lekce 9:** Inflace
- **Lekce 10:** Hodnota
- **Lekce 11:** Peníze
- **Lekce 12:** Historie a úpadek peněz
- **Lekce 13:** Šílenství frakčních rezerv
- **Lekce 14:** Zdravé peníze

Opět budu schopen pouze lehce zmapovat povrch. Bitcoin je nejen ambiciózní, ale má také široký a hluboký záběr, takže není možné pokrýt všechna relevantní témata v jediné lekci, eseji, článku nebo knize. Mám dokonce pochybnosti, zdali je něco takového vůbec reálné.

Bitcoin je novou formou peněz, a proto je pro jeho pochopení naprosto klíčové nastudovat si ekonomii. Ekonomie, která se zabývá podstatou lidského jednání a interakcí jednotlivých tržních subjektů, je pravděpodobně jedním z největších a zároveň nejzamotanějších kousků skládačky jménem bitcoin.

Ještě jednou zopakuji, že tyto lekce jsou rozborem různých věcí, které mě bitcoin naučil. Jsou osobní reflexí mé cesty dolů králičí norou. Vzhledem k tomu, že nemám ekonomické vzdělání, se nacházím rozhodně mimo svou komfortní zónu a jsem si zejména vědom toho, že jakékoliv mé případné poznatky jsou neúplné. Budu se snažit nastínit, co jsem se naučil, i když riskuji, že ze sebe udělám hlupáka. Koneckonců se stále snažím odpovědět na otázku: „Co vás bitcoin naučil?“

Po sedmi lekcích z pohledu filozofie se podívejme na dalších sedm lekcí optikou ekonomie. To nejlepší, co vám tedy pro tentokrát mohu nabídnout, je ekonomická třída. Cílová destinace: *zdravé peníze*.

8. Finanční negramotnost

„Co si ta paní o mně pomyslí, jaká jsem nevzdělaná holka! Ba ne, ptát se nebudu; třeba uvidím nějaký nápis.“

– Alenka

Jednou z nejpřekvapivějších věcí pro mě bylo, kolik znalostí z financí, ekonomie a psychologie je potřeba k pochopení na první pohled čistě *technického* systému – počítačové sítě. Abych parafrázoval malého chlapíka s chlupatýma nohama: „Je to nebezpečná věc, Frodo, vkročit do bitcoinu. Přečteš si whitepaper, a když si nedáš pozor na nohy, nevíš, kam tě to může zavát.“

Chcete-li pochopit nový měnový systém, musíte se seznámit s tím starým. Velmi brzy jsem si začal uvědomovat, že úroveň finančního vzdělání, jíž se mi dostalo v rámci školského systému, byla v podstatě *nulová*.

Začal jsem si klást spoustu otázek jako pětileté dítě: Jak funguje bankovní systém? Jak funguje burza? Co jsou to fiat peníze? Co jsou *běžné* peníze? Proč je tolik dluhů?[1] Kolik peněz se vlastně tiskne a kdo o tom rozhoduje?

Po lehké panice z míry mé nevědomosti jsem našel uklidnění v tom, že jsem v dobré společnosti.

[1] https://www.usdebtclock.org

> „Není ironií, že mě bitcoin naučil o penězích víc než všechny ty roky, které jsem strávil prací pro finanční instituce? … včetně začátku mé kariéry v centrální bance.“
>
> – Aaron[2]

> „Za poslední tři měsíce v kryptu jsem se naučil více o financích, ekonomii, technologiích, kryptografii, lidské psychologii, politice, teorii her, legislativě a o sobě samém než za poslední tři a půl roku studia na vysoké škole.“
>
> – Dunny[3]

To jsou jen dvě z mnoha přiznání na twitteru.[4] Bitcoin, jak jsme se dozvěděli v Lekci 1, je živá věc. Mises tvrdil, že ekonomie je také živá věc. A jak všichni víme z vlastní zkušenosti, živé věci je z podstaty podstaty obtížné pochopit.

> „Vědecká teorie je jen jednou ze zastávek na donekonečna postupujícím pátrání po poznání. Je nutně poznamenána nedostatečností přítomnou v každém lidském snažení. Uznání těchto skutečností nicméně neznamená, že je dnešní ekonomie zaostalá. Znamená pouze to, že je ekonomie živoucí věcí – a žití představuje nedokonalosti i změny.“
>
> – Ludwig von Mises[5]

Všichni čteme ve zprávách o různých finančních krizích, přemýšlíme o tom, jak fungují rozsáhlé finanční sanace, a jsme zmateni skutečností,

[2] Aaron (@aarontaycc, @fiatminimalist), tweet z 12. prosince 2018 [45]
[3] Dunny (@BitcoinDunny), tweet z 28. listopadu 2017 [24]
[4] na https://bit.ly/btc-learned naleznete víc podobných přiznání z twitteru
[5] Ludwig von Mises, *Lidské jednání*, v českém vydání z roku 2006 na straně 6 [74]

že nikdo nikdy nebyl pohnán k odpovědnosti za škody, které se pohybují v řádech bilionů. Stále jsem zmatený, ale alespoň začínám mít přehled o tom, co se ve světě financí děje.

Někteří lidé jdou dokonce tak daleko, že všeobecnou neinformovanost v těchto tématech přisuzují systémové, záměrné nedbalosti. Zatímco dějepis, fyzika, biologie, matematika a jazyky jsou součástí našeho vzdělávání, svět peněz a financí je ve školách překvapivě probírán pouze povrchně, pokud vůbec. Zajímalo by mě, zda by lidé byli stále ochotni se zadlužovat v takové míře jako v současnosti, kdyby se každému dostalo vzdělání v oblasti osobních financí, fungování peněz a dluhů. Potom si říkám, kolik vrstev hliníkové fólie je asi potřeba na kvalitní klobouk k odstínění škodlivého záření. Nejspíš tak tři.

> „Tyto krachy, tyto bailouty, to nejsou náhody. A náhoda není ani to, že ve školách neexistuje finanční vzdělávání. [...] Je to promyšlené. Stejně jako před občanskou válkou bylo nezákonné vzdělávat otroky, tak se ve škole nesmíme učit o penězích."
>
> – Robert Kiyosaki[6]

Stejně jako v Čaroději ze země Oz nám bylo řečeno, že si nemáme všímat muže za oponou. Na rozdíl od tohoto příběhu však nyní máme k dispozici skutečné kouzlo[7]: otevřenou síť k přenosu hodnoty, která je bez hranic a odolná vůči cenzuře. Žádná opona neexistuje a kouzla jsou viditelná pro všechny.[8]

Bitcoin mě naučil nahlédnout za oponu a čelit své finanční negramotnosti.

[6] Robert Kiyosaki, *Why the Rich are Getting Richer* [39]
[7] https://bit.ly/btc-wizardry
[8] https://github.com/bitcoin/bitcoin

9. Inflace

> *„Jak vidíš, tady musíš běžet ze všech sil, abys setrvala na jednom místě. Chceš-li se dostat jinam, musíš běžet aspoň dvakrát tak rychle.“*
>
> – Srdcová královna

Snaha pochopit monetární inflaci a to, jak by neinflační systém, jakým je bitcoin, mohl změnit způsob, kterým fungujeme, byla výchozím bodem mé výpravy do ekonomie. Tušil jsem, že inflace je míra, s jakou vznikají nové peníze, ale jinak jsem nevěděl o moc víc.

Zatímco někteří ekonomové tvrdí, že inflace je dobrá, jiní tvrdí, že pro zdravou ekonomiku jsou nezbytné „tvrdé“ peníze, jejichž zásobu nelze snadno navyšovat – jako tomu bylo v dobách zlatého standardu. Bitcoin, se svou fixní nabídkou 21 milionů jednotek, souhlasí s druhým táborem.

Dopady inflace nejsou obvykle zřejmé okamžitě. V závislosti na míře inflace (jakož i na dalších faktorech) může doba mezi její příčinou a následkem trvat i několik let. A nejen to, inflace ovlivňuje různé skupiny lidí více než jiné. Jak upozorňuje Henry Hazlitt v knize *Ekonomie v jedné lekci:* „Umění ekonomie spočívá ve zkoumání nejen bezprostředních, ale i dlouhodobých důsledků daného činu nebo opatření; a spočívá ve sledování dopadů tohoto opatření nejen na jednu skupinu, ale také na všechny ostatní skupiny.“

Jedním z mých osobních okamžiků prozření bylo zjištění, že vydávání nové měny – tištění dalších peněz – je naprosto odlišné od všech ostatních ekonomických aktivit. Zatímco skutečné zboží a skutečné služby vytvářejí skutečnou hodnotu pro skutečné lidi, tisk peněz dělá pravý opak: bere hodnotu všem, kteří drží měnu, jejíž množství se nafukuje.

> „Inflace, tedy prosté vydávání většího množství peněz, které vede k růstu mezd a cen, se může jevit jako vytváření větší poptávky. Vyjádřeno objemy skutečné výroby a směny skutečných věcí se ale o větší poptávku nejedná."
>
> – Henry Hazlitt[1]

Ničivá síla inflace se naplno projeví, jakmile se malá inflace změní ve velkou. Pokud dojde k hyperinflaci peněz, věci se vymknou kontrole velmi rychle.[2] Jak se nafukující měna hroutí, nedokáže uchovat hodnotu v čase a lidé se tak vrhají na jakékoliv zboží, které by ji uchovat mohlo.

Dalším následkem hyperinflace je, že všechny peníze, které si lidé v průběhu života naspořili, fakticky zmizí. Papírové peníze v peněžence samozřejmě zůstanou. Ale nebudou ničím jiným než bezcenným papírem.

9.1 Hyperinflace ve Výmarské republice (1921–1923)

[1] Henry Hazlitt, *Ekonomie v jedné lekci* ,v českém vydání knihy na straně 27 [35]
[2] https://cs.wikipedia.org/wiki/Hyperinflace [83]

Hodnota peněz klesá i při takzvané „mírné“ inflaci. Jen se to děje natolik pomalu, že si většina lidí poklesu své kupní síly nevšimne. A jakmile se tiskařské stroje rozběhnou, lze měnu snadno nafouknout, a dříve mírná inflace může stisknutím tlačítka narůst do ohromné výše. Jak upozornil Friedrich Hayek v jednom ze svých esejů, mírná inflace obvykle vede k absolutní inflaci.

> „‚Mírná‘ stabilní inflace nemůže pomoci – může vést pouze k naprosté inflaci.“
>
> – Friedrich Hayek[3]

Inflace je obzvláště zákeřná, neboť zvýhodňuje ty, kteří mají blíže k tiskárnám peněz. Trvá totiž nějakou dobu, než se nově vytvořené peníze dostanou do oběhu a ceny se tomu přizpůsobí. Takže pokud se vám podaří získat více peněz dříve, než dojde ke znehodnocení peněz všech ostatních, máte před inflační křivkou náskok. To je také důvod, proč lze inflaci považovat za skrytou daň, protože na ní nakonec vydělají vlády, zatímco všichni ostatní na ni doplatí.

> „Myslím, že nepřeháním, když řeknu, že dějiny jsou z velké části dějinami inflace, a to obvykle inflace vyvolané vládami a ve prospěch vlád.“
>
> – Friedrich Hayek[4]

Dosud byly všechny vládou kontrolované měny buď nahrazeny jinými, nebo se zcela zhroutily. Bez ohledu na to, jak malá je míra inflace, její „stabilní“ růst je jen jiným vyjádřením exponenciálního růstu. Stejně

[3] Friedrich Hayek, *1880s Unemployment and the Unions* [33]
[4] Friedrich Hayek, *Good Money* [34]

jako v přírodě, tak i v ekonomice se všechny exponenciálně rostoucí systémy nakonec musí stabilizovat, jinak je postihne katastrofický kolaps.

„V mé zemi se to stát nemůže," říkáte si pravděpodobně. Pokud jste ale z Venezuely, která v současnosti trpí hyperinflací, tak už si to asi nemyslíte. Při míře inflace přesahující milion procent jsou peníze v podstatě bezcenné.

K inflaci nemusí dojít během několika příštích let, nebo se nemusí týkat konkrétní měny používané ve vaší zemi. Pohled na seznam historických měn však ukazuje, že v dostatečně dlouhém časovém období k ní nevyhnutelně dojde. Pamatuji si a používal jsem spoustu z měn, které jsou v seznamu uvedeny: rakouský šilink, německou marku, italskou liru, francouzský frank, irskou libru, chorvatský dinár atd. Moje babička dokonce používala rakousko-uherskou korunu. S postupem času se aktuálně používané měny pomalu, ale jistě přesunou na svůj hřbitov. Podlehnou hyperinflaci nebo budou nahrazeny novými. Brzy se stanou historickými měnami. Znehodnotíme je.

> „Dějiny ukázaly, že vlády pokaždé nevyhnutelně podlehnou pokušení navýšit objem peněz."
>
> – Saifedean Ammous[5]

V čem je bitcoin jiný? Na rozdíl od vládou vydávaných měn mají peněžní statky neregulované vládou, ale řídící se fyzikálními zákony[6], tendenci přežít a dokonce si v průběhu času udržet svou hodnotu. Zatím nejlepším příkladem je zlato, které si, jak ukazuje příznačně pojmenovaný indikátor *poměru zlata ke slušnému pánskému obleku*[7],

[5] Saifedean Ammous, *Bitcoinový standard*, s.73 [1]
[6] Gigi, *Bitcoin's Energy Consumption – A shift in perspective* [29]
[7] Gold-to-Decent Suit Ratio. Historie ukazuje, že cena unce zlata odpovídá ceně slušného pánského obleku, podle dat společnosti Sionna Investment Managers [42]

drží svou hodnotu po stovky a dokonce tisíce let. Možná není dokonale „stabilní“, což je pochybný pojem sám o sobě, ale hodnota, kterou si drží, zůstane přinejmenším řádově stejná.

Pokud si peněžní statek nebo měna dobře drží svou hodnotu v čase a prostoru, jsou považovány za *tvrdé*. Pokud si svou hodnotu neudrží z důvodu snadného znehodnocení nebo nafouknutí zásob, jedná se o měkkou měnu. Pojem tvrdosti je pro pochopení bitcoinu zásadní a zaslouží si důkladnější rozbor. Vrátíme se k němu v poslední ekonomické lekci o zdravých penězích.

Vzhledem k tomu, že hyperinflací trpí stále více zemí, bude stále více lidí muset čelit realitě tvrdých a měkkých peněz. Při troše štěstí možná i někteří centrální bankéři budou nuceni přehodnotit svou měnovou politiku. Ať už se stane cokoliv, poznatky, které jsem díky bitcoinu získal, budou pravděpodobně neocenitelné bez ohledu na výsledek.

Bitcoin mě poučil o skryté dani inflace a o katastrofě hyperinflace.

10. Hodnota

> *Ale to k ní zvolna hupkal zpátky Bílý Králík a starostlivě se rozhlížel, jako by byl něco ztratil.*
>
> – Lewis Carroll*, Alenka v kraji divů*

Hodnota je poněkud paradoxní záležitost a existují různé teorie[1], které se snaží vysvětlit, proč si určitých věcí ceníme více než jiných. Lidé si tento paradox uvědomují již tisíce let. Jak napsal Platón ve svém dialogu s Euthydémem, některých věcí si ceníme proto, že jsou vzácné, a ne pouze na základě jejich nezbytnosti pro naše přežití.

> „A jsi-li rozumný, dáš stejnou radu i svým žákům, aby se nikdy nebavili s nikým jiným než s tebou a mezi sebou. Neboť vzácné je to, Euthydéme, co je drahé, zatímco voda je nejlevnější, i když nejlepší, jak pravil Pindaros."
>
> – Platón[2]

Tento paradox[3] hodnoty vypovídá něco zajímavého o nás lidech: zdá se, že věci hodnotíme na subjektivním[4] základě, ale činíme tak podle určitých nenahodilých kritérií. Něco pro nás může být cenné

[1] Viz *Teorie hodnoty* na Wikipedii [102]
[2] Platón, *Euthydemos* [60]
[3] Viz *Paradox hodnoty* na Wikipedii [96]
[4] Viz *Subjektivní teorie hodnoty* na Wikipedii [100]

z různých důvodů, ale věci, kterých si ceníme, mají určité společné charakteristiky. Pokud můžeme něco velmi snadno okopírovat nebo pokud je to přirozeně hojné, nepovažujeme to za hodnotné.

Zdá se, že si něčeho ceníme, protože je to vzácné (zlato, diamanty, čas), obtížně nebo pracně vyrobitelné, nelze to nahradit (stará fotografie milované osoby) nebo je to užitečné tak, že nám to umožňuje dělat věci, které bychom jinak dělat nemohli. Případně se jedná o kombinaci těchto faktorů, jak je v sobě kombinují například velká umělecká díla.

Bitcoin je všechno výše uvedené: je extrémně vzácný (21 milionů), stále obtížněji se vyrábí (postupné snižování těžařské odměny skrze tzv. halvingy), nelze ho nahradit (ztracený soukromý klíč je navždy pryč) a umožňuje nám dělat některé docela užitečné věci. Je to pravděpodobně nejlepší nástroj pro přenos hodnoty přes hranice, jelikož je odolný vůči cenzuře a konfiskaci. Navíc je to samosprávné úložiště hodnoty, které umožňuje jednotlivcům uchovávat své bohatství nezávisle na bankách a vládách, abychom jmenovali alespoň dva příklady.

Bitcoin mě naučil, že hodnota je subjektivní, ale není nahodilá.

11. Peníze

„Jedno vejce prosím," řekla nesměle. „Po čempak jsou?"
„Po pěti a půl krejcaru za jedno – po dvou krejcarech dvě," odvětila Ovce.

– Lewis Carroll*, Alenka v kraji divů*

Co jsou to peníze? Používáme je denně, ale odpovědět na tuto otázku je překvapivě obtížné. Jsme na nich velkou měrou závislí, a pokud jich máme příliš málo, stává se náš život velmi složitým. Přesto o věci, která podle všeho otáčí světem, přemýšlíme jen zřídka. Bitcoin mě donutil na tuto otázku odpovídat znovu a znovu: „Co to, k čertu, jsou peníze?"

