Bitcoin je budoucnost

VIJAY BOYAPATI

PŘEDMLUVA **JOSEF TĚTEK**

BRAINS Publishing

BRAINS Publishing

Bitcoin je budoucnost

Vijay Boyapati

BRAINS Publishing

Bullish Case for Bitcoin

Překlad © Klára Ježková

Ilustrace na obálce a v úvodu kapitol © @BitcoinUltras

Grafy © Sanjay Mavinkurve

www.bullishcaseforbitcoin.com

ISBN 978-80-908709-2-5

BRAIINS

Firma Braiins, založená v roce 2011 se sídlem v Praze, je světovým lídrem v oblasti těžby bitcoinu.

Společnost se specializuje na **vývoj softwarových a hardwarových nástrojů pro bitcoinové těžaře** a provozuje nejdéle fungující těžební pool na trhu. Produkty společnosti Braiins se používají na stovkách tisíc zařízení po celém světě.

Více o společnosti a jejích produktech naleznete na adrese braiins.com.

BRAIINS POOL

Formerly **Slush Pool**

BRAIINS OS+

STRATUM V2

BRAIINS Insights

FARM PROXY

FARM MONITOR

OBSAH

Mým dětem, které se jmenují Addie, Will a Vivi.
Upřímně věřím, že bitcoin pro vás vytvoří lepší svět.


HODL

PŘEDMLUVA

Pandemie z roku 2020 otřásla světovou ekonomikou a donutila nás provést během několika měsíců digitální transformaci, která by se jinak táhla dobrých deset let. Obliba čistě digitálních služeb raketově vzrostla a mnoho tradičních kamenných provozoven zavřelo. Miliony podniků a miliardy lidí se zničehonic ocitly uprostřed největšího převratu svého života.

Naše firma se během druhého čtvrtletí 2020 ze všech sil snažila přizpůsobit novým omezením postcovidového světa. Vybudovali jsme optimalizovanou organizaci, která dodávala podnikový software, držela půl miliardy dolarů v hotovosti a další měla na cestě. Bezprostřední potíže jsme tedy zvládli, ale na obzoru se rýsovalo další, větší nebezpečí, které ohrožovalo naše přežití.

V důsledku politické reakce vlády Spojených států na pandemii stoupla míra peněžní inflace na trojnásobek. Stručně řečeno, náklady kapitálu překročily 20 procent, zatímco předpokládaná výnosnost jakékoliv tradiční strategie finančního investování se rovnala nule. Tudíž se nám začala hromadit hotovost a jako koule na noze nás tížila starost o budoucí peněžní toky. Jestliže stabilní, ziskové hodnotové cenné papíry rostou podstatně pomaleji než míra peněžní inflace, nelze je použít jako uchovatel hodnoty a rychle ztrácejí zájem investorů.

Popsaný problém existoval už deset let před pandemií, jen nebyl tolik naléhavý. V období 2010 až 2019 činila míra peněžní inflace přibližně 7 % a investoři neúnavně tlačili na generální a finanční ředitele, aby dostali peněžní toky nad tuto úroveň, děj se co děj. Často to znamenalo zadlužit se a veškerou volnou hotovost použít ke zpětnému odkupu vlastních akcií nebo k mnohonásobným akvizicím za použití kombinace dluhu a vlastního kapitálu, jen aby výnosy a očekávaný příjem investorů rostly rychleji než minimální

míra návratnosti odpovídající výše zmíněné inflaci. Akvizice však zpravidla výnosnost akcií v dlouhodobém horizontu oslabovaly, navíc se vedení společností potýkalo s problémy při začleňování převzatých podniků a nemohlo se soustředit na hlavní předmět činnosti. Jakmile byla společnost plně napákovaná na dluhu nebo jakmile neměla možnost dalších akvizic, ocitala se ve slepé uličce.

Sedmiprocentní minimální míra návratnosti způsobila, že úmrtnost společností v období 20 let poté, co se naše firma stala veřejně obchodovanou, dosáhla 99 %. Jedna společnost za druhou si ukousla příliš velké sousto, poškodila si bilanci nadměrným zadlužením a zatížila si výsledovku příliš mnoha nesourodými obchodními jednotkami. Když ve druhém čtvrtletí 2020 minimální míra návratnosti vzrostla na trojnásobek, bylo jasné, že takové inflační břemeno nás zanedlouho „položí". Nezměníme-li taktiku, postačí, aby se několik centrálních bankéřů rozhodlo natisknout další peníze, a rázem znehodnotí veškeré plody práce tisíců našich zaměstnanců. Lopotit se čím dál usilovněji za peníze, které stále rychleji ztrácejí hodnotu, je cesta do otroctví.

Řešení našeho problému se objevilo samo v podobě oživení ve tvaru písmene K. V podstatě došlo k tomu, že ačkoliv podnikání dál skomíralo, finanční trhy se díky peněžním pobídkám rychle zotavily. Klíčem k hospodářské životaschopnosti v období vysoké peněžní inflace je silná bilance aktiv, jež se zhodnocují rychleji, než se stihnou kazit peníze. Proto jsme se začali poohlížet po vhodné kombinaci aktiv, jimiž bychom v bilanci nahradili hotovost a státní dluhopisy. Během pátrání jsme objevili jednak bitcoin a jednak tuto skvělou knihu, jejímž autorem je Vijay Boyapati.

Text knihy Bitcoin je budoucnost původně vyšel jako dlouhý článek pod názvem „The Bullish Case for Bitcoin". Jedná se o mistrovské dílo podané s elegancí a jasnozřivostí člověka obdařeného širokým rozhledem, zběhlého v matematice, počítačové vědě, ekonomii,

filozofii, politice a technice. Po březnu 2020 mi bylo jasné, že svět potřebuje nové peníze založené na technologii. V únoru 2018, kdy Boyapati poprvé zveřejnil svou práci, ovšem takový vhled vyžadoval mnohem větší prozíravost, odvahu a přesvědčení.

Boyapati zhuštěnou, přehlednou formou nastiňuje teorii peněz, anatomii bitcoinu, důvody, proč bitcoin předčí dřívější zlatý a fiatový standard, a popisuje, jakou naději bitcoin přináší lidské civilizaci. Způsobem srozumitelným i laikovi popisuje princip závislosti na minulém vývoji a průběh přeměny statku v peníze. Zabývá se také nejčastějšími otázkami, s nimiž se nováčci potýkají ve snaze porozumět podstatě a významu bitcoinu jakožto prvního systému digitálních peněz. Kniha *Bitcoin je budoucnost* mě okamžitě zaujala natolik, že jsem ji zařadil na seznam doporučené četby pro všechny manažery a členy vedení mé společnosti. Studovali jsme bitcoin a zvažovali, jakou logickou cestou se vydat dál. V této knize Boyapati aktualizuje myšlenky představené v původním článku a rozpracovává je do mnohem větší šíře.

Ve třetím čtvrtletí 2020 se MicroStrategy rozhodla učinit z bitcoinu své hlavní rezervní aktivum, čímž se stala první veřejně obchodovanou společností, která přešla na bitcoinový standard. Postupně jsme získali bitcoin v hodnotě miliard dolarů. Doporučujeme knihu Bitcoin je budoucnost všem zaměstnancům, akcionářům a ostatním členům naší společnosti, kteří chtějí pochopit, odkud bitcoin vzešel, kam směřuje a co nám přináší, ať už jako digitální rezervní aktivum, nebo jako první světový systém digitálních peněz. Doufám, že pro vás toto dílo bude stejně přínosné, jako bylo pro nás.

Michael J. Saylor
předseda představenstva a CEO MicroStrategy
Miami Beach, Florida
27. března 2021

PŘEDMLUVA K ČESKÉMU VYDÁNÍ

Vijayův původní článek „The Bullish Case For Bitcoin“, ze kterého vzešla tato kniha, jsem poprvé četl v roce 2018; ke své vlastní škodě jsem textu nevěnoval příliš pozornosti, jelikož jsem tehdy ještě byl zaslepený vidinou multicoinové – dnes bych řekl spíše shitcoinové – budoucnosti. Jako každé zásadní dílo i Vijayovo stručné pojednání o bitcoinové budoucnosti nabývá s časem na významu a události potvrzují jeho pravdivost. Během pěti let od původního čtení jsem takříkajíc snědl svůj klobouk, napsal vlastní ódu na bitcoin a uznal, že bitcoinoví maximalisté (čti bullshitoví minimalisté) měli ve všem pravdu. A Vijayova analýza role bitcoinu v dnešním světě se s každým dalším rokem potvrzuje jako zcela výstižná.

Kniha *Bitcoin je budoucnost*, je skvělým úvodním textem pro všechny, kdo chtějí v krátkém čase a bez ideologických příkras zjistit, co na tom bitcoinu všichni máme, a proč tak sveřepě odmítá umřít. Je to totiž právě nevůle bitcoinu odejít do věčných lovišť, která postupem času nalomí sebedůvěru většiny skeptiků, a přiměje je bitcoinu věnovat pozornost. Jak Vijay Boyapati dokládá v kapitole Průběh monetizace, adopce bitcoinu probíhá v „hype cyklech“, tj. střídajících se fázích maniakálního zájmu spojeného s raketovým růstem ceny a následných depresivních propadů a opadnutí pozornosti. Bitcoin je však s každým dalším cyklem ověřenější a důvěryhodnější, a bitcoineři silnější co do počtu i přesvědčení; výsledkem je postupný a patrně nevyhnutelný nástup nových nestátních peněz, kterým fiatové peníze nemohou ze své povahy konkurovat. „Jak budou fiatové měny v nadcházejících letech pokračovat v historickém vývoji směrem k bezcennosti, bude bitcoin získávat po celém světě stále větší oblibu coby prostředek pro ochranu úspor,“ konstatuje Vijay.

O fenoménu monetizace, tj. přerodu spekulativního instrumentu do plnohodnotných peněz, toho ostatně doposud mnoho napsáno nebylo – což je poměrně logické, jelikož k takové události nedochází v lidské historii často. Vznik bitcoinu inspiroval novou vlnu textů, které se procesem „monetizace od nuly" zabývají, a Vijay byl jeden z prvních, kdo se tímto tématem seriózně zaobíral, přičemž své myšlenky umí podat velmi srozumitelně a čtivě. Zájemcům o hlubší pojednání o monetizaci bitcoinu bych k dalšímu čtení doporučil *Gradually, then Suddenly* od Parkera Lewise, *Layered Money* od Nika Bhatii, a *Bitcoin is Venice* od Allena Farringtona. O kvalitní bitcoinovou literaturu zkrátka již dnes není taková nouze jako před pěti a více lety. Dnešní nově příchozí tak již nemusí opakovat staré chyby.

Vijay Boyapati chápe bitcoin především jako peníze. Je to právě toto pojetí, které poskytuje logický rámec pro zavrhnutí desítek tisíc všemožných shitcoinů. Jak Vijay vysvětluje, bitcoin a kryptoměny si nekonkurují na základě technických vlastností, nýbrž na základě vlastností peněžních. A právě na poli peněžních vlastností altcoiny oproti bitcoinu kulhají na obě nohy, jelikož kvůli své centralizaci nedokáží zaručit neměnnou měnovou politiku, která je předpokladem vzácnosti, jedné z kriticky důležitých peněžních vlastností. Altcoiny, které lze libovolně tvořit z ničeho, se pak principiálně neliší od fiatu.

Vijay rovněž identifikuje reálná rizika bitcoinu, která bývají často opomíjena buďto vinou růžových brýlí nadšených „takybitcoinerů", anebo naopak kvůli populistickému trefování se do domněle neřešitelných problémů, jakým je dnes oblíbený „security budget". Dle Vijaye mezi hlavní rizika patří riziko protistrany, tj. ponechání bitcoinu ve správě burzám a podobným institucím, které mají ve zvyku krachovat; dále to jsou rizika konfiskace ze strany státu, riziko emise papírových bitcoinů – jež se s nástupem amerických spotových ETF stává velmi akutním – a riziko nízké zaměnitelnosti,

které, věřím, výrazně snížila nedávná implementace coinjoinu do hardwarových peněženek Trezor.

Text Vijaye Boyapatiho zkrátka naplňuje čtenáře racionálním optimismem. Bitcoin není instrument na rychlé zbohatnutí, není však ani technologickým módním výstřelkem, který by mohl být rychle překonán. Bitcoin je unikátní pokus o odluku peněz od státu a Vijay metodicky vysvětluje, proč zrovna tento pokus má velmi vysokou naději na úspěch. Bitcoin coby celosvětové nestátní peníze představuje ideu, jejíž čas nadešel. Fiat se stane věcí minulosti, jelikož budoucnost patří bitcoinu.

Josef Tětek
Praha
27. října 2023


THE TI
Chancellor on brink
Second bailout for L

PROLOG

PROMÉTHEUS

Tajuplný příběh zrodu bitcoinu působí tak fantasticky, že mnozí pochybují o jeho pravdivosti. Nejspíš se nikdy nedozvíme, jak to přesně bylo, nicméně to podstatné známe: dne 3. ledna 2009 neidentifikovaná osoba na neznámém místě stiskla tlačítko na počítačové klávesnici a spustila jeden z nejdůležitějších programů v dějinách. Počítač začal hledat digitální jehlu v kupce sena – jeden určitý vzorec nazývaný hash, který měl potvrdit první blok v účetní knize finančních transakcí, nyní známé jako blockchain. Během několika minut nebo hodin – nikdo neví s jistotou, za jak dlouho – byl první hash nalezen, počáteční blok (genesis blok) potvrzen a zrodila se první skutečně decentralizovaná digitální měna na světě. Totožnost záhadné osoby, která stvořila bitcoin, zůstává kupodivu dodnes tajemstvím. Jediné, co známe, je pseudonym: Satoshi Nakamoto.

Ani ne dva měsíce předtím, 31. října 2008, Nakamoto zveřejnil technický popis bitcoinu v cypherpunkerské mailingové skupině, e-mailové skupině zájemců o kryptografii, zkoumání a prolamování kódů.[1] Mnozí její členové označovali sami sebe za cypherpunkery – pomocí kryptografických nástrojů posilujících soukromí se snažili přetvořit společnost a osvobodit ji od státní kontroly. Nakamotův e-mail byl jeho úplně prvním příspěvkem do skupiny a nedočkal se nikterak nadšeného přijetí, spíše všeobecné skepse. Dokonce i v komunitě, která za sebou měla nezanedbatelnou historii pokusů o vynalezení digitální měny, chápal význam Nakamotova sdělení málokdo. Výjimkou byl Hal Finney, nadaný kryptograf a počítačový vědec, který tvorbě digitální měny věnoval většinu

1 https://www.bullishcaseforbitcoin.com/references/bitcoin-announcement

své kariéry a dobře znal potíže, na které tato snaha naráží. Finney později na oznámení o stvoření bitcoinu vzpomínal takto:

> *„Když Satoshi v e-mailové skupině oznámil vznik bitcoinu, reakce byla přinejlepším skeptická. Kryptografové už viděli příliš mnoho velkolepých nápadů od lidí, kteří netuší, o čem mluví. Proto máme sklon k ukvapeným reakcím.“*[2]

Finney tragicky zemřel 28. srpna 2014 na komplikace spojené s Lou Gehrigovou chorobou. Předtím však mnohokrát významně přispěl k vývoji digitální měny, zejména bitcoinu.

GORDICKÝ UZEL

Od okamžiku, kdy Tim May, vědec pracující původně pro společnost Intel a zakladatel cypherpunkového hnutí, v roce 1992 představil na malém shromáždění podobně naladěných radikálů ze Silicon Valley *Manifest kryptoanarchie*, cypherpunkeři chápou, že je nanejvýš důležité vytvořit digitální, nestátní formu peněz. Jak May napsal ve svém manifestu:

> *„Výpočetní technika stojí na bodu zlomu, kdy bude schopna poskytnout jednotlivcům i celým skupinám možnost komunikovat navzájem v naprosté anonymitě. Budeme vyměňovat zprávy, uzavírat obchody a vyjednávat smlouvy*

2 https://www.bullishcaseforbitcoin.com/references/finney-skepticism

elektronicky, aniž bychom věděli pravé jméno nebo právní status druhé strany.“[3]

K uzavírání obchodů ovšem potřebujeme peníze, které jsou v každé rozvinuté ekonomice tím nejdůležitějším statkem, protože je na nich postaveno nejen veškeré obchodování, ale také spoření. Po tisíciletí tuto úlohu zastával starobylý a úctyhodný cenný kov – zlato. Jeho Achillovou patou je však fyzická povaha, která je činí zranitelným vůči centralizaci, konfiskaci a útokům ze strany státu. Ve dvacátém století navíc stát ovládl tvorbu peněz a dohled nad nimi, čímž zlato o postavení světové měny přišlo. Cypherpunkeři doufali, že se jim podaří vytvořit digitální měnu imunní vůči donucovací moci státu – přáli si umožnit anonymní platby a současně odstranit slabiny vlastní zlatu.

V roce 1983 americký počítačový vědec David Chaum zveřejnil návrh měny eCash. Byl to první pokus o systém chránící finanční soukromí uživatelů pomocí kryptografie. V roce 1989 Chaum ve snaze o komerční využití svého vynálezu založil společnost DigiCash, ale finančního úspěchu se nedočkal. Navíc eCash trpěl problémem centralizace, jelikož byl navázán na společnost, která ho vytvořila, přičemž u každých peněz vydávaných nějakou ústřední autoritou je právě tato autorita jejich hlavní slabinou. A skutečně došlo k tomu, že DigiCash v roce 1998 zbankrotovala, a provoz systému eCash byl ukončen. Tak se stalo, že nejnadanější kryptografové a cypherpunkeři napřeli během 90. let 20. století své snahy směrem k vytvoření nějaké formy digitálních peněz neovládaných žádnou centrální mocí. Adam Back, Nick Szabo, Wei Dai a další cypherpunkeři dosáhli koncem 90. let při vývoji digitální měny významného pokroku, ale

3 https://www.bullishcaseforbitcoin.com/references/anarchist-manifesto

Přeložil Petr Žílka. Celý Manifest kryptoanarchie je dostupný z https://libinst.cz/wp-content/uploads/2020/08/havel.pdf. (pozn. překl.)

hlavní problém zůstával nevyřešen: jak udržet digitální vzácnost bez centrální autority, která by na ni dohlížela? Už v 16. století filozofická a teologická škola ve španělské Salamance rozpoznala, že hodnota peněz je dána právě jejich vzácností. V digitálním světě, kde lze data levně kopírovat a přenášet, se ale vzácnost doposud dala zajistit jedině uplatněním státní moci, jako tomu je například v případě duševního vlastnictví.

Britský kryptograf Adam Back vynalezl v roce 1997 systém HashCash, který obsahoval zásadní inovaci nezbytnou pro funkční zajištění digitální vzácnosti: důkaz o vykonané práci *(proof-of-work)*. Back se původně pokoušel vyřešit problém se stále nákladnějším odstraňováním e-mailového spamu. Navrhl, aby počítač hledal digitální otisk *(hash)*, jehož nalezení se neobejde bez náročného vyhledávání vyžadujícího velké množství práce, která spotřebovává energii, a tudíž stojí peníze. Jakmile je ale hash vytvořen, dá se rychle a levně ověřit a umožňuje zjistit, kolik energie bylo vynaloženo a s přibližně jakými náklady. V podstatě hash představoval kryptografický důkaz, že byla vykonána práce. Podle Backova návrhu by odesílatel musel ke každému e-mailu připojit jedinečný hash jako důkaz, že vynaložil jisté zanedbatelné náklady v haléřové výši. Tyto náklady by nijak neovlivnily běžné používání elektronické pošty, ale hromadné rozesílání spamu by se s nimi prodražilo natolik, že by bylo v podstatě neproveditelné. HashCash bohužel na trhu neuspěl, navíc postrádal důležité prvky, jež by mu dovolovaly fungovat jako peníze. Později ovšem důkaz o vykonané práci bude tím hlavním, co v decentralizovaném systému umožní uzavírat transakce mezi účastníky bez nutnosti vzájemné důvěry.