Mluvíme-li v našem „moderním" světě o penězích, lidé si pravděpodobně vybaví šustivé papírky, přestože většina našich peněz dávno není nic než číslo na bankovním účtu. Peníze v podobě jedniček a nul už používáme – v čem je tedy bitcoin odlišný? Bitcoin je jiný, protože z podstaty jde o zcela jiný typ peněz, než jaké používáme v současnosti. Abychom to pochopili, budeme se muset blíže podívat na to, co jsou peníze, jak vznikly a proč se po většinu historie používalo k obchodu zlato a stříbro.

Mušle, zlato, stříbro, papír, bitcoin. Nakonec **peníze jsou to, co lidé používají jako peníze**, bez ohledu na jejich tvar a formu nebo naopak absenci výše zmíněného.

Peníze jsou nesmírně důmyslným vynálezem. Svět bez nich je šíleně komplikovaný: Kolik ryb mi zaplatí nové boty? Za kolik krav si koupím dům? Co když zrovna nic nepotřebuji, ale musím se zbavit jablek, která brzy shnijí? Nepotřebujete velkou představivost, abyste si uvědomili, že výměnný obchod je zoufale neefektivní.

Na penězích je skvělé to, že je lze směnit za *cokoliv jiného* – to je vynález! Jak skvěle shrnuje Nick Szabo[1] v pojednání o původu peněz[2], my lidé jsme coby peníze používali nejrůznější věci: korálky ze vzácných materiálů, kupříkladu ze slonoviny, mušlí nebo některých kostí, různé druhy šperků a později i vzácné kovy, jako stříbro a zlato.

> „V tomto smyslu se spíše jedná o drahý kov. Místo toho, aby se nabídka měnila a hodnota zůstávala stejná, je nabídka předem určena a mění se hodnota."
>
> – Satoshi Nakamoto[3]

Protože jsme líní tvorové, nepřemýšlíme příliš o věcech, které prostě fungují. Peníze pro většinu z nás fungují dobře. Stejně jako u aut nebo počítačů, je většina z nás nucena přemýšlet o jejich vnitřním fungování pouze v případě, když se rozbijí. Lidé, kteří viděli, jak jejich životní úspory zmizely kvůli hyperinflaci, znají hodnotu tvrdých peněz. Stejně jako lidé, kteří viděli, jak jejich přátelé a rodina zmizeli kvůli zvěrstvům nacistického Německa nebo sovětského Ruska, znají hodnotu soukromí.

S penězi je to tak, že jsou všeobjímající. Peníze tvoří polovinu každé transakce, což lidem, kteří peníze vytvářejí, propůjčuje obrovskou moc.

[1] http://unenumerated.blogspot.com
[2] Nick Szabo. *Shelling Out: The Origins of Money* [69]
[3] Satoshi Nakamoto v e-mailové odpovědi Seppovi Hasslbergerovi [50]

> „Vzhledem k tomu, že peníze tvoří polovinu každé obchodní transakce a že celé civilizace doslova vznikají a zanikají na základě kvality svých peněz, mluvíme o úžasné síle, která se skrývá pod rouškou noci. Je to moc spřádat iluze, které se zdají být skutečné tak dlouho, dokud trvají. To je samotné jádro moci centrální banky."
>
> – Ron Paul[4]

Bitcoin tuto moc eliminuje mírovou cestou, protože odstraňuje samu tvorbu peněz a činí tak bez použití síly.

Peníze prošly několika obměnami. Většina z nich byla dobrá. Nějakým způsobem naše peníze vylepšily. Velmi nedávno se však vnitřní fungování našich peněz porouchalo. Dnes jsou téměř všechny naše peníze jednoduše vytvářeny z ničeho těmi, kdo mají moc. Abych pochopil, jak k tomu došlo, musel jsem se seznámit s historií a následným úpadkem peněz.

Zda bude k nápravě této zkaženosti zapotřebí série katastrof, nebo jen monumentální vzdělávací úsilí, se teprve ukáže. Modlím se k bohům zdravých peněz, aby to bylo to druhé.

Bitcoin mě naučil, co jsou to peníze.

[4] Ron Paul, *End the Fed* [57]

12. Historie a úpadek peněz

> *Nedbaly prostých ponaučení, která jim jejich přátelé vštěpovali; tak například: že se spálíš, když držíš moc dlouho v ruce žhavý pohrabáč, že ti obyčejně teče krev, když se hodně hluboko řízneš nožem, a také nezapomínala na to, že když si pořádně přihneš z lahvičky označené jed, dříve nebo později ti to nebude dělat dobře.*
>
> – Lewis Carroll, *Alenka v kraji divů*

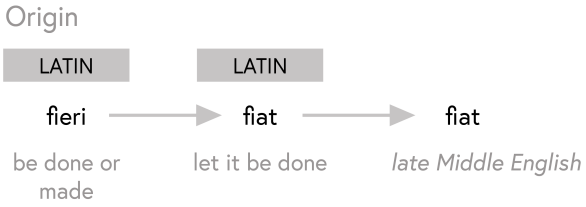
Mnoho lidí si myslí, že peníze jsou kryté zlatem, které je uzamčeno ve velkých trezorech chráněných silnými zdmi. To přestalo být pravdou před mnoha desetiletími. Už ani nevím, co jsem si myslel já, neboť jsem na tom byl mnohem hůř. Prakticky vůbec jsem nerozuměl zlatu, papírovým penězům ani tomu, proč by vůbec měly být něčím kryty.

Součástí poznávání bitcoinu je i poznávání fiat peněz[1]: co znamenají, jak vznikly a proč možná nejsou tím nejlepším nápadem, který jsme kdy měli. Co přesně jsou fiat peníze? A jak jsme se dostali k jejich používání?

Fiat jednoduše znamená, že je něco nařízeno formálním schválením nebo ustanovením. Fiat peníze jsou tedy penězi prostě proto, že někdo říká, že to jsou peníze. Vzhledem k tomu, že všechny vlády dnes používají fiat měnu, je ten někdo vaše vláda. Bohužel nemáte možnost s tím nesouhlasit. Rychle pocítíte, že toto uspořádání je

[1] Česky též „měna s nuceným oběhem“ nebo „zákonná měna“. (pozn. překl.)

všechno, jen ne nenásilné. Pokud odmítnete používat danou papírovou měnu k podnikání a placení daní, jediní lidé, se kterými budete moci diskutovat o ekonomice, budou vaši spoluvězni.



12.1 Pozdně středoanglicky, z latinského fiat – 3. osoba jednotného čísla konjunktivu slovesa fierī (ve funkci pasívního tvaru facĕre, dělat), překládá se jako ‚budiž!' (wiki)

Hodnota fiat peněz nevyplývá z jejich přirozených vlastností. To, jak dobrý je určitý typ fiat peněz, souvisí pouze s politickou a fiskální (ne) stabilitou těch, kteří je uvádějí do oběhu. Jejich hodnota je stanovena nařízením, svévolně.

Donedávna se používaly dva druhy peněz: **komoditní peníze**, vyrobené z drahých věcí, a **reprezentativní peníze**, které cennou věc pouze zastupují, a to většinou písemně.

Komoditních peněz jsme se již dotkli výše. Lidé jako peníze používali zvláštní kosti, mušle a drahé kovy. Později se jako peníze používaly především mince z drahých kovů, jako je zlato a stříbro. Nejstarší dosud nalezená mince je vyrobena z přírodní směsi zlata a stříbra a vznikla před více než 2 700 lety.[2] Pokud bitcoin přináší něco nového, pak to rozhodně není koncept mince.

[2] Podle řeckého historika Hérodota, píšícího v pátém století před naším letopočtem, byli Lýdové prvními uživateli zlatých a stříbrných mincí [47]

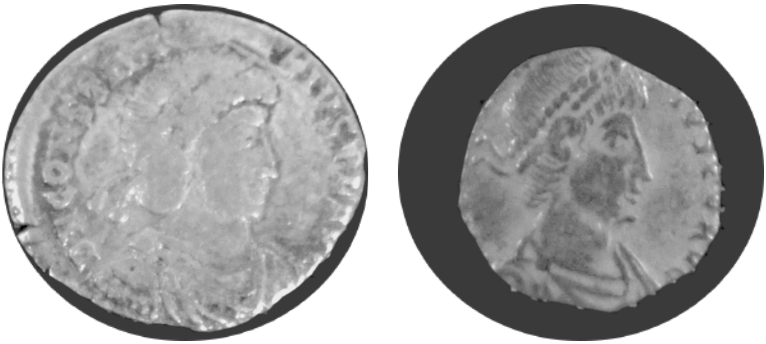
12.2 Statér z élektronu, lýdská mince. Licence obrázku cc-by-sa Classical Numismatic Group, Inc.

Ukázalo se, že hromadění mincí, dnešním slovníkem hodlování[3], je téměř stejně staré jako mince samy. Nejstarším hodlerem mincí byl člověk, jenž téměř stovku takových mincí uložil do hrnce a zakopal do základů chrámu, kde byly nalezeny o 2 500 let později. Zatraceně dobrá studená peněženka, pokud se ptáte na můj názor.

Jednou z nevýhod používání mincí z drahých kovů je, že je lze zmenšovat ořezáváním, což efektivně snižuje hodnotu mince. Z oddělených částí lze, po jejich opětovném slití, razit mince nové, čímž se časem nafoukne peněžní zásoba a každá jednotlivá mince se znehodnotí. Lidé ze svých stříbrných dolarů doslova holili, co se dalo. Zajímalo by mě, jak v té době vypadaly reklamy na *Dollar Shave Club.*

Jelikož vlády tolerují inflaci jen tehdy, pokud ji samy způsobují, snažily se toto partyzánské znehodnocování zastavit. Ve stylu hry na policajty a zloděje byli „ořezávači“ mincí stále nápaditější a nutili „pány mincovny“ být ještě vynalézavější v protiopatřeních. Jedním z „pánů mincovny“ býval Isaac Newton, světoznámý fyzik proslulý svou knihou *Principia Mathematica*. Právě jemu se připisuje přidání drobných proužků na okraj mince, které přežily dodnes. Časy snadného holení mincí tak byly nenávratně pryč.

[3] bit.ly/hodlovani



12.3 Stříbrné mince v různém stupni ořezání

Ačkoliv jsou tyto metody znehodnocování[4] drženy na uzdě, mince stále trpí dalšími problémy. Jsou neskladné a nevhodné k přepravě, zejména je-li třeba realizovat převod velké hodnoty. Přijít s obrovským pytlem stříbrných dolarů pokaždé, když si chcete koupit mercedes, není příliš praktické.

Když už mluvíme o německých věcech: Další zajímavý příběh se týká toho, jak americký dolar získal své jméno. Slovo „dolar" je odvozeno z německého slova *Thaler*, zkráceniny pro *Joachimsthaler*[5], což byla mince ražená ve městě Sankt Joachimsthal.[6] Thaler je v němčině označení pro někoho (nebo něco) pocházejícího z údolí, a protože byly tyto stříbrné mince raženy v Jáchymovském údolí (Joachimsthal), lidé je jednoduše označovali jako *Thaler*. *Thaler* (německy) se vyvinul na *daalders* (holandsky) a nakonec na *dollars* (anglicky).

Zavedení reprezentativní měny předznamenalo pád tvrdých peněz. V roce 1863 byly představeny zlaté certifikáty a o nějakých patnáct let později byl stříbrný dolar také pomalu, ale jistě nahrazen papírovým zástupcem: stříbrným certifikátem.[7]

[4] Kromě ořezávání patřily mezi nejčastější metody znehodnocování mincí tzv. vytřásání (s mincemi se třáslo v pytli a obroušený prach se sesbíral) a děrování (z těla mince se vyrazila díra a její okraje rozklepaly, aby se otvor zase zavřel)
[5] Viz heslo *Thaler* na anglické Wikipedii [101]
[6] Jáchymovský tolar z Jáchymova u Karlových Varů poblíž česko-německé hranice. (pozn. překl.)
[7] Viz článek *Silver certificate* na anglické Wikipedii [99]

12.4 Původní „dolar“ s vyobrazením svatého Jáchyma v plášti a s poutnickou čapkou. Licence obrázku cc-by-sa Berlin-George

Trvalo zhruba 50 let od zavedení prvních stříbrných certifikátů, než se tyto kusy papíru proměnily v to, co dnes označujeme jako americký dolar.

12.5 Americký stříbrný dolar z roku 1928 – „SPLATNÝ DRŽITELI NA VYŽÁDÁNÍ“. Obrázek pochází z Národní numismatické sbírky Smithsonova institutu

Všimněte si, že americký stříbrný dolar z roku 1928 na obrázku 12.5 se stále jmenuje stříbrný certifikát, což naznačuje, že se skutečně jedná o pouhý dokument uvádějící, že držitel tohoto kusu papíru má nárok na kus stříbra. Zajímavé je, že text, kde se toto píše, se postupem času zmenšoval. Stopa po „certifikátu“ po čase zcela zmizela a nahradilo ji uklidňující prohlášení, že se jedná o bankovky Federálního rezervního systému.

Jak bylo uvedeno dříve, totéž se stalo se zlatem. Většina světa fungovala na bimetalickém standardu, což znamená, že mince se vyráběly především ze zlata a stříbra. Zavedení certifikátů na zlato, které bylo možné vyměnit za zlaté mince, pravděpodobně přineslo technologické zlepšení. Papír je pohodlnější, lehčí, a protože jej lze libovolně dělit tak, že se na něj jednoduše vytiskne menší číslo, je snazší rozdělit měnu na menší jednotky.

Aby se držitelům (uživatelům) připomnělo, že tyto certifikáty reprezentují skutečné zlato a stříbro, byly barevně odlišeny a na samotném certifikátu to bylo jasně uvedeno. Tento nápis lze plynule přečíst odshora dolů:

> „Tímto se potvrzuje, že ve státní pokladně Spojených států amerických bylo uloženo sto dolarů ve zlaté minci splatné držiteli na vyžádání.“

12.6 Americký zlatý certifikát na 100 dolarů z roku 1928. Obrázek pochází z Národní numismatické sbírky, Národní muzeum americké historie.

V roce 1963 byla ze všech nově vydávaných bankovek odstraněna slova „SPLATNÉ DRŽITELI NA VYŽÁDÁNÍ“. O pět let později vyplácení papírových bankovek zlatem a stříbrem skončilo.

Slova naznačující původ a myšlenku papírových peněz byla odstraněna.

Zlatá barva z bankovek zmizela. Zůstal jen papír a s ním i možnost vlády tisknout libovolné množství.Zrušením zlatého standardu roku 1971 byla tato sto let trvající finta dokonána. Peníze se staly iluzí,

kterou všichni sdílíme dodnes: fiat penězi, majícími hodnotu proto, že někdo, kdo velí armádě a řídí věznice, říká, že nějakou hodnotu mají. Na každé dolarové bankovce, která je dnes v oběhu, můžeme jasně číst: „TATO BANKOVKA JE ZÁKONNÝM PLATIDLEM“. Jinými slovy: Je cenná, protože to je na ní napsáno.

12.7 Dnes používaná americká dvacetidolarová bankovka série 2004 – „TATO BANKOVKA JE ZÁKONNÝM PLATIDLEM“.

Mimochodem, na dnešních bankovkách se skrývá ještě jedno zajímavé poučení. Na druhém řádku stojí, že se jedná o zákonné platidlo „PRO VŠECHNY DLUHY, VEŘEJNÉ I SOUKROMÉ“. To, co ekonomům může být samozřejmé, mě překvapilo: Všechny peníze jsou dluh. Z toho mě bolí hlava ještě teď a pátrání po vztahu peněz a dluhu přenechám coby cvičení laskavému čtenáři.

Jak jsme viděli, zlato a stříbro se jako peníze používaly po tisíciletí. Postupem času byly mince ze zlata a stříbra nahrazeny papírem, jenž začal být pomalu akceptován jako platidlo. Toto přijetí vytvořilo iluzi, že papír sám představuje hodnotu. Posledním krokem bylo úplné zpřetrhání vazby mezi reprezentací a skutečností: zrušení zlatého standardu a přesvědčení všech, že papír je sám o sobě vzácný.

Bitcoin mě poučil o historii peněz a o největší lsti v dějinách ekonomie zvané fiat měna.

13. Šílenství frakčních rezerv

> *Ale pozdě bycha honit! Alenka rostla a rostla, a tak chtíc nechtíc klekla na zem: za chvíli už ani v pokleku nevydržela, zkusila si tedy lehnout a loktem se opřít o dveře a druhou rukou si podložit hlavu. Ale pořád rostla, a tak jí nakonec nezbylo než vystrčit jednu ruku z okna a jednu nohu strčit do komína a pak si řekla: „Už nemohu nic dělat, ať se stane co stane. Co mě ještě čeká?“*
>
> – Lewis Carroll*, Alenka v kraji divů*

Hodnota a peníze nejsou triviální témata, zejména v dnešní době. Stejně netriviální je i proces vzniku peněz v našem bankovním systému a nemohu se zbavit dojmu, že je to tak záměrně. To, s čím jsem se dříve setkával pouze v akademických a právnických textech, se zdá být běžnou praxí i ve finančním světě: nic není vysvětleno jednoduše, ne proto, že by to bylo skutečně složité, ale proto, že pravda je skryta za mnoha vrstvami žargonu a zdánlivé složitosti. „Expanzivní měnová politika, kvantitativní uvolňování, fiskální stimuly pro ekonomiku“. Publikum souhlasně přikyvuje, zhypnotizováno líbivými slovy.

Bankovnictví částečných rezerv a kvantitativní uvolňování jsou dva z těchto líbivých výrazů, které zastírají, co se ve skutečnosti děje, tím, že to maskují za něco složitého a nepochopitelného. Kdybyste se je pokusili vysvětlit pětiletému dítěti, šílenost obou vám bude rychle zřejmá.

Godfrey Bloom to během společné rozpravy v Evropském parlamentu řekl mnohem lépe, než bych to kdy dokázal já:

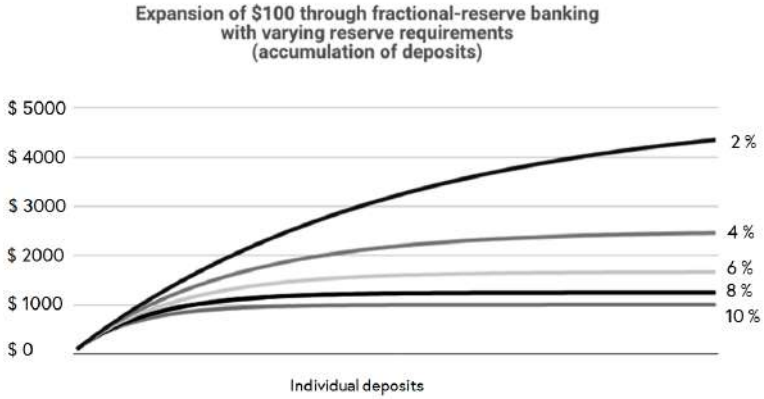
> „[...] nerozumíte ani trochu konceptu bankovnictví. Všechny banky jsou na mizině. Banco Santander, Deutsche Bank, Royal Bank of Scotland – všechny jsou na mizině! A proč jsou na mizině? Není to zásahem vyšší moci. Nejedná se o nějakou tsunami. Jsou na mizině, protože máme systém zvaný ‚bankovnictví částečných rezerv', což znamená, že banky mohou půjčovat peníze, které ve skutečnosti nemají! Je to zločinný skandál a trvá už příliš dlouho. [...] Dochází k padělání – někdy nazývanému kvantitativní uvolňování – ale jinak jenom padělání pod jiným jménem. Umělé tištění peněz, které kdyby prováděl jakýkoliv obyčejný člověk, šel by na hodně dlouho do vězení [...] a dokud nezačneme za tuto nehoráznost posílat bankéře – a mezi ně počítám i centrální bankéře a politiky – do vězení, bude to pokračovat."
>
> – Godfrey Bloom[1]

Zopakuji ještě jednou to nejdůležitější: banky mohou půjčovat peníze, které ve skutečnosti nemají.

Bankovnictví frakčních rezerv umožňuje bance ponechat si jen malou část neboli *frakci* z každého přijatého dolaru. Je to někde mezi 0 a 10 %, obvykle na spodní hranici tohoto rozmezí, což situaci ještě zhoršuje.

Pro lepší pochopení této bláznivé myšlenky si to ilustrujme na konkrétním příkladu: stačí použít zlomek 10 % a měli bychom být schopni provést všechny výpočty jednoduše z hlavy. Pokud si tedy do banky uložíte 100 dolarů, protože je nechcete schovávat pod

[1] Společná rozprava ohledně bankovní unie [17]



13.1 Efekt depozitního multiplikátoru

polštářem, banka je povinna si ponechat pouze dohodnutou *malou* část. V našem případě by to bylo 10 dolarů, protože 10 % ze 100 dolarů je 10 dolarů. Jednoduché, že?

Co tedy banky udělají se zbytkem peněz? Co se stane s vašimi 90 dolary? Udělají to, co banky dělávají, půjčí je dalším lidem. Výsledkem je efekt depozitního multiplikátoru, který nesmírně zvyšuje nabídku peněz v ekonomice. Váš původní vklad 100 dolarů se brzy změní na 190 dolarů. Půjčením 90 % z nově vytvořených 90 dolarů se v ekonomice brzy objeví 271 dolarů. A poté 343,90 dolaru. Nabídka peněz se rekurzivně zvyšuje, protože banky doslova půjčují peníze, které nemají.[2] Aniž by řekly abrakadabra, přemění banky magicky 100 dolarů na tisíc dolarů nebo více. Ukazuje se, že vyčarovat desetinásobek je hračka. Stačí pár kol půjčování.

Nechápejte mě špatně: na půjčování není nic špatného. Stejně tak není nic špatného na úrocích. Dokonce není nic špatného ani na tom, když si ve starých dobrých bankách uložíte své bohatství na bezpečnější místo, než je váš šuplík s ponožkami.

[2] Viz heslo *Money multiplier* na anglické WIkipedii [93]

13.2 Janet Yellenová (tehdejší předsedkyně Fedu) ostře vystupuje proti auditu Fedu, zatímco muž s transparentem důrazně doporučuje koupit bitcoin.

Centrální banky jsou však jiné bestie. Zrůdy finančních regulací, napůl veřejné, napůl soukromé, hrající si na bohy s něčím, co má dopad na každého, kdo je součástí naší globální civilizace. Bez špetky svědomí, zaměřené pouze na bezprostřední budoucnost a zjevně bez jakékoliv odpovědnosti nebo možnosti kontroly (viz obrázek 13.2).

Bitcoin je sice prozatím inflační, ale poměrně brzy přestane být. Striktně omezená nabídka 21 milionů bitcoinů nakonec inflaci zcela odstraní. Nyní máme dva měnové světy: inflační, kde se peníze tisknou svévolně, a svět bitcoinu, kde je konečná nabídka pevně daná a pro každého snadno auditovatelná. Jeden je nám vnucován násilím, do druhého se může zapojit každý podle svého zájmu. Žádné překážky při vstupu, nikdo nemusí žádat o povolení. Dobrovolná účast. V tom je krása bitcoinu.

Řekl bych, že spor mezi keynesiánskými[3] a rakouskými[4] ekonomy už není čistě akademický. Satoshimu se podařilo vybudovat systém přenosu hodnoty na steroidech a vytvořit přitom nejzdravější peníze, jaké kdy

[3] Teorie podle Johna Maynarda Keynese a jeho žáků [86]
[4] Škola ekonomického myšlení založená na metodologickém individualismu [76]

existovaly. Ať tak či onak, podvod, kterým je bankovnictví částečných rezerv, časem odhalí více a více lidí. Pokud dojdou k podobným závěrům jako většina Rakušáků a bitcoinerů, možná se připojí ke stále rostoucímu internetu peněz. Pokud se tak rozhodnou, nikdo jim v tom nezabrání.

Bitcoin mě naučil, že bankovnictví frakčních rezerv je čiré šílenství.

14. Zdravé peníze

> *„Nejprve musím,“ řekla si Alenka při tom bloudění lesem, „narůst zas do správné velikosti; a potom se musím dostat do té krásné zahrady. To bude myslím nejlepší.“*
>
> – Lewis Carroll*, Alenka v kraji divů*

Nejdůležitějším poznatkem, který jsem si z bitcoinu odnesl, je, že z dlouhodobého hlediska jsou tvrdé peníze lepší než měkké. Jakoukoliv světově obchodovatelnou měnu, která slouží jako spolehlivý uchovatel hodnoty, můžeme označit za tvrdé nebo též zdravé peníze.

Pochopitelně, že bitcoin je stále mladý a volatilní. Kritici budou tvrdit, že neukládá hodnotu spolehlivě. Argument volatility se však míjí účinkem. Volatilita se dá očekávat. Trhu bude chvíli trvat, než zjistí spravedlivou cenu těchto nových peněz. Také, jak se často žertem zdůrazňuje, je hodnota bitcoinu založena na chybě měření. Pokud uvažujete v dolarech, neuvědomujete si, že jeden bitcoin bude mít vždy hodnotu jednoho bitcoinu.

> „Nezbytnou podmínkou smysluplné spravedlivé ceny peněz je pevná peněžní zásoba nebo zásoba, která se mění pouze podle objektivních a vypočitatelných kritérií.“
>
> – Fr. Bernard W. Dempsey, S.J.[1]

[1] Perry J. Roets, S.J., *Review of Social Economy* [62]

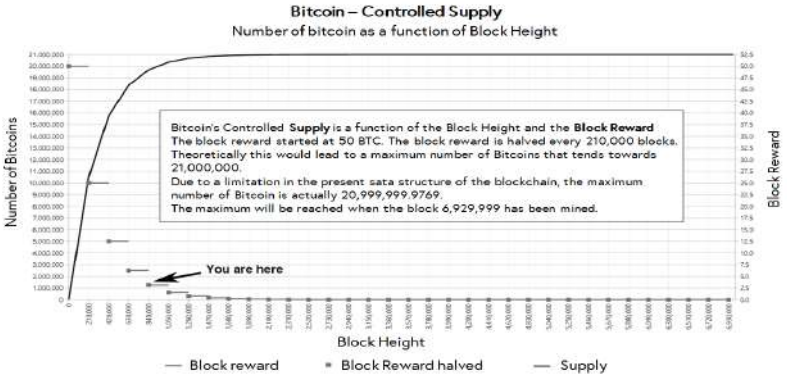
Jak nám ukazuje rychlá prohlídka hřbitova zapomenutých měn, peníze, které lze vytisknout, budou vytištěny. Zatím žádný člověk v historii nedokázal tomuto pokušení odolat.

Bitcoin se pokušení tisknout peníze zbavil důvtipným způsobem. Satoshi si byl vědom naší chamtivosti a omylnosti – proto zvolil něco spolehlivějšího než lidskou zdrženlivost: matematiku.

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50*10^8}{2^i} \right\rfloor}{10^8}$$

14.1 Vzorec nabídky bitcoinu

Tento vzorec je sice užitečný pro popis nabídky bitcoinu, ale ve skutečnosti ho nikde v kódu nenajdete. Emise nových bitcoinů probíhá algoritmicky řízeným způsobem, a to snižováním odměny vyplácené těžařům. Výše uvedený vzorec slouží pouze k rychlému shrnutí toho, co se odehrává pod pokličkou. Co se skutečně děje, lze nejlépe vidět na změně odměny za vytěžený blok. Ta je vyplácena každému nálezci platného bloku, k čemuž dochází zhruba každých 10 minut, a snižuje se vždy po přibližně čtyřech letech.



14.2 Kontrolovaná nabídka bitcoinu

Vzorce, logaritmické funkce a exponenciály nejsou zrovna intuitivní na pochopení. Konceptu zdravých peněz by se dalo lépe porozumět, pokud se na něj podíváme jiným způsobem. Jakmile víme, kolik něčeho je, a známe-li, jak těžké je to vyrobit nebo sehnat, okamžitě pochopíme hodnotu takové věci. To, co platí pro Picassovy obrazy, kytary Elvise Presleyho a stradivárky, platí i pro fiat měnu, zlato a bitcoin.

Tvrdost fiat měny závisí na tom, kdo má pod palcem příslušné tiskařské stroje. Některé vlády mohou být ochotnější tisknout velké množství měny než jiné, což povede k oslabení měny. Jiné vlády mohou být ohledně tisku peněz více restriktivní, což vyústí v měnu tvrdší.

> „Jedním z důležitých aspektů této nové reality je, že instituce jako Fed nemohou zkrachovat. Mohou si vytisknout libovolné množství peněz, které pro sebe mohou potřebovat, a to prakticky s nulovými náklady."
>
> – Jörg Guido Hülsmann[2]

Před zavedením fiat měn byla tvrdost peněz určena přirozenými vlastnostmi věcí, které jsme jako peníze používali. Množství zlata na Zemi je omezeno fyzikálními zákony. Zlato je vzácné, protože srážky supernov a neutronových hvězd jsou ojedinělé. Přírůstek nového zlata je omezen, neboť jeho těžba je poměrně náročná. A poněvadž se jedná o těžký prvek, je většinou ukryto hluboko pod povrchem.

Zrušení zlatého standardu dalo vzniknout nové realitě: k přidání nových peněz stačí pár kapek inkoustu. V našem moderním světě vyžaduje přidání několika nul k zůstatku na bankovním účtu ještě menší úsilí: stačí zmáčknout klávesu a přehodit několik bitů v počítačích bank.

[2] Jörg Guido Hülsmann, *The Ethics of Money Production* [38]

$$\frac{190,000t}{3,100t} = 61$$

14.3 Poměr zásob k přírůstku u zlata

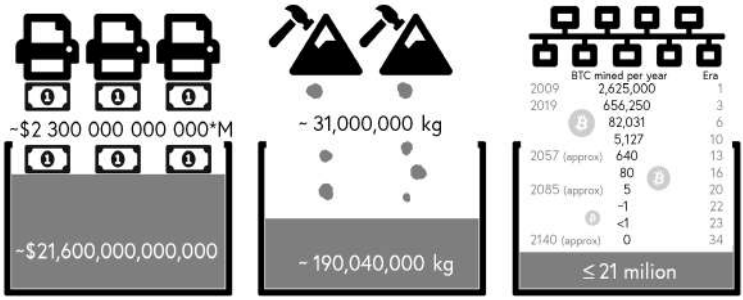
Výše načrtnutý princip lze obecněji vyjádřit jako poměr „zásob“ a „přírůstku“. Zjednodušeně řečeno, zásoba vyjadřuje, kolik dané věci aktuálně existuje. Pro naše účely je zásoba měřítkem současné nabídky peněz. Přírůstek je to, kolik se vyrobí za určité období (např. za rok). Klíčem k pochopení zdravých peněz je porozumění tomuto poměru zásob k přírůstku.

Výpočet poměru zásob k přírůstku peněz u fiat měny je obtížný, protože množství peněz závisí na tom, jak se na ně díváte. Můžete počítat pouze bankovky a mince (M0), přidat cestovní šeky a vklady na běžných účtech (M1), dále spořicí účty a termínované vklady (M2), a dokonce k tomu všemu přidat repo operace a cenné papíry (M3). Navíc se způsob, jakým se toto vše definuje a měří, v jednotlivých zemích liší, a protože americký Federální rezervní systém přestal zveřejňovat[3] čísla pro M3, budeme se muset spokojit s peněžní zásobou M2. Rád bych si tato čísla ověřil, ale nezbývá nám, než se spolehnout na údaje Fedu.

Zlato, jeden z nejvzácnějších kovů na Zemi, má nejvyšší poměr zásob k přírůstku. Podle údajů výzkumné agentury US Geological Survey bylo dosud vytěženo něco přes 190 000 tun. V posledních několika letech se ročně vytěží přibližně 3 100 tun zlata.[4]

Na základě těchto čísel můžeme snadno vypočítat, že poměr zásob k přírůstku zlata je přibližně 61 (viz obrázek 14.3)

[3] Federal Reserve. Money Stock Measures – Discontinuance of M3 [61]
[4] U.S. Geological Survey. National Minerals Information Center – Mineral Commodity Summaries [68]



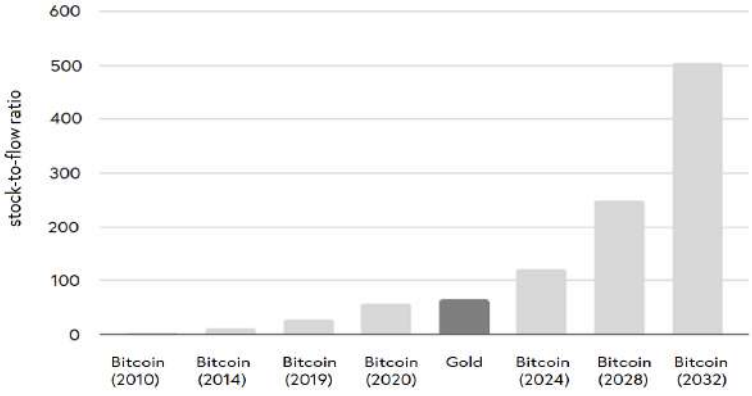
14.4 Vizualizace poměru zásob k přírůstku u dolaru, zlata a bitcoinu

Nic nemá vyšší poměr zásob k přírůstku než právě zlato. Proto bylo zlato až dosud nejtvrdšími a nejzdravějšími existujícími penězi. Často se říká, že všechno dosud vytěžené zlato by se vešlo do dvou olympijských plaveckých bazénů. Podle mých výpočtů[5] bychom potřebovali takové bazény čtyři. Možná je nutné toto přirovnání aktualizovat, nebo se olympijské bazény zmenšily.

Na řadu přichází bitcoin. Jak pravděpodobně víte, těžba bitcoinu je v posledních letech v kurzu. Je to proto, že se stále nacházíme v raném období *těžařských odměn*, kdy jsou těžební uzly za své výpočetní úsilí odměňovány *velkým množstvím* bitcoinů. V současné době se nacházíme v éře odměn číslo 4, která začala v roce 2020 a skončí na začátku roku 2024, pravděpodobně v květnu. Zatímco nabídka bitcoinů je předem daná, vnitřní fungování bitcoinu umožňuje pouze přibližné datování. Přesto můžeme s jistotou předpovědět, jak vysoký bude poměr zásob k přírůstku. Pozor, spoiler: bude vysoký.

Jak vysoký? Inu, ukazuje se, že bitcoin bude nekonečně tvrdý. (viz obrázek 14.4)

[5] https://bit.ly/gold-pools



14.5 Rostoucí poměr zásob k přírůstku bitcoinu v porovnání se zlatem

V důsledku exponenciálního poklesu odměny za těžbu se sníží přísun nových bitcoinů, což povede k raketovému nárůstu poměru zásob k přírůstku. V roce 2020 bitcoin téměř dostihl zlato, a za další čtyři roky je překoná opětovným zdvojnásobením své solidnosti (soundness). K takovému zdvojnásobení dojde celkem čtyřiašedesátkrát. Silou exponenciál klesne za 50 let počet ročně vytěžených bitcoinů pod 100 a za 75 let pod 1 bitcoin. Globální pramen, jenž představuje emise nových bitcoinů odměnou za vytěžení bloku, vyschne někdy kolem roku 2140, čímž se produkce bitcoinu fakticky zastaví. To je běh na dlouhou trať. Pokud toto čtete, jste pořád ještě na začátku.

Jak se bitcoin přibližuje nekonečnému poměru zásob k přírůstku, stává se nejzdravějšími penězi za dobu naší existence. Nekonečnou solidnost je těžké překonat.

Z ekonomického hlediska je *úprava obtížnosti* pravděpodobně nejdůležitější složkou bitcoinu. Obtížnost těžby závisí na tom, jak rychle se nové bitcoiny těží. Právě dynamické přizpůsobování obtížnosti těžby nám umožňuje předvídat budoucí nabídku bitcoinu.