V roce 1998 americký počítačový vědec Wei Dai vytvořil systém nazvaný b-money, který řešil zásadní nedostatek Chaumova eCashe, totiž jeho centralizovanou povahu. Dai navrhl, aby se namísto ústřední autority dohlížející na omezenou peněžní zásobu použil distribuovaný systém, kde každý účastník povede samostatný účetní

záznam o množství peněz v držení každého jednotlivce v systému. Tím by se případný nátlak státu na libovolný uzel sítě stal neúčinným. Daiův návrh byl ale obtížně proveditelný, protože předpokládal komunikaci téměř v reálném čase, neustále propojenými a nezmanipulovatelnými kanály. Systém se nikdy nerozběhl v praxi.

V témže roce, kdy Dai navrhl b-money, vytvořil všestranně nadaný americký vědec Nick Szabo jiný systém digitálních peněz a nazval jej bit gold. Stejně jako b-money se Szaboův projekt bit gold nedočkal realizace, ale i tak znamenal zásadní skok vpřed, protože vzácnost určitého statku nepojal jako jeho fyzický nedostatek, nýbrž jako vlastnost spočívající v ověřitelnosti nákladů na jeho vytvoření. Szabo pro tuto vlastnost vymyslel nový termín „nezfalšovatelná nákladnost" *(unforgeable costliness)*. Bit gold vycházel z Backovy koncepce důkazu o vykonané práci a umožňoval účastníkům vytvářet tokeny (tj. mince) tak, že předloží hash, jehož nezfalšovatelná nákladnost bude sloužit coby brzda bránící nadměrnému růstu peněžní zásoby. Vlastnictví tokenů se bude zapisovat do registru běžícího na mnoha serverech, jež budou dohromady tvořit „klub vlastníků". Je zde patrná podobnost s Daiovými b-money, jen způsob fungování se poněkud liší. Szaboův návrh se už už dotýkal řešení, které by umožnilo vznik decentralizovaných peněz, ale trpěl některými zásadními nedostatky. Za prvé, kvůli rostoucímu výkonu počítačů by vytvoření stejného hashe dnes bylo snazší než v minulosti, takže hashe získané v různých bodech časové osy by měly odlišnou hodnotu, což by narušovalo důležitou vlastnost peněz, totiž zaměnitelnost. Bit gold by se tak coby digitální komodita podobal spíše diamantům (nestejný tvar a kvalita, nesnadná zaměnitelnost) než zlatu. Za druhé, registr vlastnictví byl zranitelný vůči Sybiliným útokům.[4] Ty by mohly systém narušit tím, že by vytvořily velké

4 Hackerský útok, při kterém útočník usilující o ovládnutí sítě uživatelů založené na vzájemné důvěře vytvoří velké množství účtů pod falešnými jmény a s jejich pomocí se zmocní většiny sítě. Název pochází ze stejnojmenné knihy pojednávající o psychiatrické pacientce s poruchou osobnosti. (pozn. red.)

množství falešných členů klubu vlastníků, kteří by poté vykazovali zfalšované zůstatky a připisovali na účet útočníka peníze, které by ve skutečnosti neměli. Szabo sice navrhl, jak tyto problémy odstranit, ale jeho řešení byla složitá, a bit gold tak zůstal pouhou teorií.

Přehoupli jsme se do dalšího století a naděje, že se sen cypherpunkerů o vzniku decentralizované digitální měny podaří uskutečnit, začala uvadat. Hal Finney, který každý pokus o vytvoření nestátních peněz pozorně sledoval, se v roce 2004 pokusil tento sen oživit a navrhl systém RPOW (opakovaně použitelné důkazy o vykonané práci – *reusable proofs-of-work*), který byl zjednodušenou verzí Szaboova bit gold. Na rozdíl od Szaboa nebo Daie dokonce spustil funkční prototyp, ale RPOW trpěl podobným neduhem jako Chaumův eCash, totiž závislostí na ústřední moci. Finney se problém centralizace pokusil odstranit a nahradil ústřední autoritu nezmanipulovatelným hardwarovým zařízením, které mělo uživatelům na dálku potvrzovat správnost zůstatku. Hardware by byl mnohem důvěryhodnější než vydíratelná společnost, ale zato by se dal snadno vypnout.

V roce 2008, zatímco se svět propadal do nejhorší hospodářské krize za celé generace, většina členů e-mailové kryptografické skupiny usoudila, že vytvořit decentralizovanou digitální měnu je pravděpodobně nemožné. Proto když Satoshi Nakamoto sebevědomě oznámil, že problém decentralizovaných peněz vyřešil, jen hrstka členů skupiny ho brala vážně.

PRŮLOM

Několik týdnů po oznámení vzniku bitcoinu začal Hal Finney zasypávat Satoshiho Nakamota dotazy ohledně nového vynálezu. Finney rychle pochopil genialitu bitcoinu a uvědomil si, jaký důmyslný intelektuální skok Nakamoto při vytváření nových

digitálních peněz nezávislých na centrální autoritě provedl. Žádná z myšlenek, na nichž byl bitcoin postaven, nebyla nová, ani použitá kryptografie nebyla inovativní. Nakamoto jen postavil systém, kde spolu v dokonalé rovnováze působily ekonomická motivace a kryptografické zabezpečení.

Vynalezením bitcoinu Nakamoto vyřešil zásadní problém, s nímž se počítačová věda potýkala od konce 70. let 20. století – problém byzantských generálů.[5] Jde o to, jak mohou různé subjekty, které si navzájem nedůvěřují, dokonce mohou být i nepřáteli, koordinovat své konání, dosáhnout společného cíle a nespoléhat přitom na zprostředkovatele, jemuž by důvěřovali všichni zúčastnění. Jak v roce 2011 vysvětlil Nick Szabo:

> *„Nakamoto odstranil vážný bezpečnostní nedostatek mého návrhu [bit gold], když určil, že důkaz o vykonané práci musí podávat uzel v peer-to-peer systému odolném vůči problému byzantských generálů. Snížil tak riziko, že většinu uzlů ovládne nedůvěryhodný subjekt a naruší důležité bezpečnostní funkce. Tato inovace možná není patrná na první pohled, ale při hlubším zkoumání je zjevná.“*[6]

Jednalo se o zásadní technický průlom, a přestože to většině členů e-mailové kryptografické skupiny nebylo 31. října 2008 ještě zcela zřejmé, vynález Satoshiho Nakamota nakonec promění celý svět.

---

5 Matematický problém, jak v systému s mnoha účastníky dosáhnout konsenzu, když někteří hráči mohou jednat nečestně. V bitcoinu se týká úskalí, jak udržovat záznamy v účetní knize bez centrální autority. Satoshi Nakamoto v bitcoinovém whitepaperu načrtl řešení tohoto problému v praxi pomocí systému důkazu o vykonané práci, který motivuje těžaře připojovat svoje bloky k nejdelšímu řetězci, a tím pádem udržovat jednotný záznam o chodu sítě. (pozn. red.)

6 https://www.bullishcaseforbitcoin.com/references/szabo-bit-gold

KAPITOLA 1

GENEZE BITCOINU A PŮVOD PENĚZ

Jakmile tržní kapitalizace bitcoinu překročí bilion dolarů, bude investorům nejspíš bez dalšího vysvětlování jasné, že bitcoin je budoucnost. Nebo jim naopak bude připadat pošetilé investovat do digitálního aktiva nekrytého žádnou komoditou ani vládou, jehož cenový vývoj navíc mnozí přirovnávají k tulipánové mánii[1] nebo k dotcom bublině.[2] Přitom ani jedno neplatí beze zbytku. Budoucnost v bitcoinu je lákavá, ale zdaleka ne jednoznačná. Investovat do bitcoinu je rizikové, ale zároveň to znamená obrovskou příležitost, jak vysvětlím dále.

GENEZE BITCOINU

Nikdy v dějinách světa nebylo možné přenášet hodnotu na dálku, aniž by zúčastněné strany musely spoléhat na důvěryhodného prostředníka, například na banku nebo vládu. V roce 2008 Satoshi Nakamoto, jehož pravou totožnost dodnes neznáme, zveřejnil devítistránkové pojednání, kde popsal řešení problému, s nímž se počítačová věda potýkala dlouhá léta – problému byzantských generálů.[3]

---

1 Jedna z prvních ekonomických bublin. V Holandsku počátkem 17. století prudce vzrostla poptávka po cibulkách šlechtěných tulipánů a spolu s tím jejich cena a lidé je začali nakupovat jako spekulaci. Když se ale posléze poptávka srovnala s přebujelou nabídkou, bublina splaskla a mnoho lidí o investované prostředky přišlo. (pozn. red.)

2 V češtině též internetová horečka, je to obdobný případ, tentokrát z konce 90. let 20. století, kdy lidé masivně vydávali a nakupovali akcie internetových firem, z nichž mnohé zatím nijak negenerovaly zisk, ale sázely na růstový potenciál nové technologie internetu jako takového. Cena nadhodnocených akcií kolem roku 2001 klesla, mnohé z firem rázem přišly o prostředky a byly nuceny ukončit svůj provoz. (pozn. red.)

3 https://www.bullishcaseforbitcoin.com/references/white-paper

Bitcoinový whitepaper v češtině: https://cs.braiins.com/blog/the-bitcoin-whitepaper-cz-cesky-preklad (pozn. překl.)

Nakamotovo řešení a systém, který na něm postavil a nazval bitcoin, poprvé v historii umožnily přenášet hodnotu na velkou vzdálenost rychle a s minimálními požadavky na důvěru. Vznik bitcoinu ovlivnil ekonomii i počítačovou vědu tak dalekosáhle, že by si Nakamoto zasloužil *jak* Nobelovu cenu za ekonomii, *tak* Turingovu cenu. Této dvojí pocty se zatím jako jedinému dostalo Herbertu Simonovi.

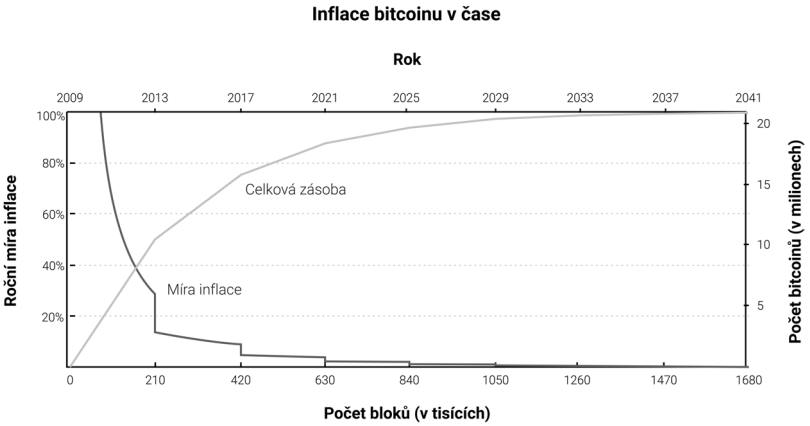
Investora zaujme především skutečnost, že vynálezem bitcoinu vznikl nový vzácný digitální statek – „mince" bitcoinu. Jedná se o přenositelné digitální tokeny vytvářené v bitcoinové síti pomocí procesu nazývaného těžba. Těžbu bitcoinů můžeme zhruba přirovnat k těžbě zlata, až na to, že vznik bitcoinových mincí se řídí přesně stanoveným, předvídatelným harmonogramem. Protokol nedovoluje vytěžit celkem více než 21 milionů mincí, z nichž většina už vytěžena byla. V době psaní této knihy bylo na světě přibližně 18,7 milionu bitcoinů. Každé čtyři roky se počet nových bitcoinů vznikajících těžbou snižuje na polovinu a do roku 2140 by tvorba nových mincí měla být zcela ukončena.

Mince nejsou kryty žádnou fyzickou komoditou ani jejich hodnotu nezaručuje nějaká vláda či obchodní společnost, což u zájemců o investování do bitcoinu pochopitelně vyvolává otázku: proč tedy vůbec mají nějakou hodnotu? Na rozdíl od akcií, dluhopisů, nemovitostí, případně komodit jako ropa nebo pšenice, nelze hodnotu bitcoinů určit obvyklou metodou, tj. analýzou diskontovaných peněžních toků[4], ani na základě poptávky dané jejich využitím při výrobě statků vyššího řádu.[5] Bitcoinové mince patří

4 DCF (discounted cash-flow) je způsob oceňování firem, nemovitostí či majetku obecně, který vychází z předpokladu, že hodnotu určuje očekávaný výnos. Metoda spočívá v diskontování (přepočítání a sečtení) budoucích výnosů na současnou hodnotu s použitím odhadované míry výnosu. Používá se zejména u investic – pokud je DCF daného aktiva vyšší než výše současné investice, slibuje v budoucnu zisky. (pozn. red.)

5 Podle teorie ekonoma Carla Mengera statky vyššího řádu na rozdíl od statků prvního řádu neuspokojují potřeby člověka přímo, ale slouží k výrobě statků prvního řádu. (pozn. red.)

do zcela odlišné skupiny statků, totiž statků peněžních, jejichž hodnota se určuje metodami teorie her. To znamená, že každý účastník trhu oceňuje daný statek na základě svého odhadu, zda a nakolik si stejného statku budou cenit ostatní účastníci trhu. Abychom pochopili, proč je hodnota peněžních statků dána teorií her, potřebujeme prozkoumat původ peněz.



PŮVOD PENĚZ

Nejstarší lidské společnosti mezi sebou obchodovaly přímou směnou, což je nesmírně neefektivní a podstatně to omezuje jak objem transakcí, tak vzdálenost, na kterou je lze uskutečňovat. Velkou nevýhodou přímé směny je problém dvojí shody potřeb: pěstitel jablek například chce uzavřít obchod s rybářem, ale pokud rybář právě v tom okamžiku nemá o jablka zájem, z transakce sejde. Časem lidé zatoužili vlastnit určité předměty pro jejich vzácnost a symbolickou hodnotu a začali takto sbírat například lastury, zvířecí zuby nebo pazourky. Jak dokládá Nick Szabo ve skvělém eseji o původu peněz, touha po sběratelských předmětech pravěkého člověka zásadně evolučně zvýhodnila oproti jeho nejbližšímu

biologickému konkurentovi – neandertálci. Szabo píše: „První a zásadní evoluční funkcí sběratelských předmětů bylo sloužit jako prostředek uchování a přenosu bohatství.“[6]

Sběratelské předměty byly v podstatě primitivními penězi, protože umožňovaly za prvé obchod mezi jinak nepřátelskými kmeny a za druhé předávání bohatství mezi generacemi. Ve společnostech doby kamenné však k obchodování a k předávání sběratelských předmětů docházelo poměrně zřídka. Spíše než jako prostředek směny, jak to známe u moderních peněz, tyto statky sloužily coby uchovatel hodnoty. Szabo vysvětluje:

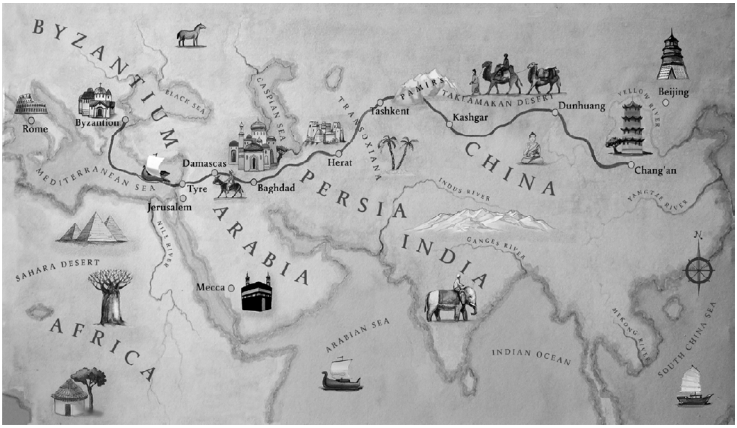
> *„Primitivní peníze se na rozdíl od těch moderních pohybovaly velmi pomalu – průměrný jedinec měl během života jen hrstku příležitostí k jejich směně. Ovšem trvanlivý sběratelský předmět, který bychom dnes označili jako rodinný majetek, mohl vydržet po mnoho generací, s každým přenosem na nového majitele podstatně získával na hodnotě, a často jen díky němu byl takový přenos bohatství vůbec možný.“*

Při rozhodování, které sběratelské předměty shromažďovat nebo vyrábět, čelil dávný člověk dilematu z oblasti teorie her: o co budou mít ostatní lidé zájem? Kdo se trefil v odhadu, získal vlastnictvím daných věcí obrovskou výhodu, mohl snáze obchodovat a shromažďovat bohatství. Narragansettové a některé další kmeny původních obyvatel Ameriky se například specializovali na výrobu jinak nepotřebných předmětů čistě jen pro jejich směnnou hodnotu. Je třeba dodat, že čím dříve někdo odhadl budoucí poptávku po určitém statku, tím větší výhodu získal jeho vlastnictvím – mohl si jej obstarat levněji, dokud o něj ještě nebyl velký zájem, a se

6 https://www.bullishcaseforbitcoin.com/references/shelling-out

stoupající poptávkou směnná hodnota takového předmětu rostla. Navíc už samotná skutečnost, že lidé něco shromažďují, protože předpokládají, že po tom v budoucnosti bude poptávka jako po uchovateli hodnoty, urychluje všeobecné přijetí takových předmětů pro tentýž účel. Toto zdánlivé zacyklení je ve skutečnosti smyčka zpětné vazby, díky níž společnosti rychle přecházejí na jednotný uchovatel hodnoty. Teorie her tento jev označuje pojmem Nashova rovnováha.[7] Pro lidskou společnost je velmi výhodné, aby její uchovatel hodnoty dosáhl Nashovy rovnováhy, protože se tím nesmírně usnadní obchodování a dělba práce, což dláždí cestu k dalšímu rozvoji civilizace.

Postupem tisíciletí se lidské společnosti rozvíjely, vznikaly obchodní stezky a předměty používané k uchování hodnoty si začaly navzájem konkurovat. Kupci a obchodníci si museli vybrat, zda výdělek uloží do uchovatele hodnoty používaného v jejich vlastní společnosti, ve společnosti, s níž obchodují, nebo jestli je nějakým způsobem nakombinují. Uložit úspory do cizího uchovatele hodnoty znamenalo rozšířit si možnosti obchodování s dotyčnou cizinou.



7 https://www.bullishcaseforbitcoin.com/references/nash-equilibrium

Obchodníci, kteří ukládali úspory do cizího uchovatele hodnoty, se ve vlastním zájmu snažili podporovat jeho přijímání také ve své domovské společnosti, protože tím rostla kupní síla jejich úspor. Z výhod importovaného uchovatele hodnoty ovšem těžili nejen obchodníci, ale i lidská společenství jako taková. Pokud dvě společnosti převzaly stejný uchovatel hodnoty, jejich vzájemný obchod byl rázem mnohem méně nákladný a mnohem lépe rozmnožoval všeobecné bohatství. Teprve v devatenáctém století ovšem na jednotný uchovatel hodnoty přešla většina světa. Stalo se jím zlato. Tato éra pak přinesla vůbec největší rozmach obchodu v dějinách. John Maynard Keynes o tehdejších blažených časech napsal:

> *„Jakou neobyčejnou epizodou v ekonomickém pokroku lidstva byla [tehdejší] éra… Každému, kdo měl schopnosti či vůbec povahu překračující průměr, se nabízel únik do středních a vyšších vrstev, jimž život lacino a téměř bez starostí nabízel výhody, pohodlí a vymoženosti převyšující možnosti nejbohatších a nejmocnějších panovníků jiných dob. Obyvatelé Londýna mohli v posteli usrkávat svůj ranní čaj a přitom si po telefonu objednávat různé produkty z celého světa v takovém množství, jež se jim zdálo příhodné, a zároveň s důvěrou očekávat, že jim budou brzy doručeny až ke dveřím.“*[8]

8 https://www.bullishcaseforbitcoin.com/references/lord-keynes-quote

Přeložil Pavel Pšeja. IN: Keynes, John Maynard. *Ekonomické důsledky míru*. Brno, Centrum pro studium demokracie a kultury, 2004, s. 12 (pozn. překl.)