Jednoduchost algoritmu pro úpravu obtížnosti by mohla odvádět pozornost od jeho hloubky, ale právě tato úprava obtížnosti je skutečnou revolucí einsteinovských rozměrů. Zajišťuje, že bez ohledu na to, jak velké nebo malé úsilí je vynaloženo na těžbu, zůstane kontrolovaná nabídka bitcoinu zachována. Bez ohledu na to, kolik energie kdokoliv do těžby bitcoinu vloží, jeho celková odměna se, na rozdíl od každého jiného zdroje, nezvýší.

Stejně jako $E=mc^2$ určuje univerzální limit rychlosti v našem vesmíru, úprava obtížnosti udává **univerzální peněžní limit** v bitcoinu.

Nebýt této úpravy obtížnosti, byly by již všechny bitcoiny vytěženy. Nebýt této úpravy obtížnosti, bitcoin by pravděpodobně nepřežil už ve svých počátcích. Tato vlastnost je tím, co zabezpečuje síť během doby emise. Je něčím, co zajišťuje stabilní a spravedlivou distribuci nových bitcoinů. Je to termostat, který reguluje měnovou politiku bitcoinu.

Einstein nám ukázal něco nového: ať na objekt tlačíte sebevíc, v určitém okamžiku z něj už větší rychlost nedostanete. Satoshi nám také předvedl něco nového: ať už budete toto digitální zlato kopat jakkoliv usilovně, v určitém okamžiku z něj nebudete schopni získat více bitcoinů. Poprvé v historii lidstva máme peněžní statek, kterého, ať se snažíte sebevíc, nebudete schopni vyrobit více.

Bitcoin mě naučil, že zdravé peníze jsou naprosto zásadní.

Kapitola III.

Technologie

Technologie

> *„Už si dám lepší pozor,“ řekla si a rovnou sebrala zlatý klíček a odemkla dvířka do zahrady.*
>
> – Lewis Carroll*, Alenka v kraji divů*

Zlaté klíče, náhodně fungující hodiny, závody v řešení podivných hádanek a tvůrci, kteří nemají tváře ani jména. To, co zní jako pohádky z Kraje divů, je ve světě bitcoinu na denním pořádku.

Jak jsme již zjistili v Kapitole II, mnohé aspekty našeho současného finančního zřízení jsou v konceptu vadné. Stejně jako Alenka můžeme jen doufat, že si tentokrát poradíme lépe. Díky pseudonymnímu vynálezci však nyní máme k dispozici neuvěřitelně sofistikovanou technologii: bitcoin.

Zvládání problémů v radikálně decentralizovaném a nepřátelském prostředí vyžaduje jedinečná řešení. To, co by jinak bylo triviální, je v tomto podivném světě uzlů přesným opakem. Bitcoin ve většině případů spoléhá na silnou kryptografii, alespoň pokud se díváme optikou technologie. Jak silná tato kryptografie je, prozkoumáme v jedné z následujících lekcí.

Kryptografie je tím, co bitcoin využívá k odstranění důvěry v autoritu. Místo na centralizované instituce se systém spoléhá na konečnou autoritu našeho vesmíru: fyziku. Některá zrnka důvěry však stále přetrvávají. Ta prozkoumáme ve druhé lekci této kapitoly.

Kapitola III – Technologie

- **Lekce 15:** Síla v číslech
- **Lekce 16:** Úvahy na téma „Nedůvěřuj, ale ověřuj“
- **Lekce 17:** Určování času vyžaduje práci
- **Lekce 18:** Postupujte pomalu a nic nerozbíjejte
- **Lekce 19:** Soukromí není mrtvé
- **Lekce 20:** Cypherpunkeři píší kód
- **Lekce 21:** Metafory o budoucnosti bitcoinu

Posledních pár lekcí se zabývá étosem technologického vývoje bitcoinu, který je pravděpodobně stejně důležitý jako samotná technologie. Bitcoin není další nablýskaná aplikace ve vašem telefonu. Je to základ nové ekonomické reality, a proto by se k němu mělo přistupovat jako k finančnímu softwaru jaderné třídy.

Kde se v této finanční, společenské a technologické revoluci nacházíme? Sítě a technologie minulosti nám mohou posloužit jako metafory pro budoucnost bitcoinu, kterou se zabýváme v poslední lekci této kapitoly.

Ještě jednou – připoutejte se a užijte si cestu. Čeká nás, stejně jako u všech exponenciálních technologií, parabolická jízda.

15. Síla v číslech

„Tak tedy: čtyřikrát pět je dvanáct, čtyřikrát šest je třináct a čtyřikrát sedm je – ach, jéje! Takhle se do dvaceti vůbec nedopočítám!“

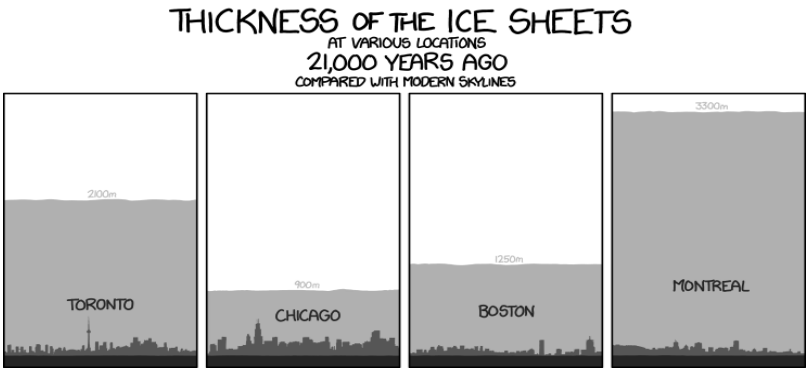
– Alenka

Čísla jsou nezbytnou součástí našeho každodenního života. Velká čísla však nejsou pro většinu z nás příliš pochopitelná. Ta největší, s nimiž se v běžném životě setkáváme, se pohybují v řádu milionů, miliard nebo bilionů. Můžeme se dočíst o milionech lidí žijících v chudobě, miliardách dolarů vynaložených na záchranu bank a bilionech státního dluhu. Přestože je těžké se v těchto titulcích vyznat, s velikostí těchto čísel jsme do jisté míry srozuměni.

Ačkoliv nám miliardy a biliony mohou připadat povědomé, naše intuice při takto velkých číslech již začíná selhávat. Máte představu, jak dlouho byste museli čekat, než uplyne milion / miliarda / bilion vteřin? Jste-li na tom podobně jako já, budete ztraceni, pokud si tato čísla nepřelouskáte do důsledku.

Podívejme se na tento příklad blíže: rozdíl mezi uvedenými hodnotami je nárůst o tři řády: 10^6, 10^9, 10^{12}. Přemýšlet v sekundách není příliš praktické, takže si to převedeme na něco, co nám hlava pobere:

- 10^6: Milion vteřin uplynul během půldruhého týdne.
- 10^9: Jedna miliarda sekund začala před téměř 32 lety.
- 10^{12}: Před jedním bilionem vteřin byl Manhattan pokrytý silnou vrstvou ledu.



15.1 V době před jedním bilionem vteřin.[1] Zdroj: xkcd #1125

Jakmile vstoupíme do oblasti moderní kryptografie přesahující astronomické hranice, naše intuice katastrofálně selhává. Bitcoin je postaven na velkých číslech a praktické nemožnosti je uhodnout. Tato čísla jsou mnohem, mnohem větší než cokoliv, s čím se můžeme setkat v běžném denním životě. O mnoho řádů vyšší. Pochopení toho, jak velká tato čísla skutečně jsou, je zásadní pro celkové pochopení bitcoinu.

Jako konkrétní příklad uveďme SHA-256[2], jednu z hashovacích funkcí[3] používaných v bitcoinu. Je přirozené, že si 256 bitů představíme jako „dvě stě padesát šest“, což není vůbec velké číslo. Číslo v SHA-256 však hovoří o řádových hodnotách – což je něco, s čím si náš mozek neumí dobře poradit.

Délka bitů je sice vhodnou metrikou, ale skutečný význam 256bitového zabezpečení se ztrácí v překladu. Podobně jako u výše uvedených milionů (10^6) a miliard (10^9) jde v případě SHA-256 o hodnotu exponentu (2^{256}).

[1] Jeden bilion vteřin (10^{12}) byl před 31 710 lety. Poslední ledovcové maximum nastalo před 33 000 lety [88]
[2] SHA-256 je součástí rodiny kryptografických hashovacích funkcí SHA-2 vyvinutých Národní bezpečnostní agenturou Spojených států, NSA [97]
[3] V bitcoinu se SHA-256 používá v blokovém hashovacím mechanismu.

Jak přesně je tedy algoritmus SHA-256 silný?

> „SHA-256 je velmi silný. Není to jako postupný krok od MD5 k SHA1. Pokud nedojde k nějakému masivnímu průlomu, může vydržet několik desetiletí."
>
> – Satoshi Nakamoto[4]

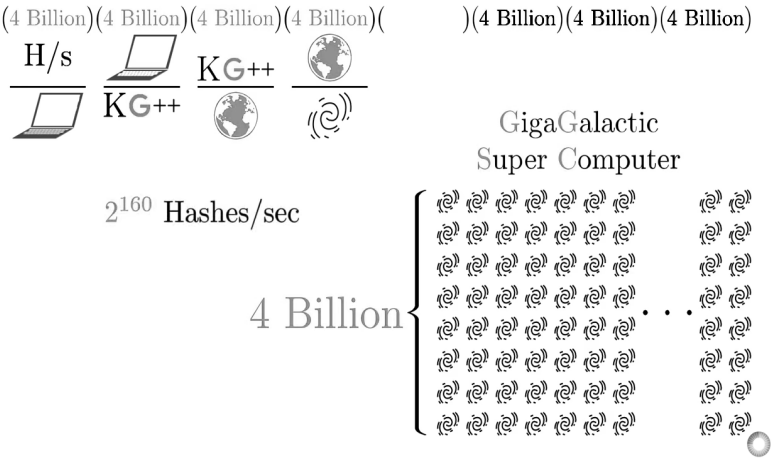
Řekněme si to takto. 2^{256} se rovná následujícímu číslu[5]:

> 115 tredeciliard 792 tredecilionů 89 duodeciliard 237 duodecilionů 316 undeciliard 195 undecilionů 423 noniliard 570 nonilionů 985 oktiliard 8 oktilionů 687 septiliard 907 septilionů 853 sextiliard 269 sextilionů 984 kvintiliard 665 kvintilionů 640 kvadriliard 564 kvadrilionů 39 triliard 457 trilionů 584 biliard 7 bilionů 913 miliard 129 milionů 639 tisíc 936

To je spousta valionů! Představit si takové číslo je v podstatě nemožné. Ve fyzickém světě není nic, s čím by se dalo srovnat.

Je mnohem větší než počet atomů v pozorovatelném vesmíru. Lidský mozek prostě není stvořen k tomu, aby něco takového dokázal pochopit.

[4] Satoshi Nakamoto v odpovědi na otázku o rozporu SHA-256 [54]
[5] Je zapotřebí upozornit na různé systémy v pojmenování vysokých čísel. Zde je použita tzv. dlouhá škála. (pozn. překl.)



15.2 Ilustrace SHA-256 zabezpečení. Originální grafika od Granta Sandersona, popularizátora matematiky z YouTube kanálu 3Blue1Brown.

Jednou z nejlepších vizualizací skutečné síly algoritmu SHA-256 je video[6] Granta Sandersona, příhodně nazvané „Jak bezpečné je 256bitové zabezpečení?“ Krásně ukazuje, jak velký je 256bitový prostor. Udělejte si laskavost a věnujte pět minut jeho zhlédnutí. Stejně jako všechna ostatní videa od *3Blue1Brown* je nejen fascinující, ale také mimořádně dobře zpracované. Varování: Hrozí vám pád do králičí nory matematiky.

Bruce Schneier[7] použil fyzikální limity výpočtů, aby toto číslo uvedl do souvislostí: i kdybychom dokázali vytvořit Dysonovu sféru[8] kolem našeho Slunce a postavit optimální počítač[9] využívající veškerou poskytnutou energii k dokonalému propočítávání bitů, který bychom nechali běžet 100 miliard miliard let, stále bychom měli pouze 25% šanci najít jehlu v 256bitové kupce sena.

[6] Video najdete na https://youtu.be/S9JGmA5_unY
[7] Bruce Schneier. *Schneier on Security* [65]
[8] Dysonova sféra je hypotetická megastruktura, která kompletně obepíná hvězdu a zachycuje vysoké procento její energetické produkce [81]
[9] Viz článek *Landauer's principle* na anglické Wikipedii [87]

> „Tato čísla nemají nic společného s technologií přístrojů, jsou to maximální hodnoty, které dovolí termodynamika. A silně naznačují, že útoky hrubou silou proti 256bitovým klíčům budou neproveditelné, dokud nebudou počítače postaveny z něčeho jiného než z hmoty a nebudou zabírat něco jiného než prostor."
>
> – Bruce Schneier[10]

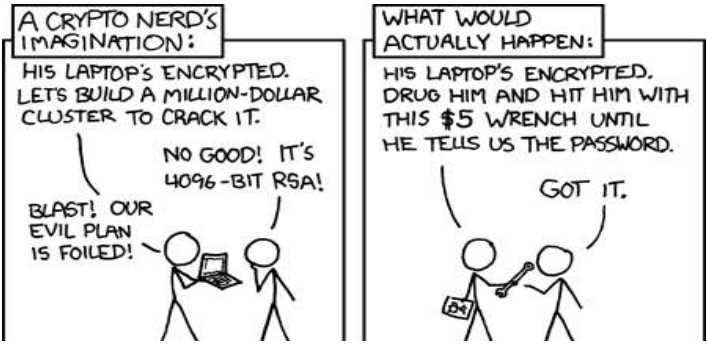
Hloubku tohoto faktu lze jen stěží vyjádřit. Silná kryptografie převrací poměr sil, na který jsme zvyklí v hmotném světě. Nezničitelné věci v reálu neexistují. Použijete-li dostatečnou sílu, budete schopni otevřít jakékoliv dveře, bednu, nebo truhlu s pokladem.

Bitcoinová truhla je velmi odlišná. Je zabezpečena silnou kryptografií, která nepodléhá hrubé síle. A dokud platí základní matematické předpoklady, je hrubá síla to jediné, co máme k dispozici. Ano, je tu také možnost útoku hasákem za 5 dolarů (obrázek 15.3). Ale mučení nebude fungovat proti všem bitcoinovým adresám a kryptografické stěny bitcoinu útokům hrubou silou odolají. I kdybyste se na ně vrhli silou tisíce Sluncí. A to doslova.

Tato skutečnost a její důsledky byly výstižně shrnuty ve výzvě ke kryptografickému zbrojení: „Žádná donucovací síla nikdy nevyřeší matematický problém."

> „Není vůbec samozřejmé, že by svět musel fungovat tímto způsobem. Ale vesmír se na šifrování tak nějak usmívá."
>
> – Julian Assange[11]

[10] Bruce Schneier, *Applied Cryptography* [64]
[11] Julian Assange, *A Call to Cryptographic Arms* [5]



15.3 Útok hasákem za 5 dolarů. Zdroj xkcd 538

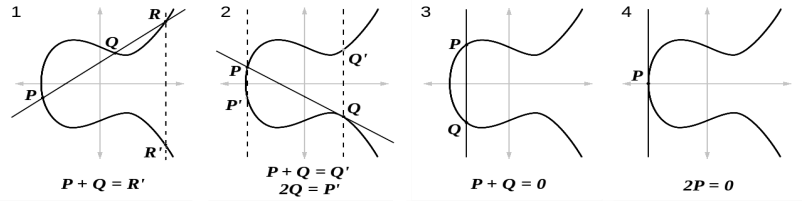
Nikdo zatím s jistotou neví, zda je úsměv vesmíru upřímný, nebo ne. Je možné, že náš předpoklad matematické asymetrie je mylný a zjistíme[12], že P se ve skutečnosti rovná NP, nebo najdeme překvapivě rychlá řešení určitých problémů[13], které v současnosti považujeme za složité. Pokud by tomu tak bylo, kryptografie, jak ji známe, přestane existovat a důsledky by nejspíš změnily svět k nepoznání.

„Vires in Numeris“ = „Síla v číslech“

Vires in numeris není jen chytlavé heslo používané bitcoinery. Uvědomění si, že v číslech se skrývá nezměrná síla, je hluboké. Pochopení této skutečnosti a převrácení stávající rovnováhy sil, které umožňuje, změnilo můj pohled na svět a budoucnost, která nás čeká.

Jedním z přímých důsledků tohoto jevu je skutečnost, že nemusíte nikoho žádat o povolení ke vstupu do bitcoinu. Neexistuje žádná stránka, na které byste se museli zaregistrovat, žádná správcovská organizace ani vládní agentura, které byste museli posílat formuláře se žádostí o povolení. Stačí vygenerovat velké číslo a můžete v podstatě začít. Ústřední autoritou pro zakládání účtů je matematika. A jen bůh ví, kdo ovládá ji.

[12] Více o problému *P versus NP* na Wikipedii [95]
[13] Tzv. diskrétní logaritmus, viz Wikipedia [79]



15.4 Příklady eliptických křivek. Grafika se svolením cc-by-sa Emmanuel Boutet.

Bitcoin je postaven na našem nejlepším porozumění realitě. Ačkoliv je ve fyzice, informatice a matematice stále mnoho otevřených problémů, některými věcmi jsme si celkem jisti. Jednou z takových věcí je, že existuje asymetrie mezi nalezením řešení a ověřením správnosti těchto řešení. Dále to, že k výpočtům je potřeba energie. Jinými slovy: najít jehlu v kupce sena je těžší než ověřit, zda ta špičatá věc ve vaší ruce je skutečně jehla, nebo ne. A najít jehlu vyžaduje práci.

Rozsáhlost prostoru bitcoinových adres je skutečně ohromující. Počet soukromých klíčů ještě více. Je fascinující, jak velká část našeho moderního světa se redukuje na nepravděpodobnost nalezení jehly v nezměrně obrovském stohu. Nyní si tuto skutečnost uvědomuji více než kdy jindy.

Bitcoin mě naučil, že v číslech je síla.

16. Úvahy na téma „Nedůvěřuj, ale ověřuj“

„Nejprve svědectví,“ řekl král, „a potom rozsudek.“

– Lewis Carroll*, Alenka v kraji divů*

Cílem bitcoinu je nahradit konvenční měnu, nebo k ní alespoň poskytnout alternativu. Konvenční měna je vázána na centralizovanou autoritu, ať už mluvíme o zákonném platidle, jako je americký dolar, nebo o moderních herních penězích, jakými jsou V-Bucks ve hře Fortnite. V obou případech jste vázáni důvěrou v centrální moc, která vaše peníze vydává, spravuje a uvádí do oběhu. Bitcoin tato pouta rozvazuje a hlavním problémem, který řeší, je otázka *důvěry*.

„Základním problémem konvenční měny je důvěra, která je nutná k jejímu fungování. […] Je potřeba zavést systém elektronických plateb založený na kryptografických záznamech, nikoliv na důvěře.“

– Satoshi Nakamoto[1]

Bitcoin řeší problém důvěry tím, že je zcela decentralizovaný, bez ústředního serveru nebo důvěryhodných stran. Dokonce ani ne důvěryhodných třetích stran, ale prostě důvěryhodných stran a tečka.

[1] Satoshi Nakamoto, oficiální představení bitcoinu [51] a bitcoinový whitepaper [48]

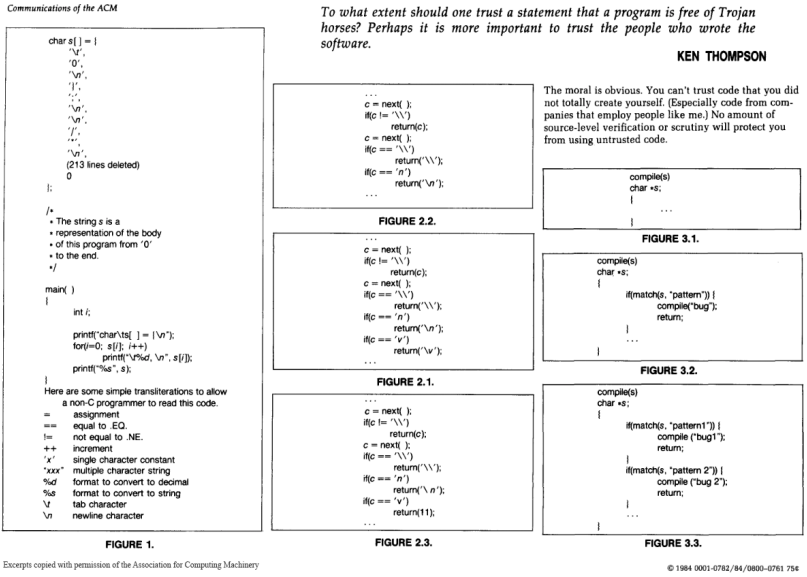
Když neexistuje centrální autorita, není jednoduše komu věřit. Inovací je úplná decentralizace. Právě ona je podstatou odolnosti bitcoinu, důvodem, proč je stále naživu. Decentralizace je také příčinou, proč máme těžbu, uzly, hardwarové peněženky a ano, blockchain. Jediné, čemu musíte „věřit", je, že naše chápání matematiky a fyziky není úplně mimo a že většina těžařů jedná čestně (k čemuž jsou motivováni).

Zatímco v běžném světě platí zásada „důvěřuj, ale prověřuj", u bitcoinu platí zásada „nedůvěřuj, ale ověřuj". Satoshi velmi jasně zdůraznil důležitost odstranění důvěry jak v úvodu, tak v závěru whitepaperu.

> „Závěr: Předložili jsme systém elektronických transakcí, který není závislý na důvěře."
>
> – Satoshi Nakamoto

Všimněte si, že výraz „není závislý na důvěře" je zde použit ve velmi specifickém kontextu. Mluvíme o důvěryhodných třetích stranách, tj. jiných subjektech, kterým věříte, když produkují, drží a zpracovávají vaše peníze. Předpokládá se například, že můžete důvěřovat svému počítači.

Jak ukázal Ken Thompson ve své přednášce při udílení Turingovy ceny, důvěra je ve světě počítačů velmi ošemetná věc. Při spouštění programu musíte důvěřovat nejrůznějšímu softwaru (a hardwaru), jenž by teoreticky mohl program, který se snažíte spustit, škodlivým způsobem změnit. Jak shrnul Thompson ve svých *Úvahách o důvěře v důvěru*: „Poučení je zřejmé. Nemůžete důvěřovat kódu, který jste sami zcela nevytvořili."


Communications of the ACM

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

```
char s[ ] = {
        '\t',
        '0',
        '\n',
        '}',
        ';',
        '\n',
        '\n',
        '/',
        '*',
        '\n',
        (213 lines deleted)
        0
};

/*
 * The string s is a
 * representation of the body
 * of this program from '0'
 * to the end.
 */

main( )
{
        int i;

        printf("char\ts[ ] = {\n");
        for(i=0; s[i]; i++)
                printf("\t%d, \n", s[i]);
        printf("%s", s);
}
```

Here are some simple transliterations to allow a non-C programmer to read this code.

=	assignment
==	equal to .EQ.
!=	not equal to .NE.
++	increment
'x'	single character constant
"xxx"	multiple character string
%d	format to convert to decimal
%s	format to convert to string
\t	tab character
\n	newline character

FIGURE 1.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
...
```

FIGURE 2.2.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
if(c == 'v')
        return('\v');
...
```

FIGURE 2.1.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\ n');
if(c == 'v')
        return(11);
...
```

FIGURE 2.3.

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code.

```
compile(s)
char *s;
{
        ...
}
```

FIGURE 3.1.

```
compile(s)
char *s;
{
        if(match(s, "pattern")) {
                compile("bug");
                return;
        }
        ...
}
```

FIGURE 3.2.