KAPITOLA 2

VLASTNOSTI DOBRÉHO UCHOVATELE HODNOTY

V konkurenci různých uchovatelů hodnoty záleží na konkrétních vlastnostech každého z nich, který nakonec převáží a postupně přitáhne větší poptávku. V minulosti se k uchovávání hodnoty používalo ledacos a teprve čas ukázal, co musí vhodný statek splňovat:

- **Trvanlivost**: Statek se nesmí snadno kazit nebo poškozovat. Například obilí tedy nebude zrovna vhodným uchovatelem hodnoty.

- **Přenositelnost**: Statek se musí snadno přepravovat a skladovat a musí být zabezpečitelný proti ztrátě nebo odcizení, aby se s ním dalo obchodovat na velké vzdálenosti. Kráva je tudíž horším uchovatelem hodnoty než zlatý náramek.

- **Zaměnitelnost**: Jeden kus statku by měl být zaměnitelný za jiný kus ve stejném množství. Nestejnorodý statek neřeší problém shody potřeb. Zlato je tedy lepší než diamanty, které mají nepravidelný tvar a kvalitu.

- **Ověřitelnost**: Pravost statku musí být možno snadno a rychle ověřit. Snadná ověřitelnost při obchodování zvyšuje důvěru příjemce a zvyšuje pravděpodobnost, že se transakce uskuteční.

- **Dělitelnost**: Statek se musí snadno dělit na menší části. V prehistorických společnostech, kde se obchodovalo jen zřídka, neměla tato vlastnost velkou váhu, ale s rozkvětem obchodu a se

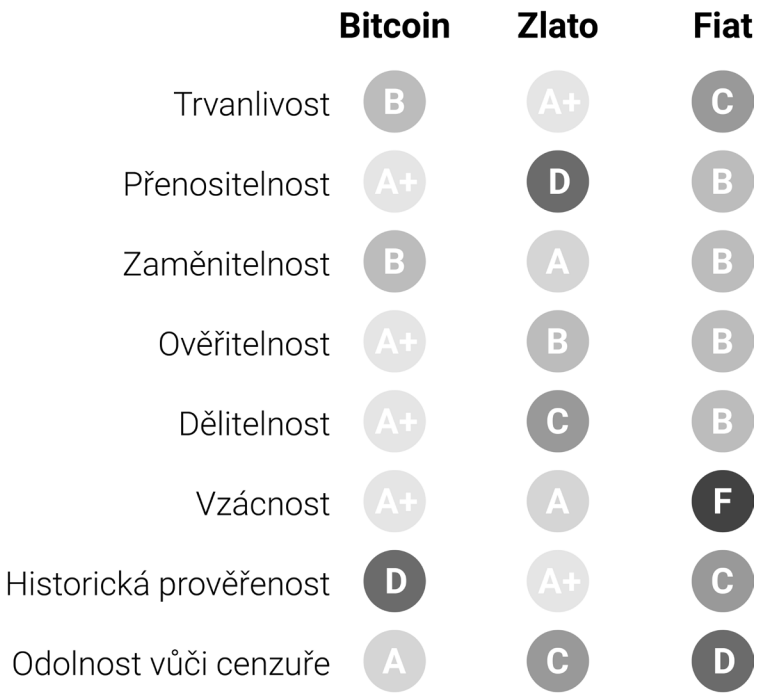
zmenšováním a zpřesňováním obchodovaných množství její význam vzrostl.

- **Vzácnost**: Peněžní statek se musí vyznačovat vlastností, kterou Nick Szabo nazval *nezfalšovatelná nákladnost*. Jinými slovy, nesmí být hojný ani snadno obstaratelný či vyrobitelný ve větším množství. Vzácnost je možná tou nejdůležitější vlastností uchovatele hodnoty, jelikož těží z přirozené lidské touhy shromažďovat to, co není jednoduše k mání. Je zdrojem přirozené hodnoty předmětu sloužícího k jejímu uchování.

- **Historická prověřenost**: Čím déle je nějaký statek považován za cenný, tím oblíbenější bude coby uchovatel hodnoty. Jednou zavedený uchovatel hodnoty pak bývá obtížné nahradit něčím novým, ledaže by to silou prosadil dobyvatel nebo by se novinka ukázala být podstatně výhodnější z hlediska vlastností uvedených výše.

- **Odolnost vůči cenzuře**: Novou vlastností, která v naší moderní digitální společnosti se všudypřítomným sledováním nabývá stále více na významu, je odolnost vůči cenzuře – nakolik je pro třetí subjekt, například korporaci nebo stát, obtížné zabránit majiteli určitého statku, aby ho držel nebo užíval. Statky odolné vůči cenzuře potřebují hlavně lidé v režimech usilujících o mocenskou kontrolu nad kapitálem nebo tam, kde jsou některé způsoby pokojného obchodování postaveny mimo zákon.

Následující tabulka ukazuje hodnocení bitcoinu, zlata a fiat peněz (například dolaru) z hlediska výše uvedených vlastností. Poté následuje podrobnější rozbor.



TRVANLIVOST

Králem trvanlivosti je bezesporu zlato. Naprostá většina jeho dosavadní produkce, včetně zlata faraonů, přetrvala dodnes a nejspíš tu bude i za tisíc let. Zlaté mince, které ve starověku sloužily jako peníze, si i nyní uchovávají značnou hodnotu. Fiat měny a bitcoiny jsou v podstatě digitální záznamy, které mohou nabýt fyzické podoby (například papírové bankovky), proto bychom neměli hledět na trvanlivost jejich hmotného nosiče (potrhanou bankovku lze vyměnit za novou), nýbrž na trvanlivost subjektu, který je vydává. Pokud jde o fiat měny, vlády během staletí přicházely a odcházely a s nimi mizely i jejich peníze. Papírová

marka, rentová marka a říšská marka Výmarské republiky jsou dnes bezcenné, protože subjekt, který je vydával, už neexistuje. Z hlediska historické zkušenosti by tedy bylo pošetilé připisovat fiat měnám dlouhodobou trvanlivost – tak trochu výjimkou jsou v tomto ohledu pouze americký dolar a britská libra. Bitcoiny nevydává žádná centrální autorita a dá se předpokládat, že přetrvají, dokud bude fungovat síť, která je udržuje. Zatím je ovšem bitcoin pořád v plenkách a bylo by předčasné vyvozovat ohledně jeho trvanlivosti jednoznačné závěry. Nicméně je povzbudivé, že síť funguje už nemálo let navzdory nepřehlédnutelným pokusům některých států o regulaci a navzdory hackerským útokům. Svědčí to o pozoruhodné míře *antifragility*.[9]

PŘENOSITELNOST

Bitcoin je nejsnáze přenositelný uchovatel hodnoty, jaký kdy lidstvo používalo. Soukromé klíče ke stovkám milionů dolarů uložíte na malý USB disk a snadno přemístíte doslova kamkoliv. I takto vysoké částky lze navíc posílat téměř okamžitě z jednoho konce světa na druhý. Vysokou přenositelnost mají i fiat měny, protože jsou v zásadě digitální. Kvůli vládním regulacím a kapitálovým kontrolám ale přesuny velkých hodnot zpravidla trvají celé dny a někdy ani nejsou možné. Kapitálové kontroly[10] se dají obejít

9 https://www.bullishcaseforbitcoin.com/references/anti-fragility

10 Kapitálovou kontrolou se rozumí zásah státního aparátu (nejčastěji vlády nebo centrální banky) do peněžních toků firem i jednotlivců na území daného státu s cílem regulovat pohyb jak příchozího, tak odchozího kapitálu. Nejčastěji nabývají podoby zdanění, cla nebo regulace objemu obchodu a státní aparát pomocí nich reguluje, kolik domácího kapitálu může být v rukou cizích entit i kolik zahraničního kapitálu mohou držet občané a firmy daného státu. (pozn. red.)

pomocí hotovosti, což ale zase znamená značné riziko při jejím uchovávání a přepravě. Zlato, které je fyzické povahy a má neuvěřitelnou hustotu, je přenositelné zdaleka nejméně. Není divu, že většina zlatých slitků se vůbec nepřemísťuje. Při jejich prodeji si kupující a prodávající obvykle mezi sebou pouze převedou vlastnické právo, aniž by si slitek fyzicky předali, což ovšem oslabuje jistotu kupujícího, že zlato skutečně vlastní. Přeprava fyzického zlata na velké vzdálenosti je nákladná, nebezpečná a časově náročná.

ZAMĚNITELNOST

Vzorem zaměnitelnosti je zlato. Roztavenou zlatou unci v podstatě nelze odlišit od jiné a tato vlastnost se při obchodování se zlatem odjakživa využívala. Naproti tomu fiat měny jsou zaměnitelné jen natolik, nakolik jim to dovolí jejich emitenti. Obchodníci, kteří přijímají fiatové bankovky, sice většinou berou jednu jako druhou, ale v minulosti už se stalo, že se s bankovkami vysokých hodnot zacházelo jinak než s menšími. Například indická vláda ve snaze skoncovat s nezdaněným šedým trhem úplně vyřadila bankovky v hodnotě 500 a 1 000 rupií. Ty se pak následně obchodovaly za nižší než nominální hodnotu, takže přestaly být plně zaměnitelné s bankovkami nižších denominací. Bitcoiny jsou zaměnitelné na úrovni sítě, to znamená, že síť s každým přenášeným bitcoinem zachází stejně. Jelikož jsou ale mince na blockchainu (veřejném záznamu všech transakcí, které se kdy v bitcoinové síti uskutečnily) vysledovatelné, může se konkrétní bitcoin „ušpinit“ použitím při nezákonné transakci a obchodníky lze donutit, aby „špinavé“ mince nepřijímali. Dokud v bitcoinovém protokolu nedojde k vylepšení soukromí a anonymity, nelze u bitcoinů hovořit o totožné míře zaměnitelnosti jako u zlata.

OVĚŘITELNOST

Pravost jak fiat měn, tak zlata se v praxi dá ověřit celkem snadno, přesto se občané navzdory všem ochranným prvkům, které státy na své bankovky přidávají, občas nechají napálit falzifikátem. Ani zlato není vůči padělání imunní. Jistým vychytralým zločincům se dokonce podařilo podsunout investorům za cenu pravého zlata pozlacený wolfram.[11] Naproti tomu bitcoin lze ověřit s matematickou přesností. Vlastník může pomocí kryptografických podpisů veřejně prokázat, že dotyčné mince skutečně drží.

DĚLITELNOST

Bitcoiny se dělí na stomiliontiny. I takto nepatrné částky lze posílat, i když to kvůli poplatkům v síti může být neekonomické. Fiat měny jsou obvykle dělitelné až na úroveň drobných mincí s nepatrnou kupní silou, takže pro praktické použití je jejich dělitelnost dostatečná. Zlato sice je fyzicky dělitelné, ale s droboučkými zlomky v nízké hodnotě, vhodnými pro běžné každodenní transakce, by se obtížně manipulovalo.

VZÁCNOST

Vlastností, která nejzřetelněji odlišuje bitcoin od fiat měn a zlata, je jeho předem daná vzácnost. Protokol nikdy nedovolí vytvořit více než 21 milionů mincí. Vlastník bitcoinů tak bude mít přehled, jaké procento celkové peněžní zásoby drží. Má-li někdo například 10 bitcoinů, ví, že stejné množství jako on může vlastnit nanejvýš

11 https://www.bullishcaseforbitcoin.com/references/fake-gold

2,1 milionu lidí (necelé 0,03 % světové populace). Zlato je odjakživa poměrně vzácné, ale není imunní vůči zvyšování celkové zásoby. Pokud by se objevil nový, ekonomicky výhodný způsob jeho získávání (například těžba z mořského dna[12] nebo na asteroidech[13]), zásoba by dramaticky vzrostla. A konečně fiat měny, historicky poměrně nedávný vynález, prokázaly sklon k neustálému zvyšování nabídky. Státy mají neodolatelné nutkání nafukovat peněžní zásobu, kdykoliv se potřebují vypořádat s krátkodobými politickými problémy. Kvůli inflačním choutkám vlád celého světa tak musí vlastník fiat měny počítat s tím, že jeho úspory budou postupem času pravděpodobně ztrácet na hodnotě.

HISTORICKÁ PROVĚŘENOST

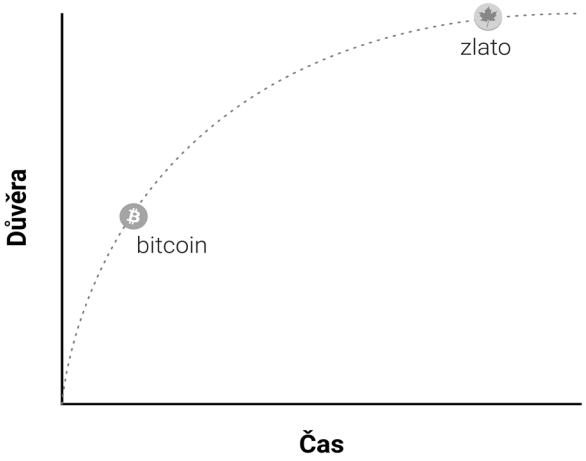
Žádný peněžní statek nemá tak dlouhou a barvitou historii jako zlato, kterého si lidé cení od samého vzniku civilizace. Mince vyražené v dávných dobách si dodnes uchovávají nezanedbatelnou hodnotu.[14] Totéž nelze říci o fiat měnách, které jsou poměrně nedávnou historickou anomálií. Už od svého zrodu pokaždé téměř nevyhnutelně směřují k naprosté bezcennosti. Málokterý stát v dějinách odolal pokušení uchýlit se k inflaci jako rafinovanému způsobu neviditelného zdanění občanů. Jestli dvacáté století, v němž fiatové peníze ovládly světový měnový řád, přineslo nějakou ekonomickou pravdu, pak je to poučení, že fiatovým penězům nelze důvěřovat, že by si dlouhodobě, nebo aspoň střednědobě, uchovaly hodnotu. Bitcoin navzdory své krátké existenci tolikrát obstál ve zkoušce trhem, že s největší pravděpodobností v dohledné době zůstane

12 https://www.bullishcaseforbitcoin.com/references/deep-sea-mining

13 https://www.bullishcaseforbitcoin.com/references/asteroid-mining

14 https://www.bullishcaseforbitcoin.com/references/hoxne-hoard

hodnotným aktivem. Lindy efekt[15] nás navíc učí, že čím déle tu bitcoin bude, tím větší budou mít lidé důvěru v jeho další přetrvání i ve vzdálené budoucnosti.[16] Jinými slovy, důvěra společnosti v nový peněžní statek mívá průběh, jaký ukazuje následující graf:



Pokud se bitcoin dožije dvacátých narozenin, budou téměř všichni věřit, že tu zůstane navždy, podobně jako jsou přesvědčeni, že v moderním světě bude trvale k dispozici internet.

ODOLNOST VŮČI CENZUŘE

Na první vlně poptávky po bitcoinech se do značné míry podílel nelegální drogový trh, z čehož mnozí mylně usoudili, že hlavním

15 Lindy efekt je odpozorovaný fenomén, který říká, že životnost technologie, ideje či instituce je úměrná jejímu dosavadnímu stáří. Je-li technologie stará x let, pravděpodobně bude fungovat ještě dalších x let. Jinými slovy, čím déle technologie existuje, tím větší je její šance na přežití. (pozn. red.)

16 https://www.bullishcaseforbitcoin.com/references/lindy-effect

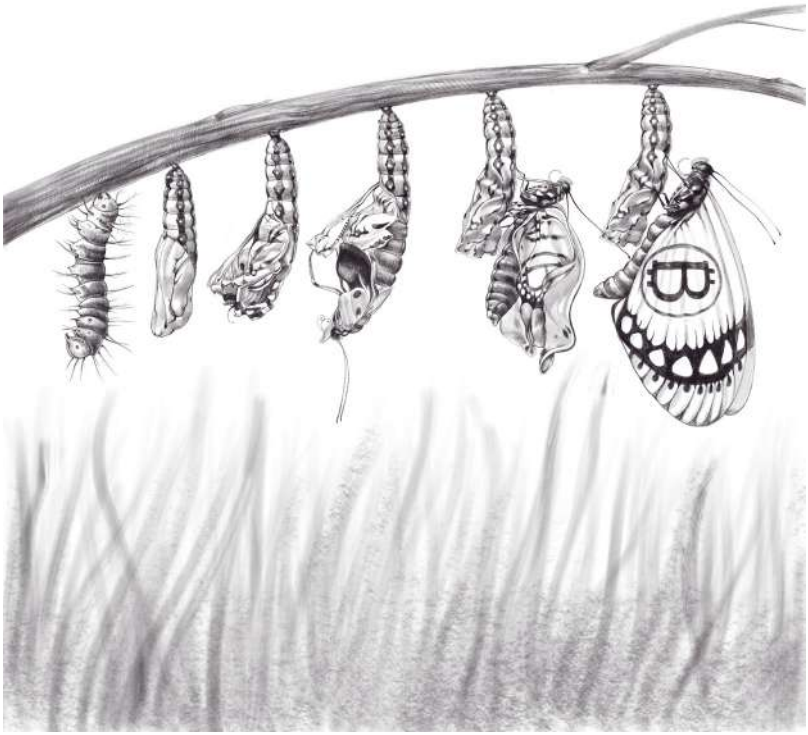
důvodem zájmu je zdánlivá anonymita. Přitom se ani zdaleka nejedná o anonymní měnu. Všechny transakce v bitcoinové síti se trvale zaznamenávají do veřejné účetní knihy a analýzou jejich historie lze při případném vyšetřování odhalit zdroj přesouvaných finančních prostředků. Právě to vedlo k dopadení pachatele nechvalně proslulého vykradení burzy MtGox.[17] Při dostatečné obezřetnosti a pečlivosti může uživatel bitcoinu opravdu skrýt svou identitu, ale to není hlavní důvod, proč byla tato měna při obchodování s drogami tak oblíbená. Její využití při zakázaných činnostech plyne především ze skutečnosti, že ke vstupu do bitcoinové sítě není třeba *žádného povolení*. Do přenosu bitcoinů nikdo nezasahuje, nikdo nerozhoduje, zda je transakce přípustná, nebo ne. Bitcoin je postaven jako distribuovaná peer-to-peer síť, takže je vůči cenzuře odolný ze samotné podstaty. Tím se naprosto liší od fiatového bankovního systému, který podléhá státním regulacím – banky a jiné finanční instituce jsou povinny hlásit pokusy o použití peněžních statků v rozporu se zákonem a předcházet jim. Klasickým příkladem regulace finančních transakcí jsou kapitálové kontroly. Rozhodne-li se dejme tomu bohatý milionář uprchnout ze státu s despotickým režimem, možná zjistí, že je pro něj nemožné nebo nebezpečné poslat si majetek do nového místa bydliště. Zlato sice nemá státního emitenta, ale kvůli své hmotné povaze se obtížně převáží a daleko více než bitcoin podléhá státní moci. Jako příklad regulace můžeme uvést indický zákon o kontrole zlata.[18]

Bitcoin vyniká nad všechny moderní i historické peněžní statky ve většině výše uvedených vlastností. To je samo o sobě pádným důvodem, proč by ho mělo začít používat co nejvíce lidí. Zejména účinná kombinace odolnosti vůči cenzuře a absolutní vzácnosti je silná motivace a přitahuje movité investory, aby část svého bohatství vložili do této rodící se třídy aktiv.