```
compile(s)
char *s;
{
        if(match(s, "pattern1")) {
                compile ("bug1");
                return;
        }
        if(match(s, "pattern 2")) {
                compile ("bug 2");
                return;
        }
        ...
}
```

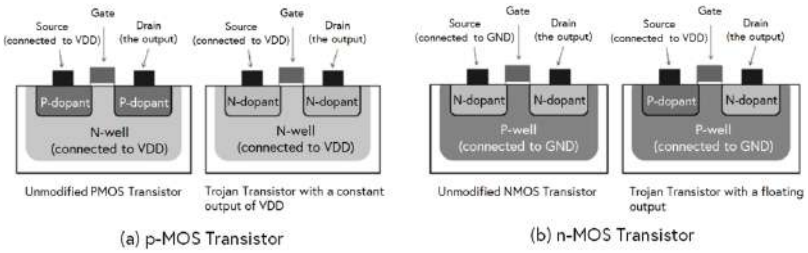
FIGURE 3.3.

16.1 Výňatek ze studie Kena Thompsona *Reflections of Trusting Trust*

Thompson ukázal, že i když máte přístup ke zdrojovému kódu, může být váš kompilátor – nebo jakýkoliv jiný program či hardware pracující s vaším programem – kompromitován a odhalení těchto zadních vrátek bude velmi obtížné. V praxi tedy opravdový systém bez důvěry neexistuje. Veškerý svůj software i veškerý svůj hardware (assemblery, kompilátory, linkery atd.) byste museli vytvořit sami od začátku, bez pomoci jakéhokoliv externího softwaru nebo softwarově podporovaných strojů.

> „Chcete-li upéct jablečný koláč od základu, musíte nejprve vymyslet vesmír."
>
> – Carl Sagan[2]

[2] Carl Sagan. *Kosmos* [63]



16.2 Skryté hardwarové trojské koně na úrovni dopování polovodičů, ilustrace od autorů Becker, Regazzoni, Paar, Burleson.

Hack Kena Thompsona je obzvláště důmyslnou a těžko odhalitelnou formou útoku. Pojďme se tedy krátce podívat na složitě odhalitelná zadní vrátka, která fungují bez úpravy jakéhokoliv softwaru. Výzkumníci našli způsob, jak ohrozit bezpečnostně kritický hardware změnou polarity nečistot v křemíku.[3] Pouhou změnou fyzikálních vlastností látky, ze které jsou vyrobeny počítačové čipy, se jim podařilo kompromitovat kryptograficky bezpečný generátor náhodných čísel. Protože tato změna není vidět, nelze taková zadní vrátka odhalit optickou kontrolou, která je u těchto čipů jedním z nejdůležitějších mechanismů pro odhalení neoprávněné manipulace.

Zní to děsivě? No, i kdybyste byli schopni sestavit vše od nuly, stejně byste museli věřit základní matematice. Museli byste věřit, že secp256k1 je eliptická křivka bez zadních vrátek. Ano, do matematických základů kryptografických funkcí lze vložit škodlivá zadní vrátka a pravděpodobně se to již minimálně jednou stalo. Existují dobré důvody, proč být paranoidní, a skutečnost, že vše od hardwaru přes software až po používané eliptické křivky může mít zadní vrátka[4], patří mezi ně.

> „Nedůvěřuj, ale ověřuj."
>
> – Bitcoineři celého světa

[3] Viz článek *Stealthy Dopant-level Hardware Trojans* [9]
[4] Více v článku *Elliptic-curve cryptography* na Wikipedii [82]

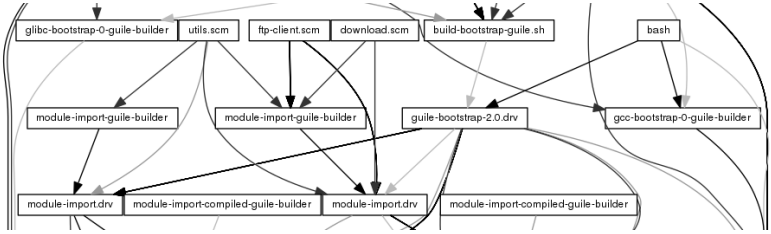
Výše uvedené příklady by měly ilustrovat, že výpočetní technika bez *důvěry* je utopie. Bitcoin je pravděpodobně jediný systém, který se této utopii blíží nejvíce, ale i tak potřebu důvěry *pouze minimalizuje* – jeho cílem je odstranit důvěru všude, kde je to možné. Řetězec důvěry je pravděpodobně nekonečný, protože budete muset věřit také tomu, že výpočet vyžaduje energii, že P se nerovná NP a že se skutečně nacházíte v realitě a nejste uvězněni zlomyslnými agenty v simulaci.

Vývojáři pracují na nástrojích a postupech, které mají zbývající prvky důvěry ještě více minimalizovat. Bitcoinoví developeři například vytvořili Gitian[5], což je metoda distribuce softwaru pro vytváření reprodukovatelných sestav. Myšlenka spočívá v tom, že pokud je více vývojářů schopno reprodukovat identické binární soubory, snižuje se pravděpodobnost zneužití. Efektní zadní vrátka nejsou jediným vektorem útoku. Reálnou hrozbou je i prosté vydírání nebo násilné vymáhání. Stejně jako v případě hlavního protokolu se k minimalizaci důvěry využívá decentralizace.

Stále jsou vyvíjeny různé snahy o zlepšení problému bootstrappingu (což je v podstatě variace na odvěké dilema slepice vs. vejce), na který tak brilantně poukázal hack Kena Thompsona. Jednou z takových snah je Guix[6] (vyslovuje se stejně jako anglické slovo *geeks*), který používá funkčně deklarovanou správu balíčků, což vede přímo k sestavám reprodukovatelným bit po bitu. Výsledkem je, že už nemusíte důvěřovat žádným serverům poskytujícím software, neboť si můžete ověřit, že do předkládané binární verze nebylo zasahováno, a to tím, že ji sestavíte od začátku.

Nedávno byla do zdrojového kódu sloučena žádost o přijetí změn (merged pull request), jejímž cílem bylo začlenit Guix do procesu sestavování bitcoinu.[7]

[5] https://gitian.org/
[6] https://guix.gnu.org
[7] Viz pull request 15277 na bitcoin core https://github.com/bitcoin/bitcoin/pull/15277



16.3 Co bylo dřív – slepice, nebo vejce?

Bitcoin naštěstí nespoléhá na jediný algoritmus nebo kus hardwaru. Jedním z důsledků radikální decentralizace bitcoinu je distribuovaný bezpečnostní model. Ačkoliv výše popsaná zadní vrátka nelze brát na lehkou váhu, nemůžeme předpokládat, že by byla kompromitována každá softwarová peněženka, každá hardwarová peněženka, každá kryptografická knihovna, každá implementace uzlu a každý kompilátor každého jazyka. Je to možné, ale velmi nepravděpodobné.

Je třeba poznamenat, že soukromý klíč můžete vygenerovat, aniž byste se museli spoléhat na výpočetní hardware nebo software. Můžete si několikrát hodit mincí, i když v závislosti na použité minci a stylu házení nemusí být tento zdroj náhodnosti dostatečně náhodný. Existuje proto důvod, proč úložné protokoly, jako je Glacier[8], doporučují používat jako jeden ze dvou zdrojů entropie hrací kostky třídy přesnosti určené pro kasina.

Bitcoin mě donutil zamyslet se nad tím, co vlastně obnáší nevěřit nikomu. Upozornil mě na problém bootstrappingu a na implicitní řetězec důvěry při vývoji a provozování software. Uvědomil jsem si také mnoho způsobů, jakými lze software a hardware kompromitovat.

Bitcoin mě naučil nedůvěřovat, ale ověřovat.

[8] https://glacierprotocol.org

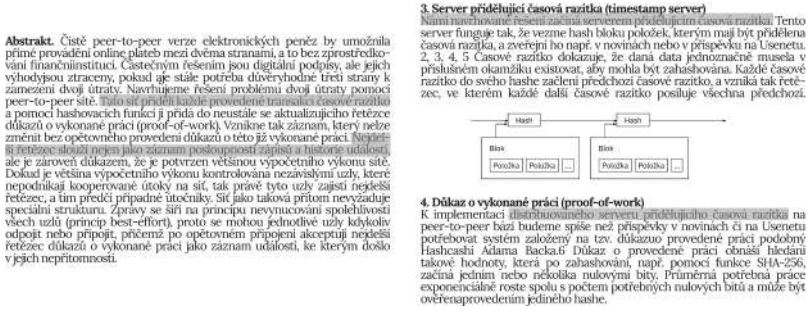
17. Určování času vyžaduje práci

„Jeje! Jeje! Přijdu pozdě.“

– Bílý králík

Často se uvádí, že bitcoiny se těží tak, že tisíce počítačů pracují na řešení velmi složitých matematických problémů. Je třeba vyřešit určité úlohy, a pokud spočítáte správnou odpověď, „vyrobíte“ tím bitcoin. Tento zjednodušený pohled na těžbu bitcoinů je sice možná srozumitelnější, ale poněkud se míjí s podstatou věci. Bitcoiny se nevyrábějí ani nevytvářejí a celé to utrpení ve skutečnosti nespočívá v řešení konkrétních matematických úloh. A navíc ta matematika ani není nijak zvlášť složitá. Co je složité, je *určování* času v decentralizovaném systému.

Jak je vysvětleno ve whitepaperu, systém důkazu o vykonané práci (neboli těžba) je způsob, jak implementovat distribuovaný server časových razítek.



Abstrakt. Čistě peer-to-peer verze elektronických peněz by umožnila přímé provádění online plateb mezi dvěma stranami, a to bez zprostředkování finančníinstituci. Částečným řešením jsou digitální podpisy, ale jejich výhodyjsou ztraceny, pokud aje stále potřeba důvěryhodné třetí strany k zamezení dvojí útraty. Navrhujeme řešení problému dvojí útraty pomocí peer-to-peer sítě. Tato síť přidělí každé provedené transakci časové razítko a pomocí hashovacích funkcí ji přidá do neustále se aktualizujícího řetězce důkazů o vykonané práci (proof-of-work). Vznikne tak záznam, který nelze změnit bez opětovného provedení důkazů o této již vykonané práci. Nejdelší řetězec slouží nejen jako záznam posloupnosti zápisů a historie událostí, ale je zároveň důkazem, že je potvrzen většinou výpočetního výkonu sítě. Dokud je většina výpočetního výkonu kontrolována nezávislými uzly, které nepodnikají kooperované útoky na síť, tak právě tyto uzly zajistí nejdelší řetězec, a tím předčí případné útočníky. Síť jako taková přitom nevyžaduje speciální strukturu. Zprávy se šíří na principu nevynucování spolehlivosti všech uzlů (princip best-effort), proto se mohou jednotlivé uzly kdykoliv odpojit nebo připojit, přičemž po opětovném připojení akceptují nejdelší řetězec důkazů o vykonané práci jako záznam událostí, ke kterým došlo v jejich nepřítomnosti.

3. Server přidělující časová razítka (timestamp server)

Námi navrhované řešení začíná serverem přidělujícím časová razítka. Tento server funguje tak, že vezme hash bloku položek, kterým mají být přidělena časová razítka, a zveřejní ho např. v novinách nebo v příspěvku na Usenetu. 2, 3, 4, 5 Časové razítko dokazuje, že daná data jednoznačně musela v příslušném okamžiku existovat, aby mohla být zahashována. Každé časové razítko do svého hashe začlení předchozí časové razítko, a vzniká tak řetězec, ve kterém každé další časové razítko posiluje všechna předchozí.

4. Důkaz o vykonané práci (proof-of-work)

K implementaci distribuovaného serveru přidělujícího časová razítka na peer-to-peer bázi budeme spíše než příspěvky v novinách či na Usenetu potřebovat systém založený na tzv. důkazuo provedené práci podobný Hashcashi Adama Backa.6 Důkaz o provedené práci obnáší hledání takové hodnoty, která po zahashování, např. pomocí funkce SHA-256, začíná jedním nebo několika nulovými bity. Průměrná potřebná práce exponenciálně roste spolu s počtem potřebných nulových bitů a může být ověřenaprovedením jediného hashe.

17.1 Výňatky z whitepaperu. Říkal někdo timechain?

Když jsem se poprvé seznamoval s tím, jak bitcoin funguje, také jsem si myslel, že důkaz o vykonané práci (proof-of-work) je neefektivní a nehospodárný. Po nějaké době jsem svůj pohled na energetickou spotřebu bitcoinu začal měnit.[1] Zdá se, že technologie důkazu o vykonané práci je ještě dnes, v roce 13 AB (After Bitcoin), široce nepochopena.

Vzhledem k tomu, že problémy, které je třeba v rámci důkazu o vykonané práci vyřešit, jsou uměle vytvořeny, domnívá se mnoho lidí, že jde o zbytečnou práci. Pokud se soustředíme čistě na samotné výpočty, je to pochopitelný závěr. V bitcoinu však nejde o výpočty.

Jde o to se nezávisle dohodnout na posloupnosti událostí.

Důkaz o vykonané práci je systém, ve kterém každý může potvrdit, co, a v jakém pořadí, se událo. Toto nezávislé ověření vede ke konsensu, tedy vzájemné dohodě více stran, o tom, co kdo vlastní.

V radikálně decentralizovaném prostředí nedisponujeme luxusem absolutního času. Jakékoliv hodiny by zavedly důvěryhodnou třetí stranu, centrální bod v systému, na který by bylo nutno spoléhat a který by mohl být napaden. „Načasování je zásadním problémem," jak upozorňuje Grisha Trubetskoy.[2] A Satoshi tento problém geniálně vyřešil zavedením decentralizovaných hodin prostřednictvím řetězce bloků důkazu o vykonané práci. Všichni se předem dohodnou, že řetězec s největším množstvím kumulované práce je zdrojem pravdy.

A to je z definice tím, co se skutečně stalo. Této dohodě se dnes říká Nakamotův konsensus.

[1] Gigi. *Bitcoin's Energy Consumption – A shift in perspective* [29]
[2] Grisha Trubetskoy. *Blockchain Proof-of-Work Is a Decentralized Clock* [72]

> „Tato síť přidělí každé provedené transakci časové razítko a pomocí hashovacích funkcí ji přidá do neustále se aktualizujícího řetězce [... který...] je zároveň důkazem, že je potvrzen většinou výpočetního výkonu sítě."
>
> – Satoshi Nakamoto[3]

Bez konzistentního způsobu určování času nelze jednoznačně rozlišit, co se stalo dříve a co později. Spolehlivé uspořádání je nemožné. Jak bylo uvedeno výše, Nakamotův konsensus je způsob, jak bitcoin konzistentně určuje čas. Motivační struktura systému vytváří pravděpodobnostní, decentralizované hodiny tím, že využívá jak chamtivosti, tak sobeckého zájmu konkurujících si účastníků. Skutečnost, že tyto hodiny jsou nepřesné, je irelevantní, protože pořadí událostí je nakonec určeno jednoznačně a může je ověřit kdokoliv.

Technologie důkazu o provedené práci radikálně decentralizuje samotnou práci i její ověření. Každý se může libovolně připojit i odejít a každý může kdykoliv vše validovat. A nejen to, každý může ověřit stav systému *individuálně*, aniž by se při tom musel spoléhat na někoho jiného.

Pochopení principu důkazu o provedené práci vyžaduje čas. Je často neintuitivní, a i když jsou pravidla jednoduchá, tak vedou k poměrně složitým jevům. Mně pomohla změna pohledu na těžbu. Užitečná, nikoliv zbytečná. Ověřování, a ne výpočty. Čas, ne bloky.

Bitcoin mě naučil, že určování času je ošemetné, zejména pokud se nacházíte v decentralizovaném prostředí.

[3] Satoshi Nakamoto, *Bitcoinový whitepaper* [48]

18. Postupujte pomalu a nic nerozbíjejte

A dál pluje i člun. Zvolna končí den.
Vesluji sám. Však šťasten. Okouzlen.

– Lewis Carroll*, Alenka v kraji divů*

Možná je to už mrtvá mantra, ale většina technologického světa stále funguje podle hesla „Buď rychlý a rozbíjej věci." Myšlenka, že nezáleží na tom, jestli se vám něco povede hned napoprvé, je základním pilířem mentality „Selhávej brzy, selhávej často." Úspěch se měří růstem, takže dokud rostete, je vše v pořádku. Pokud něco napoprvé nefunguje, jednoduše změníte směr a pokračujete jinak. Jinými slovy: házejte dostatečné množství sraček proti zdi a uvidíte, co se přilepí.

Bitcoin je velmi odlišný. Je jiný už z podstaty. Je rozdílný z nutnosti. Jak upozornil Satoshi, o elektronickou měnu se lidé pokoušeli již mnohokrát a všechny předchozí pokusy ztroskotaly na tom, že existovala hlava, kterou bylo možné useknout. Inovace bitcoinu spočívá v tom, že je zvířetem bez hlavy.

„Mnoho lidí automaticky odmítá elektronickou měnu jako ztracený případ kvůli všem společnostem, které od 90. let zkrachovaly. Doufám, že je zřejmé, že to byla pouze centrálně řízená povaha těchto systémů, která je odsoudila k zániku."

– Satoshi Nakamoto[1]

[1] Satoshi Nakamoto, v odpovědi Seppovi Hasslbergerovi [52]

Jedním z důsledků této radikální decentralizace je přirozená rezistence vůči změnám. Na základní vrstvě bitcoinu nefunguje a nikdy nebude fungovat heslo „Buď rychlý a rozbíjej věci“. I kdyby něco takového bylo žádoucí, nebylo by to možné bez přesvědčení každého účastníka, aby změnil své jednání. V tom spočívá distribuovaný konsensus. Taková je povaha bitcoinu.

> „Podstata bitcoinu spočívá v tom, že vydáním verze 0.1 byla již natrvalo určena jeho základní koncepce.“
>
> – Satoshi Nakamoto[2]

To je jedna z mnoha paradoxních vlastností bitcoinu. Všichni si myslíme, že každý software lze snadno měnit. Ale povaha této bestie způsobuje, že změnit ji je zatraceně těžké.

Jak krásně ukazuje Hasu v článku o společenské smlouvě bitcoinu, změna pravidel bitcoinu je možná pouze *navržením* změny a následným *přesvědčením* všech uživatelů, aby tuto změnu přijali. Díky tomu je bitcoin vůči změnám velmi odolný, přestože se jedná o software.

Tato odolnost je jednou z nejdůležitějších vlastností bitcoinu. Kritické softwarové systémy musí být antifragilní, což je zajištěno provázaností sociální a technické vrstvy bitcoinu. Peněžní soustavy jsou ze své podstaty konkurenční, a jak víme již tisíce let, v nepřátelském prostředí jsou nezbytné pevné základy.

> „Tu spadl příval, přihnaly se vody, zvedla se vichřice, a vrhly se na ten dům; ale nepadl, neboť měl základy na skále.“
>
> – Matouš 7,25 (Český ekumenický překlad)

[2] Satoshi Nakamoto v odpovědi Gavinovi Andersonovi [52]

V tomto podobenství o domu na skále bitcoin patrně není domem. Je skálou. Neměnný, nehybný, poskytující základy pro nový finanční systém.

Jak geologové vědí, horniny a skalní útvary se neustále pohybují a vyvíjejí. Stejně tak se děje i v případě bitcoinu. Stačí jen vědět, kam a jak se dívat.

Zavedení *pay to script hash*[3] a *Segregated Witness*[4] jsou důkazem, že pravidla bitcoinu lze změnit, pokud je dostatečný počet uživatelů přesvědčen, že přijetí dané změny je pro síť přínosem. Druhá jmenovaná změna umožnila vývoj sítě *lightning network*[5], jednoho z domů budovaných na skále bitcoinu. Budoucí vylepšení, jako jsou *Schnorrovy podpisy*[6], zvýší efektivitu a soukromí, stejně jako skripty (čti: smart kontrakty), které budou díky *taprootu*[7] k nerozeznání od běžných transakcí. Moudří stavitelé skutečně staví na pevných základech.

Satoshi nebyl moudrým stavitelem jen z technologického hlediska. Chápal také, že je třeba činit i moudrá ideologická rozhodnutí.

> „Open source znamená, že kdokoliv může kód nezávisle kontrolovat. Kdyby byl kód uzavřený, nikdo by nemohl ověřit jeho bezpečnost. Myslím, že pro program tohoto typu je nezbytné, aby byl otevřený."
>
> – Satoshi Nakamoto

---

[3] Pay to script hash (P2SH) transakce byly standardizované ve vylepšovacím návrhu (BIP 16). Umožňují posílání transakcí na skriptový hash (adresy začínající na 3) namísto na hash veřejného klíče (adresy začínající na 1) [15]

[4] Segregated Witness (zkracováno jako SegWit) je implementovaná aktualizace protokolu, která má za cíl zajistit ochranu před zfalšováním transakcí a zvýšit kapacitu bloku. SegWit odděluje svědka (witness) ze seznamu vstupů [16]

[5] https://lightning.network

[6] Pieter Wuille. *Schnorr Signatures for secp256k1* [59]

[7] Gregory Maxwell. Taproot. *Privacy preserving switchable scripting* [31]

Otevřenost je pro bezpečnost klíčová a je neodmyslitelnou součástí open source a hnutí svobodného softwaru. Jak Satoshi zdůraznil, bezpečnostní protokoly a kód, který je implementuje, musí být otevřené – neexistuje bezpečnost skrze neznalost (security through obscurity). Další výhoda opět souvisí s decentralizací: kód, který lze volně spouštět, studovat, upravovat, kopírovat a distribuovat, zajišťuje, že se rozšíří široko daleko.

Radikálně decentralizovaná povaha je to, co nutí bitcoin pohybovat se pomalu a s rozmyslem. Síť uzlů, z nichž každý je řízen nezávislým jednotlivcem, je ze své podstaty odolná vůči změnám – ať už jsou škodlivé, nebo ne. Bez možnosti aktualizace uživatelům vnutit je jediným způsobem, jak zavést změny, pomalé přesvědčování každého jednotlivého uživatele, aby změnu přijal. Právě tento proces zavádění a nasazování změn bez ústředního řízení činí síť neuvěřitelně odolnou vůči škodlivým změnám. Zároveň však, oproti centralizovanému prostředí, znesnadňuje opravu dysfunkčních součástí. Což je důvodem, proč se všichni snaží především nic nerozbíjet.

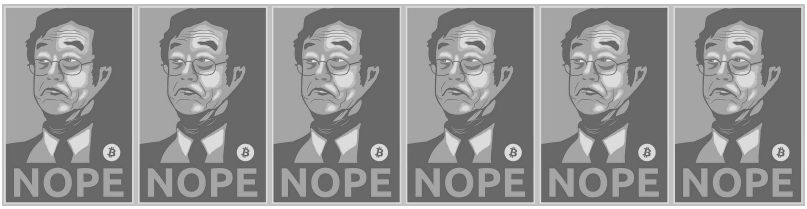
Bitcoin mě naučil, že pomalý postup je jednou z jeho vlastností, nikoliv chybou.

19. Soukromí není mrtvé

> *Hráči hráli všichni najednou, nečekali na své pořadí a v jednom kuse se hádali a rvali o ježky; netrvalo dlouho, a Královna se tak rozlítila, že každou chvilku dupla a křikla: „Srazte mu hlavu!“ nebo zas: „Srazte jí hlavu!“*
>
> – Lewis Carroll, *Alenka v kraji divů*

Pokud máme věřit odborníkům, tak soukromí je mrtvé od 80. let minulého století. Pseudonymní vynález bitcoinu a další události v nedávné historii však ukazují, že tomu tak není. Soukromí žije, byť uniknout státnímu šmírování není v žádném případě snadné.

Satoshi se usilovně snažil zahladit stopy a utajit svou totožnost. Po třinácti letech se stále neví, zda byl Satoshi Nakamoto jediná osoba, skupina lidí, muž, žena nebo umělá inteligence cestující časem, která se sama spustila, aby ovládla svět. Konspirační teorie stranou, Satoshi se rozhodl identifikovat jako japonský muž, a tak nic nepředjímám, a budu o něm hovořit v mužském rodě.



19.1 Nejsem Dorian Nakamoto

Ať už je jeho skutečná identita jakákoliv, Satoshi ji úspěšně skrýval. Dal povzbudivý příklad všem, kteří chtějí zůstat v anonymitě: na internetu si lze uchovat soukromí.

> „Šifrování funguje. Správně implementované silné šifrovací systémy jsou jednou z mála věcí, na které se můžete spolehnout."
>
> – Edward Snowden[1]

Satoshi nebyl prvním pseudonymním nebo anonymním vynálezcem a nebude ani posledním. Někteří tento pseudonymní styl publikování přímo napodobili, jako například Tom Elvis Jedusor známý z projektu MimbleWimble[2], zatímco jiní publikovali pokročilé matematické důkazy a přitom zůstali zcela anonymní.[3]

Je to zvláštní nový svět, ve kterém žijeme. Svět, kde je identita volitelná, příspěvky jsou přijímány na základě kvality a lidé mohou svobodně spolupracovat a obchodovat. Bude trvat nějakou dobu, než se s těmito novými paradigmaty sžijeme, ale pevně věřím, že to všechno má potenciál změnit svět k lepšímu.

Všichni bychom si měli připomenout, že soukromí je základním lidským právem. A dokud budou lidé tato práva uplatňovat a bránit, boj o soukromí ještě zdaleka neskončil.

Bitcoin mě naučil, že soukromí není mrtvé.

[1] Edward Snowden, odpovědi na čtenářské otázky [66]
[2] Tom Elvis Jedusor. *MimbleWimble* Origin [71]
[3] Studie *A lower bound on the length of the shortest superpattern* [3]

20. Cypherpunkeři píší kód

„*Je vidět, že si něco vymýšlíš.*“

– Holubice

Stejně jako mnoho jiných skvělých nápadů, se ani bitcoin neobjevil z ničeho nic. Vznikl využitím a zkombinováním mnoha inovací a objevů v matematice, fyzice, informatice a dalších oborech. Ačkoliv je nepochybně géniem, nebyl by Satoshi schopen bitcoin vynalézt bez velikánů, na jejichž ramenou stál.

„Kdo si jen přeje a doufá, nezasahuje aktivně do běhu událostí a do utváření vlastního osudu.“

– Ludwig Von Mises

Jedním z těchto velikánů je Eric Hughes, jeden ze zakladatelů cypherpunkového hnutí a autor *cypherpunkového manifestu*. Je těžké si představit, že by Satoshi nebyl tímto manifestem ovlivněn. Hovoří se v něm o mnoha věcech, které bitcoin umožňuje a využívá, jako jsou přímé a soukromé transakce, elektronické peníze a hotovost, anonymní systémy a obrana soukromí pomocí kryptografie a digitálních podpisů.

> „Ochrana soukromí je pro otevřenou společnost v elektronickém věku nutností. [...] Protože si přejeme soukromí, musíme zajistit, aby každá strana transakce věděla pouze to, co je pro danou transakci přímo nezbytné. [...] Proto soukromí v otevřené společnosti vyžaduje anonymní transakční systémy. Dosud byla takovým systémem především hotovost. Anonymní transakční systém není tajným transakčním systémem. [...] My, cypherpunkeři, se věnujeme budování anonymních systémů. Své soukromí bráníme pomocí kryptografie, anonymních e-mailů, digitálních podpisů a elektronických peněz. Cypherpunkeři píší kód."
>
> – Eric Hughes[1]

Cypherpunkeři nenacházejí útěchu v nadějích a přáních. Aktivně zasahují do běhu událostí a utvářejí svůj vlastní osud. Cypherpunkeři píší kód.

A tak si Satoshi v duchu pravého cypherpunkového stylu sedl a začal psát kód. Kód, který vzal abstraktní myšlenku a dokázal světu, že je skutečně funkční. Kód, který zasadil semínko nové ekonomické reality. Díky tomuto kódu si každý může ověřit, že tento nový systém opravdu funguje, a zhruba každých 10 minut bitcoin světu dokazuje, že stále žije.

Aby se ujistil, že jeho inovace překoná hranice pouhé fantazie a stane se realitou, napsal Satoshi kód implementující jeho nápad ještě před sepsáním whitepaperu. Dbal také na to, aby vydání neodkládal donekonečna. Koneckonců „vždycky se najde ještě jedna věc, kterou je třeba udělat".[2]

[1] Eric Hughes, *A Cypherpunk's Manifesto* [37]
[2] "We shouldn't delay forever until every possible feature is done" – Satoshi Nakamoto [55]

```
map<uint256, CBlockIndex*> mapBlockIndex;
const uint256 hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
CBlockIndex* pindexGenesisBlock = NULL;
int nBestHeight = -1;
uint256 hashBestChain = 0;
CBlockIndex* pindexBest = NULL;
⋮
int64 CBlock::GetBlockValue(int64 nFees) const
{
    int64 nSubsidy = 50 * COIN;

    // Subsidy is cut in half every 4 years
    nSubsidy >>= (nBestHeight / 210000);

    return nSubsidy + nFees;
}

unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
{
    const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
    const unsigned int nTargetSpacing = 10 * 60;
    const unsigned int nInterval = nTargetTimespan / nTargetSpacing;