---

17 https://www.bullishcaseforbitcoin.com/references/mtgox-forensics

18 https://www.bullishcaseforbitcoin.com/references/india-gold-act



KAPITOLA 3

VZNIK A VÝVOJ PENĚZ

Moderní monetární ekonomie je posedlá penězi ve funkci prostředku směny. Monopol na jejich vydávání si během dvacátého století přisvojily státy a tak dlouho jim ubíraly roli uchovatele hodnoty, až lidem vnukly falešnou představu, že ten nejdůležitější účel peněz je být právě prostředkem směny. Proto se bitcoin stal terčem kritiky – prý není vhodnými penězi, jelikož kvůli vysoké volatilitě nemůže dost dobře sloužit jako prostředek směny. Takovým tvrzením ovšem takříkajíc zapřahám vůz před koně. Každé peníze procházejí vývojovými fázemi, nejprve slouží k uchování hodnoty a prostředkem směny se stanou až později. Jak vysvětluje William Stanley Jevons, jeden ze zakladatelů marginalistické ekonomie[19]:

> *„Podíváme-li se do historie… zlato zřejmě sloužilo za prvé jako ceněná komodita pro dekorativní účely, za druhé pro uchování bohatství, za třetí jako prostředek směny, a konečně jako měřítko hodnoty.“*[20]

Řečeno moderní terminologií, vývoj peněz vždy probíhá ve čtyřech fázích:

1. **Sběratelský předmět**: V první fázi vývoje bude poptávka po konkrétních penězích dána výhradně jejich zvláštními vlast-

19 Ekonomická teorie, která pracuje s malými změnami v nabídce a poptávce a mezními (marginálními) náklady. Na rozdíl od klasické školy se zaměřuje více na stranu poptávky a samotného spotřebitele, který usiluje o maximální uspokojení svých potřeb s co nejmenšími náklady. Tzv. marginalistická revoluce v 70. letech 19. století odstartovala v ekonomii zájem o lidské chování při ekonomickém rozhodování. (pozn. red.)

20 https://www.bullishcaseforbitcoin.com/references/jevons-quote

nostmi, jimiž dokážou uspokojit rozmary majitele. Lastury, korálky i zlato byly původně sběratelskými předměty a teprve později začaly plnit úlohu peněz, jak ji známe dnes.

2. **Uchovatel hodnoty**: Jakmile je po penězích díky jejich zvláštním vlastnostem dostatečná poptávka, začnou se používat k ukládání hodnoty a jejímu uchování v čase. Postupně si v tomto ohledu vybudují renomé, poptávka po nich roste a jejich kupní síla stoupá. Vývoj kupní síly uchovatele hodnoty nakonec dospěje do fáze plató (stagnace), kdy jej drží velké množství lidí a příliv dalších zájemců vysychá.

3. **Prostředek směny**: Jakmile se peníze plně zavedou coby uchovatel hodnoty, jejich kupní síla se stabilizuje, následně klesnou náklady příležitosti, spojené s jejich používáním při obchodních transakcích, a dané peníze se stanou vhodným prostředkem směny. V počátcích bitcoinu si mnozí neuvědomovali, jak obrovským nákladům ušlých příležitostí se vystavují, když jeho mince používají coby prostředek směny, a nikoliv jako perspektivní uchovatel hodnoty. Toto zmatení dobře ilustruje slavný příběh o zakoupení dvou pizz za 10 000 bitcoinů (v době psaní této knihy přibližně 480 milionů dolarů).[21]

4. **Zúčtovací jednotka**: Jakmile se peníze rozšíří coby prostředek směny, obchodníci v nich začnou uvádět ceny zboží a u převážné části statků tak bude znám jejich směnný poměr vůči dotyčným penězům. Představa, že informace o ceně mnoha druhů zboží je dnes k dispozici i v bitcoinech, je obecně rozšířený omyl. Můžeme si například koupit kávu za bitcoiny, ale cena, kterou si prodávající účtuje, není ve skutečnosti v bitcoinech, nýbrž ve státních penězích, přepočítaná aktuálním směnným kurzem dané měny vůči bitcoinu. Jestliže cena bitcoinu v příslušné fiat měně

21 https://www.bullishcaseforbitcoin.com/references/pizza-story

klesne, zaplatíte odpovídající větší množství mincí. Skutečnou zúčtovací jednotkou se bitcoin stane, teprve až jej obchodníci budou přijímat bez ohledu na jeho směnný kurz vůči fiat měnám.

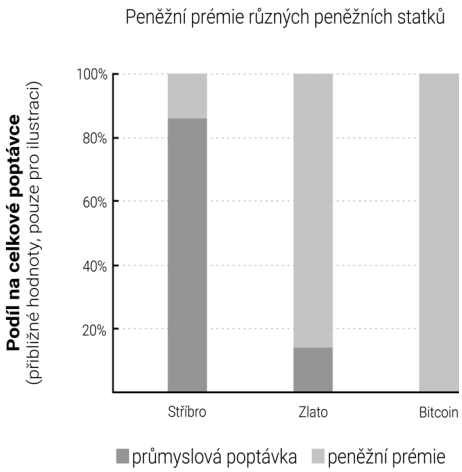
Peněžní statky, které zatím nedospěly do fáze zúčtovací jednotky, nelze považovat za plnohodnotné peníze. Takto dnes funguje zlato, které je uchovatelem hodnoty, ale státní zásahy je připravily o roli prostředku směny a zúčtovací jednotky. Někdy může úlohu prostředku směny zastávat jeden statek a ostatní role jiný. Obvykle k tomu dochází v zemích s nefunkční státní strukturou, například v Argentině nebo v Zimbabwe. Nathaniel Popper v knize *Digital Gold* píše:

„Americký dolar hladce plní všechny tři funkce peněz: je prostředkem směny, měrnou jednotkou ceny zboží i aktivem, v němž lze uchovávat hodnotu. Naproti tomu argentinské peso sloužilo jako prostředek směny při běžných nákupech, ale k uchovávání hodnoty je nepoužíval nikdo. Držet úspory v argentinských pesos se rovnalo vyhazování peněz. Proto lidé všechna pesos, která chtěli uspořit, směnili za dolary, jež si hodnotu držely mnohem lépe. Kvůli vysoké volatilitě pesos si také většinou pamatovali ceny v dolarech, které v běhu času představovaly spolehlivější měrnou jednotku.“

Bitcoin nyní přechází z první fáze proměny v peníze neboli monetizace (sběratelský předmět) do druhé (uchovatel hodnoty). Dalších několik let zřejmě potrvá, než se z perspektivního uchovatele hodnoty stane skutečným prostředkem směny, a cesta k tomuto cíli bude trnitá a plná nejistoty. Překvapivě podobnou dráhu opsalo před staletími zlato. Nikdo z našich současníků neměl dosud možnost sledovat proměnu nějakého statku v peníze v reálném čase, jako se to děje v případě bitcoinu, takže bude poučné pozorovat, jakou cestou se jeho monetizace bude ubírat.

ZÁVISLOST NA MINULÉM VÝVOJI

V průběhu monetizace prudce stoupá kupní síla peněžního statku. Bitcoin bývá v tomto ohledu nezřídka označován za bublinu, ovšem ti, kdo jej takto odsuzují a naznačují, že je hrubě nadhodnocený, bezděky uhodili hřebík na hlavičku. Společnou vlastností všech peněžních statků je skutečnost, že mají vyšší kupní sílu, než by vyplývalo z pouhé jejich užitné hodnoty. Většina peněz v dějinách ostatně vůbec žádnou užitnou hodnotu neměla. Rozdíl mezi kupní silou peněžního statku a jeho hypotetickou směnnou hodnotou založenou výhradně na jeho praktické využitelnosti označujeme pojmem peněžní prémie. Jak peněžní statek prochází jednotlivými fázemi monetizace (viz předchozí podkapitola), jeho peněžní prémie roste, ovšem ne rovnoměrně a už vůbec ne předvídatelně. Statek X může být v průběhu monetizace nahrazen statkem Y, který se ukázal být mnohem vhodnějšími penězi, načež peněžní prémie statku X klesne třeba až na nulu. Stříbro například o peněžní prémii přišlo téměř úplně, když je vlády celého světa koncem 19. století nahradily v roli peněz zlatem.



Vývoj peněžní prémie u nových peněz nelze předvídat, a to ani když pomineme vnější vlivy, například státní zásahy nebo konkurenci jiných peněžních statků. Jak poznamenal ekonom Larry White: „Tvrzení o bublině je ošemetné, jelikož se dá uplatnit na vývoj každé ceny, tudíž nijak nevysvětluje cenový vývoj konkrétního statku.“ [22]

Průběh monetizace odpovídá teorii her. Každý účastník trhu se snaží předvídat souhrnnou poptávku všech ostatních účastníků, a tedy budoucí peněžní prémii daného statku. Jelikož peněžní prémie není vázána na užitečnost statku jako takového, účastníci trhu při rozhodování, zda je levný, nebo drahý a zda jej koupit, nebo prodat, zpravidla vycházejí z historických cen. Propojenost aktuální poptávky s minulými cenami se nazývá závislost na minulém vývoji a je pravděpodobně největším zdrojem nepochopení cenových pohybů u peněžních statků. Postupně peněžní statek přijímá stále více lidí, jeho kupní síla roste a následně se proměňují představy trhu o tom, co je „levné“ a co „drahé“. Jestliže se cena peněžního statku naopak prudce propadne, může trh dojít k názoru, že předchozí ocenění bylo „nesmyslné“ nebo přehnaně nafouknuté. Závislost peněz na minulém vývoji ilustruje citát Joshe Browna, známého finančního manažera z Wall Street:

> *„Nakoupil jsem [bitcoin] při kurzu okolo 2 300 dolarů. Okamžitě jsem měl v ruce dvojnásobnou hodnotu a bitcoin rostl dál, tak jsem si začal říkat: ‚Víc už si nemůžu dovolit,‘ i když to vlastně byla jen a pouze moje utkvělá představa založená na ceně prvního nákupu. Pak se [bitcoin] minulý týden propadl kvůli krachu na čínských burzách a já jsem si pomyslel: ‚Skvělé, doufám, že půjde na dno, abych si mohl přikoupit.‘ “* [23]

22 https://www.bullishcaseforbitcoin.com/references/path-dependence

23 https://www.bullishcaseforbitcoin.com/references/josh-brown-quote

Pravda je taková, že používat v souvislosti s peněžními statky pojmy „levný“ a „drahý“ nedává žádný smysl. Cena peněžního statku neodráží jeho finanční toky ani míru jeho praktické užitečnosti, pouze ukazuje, nakolik je přijímán v té či oné roli peněz.

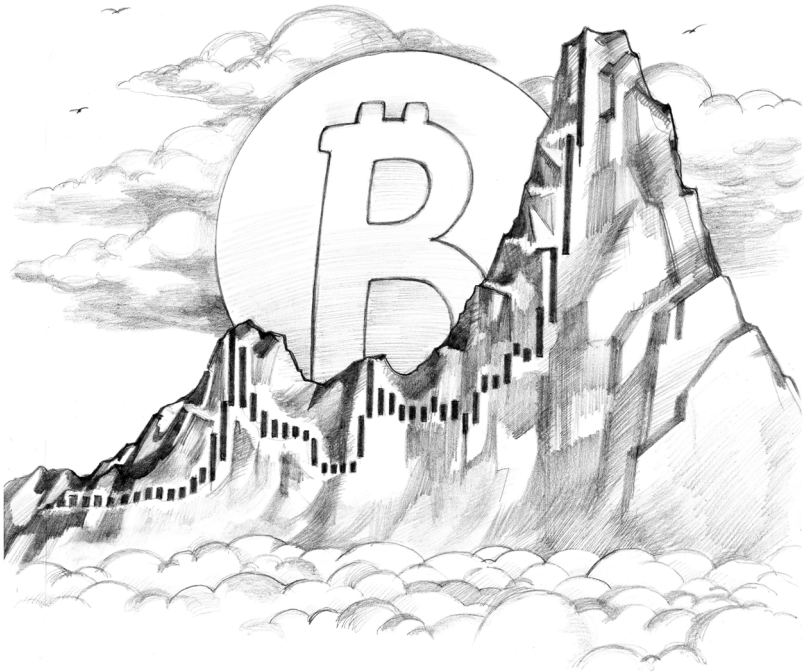
Aby toho nebylo málo, působí vedle závislosti peněz na minulém vývoji další skutečnost: účastníci trhu nejednají jako nezúčastnění pozorovatelé s jediným cílem, nakoupit nebo prodat podle předpokládaných budoucích pohybů peněžní prémie, ale také jako aktivní propagátoři. Jelikož objektivně správná výše peněžní prémie není nijak určena, mohou o nadřazenosti svého oblíbeného peněžního statku přesvědčovat ostatní účinněji než u obyčejných statků, jejichž hodnota je v konečném důsledku navázána na finanční toky nebo na užitečnost daného statku a poptávku po něm. U účastníků bitcoinového trhu můžeme na různých internetových fórech pozorovat takřka náboženské zanícení – majitelé bitcoinů horlivě vychvalují výhody tohoto aktiva a velikost bohatství, které lze investováním do něj získat. Leigh Drogen o bitcoinovém trhu poznamenal:

> *„Připomíná to náboženství – příběh, na kterém se všichni shodujeme a vyprávíme si jej navzájem. Vzpomeňme si na křivku adopce náboženství. Podobnost je téměř dokonalá – jakmile někdo přijme víru, začne o ní všem kázat a přesvědčovat je. Načež stejnou víru přijmou jeho přátelé a také začnou kázat.“*[24]

Přirovnání k náboženství může bitcoinu dodávat nádech iracionální víry, avšak z hlediska konkrétního vlastníka je zcela racionální přesvědčovat ostatní o nadřazenosti zvoleného peněžního statku

24 https://www.bullishcaseforbitcoin.com/references/leigh-drogen-quote

a z hlediska společnosti je zcela racionální přijmout ho jako standard. Peníze jsou základem veškerého obchodování a úspor, tudíž je výhodné přijmout dokonalejší peníze, protože se tím zmnohonásobí tvorba bohatství ku prospěchu všech členů společnosti.



KAPITOLA 4

PRŮBĚH MONETIZACE

HYPE CYKLY

Přestože se průběh monetizace peněžního statku neřídí žádnými předem danými pravidly, i poměrně krátká historie vývoje bitcoinu ukazuje na zajímavý vzorec. Cena bitcoinu jako by procházela soustavou stále se zvětšujících fraktálů, přičemž každé opakování odpovídá klasickému tvaru hype křivky popsané poradenskou společností Gartner, jak ukazuje graf na následující straně.

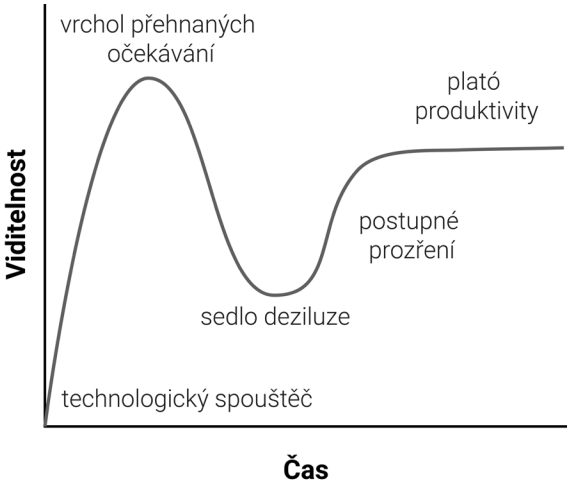
Michael Casey v článku „Speculative Bitcoin Adoption/Price Theory" (Spekulativní adopce bitcoinu – cenová teorie) dochází k závěru, že postupně rostoucí hype cykly jsou vlastně fáze křivky ve tvaru písmene S, typické pro průběh přijímání průlomových technologií a jejich zavádění do běžné praxe.[25]

Každý hype cyklus[26] začíná výbuchem nadšení pro novou technologii a účastníci trhu, k nimž se novinka během tohoto opakování dostane, vyženou cenu nahoru. První kupující v hype cyklu jsou zpravidla pevně přesvědčeni, že investují do průlomové technologie. Časem se příliv nových zájemců dosažitelných v daném cyklu vyčerpá, nadšení trhu dosáhne vrcholu a mezi kupujícími převládnou spekulanti zaměření víc na rychlý zisk než na technologii samotnou.

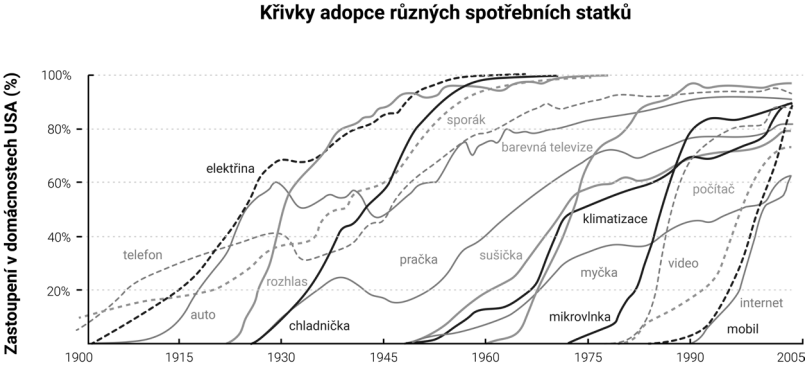
---

25 https://www.bullishcaseforbitcoin.com/references/speculative-adoption-theory

26 Americká výzkumná a poradenská společnost Gartner vypracovala křivku přijetí nové technologie, v češtině občas nazývanou též křivka humbuku (hype cycle). Jedná se o grafické znázornění pěti fází zralosti nových technologií a jejich postupného přijetí v čase. (pozn. red.)

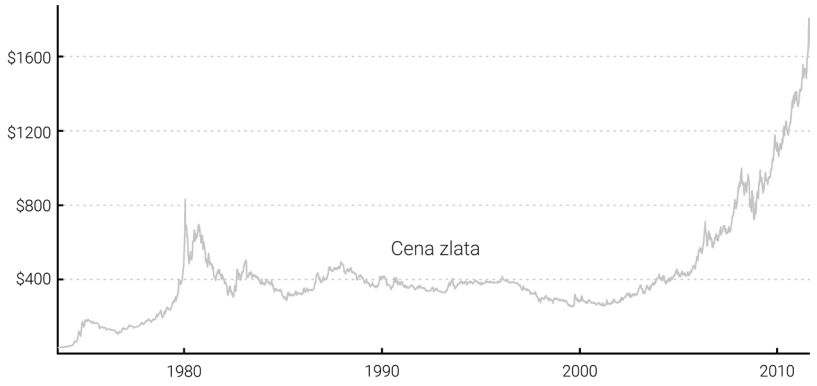


Vzápětí po vyvrcholení hype cyklu ceny prudce poklesnou a na místo spekulativní horečky nastoupí beznaděj, rozčarování veřejnosti a pocit, že technologie vlastně nebyla až tak průlomová. Nakonec cena dosáhne dna a potom postupně dospěje do vyrovnané fáze (tzv. fáze plató), kde se k původním, pevně přesvědčeným investorům, připojí nová kohorta těch, kdo dokázali přestát bolestivý pád a uvědomují si význam dané technologie.



Plató trvá dlouho a tvoří, jak říká Casey, „stabilní, nudnou nížinu“. Zájem veřejnosti ochabuje, ale technologie se dál rozvíjí a pomalu si získává další a další příznivce. Postupně se vybuduje základ pro nové opakování hype cyklu, které nastane, jakmile vnější pozorovatelé zjistí, že technologie přežila a že investice do ní možná nebude až tak riziková, jak se ve fázi propadu zdálo. Nový cyklus je daleko větší a technologii v něm přijme za svou mnohem více lidí.

Málokterý účastník hype cyklu dokáže správně předpovědět, jak vysoko vystoupá v daném opakování cena. V každém případě se cena zpravidla dostane na úroveň, která by investorům v předchozích fázích připadala nesmyslná. Propad po ukončení cyklu se v médiích obvykle dočká nějakého populárního vysvětlení. Všeobecně uváděná příčina, například krach burzy, ovšem sice může být spouštěčem, ale není pravým důvodem. Hype cykly končí, protože se vyčerpal počet účastníků trhu dosažitelný v daném cyklu.



Také zlato procházelo od konce 70. let 20. století do začátku 21. století klasickým vzorcem hype cyklů, což o mnohém svědčí. Můžeme se domnívat, že hype cyklus odráží společenské procesy spojené s průběhem monetizace.

TYPY INVESTORŮ

Na miniaturním bitcoinovém trhu se až do spuštění burzy MtGox v červenci 2010 žádné hype cykly neprojevovaly. Trh ovládala malá uzavřená skupina kryptografů, informatiků a cypherpunkerů, kteří díky své erudici dokázali rozpoznat význam průlomového vynálezu Satoshiho Nakamota a v první řadě se starali, aby protokol bitcoinu neobsahoval technické chyby. Ceny se stanovovaly ad hoc buď při přímé směně za jinou měnu, nebo při výměnném obchodu, jakým byl například nákup dvou pizz za 10 000 bitcoinů, který uskutečnil Laszlo Hanyecz. Cena bitcoinu se v tehdejších pionýrských dobách pohybovala hluboko pod jedním americkým dolarem.

V roce 2010 byl poprvé stanoven směnný kurz bitcoinu na burze. Následně trh prošel čtyřmi hlavními hype cykly a zpětně můžeme přesně určit cenová rozpětí jednotlivých cyklů. Rovněž dokážeme popsat, jaký typ investorů bitcoin přilákal v tom kterém cyklu.

0,06–30 USD (červenec 2010 – červenec 2011): V prvním cyklu vidíme vytrvalý příliv ideově motivovaných investorů, oslněných možnostmi nestátních, digitálních peněz. Libertariáni jako Roger Ver a Ross Ulbricht do bitcoinu nastoupili v naději, že všeobecné přijetí této nově se zrodivší technologie umožní působit proti zavedeným pořádkům. Cyklus dosáhl vrcholu měsíc poté, co blog Gawker zveřejnil článek o bitcoinu a jeho využití na webové stránce Silk Road, kterou založil Ulbricht. Článek si získal velkou popularitu. Silk Road umožňovala nákup zakázaných látek za bitcoiny a byla jedním z prvních zdrojů poptávky po této digitální měně.

30–1 154 USD (srpen 2011 – prosinec 2013): Ve druhém cyklu do bitcoinu nastoupili nejodvážnější investoři ochotní jít do rizika s převratnou, nevyzkoušenou technologií, například Argentinec Wences Casares, jenž v bitcoinu spatřoval možný lék na ničivé hospodářské dopady hyperinflace, kterou zažil jako dítě. Casares

coby nadaný sériový podnikatel vybavený množstvím kontaktů přesvědčil o užitečnosti bitcoinu některé vlivné technology a investory ze Silicon Valley, a proslavil se tak jako „pacient nula" při šíření takzvaného „myšlenkového viru".

Druhého hype cyklu se účastnili také bratři Winklevossovi – dvojčata, která vedla s Markem Zuckerbergem spor o zakladatelské právo k Facebooku a získala od jeho společnosti obrovské odškodné. Vyplacení vysoké sumy Winklevossovi slavili na Ibize a při náhodném setkání s investorem Davidem Azarem se tam poprvé dozvěděli o nové investiční příležitosti. Okamžitě se o bitcoin začali zajímat a nakonec do něj vložili svůj nově nabytý kapitál.

Investoři v prvním a druhém hype cyklu měli dost odvahy pustit se po neprozkoumaných, riskantních cestách, jimiž se tehdy jedině dalo dostat k bitcoinům. Hlavním zdrojem likvidity na trhu byla v tomto období burza MtGox se sídlem v Japonsku, vedená neschopným a zločinným Markem Karpelesem, který byl pro své nekalé jednání později odsouzen k trestu odnětí svobody za podíl na pádu burzy.

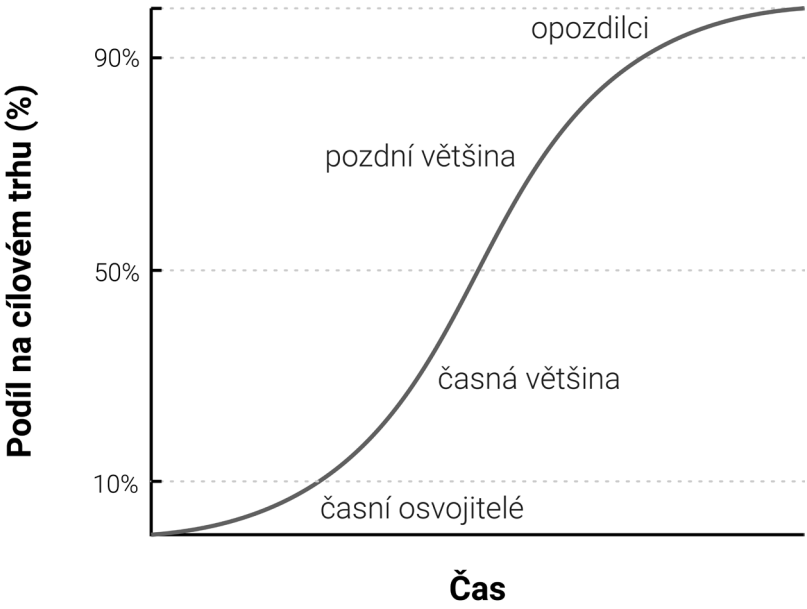
1 154–19 600 USD (leden 2014 – prosinec 2017): Třetí hype cyklus přilákal první větší příliv investorů, jimž nebyl již nijak myšlenkově blízký étos cypherpunku, ze kterého bitcoin vzešel. Na křivce adopce ve tvaru písmene S se tito noví investoři objevují jako „časní osvojitelé" (viz graf na následující straně).

Willy Woo analyzoval blockchain a burzovní data za toto období a zjistil, že mezi novými příchozími převládali drobní investoři a že počet uživatelů na celém světě vzrostl z přibližně 1–2 milionů na více než 14 milionů.[27] Cyklus uzavřela spekulativní horečka, jež následovala po spuštění laviny alternativních kryptoměn (altcoinů), které s bitcoinem soutěžily o ovládnutí trhu.

---

27 http://bullishcaseforbitcoin.com/references/willy-woo-data

Převážná většina těchto altcoinů už mezitím stačila upadnout v zapomnění.



Je třeba dodat, že růst ceny bitcoinu v uvedených hype cyklech do značné míry souvisel s rostoucím objemem likvidity a s tím, jak se nákup bitcoinů zjednodušoval. V prvních dvou cyklech byla hlavním zdrojem likvidity MtGox, ovšem obstarat a zabezpečit si na této špatně spravované burze bitcoiny bylo natolik složité, že se do toho mohli pustit jen technologicky nejzdatnější investoři. Pokud se někomu přece jen podařilo poslat na MtGox peníze, dost možná o ně nakonec stejně přišel při hackerském útoku a následném uzavření burzy. Začátkem třetího hype cyklu se začaly objevovat další burzy. Přesto se zájemci o bitcoin i po zhroucení MtGox a nástupu schopnějších konkurentů na její místo potýkali se zásadními překážkami. Málokterá banka byla ochotna

s burzami obchodovat. Některé burzy, například Coinbase, navíc nezvládaly silný provoz a trpěly výpadky služeb. Nově vznikající finanční infrastruktura se zatím stěží batolila na vratkých nohách.

Teprve po skončení třetího hype cyklu a po dvouleté stagnaci tržní ceny bitcoinu přišly vyspělé, hluboké zdroje likvidity, například mimoburzovní makléři, spolehlivější regulované burzy a termínové trhy, jako Chicagská komoditní burza (Chicago Mercantile Exchange). Když v roce 2020 začal čtvrtý hype cyklus, mohli už drobní i institucionální investoři bitcoiny nakupovat a zabezpečit poměrně jednoduše.

19 600–? USD (leden 2018 – ?): V době psaní této knihy bitcoinový trh prochází čtvrtým větším hype cyklem. Zdroje likvidity jsou nyní hlubší a vyspělejší, takže se mohou zapojit i velcí institucionální investoři – část svých prostředků už do bitcoinu umístilo několik významných správců majetku, například Paul Tudor Jones a Stanley Druckenmiller. Kromě fondů správy majetku do bitcoinu investovaly také veřejně obchodované společnosti Tesla, MicroStrategy a Square, buď částečně, nebo v případě MicroStrategy zcela, a šly tak příkladem ostatním velkým korporacím.

Trh bitcoinu je již natolik rozvinutý, že v nynějším hype cyklu bude zřejmě hrát důležitou roli institucionální poptávka. Jak ve sdělení zákazníkům napsal Philip Gradwell, CEO společnosti Chainalysis zabývající se analýzou blockchainu:

> *„Data stále zřetelněji ukazují na účast institucionálních investorů… Poptávku ženou nahoru severoameričtí investoři na fiatových burzách, přičemž mezi zájemci převažují instituce.“*[28]

28 https://www.bullishcaseforbitcoin.com/references/gradwell-quote

Podle studie vypracované Centrem pro alternativní finance při Cambridgeské univerzitě (Cambridge Centre for Alternative Finance) bylo na světě ve třetím čtvrtletí roku 2020 „celkem až 101 milionů uživatelů kryptoaktiv“.[29] Zdá se, že v nynějším hype cyklu je bitcoin, pokud jde o všeobecné přijetí, na nejlepší cestě posunout se na S-křivce z fáze „časní osvojitelé“ do fáze „časná většina“. Zpřístupnění regulovaných termínových trhů otevřelo cestu k vytvoření bitcoinového ETF (burzovně obchodovaného fondu), který v dalších cyklech přivede do bitcoinu „pozdní většinu“ a „opozdilce“.

Neumíme sice předpovědět, kam až nynější hype cyklus vystoupá, ale patrně lze předpokládat, že se v něm bitcoin do značné míry přiblíží tržní kapitalizaci zlata – svého nejbližšího příbuzného v celosvětové rodině finančních aktiv.

HALVINGY A JEJICH NÁSLEDKY

Bitcoiny vznikají procesem označovaným jako těžba, který je založen na konkurenci a na vynakládání výpočetního výkonu. Časový harmonogram vytváření nových bitcoinů je předem pevně dán bitcoinovým protokolem. Ten určuje, že přibližně každých 10 minut některý těžař (počítač zapojený do bitcoinové sítě) vytěží nový blok, za což pak obdrží pevně stanovený počet bitcoinů neboli odměnu za vytěžení bloku. Všechny bitcoiny existující v bitcoinové síti tak původně pocházejí z odměny za vytěžení bloku.

Přibližně každé čtyři roky, nebo přesněji vždy jednou za 210 000 bloků, se odměna snižuje na polovinu. Této události se říká halving (půlení). V prvních čtyřech letech existence bitcoinu činila odměna

29 https://www.bullishcaseforbitcoin.com/references/benchmarking-study

za vytěžení nového bloku 50 mincí. Další čtyři roky to bylo 25 mincí. V nynější epoše (období mezi halvingy), která začala v květnu 2020, získávají těžaři za každý blok pouze 6,25 bitcoinu. Přibližně v roce 2140 klesne odměna na nulu a těžba přestane vytvářet nové bitcoiny. Investoři by tedy určitě měli zvážit, jaký vliv mají halvingy na cenu bitcoinu a zda trh dokáže tyto nabídkové šoky, přicházející každé čtyři roky, odpovídajícím způsobem „zacenit".

Bitcoinový protokol je nastaven tak, že velikost výpočetního výkonu potřebného k vytěžení bloku se pravidelně přizpůsobuje, aby produkce nových bitcoinů během každé epochy ohraničené halvingy zůstávala víceméně rovnoměrná. Jestliže se zvýší celkový výpočetní výkon vynakládaný na těžbu, zvýší se také obtížnost těžby, a vytěžit nový bitcoin tudíž bude nákladnější. Kvůli této úpravě obtížnosti se z těžařů stávají v podstatě mezní producenti a jejich zisk z těžby se v průběhu času přibližuje k nule. Obvykle proto potřebují většinu vytěžených bitcoinů prodat, aby pokryli provozní náklady, z nichž zdaleka největší část tvoří výdaje za elektrickou energii. Tím neustále tlačí cenu bitcoinu dolů. Při každém halvingu se tlak na pokles ceny, vyvolaný prodejem vytěžených bitcoinů, sníží přibližně na polovinu.

Pokud by se nezměnilo nic jiného a zároveň by poptávka po bitcoinech zůstala stejná, vedl by halving k převisu poptávky nad nabídkou, tudíž k růstu ceny. Jelikož se ví předem, kdy k halvingu dojde, měli by účastníci trhu s touto událostí počítat a patřičně ji zohlednit v ceně („zacenit"). V minulosti se tak ovšem nedělo a cena po každém halvingu výrazně vzrostla. Dalo by se dokonce spekulovat, že halving je spouštěčem pravidelných hype cyklů na bitcoinu.

V této kapitole jsme si ukázali, že cena bitcoinu začne vždy na konci hype cyklu prudce padat, až dosáhne rovnovážného stavu mezi poptávkou skalních příznivců na jedné straně a nabídkou

spekulantů snažících se vystoupit z trhu a těžařů, kteří prodejem kryjí produkční náklady, na straně druhé. Halving tuto rovnováhu naruší a volné bitcoiny se z trhu začnou pomalu, ale jistě přesouvat do rukou dlouhodobých investorů. Množství dostupných mincí klesá, tudíž začne stoupat cena, a právě tento zdánlivě nezvratný cenový růst zřejmě spouští typické „davové šílenství", po němž následuje parabolická (růstová) fáze hype cyklu.

Možným důvodem, proč halvingy nebyly v minulosti zohledňovány v ceně, je skutečnost, že v okamžiku, kdy halving spouští nový hype cyklus, není jasné, jak velká skupina potenciálních investorů bude v daném cyklu dosažitelná a do jaké míry budou její členové ochotni ukládat úspory do bitcoinu. Věc dále komplikují složité smyčky zpětné vazby v průběhu monetizace. Jak jsme si už řekli, někteří jedinci se nespokojí s pouhou investicí do bitcoinu, ale začnou o jeho výhodách coby prostředku k uložení úspor aktivně přesvědčovat ostatní. Pravděpodobně nedokážeme změřit, o kolik se díky této propagaci zvětší skupina potenciálních investorů.

VSTUP STÁTŮ

Závěrečný hype cyklus na bitcoinu nastane, až jej do svých devizových rezerv začnou nakupovat státy. Zatím je jeho tržní kapitalizace tak nízká, že by to pro většinu zemí nemělo smysl, ale jak poroste zájem soukromého sektoru, bitcoin se co do tržní kapitalizace přiblíží zlatu a dosáhne likvidity, která většinu států přiměje do něj vstoupit. Jakmile jej do svých rezerv oficiálně zařadí první, začnou se pravděpodobně o překot přidávat další. Pokud se bitcoin nakonec stane globální rezervní měnou, pocítí to ve svých bilancích nejpříznivěji země, které jej přijaly jako první. Bohužel to s největší pravděpodobností budou ty s nejsilnější výkonnou

mocí, například diktatury jako Severní Korea. Západní demokracie budou při nákupech bitcoinu do státních rezerv nejspíš váhat a zaostávat, jednak kvůli neochotě napomáhat zmíněným diktaturám při zlepšování finanční situace a jednak proto, že mají z podstaty věci slabou výkonnou moc.

Paradoxně dnes mezi země s nejvolnějším regulatorním přístupem k bitcoinu patří Spojené státy, zatímco k nejvíce nepřátelským se řadí Čína a Rusko. Ačkoliv je to právě USA, kdo riskuje největší oslabení geopolitické pozice v případě, že bitcoin coby světová rezervní měna nahradí dolar. Francouzský prezident Charles de Gaulle už v 60. letech 20. století kritizoval Spojené státy, že si na konferenci v Bretton Woods roku 1944 ušily mezinárodní měnový pořádek na míru a těží z něj „nehoráznou výsadu". Ruské a čínské vládě se zatím nerozbřesklo, jakou geostrategickou výhodu by přijetí bitcoinu coby rezervní měny znamenalo, a zajímají se spíše o jeho možné dopady na své vnitřní trhy. Podobně jako de Gaulle, který v 60. letech 20. století pohrozil, že v odpovědi na nehoráznou výsadu USA znovu zavede klasický zlatý standard, si ale Číňané a Rusové časem uvědomí, jak je výhodné držet velkou rezervu v nestátním uchovateli hodnoty. Jelikož největší podíl těžebního výkonu se nachází právě v Číně, má tamní vláda už teď oproti ostatním daleko širší možnosti, jak bitcoiny začlenit do státních rezerv.

Američané se rádi chlubí, že jsou národem inovátorů. Výstavním klenotem jejich ekonomiky je Silicon Valley, které zatím hrálo prim také v debatách o tom, jak by regulátoři měli přistupovat k bitcoinu. I bankovní sektor a Fed už ale konečně začínají tušit, jakou existenční hrozbu by pro měnovou politiku USA znamenalo, kdyby se bitcoin stal globální rezervní měnou. Deník Wall Street Journal, známá hlásná trouba Fedu, se k ohrožení měnové politiky USA ze strany bitcoinu vyjádřil v komentáři:

„Existuje ještě jedno nebezpečí, z pohledu centrálních bank a regulátorů možná dokonce závažnější: bitcoin nemusí zkrachovat. Je-li spekulativní horečka na této kryptoměně pouhou předzvěstí jejího všeobecného přijetí coby alternativy k dolaru, ohrozí bitcoin monopol centrálních bank na peníze.“[30]

V nadcházejících letech proběhne velká bitva. Na jedné straně se podnikatelé a inovátoři budou snažit udržet bitcoin mimo regulace, na druhé straně budou komerční a centrální banky vahou svého vlivu regulaci prosazovat, aby zabránily oslabování odvětví a své moci spojené s vydáváním peněz.

PŘECHOD K PROSTŘEDKU SMĚNY

Peněžní statek se nemůže stát všeobecně přijímaným prostředkem směny (tak zní standardní ekonomická definice peněz), dokud ho většina lidí neuzná za hodnotný – paradoxně právě proto, že statek bez uznávané hodnoty nebude při směně nikdo chtít přijímat. Jak statek v očích většiny postupně získává hodnotu, začne sloužit jako její uchovatel, jeho kupní síla prudce vzroste a vzdát se ho při směně s sebou ponese náklady ušlých příležitostí. Ty pak musejí klesnout na přijatelně nízkou úroveň, aby se statek konečně mohl stát všeobecně přijímaným prostředkem směny.

Přesněji vyjádřeno, peněžní statek je vhodným prostředkem směny, pouze pokud součet nákladů ušlých příležitostí a transakčních nákladů spojených s jeho užitím při směně je nižší než náklady, které by vznikly, kdyby se obchod měl uskutečnit bez tohoto prostředku směny.

---

30 https://www.bullishcaseforbitcoin.com/references/wsj-quote

Ve společnosti založené na směnném obchodu se uchovatel hodnoty může stát prostředkem směny i tak, že jeho kupní síla vzroste kvůli mimořádně vysokým transakčním nákladům spojeným s přímou směnou. V rozvinuté ekonomice, kde jsou transakční náklady nízké, může jako prostředek směny sloužit i nově vzniklý a rychle se zhodnocující uchovatel hodnoty, například bitcoin, avšak pouze v omezené míře. Příkladem je nelegální drogový trh, kde jsou kupující ochotni obětovat příležitost spojenou s držením bitcoinů, aby co nejvíce omezili riziko, které by při nákupu drog za fiat měnu bylo značné.

Proměně nového uchovatele hodnoty ve všeobecně přijímaný prostředek směny ale v rozvinuté společnosti brání zásadní institucionální překážky. Státy chrání své peníze před konkurenčními peněžními statky a jako účinný prostředek k tomu využívají zdanění. Státní peníze jsou tak zvýhodněny nejen tím, že je po nich trvalá poptávka, ale také tím, že daně je dovoleno platit pouze v nich. Konkurenční peněžní statky jsou navíc při každé směně daněny na základě své aktuální tržní ceny, což využití uchovatele hodnoty jakožto prostředku směny podstatně ztěžuje.

Popsané znevýhodnění tržních peněžních statků ovšem jejich proměně ve všeobecně přijímaný prostředek směny nemůže tak docela zabránit. Státní peníze mohou například ztratit důvěru lidí a postupně se stát naprosto bezcennými. Tento jev se nazývá hyperinflace. Při ní se hodnota státních peněz nejprve zhroutí v poměru k nejlikvidnějšímu statku, který je v dané společnosti dostupný, například ke zlatu nebo zahraniční měně, třeba americkému dolaru. Nejsou-li likvidní peněžní statky k dispozici nebo je-li jejich nabídka omezená, dochází k hyperinflaci státních peněz vůči hmotným statkům, například nemovitostem a komoditám. Když se řekne hyperinflace, představíme si většinou samoobsluhu s prázdnými regály, odkud si zákazníci odnesli vše, co se odnést dalo, jen aby předběhli prudký pád hodnoty státních peněz.