    // Genesis block
    if (pindexLast == NULL)
        return bnProofOfWorkLimit.GetCompact();
```

20.1 Ukázka kódu z bitcoinu verze 0.1.0

> „Musel jsem nejprve napsat celý kód, abych mohl přesvědčit sám sebe, že dokážu vyřešit každý problém. Až pak jsem napsal ten dokument.“
>
> – Satoshi Nakamoto[3]

V dnešním světě nekonečných slibů a jejich pochybného uskutečňování bylo takového odhodlaného budování zoufale zapotřebí. Buďte cílevědomí, přesvědčte se, že problémy skutečně dokážete vyřešit, a realizujte řešení. Všichni bychom se měli snažit být trochu více cypherpunkoví.

Bitcoin mě naučil, že cypherpunkeři píší kód.

[3] Satoshi Nakamoto, v e-mailové odpovědi Re: Bitcoin P2P e-cash paper [49]

21. Metafory o budoucnosti bitcoinu

... vždycky to zajímavě dopadne.

– Lewis Carroll*, Alenka v kraji divů*

V posledních několika desetiletích se ukázalo, že inovace v technologiích nemají lineární trend. Ať už věříte v technologickou singularitu, nebo ne, je nepopiratelné, že pokrok je v mnoha oblastech exponenciální. A nejen to, rychlost, s jakou jsou technologie přijímány, neustále stoupá, a než se nadějete, křoví na školním dvoře je pasé a vaše děti místo něj používají Snapchat. Exponenciální křivky mají tendenci vás profackovat mnohem dříve, než si všimnete jejich růstu.

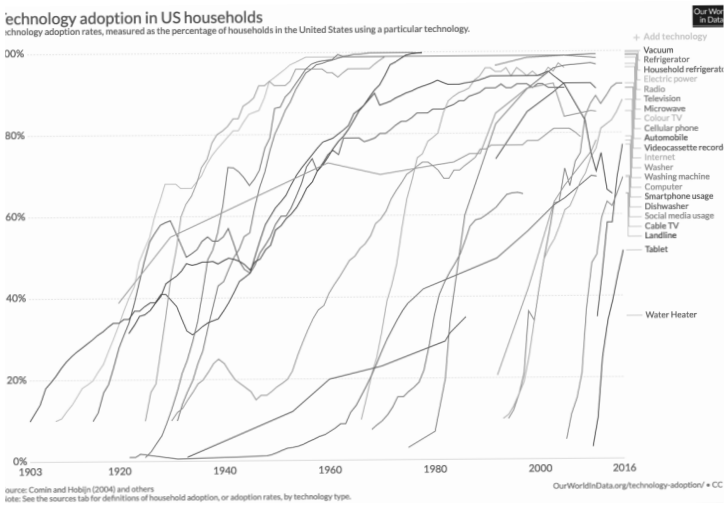
Bitcoin je exponenciální technologie postavená na exponenciálních technologiích. Web *Our World in Data*[1] krásně ukazuje rostoucí rychlost přijímání technologií, počínaje rokem 1903, kdy byly zavedeny pevné telefonní linky (viz obrázek 21.1). Pevné linky, elektřina, počítače, internet, chytré telefony – to vše se v oblastech cena-výkon a adopce vyvíjí podle exponenciálních trendů. Bitcoin také.[2]

Bitcoin nemá pouze jeden, ale vícero síťových efektů[3], z nichž všechny vedou k exponenciálnímu růstu v příslušné oblasti: cena, uživatelé, bezpečnost, vývojáři, podíl na trhu a globální adopce.

Bitcoin přežil své dětství a každým dnem roste na více frontách. Je pravda, že jeho technologie ještě nedosáhla zralosti. Možná se nachází

[1] https://ourworldindata.org
[2] Jeff Desjardins. *The Rising Speed of Technological Adoption* [22]
[3] Trace Mayer, *The Seven Network Effects of Bitcoin* [43]

ve fázi dospívání. Ale je-li technologie exponenciální, je cesta od obskurnosti k všudypřítomnosti rychlá.



21.1 Bitcoin je doslova mimo měřítka.

Ve své TED přednášce v roce 2003 použil Jeff Bezos elektřinu coby metaforu budoucnosti webu.[4] Všechny tři fenomény – elektřina, internet a bitcoin – jsou základními technologiemi, sítěmi, které *umožňují* vznik dalších věcí. Jsou z povahy věci infrastrukturou, na které je možno stavět.

Elektřinu tu máme již nějakou dobu. Považujeme ji za nedílnou součást naší společnosti. Internet je o něco mladší, ale většina lidí ho už také bere jako samozřejmost. Bitcoin je starý třináct let a do povědomí veřejnosti vstoupil během posledního cyklu. Za běžnou věc ho považují jen jeho nejstarší uživatelé. S přibývajícím časem bude stále více lidí vnímat bitcoin jako něco, co tu s námi prostě a jednoduše je.[5]

[4] http://bit.ly/bezos-web
[5] Tento jev je známý jako *Lindy Effect*. Je to teorie, která tvrdí, že budoucí životnost některých věcí nepodléhajících zkáze, jako je technologie nebo myšlenka, je úměrná jejich současnému stáří. Takže každé další období přežití prodlužuje celkovou životnost [89]

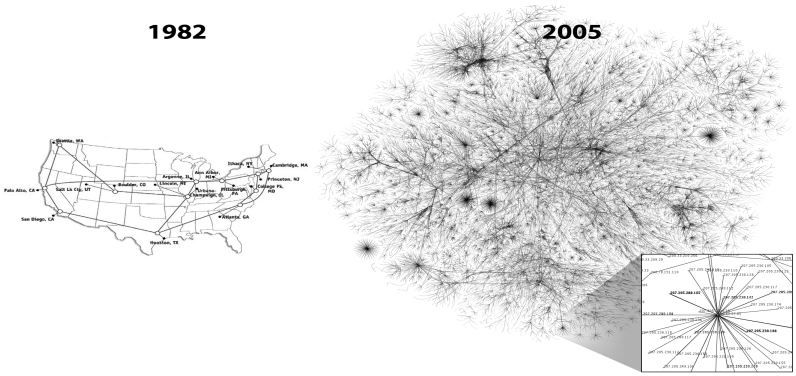
21.2 Mobilní telefon, cca 1965 vs. 2019

V roce 1994 byl internet stále ještě matoucí a nejasný. Při sledování starého záznamu pořadu Today Show je zřejmé, že to, co dnes působí přirozeně a intuitivně, tehdy takové nebylo. Bitcoin je pro většinu lidí stále matoucí a cizí, ale stejně jako je internet samozřejmostí pro digitální generaci, bude utrácení a štosování satů přirozené pro bitcoinovou generaci budoucnosti.

> „Budoucnost už je tady, jen není rovnoměrně distribuována."
>
> – William Gibson[6]

V roce 1995 používalo internet přibližně 15 % dospělých Američanů. Historické údaje Pew Research Center[7] ukazují, jak se internet provázal s našimi životy. Podle spotřebitelského průzkumu společnosti Kaspersky Lab[8] v roce 2018 použilo 13 % respondentů k placení za zboží bitcoin a jeho klony. Ačkoliv platby nejsou jediným způsobem využití bitcoinu, je to určitý ukazatel toho, kde se nacházíme v porovnání s dobou internetovou: na začátku až v polovině 90. let minulého století.

[6] William Gibson, *The Science in Science Fiction* [28]
[7] Susannah Fox; Lee Rainie. *How the internet has woven itself into American life* [27]
[8] Kaspersky Lab. From festive fun to password panic: Managing money online this Christmas [40]



21.3 Internet, 1982 vs 2005. Zdroj: cc-by Merit Network, Inc. a Barrett Lyon, Opte Project

V roce 1997 Jeff Bezos v dopise akcionářům[9] prohlásil, že „toto je první den internetu“, čímž odkryl obrovský nevyužitý potenciál internetu, a tedy i své společnosti. Bez ohledu na to, který den je prvním dnem bitcoinu, ohromné množství nevyužitého potenciálu je jasné snad i tomu nejméně zasvěcenému pozorovateli.

První bitcoinový uzel byl spuštěn v roce 2009, když Satoshi vytěžil první, tzv. *genesis blok*[10] a uvolnil software do světa. Nebyl však dlouho sám. Hal Finney byl jedním z prvních lidí, kteří se k projektu přidali a připojili se k síti. O třináct let později, v době překládání tohoto článku, běží bitcoin na cca 50 000[11] uzlech.

Základní vrstva protokolu není jedinou věcí, která exponenciálně roste. Ještě rychleji roste síť lightning network, technologie druhé vrstvy.

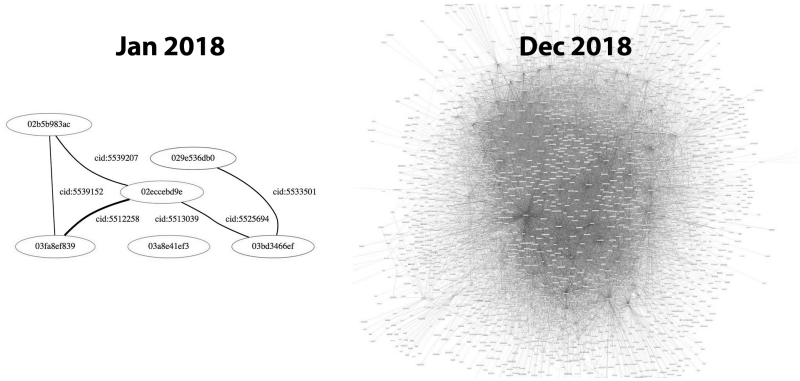
[9] Jeff Bezos. *To our shareholders* [11]
[10] Genesis blok je prvním blokem bitcoinového blockchainu. Moderní verze bitcoinu ho označuje jako blok 0, ačkoliv rané verze ho označovaly jako blok 1. Genesis blok je většinou pevně zakomponován do softwaru aplikace, která využívá bitcoinový blockchain. Jedná se o specifický případ, protože tento blok neobsahuje referenci na blok předchozí a vytváří tak neutratitelné prostředky. Parametr *coinbase* vedle základních dat obsahuje náledující text: *“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”* [14]
[11] https://bit.ly/luke-nodecount

21.4 Hal Finney je autorem prvního tweetu zmiňujícího bitcoin, z ledna 2009

V lednu 2018 měla lightning network 40 uzlů a 60 kanálů.[12] V dubnu 2019 se rozrostla na více než 4 000 uzlů a přibližně 40 000 kanálů. Mějme na paměti, že se stále jedná o experimentální technologii, kde může docházet a dochází ke ztrátám prostředků. Přesto je trend jasný: tisíce lidí ji bezstarostně a dychtivě využívají.

Vzhledem k tomu, že jsem zažil raketový vzestup webu, jsou pro mě paralely mezi internetem a bitcoinem očividné. Obojí jsou síťové a exponenciální technologie, které otevírají nové možnosti, nová odvětví a nové způsoby života. Stejně jako byla elektřina nejlepší metaforou pro pochopení toho, kam směřuje internet, může být internet nejlepší metaforou k pochopení směřování bitcoinu. Nebo řečeno slovy Andrease Antonopoulose: „Bitcoin je internet peněz.“ Tyto metafory jsou skvělou připomínkou toho, že historie se sice neopakuje, ale často se rýmuje.

[12] Wilma Woo. *'Unfairly Cheap' Lightning Network Mainnet Hits 40 Nodes, 60 Channels* [103]



21.5 Lightning Network, leden 2018 vs prosinec 2018. Zdroj: Jameson Lopp

Exponenciální technologie jsou těžko uchopitelné a často podceňované. Přestože se o ně intenzivně zajímám, neustále mě překvapuje tempo jejich pokroku a inovací. Sledovat růst ekosystému bitcoinu je jako sledovat zrychlený vzestup internetu. Je to strhující.

Moje výprava za smyslem bitcoinu mě zavedla na stezky historie hned v několika směrech. Součástí cesty bylo i pochopení starověkých společenských struktur, peněz minulosti a vývoje komunikačních sítí. Od ruční sekery až po chytrý telefon – technologie nepochybně náš život mnohokrát proměnily. Obzvláště transformující jsou síťové technologie: písmo, silnice, elektřina, internet. Všechny tyto sítě změnily svět k nepoznání. Bitcoin změnil ten můj a bude i nadále měnit mysl a srdce těch, kteří se ho odhodlají využívat.

Bitcoin mě naučil, že pochopení minulosti je nezbytné pro pochopení jeho budoucnosti. Budoucnosti, která právě začíná...

Závěrečné zamyšlení

Získané poznatky

> *Myš se na ni podívala zvědavě a jako by na ni jedním očkem mrkla, ale nic neříkala. „Začni od začátku," řekl vážně Král, „a čti až do konce; potom přestaň."*
>
> – Lewis Carroll*, Alenka v kraji divů*

Jak už jsem zmínil na začátku, myslím, že odpověď na otázku „Co vás bitcoin naučil?" bude vždy neúplná. Symbióza toho, co lze považovat za několik živých systémů – bitcoinu, technosféry a ekonomiky – je příliš provázaná. Témat je velmi mnoho a věci se vyvíjejí příliš rychle na to, aby je jediný člověk dokázal plně pochopit.

I když mu zcela nerozumíme a i přes všechny své zvláštnosti a zdánlivé nedostatky bitcoin nepochybně funguje. Bloky produkuje zhruba každých deset minut a činí tak báječně. Čím déle bude bitcoin fungovat, tím více lidí se rozhodne jej používat.

> „Je pravda, že věci jsou krásné, když fungují. Funkčnost je uměním."
>
> – Giannina Braschi[1]

[1] Giannina Braschi, *Empire of Dreams* [18]

Bitcoin je dítětem internetu. Exponenciálně roste a stírá hranice mezi obory. Není například jasné, kde končí sféra čistě technologická a kde začíná jiná. Přestože bitcoin ke svému efektivnímu fungování vyžaduje počítače, k jeho pochopení informatika nestačí. Bitcoin je nejen neohraničený, co se týče jeho vnitřního fungování, ale také bez hranic, pokud jde o akademické disciplíny.

Ekonomie, politika, teorie her, peněžní historie, teorie sítí, finance, kryptografie, teorie informací, cenzura, právo a regulace, společenské uspořádání, psychologie – tyto a mnohé další obory by mohly pomoci při snaze o porozumění tomu, jak bitcoin funguje a čím vlastně je.

Za svůj úspěch nevděčí žádnému konkrétnímu vynálezu. Je to kombinace různých dříve nesouvisejících dílků pospojovaných pobídkami z oblasti teorie her, dohromady tvořící revoluci jménem bitcoin. Právě tato krásná směs mnoha oborů dělá ze Satoshiho génia.

Stejně jako každý složitý systém musí i bitcoin hledat kompromisy v oblasti efektivity, nákladů, bezpečnosti a mnoha dalších vlastností. Stejně jako neexistuje dokonalé řešení, jak z kruhu udělat čtverec, bude i řešení problémů, které se bitcoin snaží přinést, vždy nedokonalé.

> „Nevěřím, že ještě někdy budeme mít dobré peníze, dokud je nevytrhneme z rukou vlády, tedy nemůžeme je vytrhnout z rukou vlády násilím, jediné, co můžeme udělat, je nějakou mazanou oklikou zavést něco, co oni nemohou zastavit."
>
> – Friedrich Hayek[2]

Bitcoin je tou mazanou oklikou, jak znovu zavést dobré peníze. Činí tak umístěním suverénního jedince za každý jeden uzel, podobně jako se Leonardo da Vinci snažil vyřešit neřešitelný problém kvadratury

[2] Friedrich Hayek o peněžní politice, zlatém standardu, schodku rozpočtu, inflaci a Johnu Maynardu Keynesovi, https://youtu.be/EYhEDxFwFRU

kruhu umístěním Vitruviánského muže do jeho středu. Uzly účinně odstraňují jakýkoliv koncept středu, čímž vytvářejí systém, který je překvapivě antifragilní a velmi obtížně vypnutelný. Bitcoin žije a jeho srdce bude pravděpodobně tlouct ještě dlouho poté, co se ta naše zastaví.

Doufám, že se vám těchto jednadvacet lekcí líbilo. Možná nejzásadnějším poznatkem je, že pokud chceme mít o bitcoinu alespoň přibližný ucelený obraz, měli bychom jej zkoumat komplexně, z více úhlů pohledu. Stejně jako odstranění jedné části ze složitého systému zničí celek, zkoumání jednotlivých částí bitcoinu izolovaně nejspíš povede k jeho nepochopení. Pokud jen jedna osoba vyškrtne ze svého slovníku slovo „blockchain“ a nahradí ho výrazem „řetězec bloků“, zemřu jako šťastný člověk.

V každém případě moje cesta pokračuje. Plánuji vydat se dál do hlubin králičí nory a zvu vás, abyste se k té jízdě přidali.[3]

[3] https://twitter.com/dergigi

Poděkování

„Děkuju," řekla Alenka.

– Lewis Carroll*, Alenka v kraji divů*

Děkuji nespočtu autorů a tvůrců obsahu, kteří ovlivnili mé uvažování o bitcoinu a tématech, kterých se dotýká. Je jich příliš mnoho na to, abych je uvedl všechny, ale pokusím se jmenovat alespoň některé.

- Děkuji Arjunovi Balajimu za tweet, který mě motivoval k sepsání tohoto textu.
- Díky Martymu Bentovi za nekonečné množství podnětů k přemýšlení a zábavu. Pokud nejste přihlášeni k odběru Marty's Bent a jeho Tales From The Crypt, přicházíte o hodně. Díky Mattovi a Martymu za průvodcovství králičí norou.
- Děkuji Michaelu Goldsteinovi a Pierru Rochardovi za péči a poskytování nejlepší literatury o bitcoinu prostřednictvím Nakamoto Institute. A děkuji vám za vytvoření Noded Podcastu, který podstatně ovlivnil mé filozofické názory na bitcoin.
- Díky Peteru McCormackovi za jeho upřímné tweety a podcast What Bitcoin Did, který stále poskytuje skvělé postřehy z mnoha oblastí tohoto prostoru.
- Děkuji Andreasi M. Antonopoulosovi za všechny vzdělávací materiály, které v průběhu let vydal.

- Díky Saifedeanu Ammousovi za jeho přesvědčení, drsné tweety a napsání Bitcoinového standardu.
- Děkuji Francisi Pouliotovi za sdílení jeho nadšení z objevu timechainu.
- Díky Jannikovi, Brandonovi, Mattovi, Camilovi, Danielovi, Michaelovi a Raphaelovi za poskytnutí zpětné vazby k prvním návrhům některých lekcí. Zvláštní poděkování patří Jannikovi, který několikrát provedl korekturu několika návrhů.
- Děkuji Dhruvovi Bansalovi a Mattu Odellovi za to, že si udělali čas a diskutovali se mnou o některých nápadech.
- Díky Guyi Swannovi za vytvoření audio verze na 21lessons.com.
- Děkuji své ženě za to, že se mnou a mou obsesivní povahou vydržela.
- Děkuji své rodině za podporu v časech dobrých i zlých.
- V neposlední řadě děkuji všem bitcoinovým maximalistům, shitcoinovým minimalistům, shillům, botům a shitposterům, kteří žijí v krásné zahradě, jíž je bitcoinový twitter.

A nakonec díky vám, že jste si to přečetli. Doufám, že se vám to líbilo stejně, jako mně se líbilo to psát.

Seznam obrázků a grafů

O bibliografii

> *Snad jsem neměla lézt do té králičí díry – a přec – a přec – nic naplat, zajímavý je tenhle život.*
>
> – Lewis Carroll*, Alenka v kraji divů*

O bitcoinu bylo napsáno již hodně knih, avšak většina diskuze se odehrává online, kde se tím pádem nachází i většina zdrojů.

Následující bibliografie uvádí knihy, studie a online zdroje. Pokud ke zdroji patří i webový odkaz, snažili jsme se ověřit, že všechny uvedené odkazy byly k září 2022 funkční. U knih či článků, které byly přeloženy do češtiny, uvádíme vždy českou verzi. Zdroje a odkazy z knihy naleznete též na následujícím odkazu: www.bitperia.cz/knihy/21lekci/zdroje

Bibliografie

[1] Ammous, Saifedean. *Bitcoinový standard: Decentralizovaná alternativa k centrálnímu bankovnictví*. Braiins Publishing a Konsensus Network, 2022.

[2] Ammous, Saifedean. Presentation on The Bitcoin Standard. https://www.youtube.com/watch?v=Zbm772vF-5M&t=840s, květen 2018.

[3] Pantone, Jay; Anonymous 4chan Poster; Houston, Robin; Vatter, Vince. A lower bound on the length of the shortest superpattern. https://oeis.org/A180632/a180632.pdf, říjen 2018.