Nakonec ve státní peníze všichni zcela ztratí víru, nikdo je nebude přijímat a společnost se buď vrátí ke směnnému obchodu, nebo si namísto původních peněz najde zcela jiný prostředek směny. Jako příklad tohoto procesu můžeme uvést nahrazení zimbabwského dolaru americkým dolarem. Problémem při nahrazování státních peněz penězi jiného státu je ovšem jednak nedostatek zahraničních peněz a jednak to, že nelze dost dobře získávat likviditu ze zahraničních bank.

Bitcoin je pro lidi postižené hyperinflací ideální peněžní statek, jelikož se dá snadno přesouvat do jiných zemí a nepotřebuje ke svému fungování bankovní systém. Jak budou fiatové měny v nadcházejících letech pokračovat v historickém vývoji směrem k bezcennosti, bude bitcoin získávat po celém světě stále větší oblibu coby prostředek pro ochranu úspor. Až některá země upustí od používání státních peněz a nahradí je bitcoinem, bude to znamení, že proměna z uchovatele hodnoty ve všeobecně přijímaný prostředek směny je dokončena. Daniel Krawisz pro tento proces vytvořil termín hyperbitcoinizace.[31]

31 https://www.bullishcaseforbitcoin.com/references/hyperbitcoinization

KAPITOLA 5

NOVÝ MĚNOVÝ ZÁKLAD

OBLÍBENÉ OMYLY

V předchozích kapitolách jsme si objasnili peněžní povahu bitcoinu. Nyní se tedy můžeme podívat, jaké nejčastější omyly se s tímto přelomovým peněžním statkem pojí.

JE BITCOIN BUBLINA?

Bitcoinu se vytýká, že má peněžní prémii. Prý se proto jedná o bublinu. Jenže peněžní prémii mají všechny peněžní statky. Peněžní prémie (zvýšení hodnoty statku oproti úrovni, jež by plynula čistě jen z poptávky dané jeho praktickou užitečností) je

přímo určujícím znakem každých peněz. Dalo by se tedy v jistém smyslu říci, že každé peníze vždy a všude jsou bublina. V prvních fázích adopce nových peněz může peněžní statek paradoxně být zároveň bublinou a zároveň být *podhodnocený*.

CENA BITCOINU KOLÍSÁ. LZE V NĚM UCHOVÁVAT HODNOTU?

Bitcoin kolísá, protože je nový. V prvních několika letech své existence se choval jako levná akcie. Jakmile jej někdo nakoupil ve větším množství – vzpomeňme si například na bratry Winklevossovy – cena vyletěla nahoru. Postupem let do něj vstupovalo stále více lidí, rostla likvidita a úměrně tomu se snižovala volatilita. Jakmile bitcoin dosáhne stejné tržní kapitalizace, jako má zlato, měl by také vykazovat podobnou míru volatility. Až zlato co do tržní kapitalizace překoná, klesne mu volatilita natolik, že se bude moci stát všeobecně používaným prostředkem směny. Jak už jsme uvedli, přeměna bitcoinu v peníze probíhá v řadě po sobě následujících hype cyklů. Nejnižší volatilita je ve fázi plató (stagnace), nejvyšší na vrcholu a ve fázi propadu. Každý hype cyklus vykazuje nižší volatilitu než předchozí, protože trh má větší celkovou likviditu.

JE BITCOIN PŘÍLIŠ DRAHÁ INVESTICE?

Nováčci si často stěžují, že koupit jeden bitcoin vyjde příliš draho. Mylně se totiž domnívají, že bitcoiny lze získávat pouze vcelku, nikoliv po menších částech. Bitcoinové mince jsou ovšem dělitelné, takže lze investovat už po nepatrných sumách, například po jednom dolaru. Přání vlastnit celý bitcoin bývá někdy dáno také vlastností lidské psychiky, která se nazývá jednotkové zkreslení *(unit bias)* a projevuje se podvědomým přáním beze zbytku dokončit úkol nebo splnit cíl. Podle výzkumů může být jednotkové zkreslení dokonce jednou z příčin lidského sklonu k přejídání.[32]

32 https://www.bullishcaseforbitcoin.com/references/unit-bias

Touha vlastnit celou jednotku vede mnohé investory k mylnému přesvědčení, že konkurenční kryptoměny jsou oproti bitcoinu cenově příznivější, protože jedna mince vyjde levněji. Jenomže nižší jednotková cena je u nich dána mnohem vyšší nabídkou, která je určována libovolně a sama o sobě nijak nevyjadřuje hodnotu té které kryptoměny. Spíše než na jednotkovou cenu by se investoři měli zaměřit na tržní kapitalizaci a likviditu měny jako takové. U bitcoinu je jeho mnohem větší kapitalizace a podstatně hlubší likvidita dána silným síťovým efektem a užitečností této měny coby uchovatele hodnoty.

Kromě toho se investoři obávají, že finanční výnosy na bitcoinu jsou spíše věcí minulosti než budoucnosti. Jelikož bitcoin v počátcích vyletěl jako raketa, mají teď mnozí pocit, že propásli tu pravou chvíli. Je sice pravda, že v procesu přeměny ekonomického statku v peníze získávají největší finanční výhody první vlastníci (pokud jej dokážou držet dlouhodobě), ale to neznamená, že se pozdější příchozí nemohou dočkat slušných výnosů. Postupem času bude výnosnost klesat, protože příliv dalších volných úspor do nového peněžního statku zpomalí a nakonec vyschne. Bitcoin k sobě ale může přetáhnout veškerou stávající poptávku po uchovatelích hodnoty v objemu stovek bilionů dolarů, například poptávku po zlatě, státních dluhopisech, nemovitostech a výtvarném umění. Trh tedy zatím zjevně není bitcoinem plně nasycen. I kdyby se bitcoin stal světovou rezervní měnou a příliv úspor do něj by se stabilizoval, vlastníci mincí by stále dosahovali finanční návratnosti v míře úměrné výkonnosti světového hospodářství, v němž by bitcoin fungoval jako zúčtovací jednotka.

JSOU TRANSAKČNÍ POPLATKY PŘÍLIŠ VYSOKÉ?

Kritici v poslední době namítají, že bitcoin kvůli rostoucím poplatkům za transakce není vhodným platebním systémem. Jenže zvyšování transakčních poplatků je zdravé a je třeba s ním počítat.

Musíme je totiž vnímat jako náklad, jehož hrazením umožňujeme těžařům potvrzovat transakce, a tím zabezpečovat bitcoinovou síť. Vedle transakčních poplatků dostávají těžaři už jen odměnu za vytěžení bloku, což je v podstatě inflační příjem, jehož náklady nesou stávající majitelé mincí.

Bitcoin má pevně daný časový harmonogram uvolňování nových mincí do oběhu (díky této měnové politice je dokonalým uchovatelem hodnoty), takže odměna za vytěžení bloku jednou klesne na nulu a na zabezpečování sítě budou muset stačit transakční poplatky. „Nízké" poplatky v síti by znamenaly malou bezpečnost a náchylnost k cenzurním zásahům zvenčí. Ti, kdo u alternativ k bitcoinu lákají na nízké poplatky, bezděky poukazují na slabé místo těchto takzvaných altcoinů.

Kritika „vysokých" poplatků vychází z mylného přesvědčení, že bitcoin má být především platidlem a teprve v druhé řadě uchovatelem hodnoty. Jak jsme si ukázali v kapitole o původu peněz, toto uvažování znamená zapřahat vůz před koně. Bitcoin se může stát vhodným prostředkem směny, teprve až důkladně zakoření coby uchovatel hodnoty. Navíc v době, kdy se náklady příležitosti spojené s obchodováním v bitcoinu dostanou na úroveň umožňující jeho použití coby prostředku směny, nebude většina transakcí probíhat přímo v bitcoinové síti, ale spíše v sítích druhé vrstvy s mnohem nižšími poplatky. Na těchto nadstavbových sítích si účastníci mezi sebou mohou posílat mince mimo bitcoinový blockchain *(off-chain)*, to znamená aniž by se každá transakce přenášela ke všem uzlům podkladové sítě, a do hlavní účetní knihy se zaznamenává až závěrečné vypořádání. Díky sítím druhé vrstvy lze provádět mnohem více levných a rychlých transakcí, než by bylo možné přímo na blockchainu *(on-chain)*.

Sítě druhé vrstvy, například Lightning Network, jsou vlastně moderní obdoba směnek, které se v devatenáctém století použí-

valy při převodu vlastnického práva ke zlatu. Banky je vydávaly, protože přemístit zlatý slitek bylo mnohem nákladnější než předat papírové potvrzení. Lightning Network ovšem na rozdíl od směnek umožňuje levně převádět bitcoiny zpravidla bez účasti důvěryhodné třetí strany, například právě banky. Vznik Lightning Network znamená v dějinách bitcoinu zásadní technické vylepšení, jehož užitečnost se naplno projeví, až se toto řešení v nejbližších letech dále rozvine a rozšíří.

SPOTŘEBOVÁVÁ BITCOIN PŘÍLIŠ MNOHO ELEKTŘINY?

Mnozí odpůrci bitcoinu poukazují na energetickou náročnost těžby a upozorňují, že může mít nepříznivý vliv na životní prostředí. Oblíbeným argumentem je, že bitcoinová síť spotřebovává více elektřiny než malý stát, což prý už samo o sobě svědčí v neprospěch bitcoinu. Podle výpočtů Centra pro alternativní finance při Cambridgeské univerzitě bitcoinová síť v době psaní této knihy spotřebovávala ročně přibližně 105 terawatthodin elektřiny. Investoři si mohou právem klást otázku, zda společnost v budoucnosti takto významnou spotřebu unese a zda to nepovede k politickému ohrožení další existence bitcoinu.

Politici a investoři by ale při kritickém zkoumání energetické náročnosti bitcoinu neměli zůstat u povrchních módních hesel. Nestranné posouzení musí vzít v potaz hlubší detaily, například odkud pochází energie, kterou bitcoin spotřebovává, zda škodí životnímu prostředí, zda nechybí jinde, a především, co užitečného takto vynaložená energie přináší společnosti. V této podkapitole se vynasnažím prozkoumat zmíněné detaily pomocí srovnávací analýzy bitcoinu a jeho hlavních konkurentů. Pohlížíme-li na bitcoin jako na systém umožňující uchovávat a přenášet hodnotu, jsou jeho nejbližšími konkurenty zlato a různé celosvětově používané systémy fiat měn.

Hass McCook v roce 2014 zkoumáním recenzovaných studií o ekologických dopadech těžby zlata dospěl k závěru, že roční spotřeba energie na těžbu zlata činí přibližně 475 gigajoulů neboli 132 terawatthodin.[33]

Dobývání zlata zanechává v krajině hluboké a nepřehlédnutelné ekologické stopy

Na první pohled by se sice mohlo zdát, že bitcoin spotřebovává podobné množství energie jako zlato, jenomže dobývání zlata působí na životní prostředí mnohem nepříznivěji než těžba bitcoinu. Ve studii, kterou v časopise *International Journal* of *Environmental Research and Public Health* zveřejnili Fashola a kol., se uvádí: „činnosti spojené s těžbou [zlata] mohou vytvářet velká množství odpadu obsahujícího těžké kovy, jež se nekontrolovaně uvolňují do ekosystému a způsobují v něm rozsáhlé znečištění.“[34]

33 https://www.bullishcaseforbitcoin.com/references/mccook-article

34 https://www.bullishcaseforbitcoin.com/references/gold-mining-impact

Bitcoinová těžební farma

Naproti tomu těžba bitcoinu si vystačí s počítači, na kterých běží těžební software a které jsou většinou soustředěny ve velkých datových centrech, podobně jako servery Googlu, Facebooku a Microsoftu. Zatímco zlato se musí těžit tam, kde je zlatá ruda, těžba bitcoinu může probíhat kdekoliv, stačí mít zdroj energie a internetové připojení. Navíc se bitcoiny dají snadno a levně přesouvat všude po světě. Proto se těžaři soustřeďují kolem naddimenzovaných zdrojů vyrábějících nadbytečnou energii, která nemá jiné využití. Skvěle je to vidět na vodních elektrárnách v čínské provincii Sečuán, kolem kterých vzniklo jedno z největších center bitcoinové těžby. David Stanway, hlavní zpravodaj agentury Thomson Reuters pro průmysl a životní prostředí, vysvětluje: „Sečuán je výborný příklad. V roce 2017 tento region vyrobil v hydroelektrárnách přes 75 GW energie, tedy více, než činila celková výroba ve většině zemí Asie, a více než dvojnásobek kapacity rozvodné sítě v provincii. Spousta energie se tak zbytečně promarnila.“[35]

35 https://www.bullishcaseforbitcoin.com/references/hydro-article

Jelikož přebytečná elektřina se dá kvůli ztrátám v přenosové soustavě posílat pouze na omezenou vzdálenost, těžba bitcoinu vlastně zachraňuje tu část, která by přišla vniveč, a přeměňuje ji na digitální statek snadno přemístitelný kamkoliv po světě. Můžeme na ni tedy pohlížet jako na způsob, jak zužitkovat jinak nevyužitelnou energii, jejíž výroba by bez bitcoinu byla ztrátová nebo zcela zbytečná, protože v místě pro ni není dostatečné uplatnění. Velká část této nadbytečné energie navíc pochází z obnovitelných zdrojů, jež nijak významně nepřispívají k celosvětovým emisím uhlíku. Jako příklad můžeme uvést výše zmíněnou elektřinu z vodních zdrojů v Číně[36] nebo geotermální energii využívanou k těžbě bitcoinu na Islandu. Bitcoin tak podle všeho působí na životní prostředí příznivě, protože producentům energie z obnovitelných zdrojů přináší vyšší ziskovost, čímž posiluje motivaci investovat do budoucí výroby. Společnost CoinShares v průzkumu z roku 2019 zjistila, že: „Podle konzervativního odhadu činí podíl obnovitelných zdrojů na energetickém mixu využívaném k udržování bitcoinové sítě 74,1 %, což znamená, že těžba bitcoinu je ve využívání energie z obnovitelných zdrojů na jednom z prvních míst na světě mezi ostatními velkými průmyslovými odvětvími.“[37]

Chceme-li porovnávat ekologické dopady těžby bitcoinu a udržování fiatových měnových systémů, nesmíme zapomínat, že nestačí vzít v potaz jen samotnou finanční infrastrukturu, ale je třeba zohlednit také politické náklady nutné k tomu, aby občané dané země měnovému systému dostatečně důvěřovali. Mnohokrát v dějinách se peněžní a měnové systémy po dobytí nebo rozpadu státu zcela zhroutily. Žádný měnový systém nemůže přežít bez armády bránící hranice a bez policie dohlížející na dodržování majetkových práv. V tomto ohledu je bitcoin dokonalý. Zatímco

36 Ačkoliv v době vydání českého překladu Sečuán kvůli plošnému zákazu veškerých těžebních aktivit v Číně mezi hlavními centry těžby bitcoinu již nějakou dobu nefiguruje, k podobnému využití hydroelektráren dochází momentálně například v Paraguayi. (pozn. red.)

37 https://www.bullishcaseforbitcoin.com/references/coinshares-paper-1

státní peníze potřebují ke své existenci represivní aparát (tj. stát), bitcoin položil základy nového měnového řádu, v němž na dodržování majetkových práv nemusí dohlížet žádná vláda. Dalo by se říct, že majitelé bitcoinu mají „majetkové superprávo“, jelikož vlastní hodnotný statek, který lze snadno držet a směňovat i bez podpory nebo souhlasu státu.

A konečně, objem energie spotřebované v bitcoinové síti bude úměrný velikosti celosvětové poptávky jednak po systému umožňujícím spoření a směnu bez povolení třetí strany a jednak po výhodách, jež takový systém lidem přináší. Jak vysvětlil Satoshi Nakamoto: „Užitek ze směny uskutečňované prostřednictvím bitcoinu bude mnohem vyšší než náklady na spotřebovanou elektřinu. Nemít bitcoin by tedy byl čistě ztrátový podnik.“[38]

Lidem žijícím v diktátorských režimech bitcoin přináší užitek nejen v teorii – může pro ně znamenat doslova rozdíl mezi životem a smrtí. Venezuelský ekonom Carlos Hernández v komentáři pro list New York Times popsal, jak díky vlastnictví bitcoinu dokázal přestát bouřlivou hyperinflaci a jak se jeho bratrovi podařilo uprchnout z Venezuely, aniž přišel o úspory:

> *„Všeobecně se ví, že vojáci na hranicích Venezuely obírají o peníze každého, kdo se pokouší odejít ze země. Juan měl ale úspory v bitcoinu a nedalo se k nim dostat jinak než pomocí hesla, které se naučil nazpaměť. Pro nás, kteří žijeme v hroutící se ekonomice s diktátorským režimem, nejsou ‚peníze bez hranic‘ prázdná fráze.“*[39]

38 https://www.bullishcaseforbitcoin.com/references/satoshi-electricity-quote

39 https://www.bullishcaseforbitcoin.com/references/venezuela-story

NAHRADÍ BITCOIN JINÁ KRYPTOMĚNA?

Bitcoinový protokol stojí na otevřeném softwaru, proto jej od samého začátku lze kopírovat a napodobovat. V průběhu let se objevilo mnoho imitací, od téměř přesných klonů, jako je litecoin, po propracované odvozeniny, například ethereum s distribuovanou sítí, v níž má být možné uzavírat libovolně složitá smluvní ujednání. Kritici často namítají, že bitcoin si nemůže udržet hodnotu, když je tak snadné vytvářet konkurenční kryptoměny vybavené nejmodernějšími inovacemi a softwarovými funkcemi.

Slabinou tohoto tvrzení je předpoklad, že kryptoměny si konkurují technologickými vlastnostmi. Ve skutečnosti si totiž konkurují *peněžními* vlastnostmi. Technologie má cenu, pouze pokud posiluje důvěryhodnost peněžních vlastností kryptoměny, například vzácnosti. V tomto smyslu dáváme před inovacemi přednost nudné, ověřené, stabilní technologii.

Nesčetní konkurenti bitcoinu, vzniklí za dobu jeho existence, navíc zdaleka nedisponují takovým síťovým efektem jako první a převládající technologie v odvětví. Síťový efekt, tj. přidaná hodnota používání bitcoinu daná pouhým faktem, že se jedná o dominantní síť, je výhodou sám o sobě a je zdaleka tím nejdůležitějším, co může každá technologie nabídnout.

Síťový efekt bitcoinu je dán likviditou jeho trhu, počtem lidí, kteří jej vlastní, a komunitou vývojářů, kteří udržují a vylepšují jeho software a renomé. Velcí investoři, včetně států, vždy hledají trh s největší likviditou, umožňující rychle vstoupit a vystoupit, aniž by to rozkolísalo cenu. Vývojáři se zpravidla soustřeďují kolem nejvýraznější komunity s nejbystřejšími talenty, čímž ji dále posilují. Také šíření renomé se děje samospádem: o kryptoměnách, které by bitcoinu rády konkurovaly, se vždy hovoří právě ve spojitosti s bitcoinem.

ROZŠTĚPENÍ BLOCKCHAINU – JE PRO BITCOIN NEBEZPEČNÉ?

V roce 2017 se stalo zvykem napodobit nejen software bitcoinu, ale převzít i celou historii transakcí (blockchain). Tím, že zkopírovali bitcoinový blockchain až do určitého bodu a pak z něj odštěpili nový řetězec s novou sítí (tento postup se nazývá *fork* neboli rozštěpení či rozvětvení blockchainu), se konkurenti bitcoinu zbavili problému, jak rozšířit vlastní tokeny mezi co nejvíce uživatelů.