[4] Antonopoulos, Andreas M. Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media, Inc., 2014.

[5] Assange, Julian. Cypherpunks: Freedom and the Future of the Internet – Introduction: A Call to Cryptographic Arms. https://cryptome.org/2012/12/assange-crypto-arms.htm, prosinec 2012.

[6] Valné shromáždění OSN. Všeobecná deklarace lidských práv. https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/czc.pdf, prosinec 1948.

[7] Beautyon. Why America Can't Regulate Bitcoin. https://hackernoon.com/why-america-cant-regulate-bitcoin-8c77cee8d794, březen 2018.

[8] Beautyon. Bitcoin Is. And That Is Enough. https://hackernoon.com/bitcoin-is-and-that-is-enough-e3116870eed1, říjen 2019.

[9] Becker, Georg T.; Regazzoni, Francesco; Paar, Christof a Burleston, Wayne P. Stealthy Dopant-Level Hardware Trojans: s. 197–214. In International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2013.

[10] Bent, Marty. Tales from the Crypt – A Podcast About Bitcoin. https://tftc.io/podcasts/, 2017.

[11] Bezos, Jeff. To Our Shareholders. http://media.corporate-ir.net/media_files/irol/97/97664/reports/Shareholderletter97.pdf, 1997.

[12] Bitcoin Wiki contributors. Block hashing algorithm — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Block_hashing_algorithm, 2021.

[13] Bitcoin Wiki contributors. Controlled supply — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Controlled_supply, 2022.

[14] Bitcoin Wiki contributors. Genesis block — Bitcoin Wiki. https://en.bitcoin.it/wiki/Genesis_block, 2021.

[15] Bitcoin Wiki contributors. Pay to script hash — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Pay_to_script_hash, 2017.

[16] Bitcoin Wiki contributors. Segregated Witness — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Segregated_Witness, 2021.

[17] Bloom, Godfrey. Why the whole banking system is a scam. https://youtu.be/hYzX3YZoMrs, květen 2013.

[18] Braschi, Giannina. Empire of Dreams. AmazonCrossing, 2011.

[19] Carter, Nic. Bitcoin's Existential Crisis / What is it like to be a bitcoin? https://medium.com/s/story/what-is-it-like-to-be-a-bitcoin-56109f3e6753, listopad 2018.

[20] Guix Contributors. Guix — Bootstrapping. https://guix.gnu.org/manual/en/html_node/Bootstrapping.html, 2019.

[21] Dennett, Daniel C.; Hofstadter, Douglas R. The Mind's I: Fantasies and Reflections on Self and Soul. Harvester Press, 1981.

[22] Desjardins, Jeff. The Rising Speed of Technological Adoption. https://www.visualcapitalist.com/rising-speed-technological-adoption/, únor 2018.

[23] Diamandis, Peter. *Hojnost. Budoucnost je lepší, než si myslíte.* Praha, Dokořán, 2013.

[24] Dunny. I've learned more about finance, economics, technology, cryptography, human psychology, politics, game theory, legislation, and myself in the last three months of crypto than the last three and a half years of college. https://twitter.com/BitcoinDunny/status/935330541263519745, listopad 2017.

[25] epii. New bitcoin logo. https://bitcointalk.org/index.php?topic=4994.msg140770#msg140770, květen 2011.

[26] Electronic Frontier Foundation. The Crypto Wars: Governments Working to Undermine Encryption. https://www.eff.org/files/2014/01/03/cryptowarsonepagers-1_cac.pdf, 2018.

[27] Fox, Susannah; Rainie, Lee. How the internet has woven itself into American life. https://pewrsr.ch/32M7Qmg, únor 2014.

[28] Gibson, William. The Science in Science Fiction. https://www.npr.org/2018/10/22/1067220/the-science-in-science-fiction, říjen 2018.

[29] Gigi. Bitcoin's Energy Consumption – A shift in perspective. https://dergigi.com/2018/06/10/bitcoin-s-energy-consumption/, červen 2018.

[30] Gigi. The Magic Dust of Cryptography – How digital information is changing our society. https://dergigi.com/2018/08/17/the-magic-dust-of-cryptography/, srpen 2018.

[31] Gregory Maxwell. Taproot. Privacy preserving switchable scripting. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html, leden 2018.

[32] Hasu. Unpacking Bitcoin's Social Contract. https://uncommoncore.co/unpacking-bitcoins-social-contract, prosinec 2018.

[33] Hayek, Friedrich August. 1980s Unemployment and the Unions: Essays on the Impotent Price Structure of Britain and Monopoly in the Labour Market. Institute of Economic Affairs, 1984.

[34] Hayek, Friedrich August. The Collected Works of F.A. Hayek, Volume 6, Good Money, Part II. Routledge, 1999.

[35] Hazlitt, Henry. Ekonomie v jedné lekci. https://libinst.cz/book/hazlitt-h-1946-ekonomie-v-jedne-lekci/. Praha, Liberální Institut, 2008.

[36] Held, Dan. Bitcoin's Distribution was Fair. https://danhedl.medium.com/bitcoins-distribution-was-fair-e2ef7bbbc892, 2018.

[37] Hughes, Eric. A Cypherpunk's Manifesto. https://www.activism.net/cypherpunk/manifesto.html, březen 1993.

[38] Hülsmann, Guido Jörg. Ethics of Money Production. https://mises.org/library/ethics-money-production, Ludwig von Mises Institute, 2008.

[39] Kiyosaki, Robert. Why the Rich are Getting Richer. https://youtu.be/abMQhaMdQu0, červenec 2016.

[40] Kaspersky Lab. From festive fun to password panic: Managing money online this Christmas. https://www.kaspersky.com/blog/money-report-2018/, 2018.

[41] Lopp, Jameson. No one has found the bottom of the Bitcoin rabbit hole. https://twitter.com/lopp/status/1061415918616698881, listopad 2018.

[42] Rapport, Margo. History Shows Price of an Ounce of Gold Equals Price of a Decent Men's Suit, Says Sionna Investment Managers. https://www.businesswire.com/news/home/20110819005774/en/History-Shows-Price-Ounce-Gold-Equals-Price, 2011.

[43] Mayer, Trace. The 7 Network Effects of Bitcoin. https://nakamotoinstitute.org/mempool/the-seven-network-effects-of-bitcoin/, červen 2015.

[44] Merkle, Ralph. C. DAOs, Democracy and Governance. http://www.ralphmerkle.com/papers/DAOdemocracyDraft.pdf, červenec až srpen 2016.

[45] Fiat Minimalist. Isn't it ironic that Bitcoin has taught me more about money than all these years I've spent working for financial institutions? https://twitter.com/fiatminimalist/status/1072880815661436928, prosinec 2018.

[46] The Australian Mint. Gold: The Extraordinary Metal. https://www.muenzeoesterreich.at/eng/discover/for-investors/gold-the-extraordinary-metal, listopad 2017.

[47] British Museum. The Origins of Coinage. https://www.britishmuseum.org/collection/galleries/money, 2018.

[48] Nakamoto, Satoshi. *Bitcoin: Peer-to-Peer systém elektronických peněz*. https://braiins.com/blog/the-bitcoin-whitepaper-cz-cesky-preklad. Praha, Braiins, květen 2021.

[49] Nakamoto, Satoshi. Re: Bitcoin P2P e-cash paper. https://www.metzdowd.com/pipermail/cryptography/2008-November/014832.html, listopad 2008.

[50] Nakamoto, Satoshi. Bitcoin open source implementation of P2P currency. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562, únor 2009.

[51] Nakamoto, Satoshi. Bitcoin open source implementation of P2P currency. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source, únor 2009.

[52] Nakamoto, Satoshi. Re: Bitcoin open source implementation of P2P currency. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source, únor 2009.

[53] Nakamoto, Satoshi. Re: Questions about Bitcoin. https://bitcointalk.org/index.php?topic=13.msg46#msg46, prosinec 2009.

[54] Nakamoto, Satoshi. Dealing with SHA-256 Collisions. https://bitcointalk.org/index.php?topic=191.msg1585#msg1585, červen 2010.

[55] Nakamoto, Satoshi. Re: 0.3 almost ready. https://bitcointalk.org/index.php?topic=199.msg1670#msg1670, červen 2010.

[56] Nakamoto, Satoshi. Re: Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG. https://bitcointalk.org/index.php?topic=195.msg1611\#msg1611, červen 2010.

[57] Paul, Ron. End the Fed. http://endthefed.org/books/. Grand Central Publishing, 2009.

[58] Pearson, Jordan. Inside the World of the Bitcoin Carnivores: Why a small community of Bitcoin users is eating meat exclusively. https://motherboard.vice.com/en_us/article/ne74nw/inside-the-world-of-the-bitcoin-carnivores, září 2017.

[59] Wuille, Pieter. Schnorr Signatures for secp256k1. https://github.com/sipa/bips/blob/bip-taproot/bip-0340.mediawiki#Applications, 2019.

[60] Plato. Plato in Twelve Volumes, Vol. 3. (Euthydemus section 304a/304b). http://www.perseus.tufts.edu/hopper/org/w/index.php?title=Crypto_Wars, 2022.

[61] Federal Reserve. Money Stock Measures – Discontinuance of M3. https://www.federalreserve.gov/Releases/h6/discm3.htm, 2005.

[62] Roets, Perry. Bernard W. Dempsey, S.J. Review of Social Economy, 49(4): s. 546–558, https://www.jstor.org/stable/29769582, 1991.

[63] Sagan, Carl. Kosmos. Praha, Eminent 1996.

[64] Schneier, Bruce. Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and Sons, 2017.

[65] Schneier, Bruce. Schneier on Security. https://www.schneier.com, 2019.

[66] Snowden, Edward. Edward Snowden: NSA whistleblower answers reader questions. https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower, červen 2013.

[67] Song, Jimmy. Why Bitcoin is Different. https://medium.com/@jimmysong/why-bitcoin-is-different-e17b813fd947, duben 2018.

[68] U.S. Geological Survey. National Minerals Information Center – Mineral Commodity Summaries. https://www.usgs.gov/centers/nmic/mineral-commodity-summaries, 2022.

[69] Szabo, Nick. Shelling Out: The Origins of Money. https://nakamotoinstitute.org/shelling-out/, 2002.

[70] Thompson, Ken. Reflections on Trusting Trust. In ACM Turing award lectures. str. 1983, https://users.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf, 2007.

[71] Tom Elvis Jedusor. MimbleWimble Origin. https://github.com/mimblewimble/docs/wiki/MimbleWimble-Origin, 2016.

[72] Trubetskoy, Grisha. Blockchain Proof-of-Work Is a Decentralized Clock. https://grisha.org/blog/2018/01/23/explaining-proof-of-work/, 2018.

[73] Valkenburgh, Peter Van. Coin Center's Peter Van Valkenburg on Preserving the Freedom to Innovate with Public Blockchains. http://bit.ly/valkenburgh, listopad 2018.

[74] Mises, Ludwig von. Lidské jednání. https://libinst.cz/book/mises-l-von-1949-lidske-jednani/, Praha, Liberální Institut, 2016.

[75] Wikipedia contributors. 2013–present economic crisis in Venezuela — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=2013%E2%80%93present_economic_crisis_in_Venezuela, 2022.

[76] Wikipedia contributors. Austrian School — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Austrian_School, 2022.

[77] Wikipedia contributors. Bimetallism — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Bimetallism, 2022.

[78] Wikipedia contributors. Crypto Wars — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Crypto_Wars, 2022.

[79] Wikipedia contributors. Discrete logarithm — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Discrete_logarithm, 2022.

[80] Wikipedia contributors. Dual EC DRBG — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Dual_EC_DRBG, 2022.

[81] Wikipedia contributors. Dyson sphere — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Dyson_sphere, 2022.

[82] Wikipedia contributors. Elliptic-curve cryptography — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Elliptic-curve_cryptography#Backdoors, 2022.

[83] Wikipedia contributors. Hyperinflation — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Hyperinflation, 2022.

[84] Wikipedia contributors. Illegal number — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Illegal_number, 2022.

[85] Wikipedia contributors. Illegal prime — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Illegal_prime, 2021.

[86] Wikipedia contributors. Keynesian economics — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Keynesian_economics, 2022.

[87] Wikipedia contributors. Landauer's principle — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Landauer%27s_principle, 2022.

[88] Wikipedia contributors. Last Glacial Maximum — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Last_Glacial_Maximum, 2022.

[89] Wikipedia contributors. Lindy effect — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Lindy_effect, 2022.

[90] Wikipedia contributors. List of currencies — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=List_of_currencies, 2022.

[91] Wikipedia contributors. List of historical currencies — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=List_of_historical_currencies, 2022.

[92] Wikipedia contributors. Methods of coin debasement — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Methods_of_coin_debasement, 2022.

[93] Wikipedia contributors. Money multiplier — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Money_multiplier, 2022.

[94] Wikipedia contributors. Money supply — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Money_supply, 2022.

[95] Wikipedia contributors. P versus NP problem — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=P_versus_NP_problem, 2022.

[96] Wikipedia contributors. Paradox of value — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Paradox_of_value, 2022.

[97] Wikipedia contributors. SHA-2 — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=SHA-2, 2022.

[98] Wikipedia contributors. Ship of Theseus — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Ship_of_Theseus, 2022.

[99] Wikipedia contributors. Silver certificate (United States) — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Silver_certificate_(United_States), 2022.

[100] Wikipedia contributors. Subjective theory of value — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Subjective_theory_of_value, 2022.

[101] Wikipedia contributors. Thaler — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Thaler, 2022.

[102] Wikipedia contributors. Theory of value (economics) — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Theory_of_value_(economics), 2022.

[103] Woo, Wilma. 'Unfairly Cheap' Lightning Network Mainnet Hits 40 Nodes, 60 Channels. https://bitcoinist.com/bitcoin-lightning-network-mainnet-nodes, leden 2018.

BRAIINS Publishing

Gigi

21 lekcí: Co mě naučil pád do bitcoinové králičí nory

Z anglického originálu 21 Lessons: *What I've Learned From Falling Down the Bitcoin Rabbit Hole* přeložil František Šimek

Jazyková redakce Klára Ježková

Technická redakce Lukáš Hozda

Odpovědný redaktor Jáchym Černý

Grafická úprava a sazba Sabina Heyová

Design obálky Jiří Chlebus a Sabina Heyová

Marketingová strategie Kristian Csepcsar

Vytiskla tiskárna C-CopyCentrum

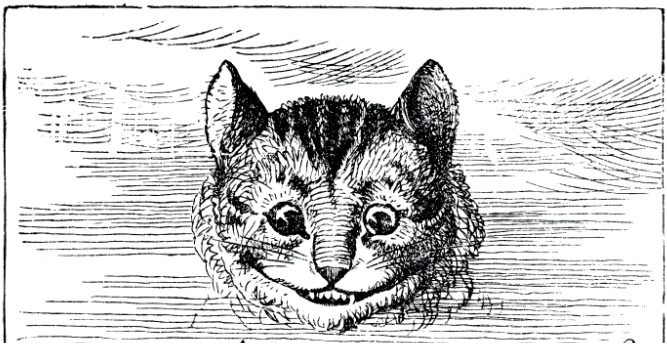
150 stran, vydání první

Vydalo nakladatelství Braiins Systems, 2022

braiins.com/publishing

Pochvaly či připomínky posílejte na publishing@braiins.cz

ISBN 978-80-908709-0-1



„Ale já nechci mezi potrhlíky," bránila se Alenka.
„Málo platné," řekla kočka, „tady jsme všichni potrhlí.
Já jsem potrhlá, ty jsi taky potrhlá."
„Jak to víš, že jsem potrhlá?" zeptala se Alenka.
„To je jisté, jinak bys sem nechodila."

Co je to bitcoin? Na tuto jednoduchou otázku je překvapivě těžké odpovědět. Bitcoin je počítačová síť, nová forma peněz, platební systém odolný proti cenzuře, finanční revoluce, mírová forma protestu a mnohem víc.

Tato kniha si neklade za cíl odpovědět na otázku, co je bitcoin. Snaží se zodpovědět jinou, osobnější otázku:
Co mě bitcoin naučil?

BRAINS Publishing

ISBN 978-80-908709-0-1
9 788090 870901