K nejvýznamnějšímu forku tohoto typu došlo 1. srpna 2017 při vzniku nové sítě nazvané bitcoin cash (bcash). Kdo před 1. srpnem 2017 vlastnil N bitcoinů, měl najednou kromě N bitcoinů také N tokenů bcash. Malá, ale hlasitá komunita podporovatelů této kryptoměny se pak neúnavně pokoušela přivlastnit si renomé bitcoinu jednak pomocí klamavého názvu nové sítě a jednak v kampani, která měla nováčky na trhu přesvědčit, že bcash je ten „pravý“ bitcoin. Pokusy selhaly a bcash má dnes vcelku zanedbatelnou tržní kapitalizaci. Noví investoři přesto dál čelí nebezpečí,

že se nějakému konkurentovi podaří bitcoin a jeho blockchain naklonovat a přetáhnout k sobě jeho tržní kapitalizaci, čímž by se *de facto* stal bitcoinem.

Rozvětvení cesty (anglicky fork)

Z velkých forků, ke kterým došlo jak na bitcoinu, tak na ethereu, lze odvodit důležité pravidlo: většina tržní kapitalizace přejde k té síti, která si udrží nejkvalitnější a nejaktivnější komunitu vývojářů. Přestože bitcoin můžeme považovat za novou formu peněz, jedná se zároveň o počítačovou síť, jejíž software je nutné udržovat a vylepšovat. Koupit si tokeny sítě, která má nezkušené vývojáře nebo jich má málo, by bylo podobné jako koupit si klon Windows, a připravit se tak o podporu nejlepších vývojářů Microsoftu. Forky z roku 2017 jasně ukázaly, že nejlepší a nejzkušenější informatici a kryptografové se soustředí na vývoj původního bitcoinu, nikoliv na jeho napodobeniny, které přesto dál vznikají jako houby po dešti.

JE BITCOIN OPRAVDU VZÁCNÝ?

Počet bitcoinů je omezen na pouhých 21 milionů. Někteří ovšem namítají, že vzácnost bitcoinu je pouhou iluzí vzhledem k tomu, jak snadno lze zkopírovat protokol a rozštěpit blockchain a kolik nových tokenů na různých kopiích bitcoinové sítě se vyrojilo. Podle této pomýlené logiky by každá kopie Mony Lisy umenšovala jedinečnost originálu. Naopak, každá kopie Leonardova mistrovského díla jen dokazuje, že existuje pouze jedna *pravá* Mona Lisa. Podobně každá kopie bitcoinu dokazuje, že existuje pouze jeden protokol s nejsilnějším síťovým efektem, nejlepším renomé a největší peněžní vahou, přes nějž lze díky tomu denně provádět transakce v hodnotě miliard dolarů.

SKUTEČNÁ RIZIKA

Nejčastější námitky proti bitcoinu vycházejí z mylných předpokladů a z nepochopení podstaty peněz. Přesto však investování do této kryptoměny obnáší některá skutečná a významná rizika. Každý zájemce by se s nimi měl seznámit a zvážit je, než do bitcoinu vloží své peníze.

RIZIKO PROTOKOLU

Může se ukázat, že bitcoinový protokol a kryptografické základy, na nichž je postaven, obsahují zásadní chybu, případně je může o bezpečnost připravit vývoj kvantových počítačů. Pokud se v protokolu objeví chyba nebo pokud nějaká nová výpočetní technologie zpochybní kryptografická východiska bitcoinu, může to vážně poškodit důvěru v tuto měnu jakožto uchovatele hodnoty. Riziko spojené s protokolem bylo největší v prvních letech vývoje, kdy ještě ani zkušeným kryptografům nebylo zřejmé, že Satoshi Nakamoto opravdu objevil řešení problému byzantských generálů.

Postupem času, jak selhávaly různé pokusy o narušení protokolu a byly odhalovány a opravovány skutečné chyby, obavy z vážných nedostatků opadly. Nebezpečí spojeného s kvantovými počítači jsou si vývojáři protokolu vědomi už léta a zkoumají možná řešení pro případ, že se tyto stroje stanou běžně dostupnými.[40] Bitcoin je však technologie, tudíž jeho protokol nikdy nemůže být zcela bez rizika, byť by se mělo projevit třeba jen v podobě mimořádné odchylky.

RIZIKO STÁTNÍHO ÚTOKU

Nebezpečí útoku ze strany státu visí nad bitcoinem jako černý mrak téměř od samého začátku a dodnes je nejzávažnějším a nejaktuálnějším z rizik, která by investoři měli vzít v úvahu. Satoshi Nakamoto v příspěvku na fóru Bitcointalk v prosinci 2010 s nelibostí komentoval záměr stránky Wikileaks, proslavené zveřejněním státních tajemství, přijímat dary v bitcoinu. Vysvětlil, že spojení Wikileaks s bitcoinem by přitáhlo nežádoucí pozornost a že nově vznikající systém zatím není dost silný, aby odolal soustředěnému útoku ze strany státu. Přesto bitcoin kvůli své decentralizované povaze a tomu, že jeho používání není podmíněno žádným povolením, brzy začal sloužit k nelegálním účelům, například k obchodování na internetovém drogovém tržišti Silk Road, spuštěném v únoru 2011. Právě kvůli Silk Road se o bitcoin poprvé začal zajímat Kongres USA. Joe Manchin, senátor za Západní Virginii, v roce 2014 veřejně apeloval na federální orgány, aby bitcoin zakázaly. Napsal:

> *„Kvůli anonymitě bitcoinu je virtuální trh mimořádně zranitelný vůči hackerům a podvodníkům, kteří uživatele bitcoinu obírají o miliony. Anonymita spolu s rychlostí způsobuje, že je velmi obtížné, ne-li nemožné, podvodné transakce zvrátit. Zároveň se k bitcoinu uchylují*

40 https://www.bullishcaseforbitcoin.com/references/quantum-computing

jedinci se zájmem o nákupy na černém trhu. Umožňuje jim anonymně obstarávat zakázané zboží, například drogy a zbraně. Již dříve jsem se obrátil na regulátory ohledně nyní uzavřeného tržiště Silk Road, které celé roky dodávalo zločincům narkotika a další zboží černého trhu, a to do značné míry právě díky existenci bitcoinu.“[41]

Manchin byl mylně přesvědčen, že bitcoin se pro nelegální obchody hodí, jelikož je anonymní. Ve skutečnosti je bitcoinový blockchain veřejně přístupný, takže státní orgány v něm pomocí analytického softwaru mohou vystopovat transakce ještě po letech. Obviňování, že bitcoin kvůli své anonymitě slouží především trestné činnosti, definitivně umlčel vývoj nástrojů pro analýzu blockchainu a jejich uplatnění v několika známých trestních případech. Postupem let se také ukázalo, že naprostá většina poptávky po bitcoinu plyne z potřeby spořit a investovat, nikoliv ze snahy o nezákonné obchodování. Právě využití bitcoinu coby uchovatele hodnoty ovšem podkopává jednu ze základních pravomocí každého státu, totiž kontrolu nad státními penězi. Státy se obávají, že by mohly přijít o vládu nad měnovou politikou, což jistě nezřídka povede k dalším pokusům napadnout bitcoin.

Státní útok může mít mnoho podob, od šikanózních předpisů svazujících používání bitcoinu – například povinnost nahlásit před odesláním totožnost příjemce – až po kriminalizaci prostého držení, nebo dokonce pokus o zabavení. Možná vám hrozba konfiskace připadá nepravděpodobná, ale v historii státy na majetková práva svých vlastních občanů takto nejednou zaútočily. V roce 1933 prezident Spojených států amerických Franklin D. Roosevelt, údajně ve snaze zmírnit Velkou depresi, vydal exekutivní příkaz č. 6102, jímž nařizoval občanům USA, aby odevzdali své zlato.

41 https://www.bullishcaseforbitcoin.com/references/manchin-letter

Vlastnit zlato se stalo nelegálním. Jelikož se tento kov obtížné přepravuje a zabezpečuje a je složité ověřit jeho kvalitu, majitelé si rezervy většinou ukládali u finančních institucí, a o to snáze na ně centrální moc vlády USA posléze dosáhla.

POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

By virtue of the authority vested in me by Section 5(b) of the Act of October 6, 1917, as amended by Section 2 of the Act of March 9, 1933, entitled "An Act to provide relief in the existing national emergency in banking, and for other purposes", in which amendatory Act Congress declared that a serious emergency exists, I, Franklin D. Roosevelt, President of the United States of America, do declare that said national emergency still continues to exist and pursuant to said section do hereby prohibit the hoarding of gold coin, gold bullion, and gold certificates within the continental United States by individuals, partnerships, associations and corporations and hereby prescribe the following regulations for carrying out the purposes of this order:

Section 1. For the purposes of this regulation, the term "hoarding" means the withdrawal and withholding of gold coin, gold bullion or gold certificates from the recognized and customary channels of trade. The term "person" means any individual, partnership, association or corporation.

Section 2. All persons are hereby required to deliver on or before May 1, 1933, to a Federal reserve bank or a branch or agency thereof or to any member bank of the Federal Reserve System all gold coin, gold bullion and gold certificates now owned by them or coming into their ownership on or before April 28, 1933, except the following:

(a) Such amount of gold as may be required for legitimate and customary use in industry, profession or art within a reasonable time, including gold prior to refining and stocks of gold in reasonable amounts for the usual trade requirements of owners mining and refining such gold.

(b) Gold coin and gold certificates in an amount not exceeding in the aggregate $100.00 belonging to any one person; and gold coins having a recognized special value to collectors of rare and unusual coins.

(c) Gold coin and bullion earmarked or held in trust for a recognized foreign government or foreign central bank or the Bank for International Settlements.

(d) Gold coin and bullion licensed for other proper transactions (not involving hoarding) including gold coin and bullion imported for reexport or held pending action on applications for export licenses.

Section 3. Until otherwise ordered any person becoming the owner of any gold coin, gold bullion, or gold certificates after April 28, 1933, shall, within three days after receipt thereof, deliver the same in the manner prescribed in Section 2; unless such gold coin, gold bullion or gold certificates are held for any of the purposes specified in paragraphs (a), (b) or (c) of Section 2; or unless such gold coin or gold bullion is held for purposes specified in paragraph (d) of Section 2 and the person holding it is, with respect to such gold coin or bullion, a licensee or applicant for license pending action thereon.

Section 4. Upon receipt of gold coin, gold bullion or gold certificates delivered to it in accordance with Sections 2 or 3, the Federal reserve bank or member bank will pay therefor an equivalent amount of any other form of coin or currency coined or issued under the laws of the United States.

Section 5. Member banks shall deliver all gold coin, gold bullion and gold certificates owned or received by them (other than as exempted under the provisions of Section 2) to the Federal reserve banks of their respective districts and receive credit or payment therefor.

Section 6. The Secretary of the Treasury, out of the sum made available to the President by Section 501 of the Act of March 9, 1933, will in all proper cases pay the reasonable costs of transportation of gold coin, gold bullion or gold certificates delivered to a member bank or Federal reserve bank in accordance with Sections 2, 3, or 5 hereof, including the cost of insurance, protection, and such other incidental costs as may be necessary, upon production of satisfactory evidence of such costs. Voucher forms for this purpose may be procured from Federal reserve banks.

Section 7. In cases where the delivery of gold coin, gold bullion or gold certificates by the owners thereof within the time set forth above will involve extraordinary hardship or difficulty, the Secretary of the Treasury may, in his discretion, extend the time within which such delivery must be made. Applications for such extensions must be made in writing under oath, addressed to the Secretary of the Treasury and filed with a Federal reserve bank. Each application must state the date to which the extension is desired, the amount and location of the gold coin, gold bullion and gold certificates in respect of which such application is made and the facts showing extension to be necessary to avoid extraordinary hardship or difficulty.

Section 8. The Secretary of the Treasury is hereby authorized and empowered to issue such further regulations as he may deem necessary to carry out the purposes of this order and to issue licenses thereunder, through such officers or agencies as he may designate, including licenses permitting the Federal reserve banks and member banks of the Federal Reserve System, in return for an equivalent amount of other coin, currency or credit, to deliver, earmark or hold in trust gold coin and bullion to or for persons showing the need for the same for any of the purposes specified in paragraphs (a), (c) and (d) of Section 2 of these regulations.

Section 9. Whoever willfully violates any provision of this Executive Order or of these regulations or of any rule, regulation or license issued thereunder may be fined not more than $10,000, or, if a natural person, may be imprisoned for not more than ten years, or both; and any officer, director, or agent of any corporation who knowingly participates in any such violation may be punished by a like fine, imprisonment, or both.

This order and these regulations may be modified or revoked at any time.

FRANKLIN D ROOSEVELT

THE WHITE HOUSE
April 5, 1933.

For Further Information Consult Your Local Bank

GOLD CERTIFICATES may be identified by the words "GOLD CERTIFICATE" appearing thereon. The serial number and the Treasury seal on the face of a GOLD CERTIFICATE are printed in YELLOW. Be careful not to confuse GOLD CERTIFICATES with other issues which are redeemable in gold but which are not GOLD CERTIFICATES. Federal Reserve Notes and United States Notes are "redeemable in gold" but are not "GOLD CERTIFICATES" and are not required to be surrendered

Special attention is directed to the exceptions allowed under Section 2 of the Executive Order

CRIMINAL PENALTIES FOR VIOLATION OF EXECUTIVE ORDER $10,000 fine or 10 years imprisonment, or both, as provided in Section 9 of the order

Exekutivní příkaz č. 6102

Digitální, decentralizovaný bitcoin naopak mnohokrát prokázal pozoruhodnou odolnost vůči útokům různých vlád, jež se pokoušely regulovat nebo zakázat jeho používání. Nezapomínejme ale, že

burzy, kde se bitcoiny směňují za fiat měny, jsou vysoce centralizované, podléhají regulacím a stát může nařídit jejich uzavření. Bez nich a bez ochoty bankovního systému obchodovat s nimi by se přitom postup přeměny bitcoinu v peníze velmi zbrzdil, ne-li zcela zastavil. Bitcoin sice má i jiné zdroje likvidity, například přímý prodej a decentralizované trhy, kde lze mince nakupovat a prodávat, ale klíčový proces cenotvorby probíhá na největších burzách, které jsou všechny centralizované.

Chce-li burza zmírnit riziko, že ji stát uzavře, musí si vybrat vhodnou jurisdikci. Například významná burza Binance začínala v Číně, ale když jí čínská vláda zakázala další provoz na svém pevninském území, přesunula centrálu do Japonska a posléze na Maltu. Vlády si však zároveň dávají pozor, aby nezadusily rodící se odvětví, které jednou může být stejně vlivné jako internet – připravily by se tím totiž o obrovskou konkurenční výhodu oproti ostatním státům.

Proces přeměny bitcoinu v peníze by mohlo zcela zastavit jedině koordinované celosvětové uzavření bitcoinových burz. Nyní probíhá závod, zda tato kryptoměna dokáže natolik prorůst celou společností, že úplné uzavření bude politicky neprůchodné, stejně jako by neprošlo úplné zrušení internetu. Nadějným znamením je v tomto směru stále širší příklon k bitcoinu mezi finančními institucemi a korporacemi, které obvykle umějí na vlády zatlačit mnohem důrazněji než drobní investoři. Největší americká kryptoburza Coinbase, v době psaní této knihy oceňovaná na 100 miliard dolarů, navíc nedávno vstoupila na burzu cenných papírů. Političtí činitelé teď zřejmě budou obezřetnější, aby se nestalo, že svými předpisy tuto tržní kapitalizaci v hodnotě miliard dolarů vymažou a poškodí miliony drobných investorů. Zároveň také pozorujeme posilování politického vlivu bitcoinu: politici a jejich voliči mu začínají fandit prostě proto, že jej vlastní, a tento fakt vytváří přirozenou hráz proti nepřátelským státním zásahům.

Možnost celosvětového uzavření burz však přetrvává a při investování do bitcoinu je s ní potřeba počítat. Jak uvádím v kapitole 4, vládám konečně začíná svítat, jaké nebezpečí pro jejich měnovou politiku představuje nestátní digitální měna odolná vůči cenzuře. Zůstává otázkou, zda se proti tomu pokusí něco podniknout dříve, než bitcoin ve společnosti zakoření natolik, že proti němu politické kroky nic nezmůžou.

RIZIKO CENTRALIZACE TĚŽAŘŮ

Bitcoin se těží na počítačích zapojených do bitcoinové sítě. Jejich úkolem je řadit transakce podle času odeslání a potvrzovat je. V této souvislosti by investoři měli vzít v potaz významné riziko, že dojde k přílišné centralizaci výpočetního výkonu těžařů (jinými slovy hashovacího výkonu). Kdyby většinu hashovacího výkonu ovládlo několik málo subjektů, mohly by na síť podniknout buď politický útok, nebo ekonomický, označovaný jako dvojí útrata.

Ke dvojí útratě může dojít tak, že těžařská společnost nebo kartel ovládající většinu celkového hashovacího výkonu smění bitcoiny za jiný hodnotný statek, například za dolary, a potom využije svou převahu v těžebním výkonu ke zpětné úpravě blockchainu, takže se bude zdát, jako by transakce vůbec neproběhla. Dvojí útrata je nákladný a nebezpečný podnik. Není zaručeno, že se zpětná změna blockchainu podaří, a i kdyby ano, dokonaný podvod by podkopal důvěru v bitcoin jako takový, takže by útočník v podstatě ohrozil vlastní úspory. Satoshi Nakamoto s nebezpečím dvojí útraty od samého začátku počítal. V bitcoinovém whitepaperu poznamenal, že motivace k poctivé těžbě bude silnější než motivace ke dvojí útratě:

> *„Pokud se chamtivému útočníkovi podaří shromáždit více výpočetní síly, než kolik mají všechny poctivé uzly, musí se rozhodnout, zda tuto sílu využije k obírání lidí vracením svých*

plateb, nebo ke generování nových mincí. Mělo by mu dojít, že dodržování pravidel, která mu umožní získat více mincí než všem ostatním dohromady, je pro něj výhodnější než podrývání systému a tím i hodnoty vlastního bohatství.“[42]

Při zveřejnění whitepaperu v roce 2008, tedy předtím než vůbec vznikla nějaká bitcoinová síť, bylo Nakamotovo tvrzení pouhou teorií vycházející z předpokladu, že útočníci budou jednat ekonomicky racionálně. Nedávný výzkum, který provedli Savolainen a Ruiz-Ogarrio, potvrdil, že platí i v praxi:

„Zjistili jsme, že doposud zaznamenaná koncentrace [těžebních] poolů neukazuje na vyšší nebezpečí dvojí útraty […] Naše výsledky tudíž přímo popírají všeobecné přesvědčení, že každá koncentrace škodí. Naopak potvrzují dobře známý postřeh z ekonomie, že to, že je něco možné, ještě neznamená, že se o to někdo bude chtít pokusit.“[43]

Nakamoto tedy v návrhu bitcoinové sítě předvídal, že se o dvojí útratu může pokusit někdo, kdo jedná ekonomicky racionálně. Nepočítal ale se soustředěným útokem na těžební firmy ze strany státu, jenž by sledoval jiné než hospodářské cíle. Stalo se už nejednou, že státy ve snaze prosadit své politické záměry jednaly proti ekonomické logice – například když vyhlásily válku sousedním státům. Politický útok na těžbu bitcoinu může být motivován snahou zabránit občanům v přístupu k prostředku, jenž umožňuje spořit a obchodovat mimo státní dohled. Nebo si stát může přát

42 Překlad Braiins. Bitcoinový whitepaper v češtině je dostupný z https://cs.braiins.com/blog/the-bitcoin-whitepaper-cz-cesky-preklad. (pozn. překl.)

43 https://www.bullishcaseforbitcoin.com/references/too-big-to-cheat-paper

odstranit bitcoin, protože jej vnímá jako systémové riziko pro svou měnovou politiku. Pokud by dokázal ovládnout dostatečně velký těžební výkon, mohl by cenzurovat nežádoucí transakce nebo jednoduše tento výkon odebrat ze sítě, čímž by nesmírně oslabil její bezpečnost a narušil důvěru v bitcoin jako takový.

Ze států, které mají motivaci zaútočit na bitcoinovou síť, disponuje v tuto chvíli největšími možnostmi Čínská lidová republika. Jelikož je velmocí ve výrobě čipů a v některých provinciích má nadbytek elektrické energie, soustředila se tam světová výroba těžebního hardwaru i největší těžařské farmy. Společnost CoinShares v průzkumu z roku 2019 odhadla, že „celých 65 % hashovacího výkonu bitcoinové sítě se nachází v Číně".[44] Pokud by čínský stát výrobce těžebního hardwaru nebo těžaře znárodnil, znamenalo by to vážné ohrožení chodu celé sítě. Útoku se nedá nijak předejít, je tu ale možnost zasadit doslova jaderný úder, který by mu vzal vítr z plachet: změnit funkci, která v bitcoinové síti podává důkaz o vykonané práci. Abychom dokázali pochopit, jakou drtivou sílu tato možnost představuje, musíme se nejprve krátce věnovat dějinám těžby bitcoinu.

Od zrodu bitcoinové sítě v roce 2009 těžaři postupně přecházejí na čím dál specializovanější stroje umožňující dosáhnout co největšího hashovacího výkonu na jednotku spotřebované elektřiny. V průkopnických dobách se těžilo na běžných počítačích, ale v květnu 2010 Laszlo Hanyecz zjistil, že mnohem efektivnější než obyčejný procesor je čip optimalizovaný pro zpracování obrazu, tzv. grafická karta. Jeho objev odstartoval mezi vývojáři těžebního hardwaru doslova závody ve zbrojení, které nakonec vedly ke vzniku aplikačně specifických integrovaných obvodů (ASIC) pro těžbu bitcoinu. První těžební stroje osazené ASIC (ASIC minery) postavil v roce 2013 čínský výrobce hardwaru Canaan Creative a dnes už v tomto

44 https://www.bullishcaseforbitcoin.com/references/coinshares-paper-2

vysoce konkurenčním oboru působí několik dalších výrobců čipů, například Bitmain a Bitfury. ASIC minery jsou počítače vyvinuté tak, aby co nejefektivněji a nejrychleji vykonávaly jednu jedinou funkci, totiž dodávaly do bitcoinové sítě důkaz o vykonané práci. Tato funkce se nazývá SHA256. Pokud je využita naplno, získává těžař dostatečný hashovací výkon, aby mohl potvrdit nový blok v blockchainu, a tudíž obdržet odměnu za jeho vytěžení.

Funkce SHA256 je základní stavební kámen bitcoinové těžby. Na vývoj a výrobu hardwaru pro její co nejoptimálnější chod byly vynaloženy miliardy dolarů. Přesto ji lze nahradit jinou funkcí, například SHA512, která by do sítě také uměla dodávat potřebný důkaz o vykonané práci. Těžební hardware optimalizovaný pro SHA256 by ale byl po takové změně rázem k ničemu a jeho výrobci i těžaři, kteří jej používají, by začali krachovat. Jde tedy o krajní řešení představitelné v případě, že by na těžbu bitcoinu zaútočil čínský stát, zároveň ale o řešení mimořádně nebezpečné. Bez souhlasu naprosté většiny uzlů v bitcoinové síti a investorů, kteří do bitcoinu vložili své úspory, by změna funkce provádějící důkaz o vykonané práci mohla vést k rozpadu sítě a k rozštěpení komunity na frakce, z nichž každá by tvrdila, že jedině síť, kde běží „jejich“ funkce, je tím pravým bitcoinem. Navíc je dnes bitcoinová síť bezpečná jen díky obrovským investicím, které byly v minulosti vloženy do těžebního hardwaru a zařízení pro SHA256. Po změně by následovalo prudké oslabení bezpečnosti, dokud by do náhradní funkce nebyl postupně nalit podobný objem prostředků. Přechod na jinou funkci důkazu o vykonané práci tedy můžeme právem považovat za doslova jaderný úder, přípustný jedině v krajním případě. I když zůstane pouhou teorií, samotná hrozba, že k němu *může* dojít, je mocným strašákem, kdyby snad nějaký stát napadlo přisvojit si hashovací výkon bitcoinové sítě pro své vlastní záměry.

RIZIKO SPRÁVCE

Obchodní společnosti a instituce často svěřují nakoupené bitcoiny do péče regulovaných správců, v jejichž rukou se pak s růstem hodnoty bitcoinu ocitá majetek za stovky miliard dolarů, který čím dál více láká hackery. Zatímco správcům fyzického zlata stačí počítat s ohrožením z bezprostředního okolí, správci bitcoinu čelí hackerům, kteří mohou na uložené prostředky zaútočit z kteréhokoliv místa na planetě. Vykradení velkého regulovaného správce by mohlo vážně narušit důvěru korporátních a institucionálních investorů v bitcoin.

Na ochranu proti rozsáhlému hackerskému útoku se zavádějí stále dokonalejší bezpečnostní postupy a vyvíjejí se nástroje pro správu finančních prostředků mimo dosah internetu. Velkou loupež sice nikdy nelze zcela vyloučit, ale podle všeho je dnes katastrofální událost podobná té, která způsobila pád první velké bitcoinové burzy MtGox, mnohem méně pravděpodobná než v počátcích bitcoinu.

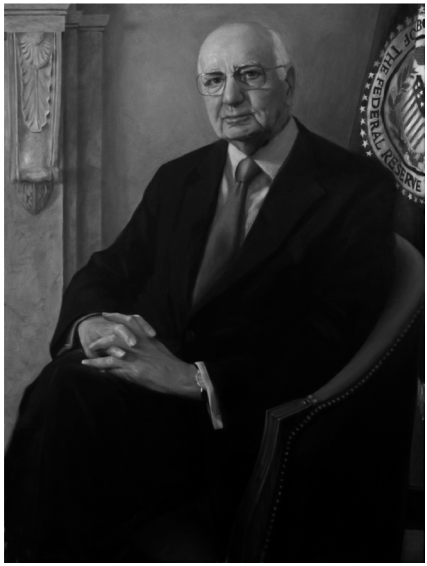
POLITIKA FEDU JAKO RIZIKO

Ve druhé polovině 70. let 20. století procházely Spojené státy obdobím vysoké inflace, která vedla k prudkému růstu ceny zlata na trhu. Události onoho desetiletí vyvrcholily krizí důvěry v americký dolar, s níž si poradil teprve nově jmenovaný předseda Federálního rezervního systému (centrální banky USA) Paul Volcker, a to pomocí drastických opatření. V roce 1980 skokově zvýšil krátkodobé úrokové sazby na dosud nevídaných 20 %, čímž americké hospodářství uvrhl do hluboké recese a na několik desetiletí oslabil cenu zlata, ale zároveň zkrotil prudkou inflaci 70. let.[45]

Zlato coby peněžní statek s tržní kapitalizací v bilionech dolarů je na politiku Fedu citlivé.

---

45 https://www.bullishcaseforbitcoin.com/references/volcker-inflation-fighting



Paul Volcker, někdejší předseda Federálního rezervního systému

Při dostatečně výrazném zvýšení úrokových sazeb se poptávka po tomto kovu, který nemá žádný přirozený výnos, přesouvá do dolaru, nesoucího úročení ve výši krátkodobých sazeb Fedu. Na bitcoinu byly cenové pohyby vzhledem k jeho nižšímu podílu na trhu prozatím dány především vstupem nových investorů, ale až se přiblíží tržní kapitalizaci zlata, budou se makroekonomická rizika plynoucí z politiky Fedu vztahovat i na něj. Pokud by rada guvernérů Fedu začala vnímat postupující monetizaci bitcoinu jako ohrožení důvěryhodnosti dolaru, mohla by se pokusit zvrátit vývoj prudkým zvýšením úrokových sazeb, podobně jako to učinil Volcker začátkem 80. let 20. století. Tuto snahu by ovšem komplikovala finanční situace Spojených států, která je nyní naprosto jiná než na konci 70. let. Od dob druhé světové války si země udržovala míru zadlužení pod 100 procenty HDP, dnes je však tato hranice překročena. Pro srovnání, v 80. letech 20. století činilo zadlužení v poměru k HDP pouhých 40 procent. Riziko spojené se zvýšením úrokových sazeb Fedu tedy sice existuje, ale centrální

bankovní systém USA by k takové politice těžko mohl přistoupit, aniž by fatálně narušil schopnost ministerstva financí obsluhovat stávající dluh. Agresivní úroková politika by ve stávající finanční situaci mohla odstartovat státní dluhovou krizi, takže ohledy na státní pokladnu mohou Fed donutit, aby držel kurz příznivý pro přeměnu bitcoinu v peníze, i když mu tím pomáhá přiblížit se co do podílu na trhu zlatu, nebo je dokonce překonat.

RIZIKO REHYPOTEKACE

Finanční instituce, které nabízejí pokročilé investiční produkty, například shortování, maržové obchodování nebo deriváty[46], zpravidla požadují, aby u nich klient předem složil kolaterál (zástavu) v podobě hotovosti, akcií, dluhopisů nebo jiných aktiv, a tento kolaterál pak používají ke zmírnění rizik spojených s neuváženými investičními rozhodnutími klienta a následnými ztrátami. Jestliže například klient makléřské firmy spekuluje na pokles ceny určité akcie, a tato akcie naopak získá na hodnotě, může makléř složený kolaterál nebo jeho část prodat, aby vzniklou ztrátu pokryl.

K rehypotekaci pak dochází, když finanční instituce použije klientův kolaterál při svém vlastním investování, čímž může zvýšit jeho výnos, ale zároveň jej vystavuje většímu riziku. Za svolení k dalšímu investování nebo půjčování složeného kolaterálu je třeba klienta nějak odměnit, například nižší úrokovou sazbou na jeho shortové obchody. Při dostatečné obezřetnosti mohou finanční instituce díky rehypotekaci nabízet investiční produkty levněji nebo dokonce zdarma a zároveň se tím posiluje likvidita na trhu. Pokud se ovšem s rehypotekací zachází neuváženě nebo pokud se příliš rozšíří, může představovat systémové riziko. Je-li

46 Obchodní strategie na burze, při které investor sází na pokles hodnoty akcie v čase, od brokera si danou akcii zapůjčí a okamžitě prodá. Akcie ale není jeho a bude ji muset vrátit. Když cena následně skutečně klesne, nakoupí akcii zpět za nižší cenu a vrátí ji brokerovi. Zaplatil tak za půjčení, přičemž výsledný rozdíl v ceně prodeje a zpětného nákupu si ponechá. (pozn. red.)

kolaterál půjčován opakovaně, prochází mnoha finančními institucemi a pak stačí, aby jedné její investice nevyšla, a spustí se dominový efekt likvidací daného aktiva v celém řetězci institucí, cena prudce spadne a nastane krize likvidity. Ve studii zpracované v roce 2010 pro Mezinárodní měnový fond (MMF) dokonce Singh a Aitken uvádějí, že rehypotekace se významně podílela na vzniku finanční krize v roce 2008: „Jestliže při posuzování poslední krize vezmeme v potaz také odhady míry rehypotekace (a s tím spojeného opakovaného použití kolaterálu), zjišťujeme, že došlo k zásadnímu zhroucení nebankovního financování bank.“[47]

Bitcoin poprvé ve větším rozsahu posloužil jako kolaterál v roce 2014 při založení kryptoburzy BitMex se sídlem v Hongkongu. Klientům stačilo vložit bitcoiny a mohli uzavírat různé derivátové kontrakty, například perpetual swap.[48] BitMex tak nabízela způsob, jak si bez finanční páky vsadit na budoucí cenu bitcoinu. Nepodmiňovala obchodování složením depozitu ve fiat měně, čímž dokázala obejít byrokratické regulace, které na tento druh trhů obvykle uvaluje mimo jiné americká Komise pro termínované obchodování s komoditami (CFTC), a mohla rychle růst. V srpnu 2020 už se na ní protočily ohromující objemy v hodnotě 75 miliard dolarů a z jejích spoluzakladatelů se stali miliardáři.[49] Průkopnický počin BitMexu – využít bitcoin jako kolaterál – ani její finanční úspěchy nezůstaly bez povšimnutí. Její příklad následovaly další společnosti, počínaje úctyhodnou Chicagskou komoditní burzou, která vznikla už v roce 1898 a dnes nabízí termínované kontrakty na bitcoin, a konče platformou BlockFi, jež klientům poskytuje úročení jejich bitcoinů. Komentátor trhů Raoul Pal označil bitcoin za „ryzí kolaterál“ a stále

47 https://www.bullishcaseforbitcoin.com/references/imf-rehypothecation-article

48 Druh finančního derivátu, který má na rozdíl od futures a opcí neomezenou dobu trvání. Z tohoto důvodu je velmi oblíbený při obchodování s kryptoměnami a bitcoinem, neboť podobně jako futures umožňuje spekulovat na pohyb ceny, ovšem bez nutnosti kontrakt neustále obnovovat. Cena perpetual swap je pevně svázána se spotovou cenou podkladového aktiva a umožňuje obchodování na páku. (pozn. red.)

49 https://www.bullishcaseforbitcoin.com/references/bitmex-story

více lidí dochází k poznání, že díky vlastnostem této kryptoměny a povaze jejího trhu se opravdu jedná o nejčistší formu kolaterálu:

1. Bitcoin má celosvětový trh s vysokou likviditou, na kterém se denně zobchodují miliardy dolarů.

2. Bitcoinové trhy mají na rozdíl od regulovaných trhů cenných papírů otevřeno nepřetržitě, takže finanční instituce mohou kolaterál v bitcoinu prodat, jakmile ve svém úvěrovém portfoliu zaznamenají zvýšené riziko.

3. Bitcoiny na rozdíl od dluhopisů nezastupují závazek třetího subjektu, čímž se snižuje riziko ztráty v důsledku selhání protistrany.

4. Bitcoiny jsou na rozdíl od zlata digitální, proto je lze snadno a levně převádět, a tedy také velmi jednoduše použít coby kolaterál.

Postupně si stále více lidí začne uvědomovat, že bitcoin představuje ideální kolaterál, a začnou jej pro tento účel více využívat, čímž zvýší poptávku a podpoří jeho přeměnu v opravdové peníze. S tím ovšem jde ruku v ruce nebezpečí nezodpovědné rehypotekace. Stále ještě se jedná o nové odvětví, a investoři by proto u institucí, které přijímají bitcoin coby kolaterál a poté s ním dále nakládají, měli velmi pozorně sledovat kvalitu nakupovaných aktiv. Riziko rehypotekace je u bitcoinu zřejmě ještě vyšší než například u akcií nebo dluhopisů. Kdyby při kritickém nedostatku likvidity muselo více finančních institucí prodat dluhopisy držené jako kolaterál, peněžní toky na těchto dluhopisech by zabránily zhroucení jejich cen. Bitcoin ale nemá žádné peněžní toky, které by posloužily jako záchranná síť, takže krize likvidity by vedla k neřízenému pádu ceny. Jak jsme si ukázali ve třetí kapitole v části o závislosti peněz na minulém vývoji, kolaps ceny bitcoinu by zásadně změnil oče-

kávání ohledně vyhlídek na budoucí přeměnu v peníze a ochromil by, nebo dokonce zastavil celý proces.

Nejúčinnější ochranu před rizikem rehypotekace poskytuje silná regulace trhu a otevřené informování o preventivních opatřeních používaných při správě investovaného kolaterálu. Za regulaci bývá často považován dohled ze strany regulatorního orgánu, například CFTC, ale v praxi těmto byrokratům dlouho trvá, než inovativní odvětví pochopí a naučí se na ně vhodným způsobem dohlížet. Často spoléhají na zastaralé předpisy sepsané před desítkami let. Zdaleka nejúčinnější regulaci provádí trh sám – nezodpovědně investující instituce je třeba nechat padnout, aby nesprávné jednání bylo potrestáno a nestalo se systémovým, jako tomu bylo při krizi na trhu s bydlením v roce 2008.

RIZIKO NEDOKONALÉ ZAMĚNITELNOSTI

Otevřenost bitcoinového blockchainu umožňuje státům označit určité mince za „špinavé“, protože byly použity při něčem nedovoleném. Díky odolnosti bitcoinového protokolu vůči cenzuře s nimi sice i nadále půjde provádět transakce, ale pokud by je někdo zakázal používat na burzách nebo u obchodníků, mohly by se stát v podstatě bezcennými. Bitcoin by tak přišel o jednu ze zásadních vlastností peněžního statku, totiž o zaměnitelnost.

Má-li se problém s nedokonalou zaměnitelností bitcoinových mincí vyřešit, je třeba zlepšit na úrovni protokolu ochranu soukromí při transakcích. Poslední dobou se v tomto směru objevují různé inovace, mezi prvními na digitálních měnách monero a zcash, ale nalezení rovnováhy mezi efektivitou bitcoinu, jeho složitostí a ochranou soukromí bude vyžadovat zásadní technické kompromisy. Stále není jasné, zda do bitcoinu lze přidat prvky, které by zlepšily soukromí a přitom nijak neomezily jeho použitelnost coby peněz.

ZÁVĚR

Bitcoin představuje nově vznikající peníze na rozhraní mezi fází sběratelského předmětu a uchovatele hodnoty. Jde o nestátní peněžní statek, který se někdy v budoucnosti možná stane celosvětovou rezervní měnou, podobně jako zlato v období klasického zlatého standardu v devatenáctém století – a právě to je hlavní důvod, proč je bitcoin budoucnost. Satoshi Nakamoto na to poukázal už v roce 2010 v e-mailové konverzaci s Mikem Hearnem: „Představme si, že jej bude využívat nějaká část světového obchodu. Ani pak nebude k dispozici více než 21 milionů mincí pro celý svět, takže cena jedné mince bude mnohem vyšší.“[50]

Geniální kryptograf Hal Finney, příjemce prvních bitcoinů odeslaných Nakamotem, se krátce poté, co bylo oznámeno spuštění prvního funkčního bitcoinového softwaru, vyjádřil ještě jednoznačněji:

> *„Představme si, že bitcoin bude úspěšný, stane se převládajícím platebním systémem a bude se používat všude na světě. Potom by celková hodnota této měny měla odpovídat souhrnné hodnotě světového bohatství. Stávající odhady veškerého majetku všech domácností na světě se podle toho, co jsem našel, pohybují mezi 100 a 300 biliony USD. Při 20 milionech mincí by tedy každá mince měla mít hodnotu asi 10 milionů USD.“*[51]

Bitcoin je zatím značně podhodnocený, i kdyby se v budoucnosti neměl stát celosvětovou rezervní měnou a pouze konkuroval zlatu jako nestátní uchovatel hodnoty. Postavíme-li vedle sebe tržní

50 https://www.bullishcaseforbitcoin.com/references/satoshi-hearn-email

51 https://www.bullishcaseforbitcoin.com/references/hal-finney-quote

kapitalizaci stávající zásoby vytěženého zlata (přibližně 10 bilionů dolarů) a dosavadní zásobu bitcoinů, vyjde nám poměr přibližně 540 000 amerických dolarů na jeden bitcoin. Jak jsme si ukázali ve druhé kapitole v pojednání o vlastnostech, jež z peněžního statku dělají vhodný uchovatel hodnoty, bitcoin je ve všech ohledech s výjimkou historické prověřenosti se zlatem srovnatelný, nebo dokonce lepší. Postupem času se naplno projeví Lindy efekt a zlato o konkurenční výhodu v podobě historické prověřenosti přijde. Máme tedy důvod očekávat, že se bitcoin během příštího desetiletí přiblíží k tržní kapitalizaci zlata, možná ji i překoná.

Tato teorie má ovšem jeden háček, totiž že velkou část tržní kapitalizace zlata vytvářejí centrální banky, které je drží jako uchovatel hodnoty. Pokud se má bitcoin tržní kapitalizaci zlata vyrovnat nebo ji překonat, budou se do hry muset zapojit státy. Těžko říci, zda si jej začnou pořizovat západní demokracie. Mnohem pravděpodobnější bohužel je, že na trh bitcoinu jako první vstoupí druhořadé diktatury a kleptokracie.

Bitcoin je ale budoucnost, i kdyby ho nezačal nakupovat žádný stát. Coby nestátní uchovatel hodnoty využívaný pouze drobnými a institucionálními investory se stále nachází teprve na začátku adopční křivky. Nyní na jeho trh vstupuje takzvaná časná většina, zatímco pozdní většinu a opozdilce dělí od vstupu do bitcoinu ještě celé roky. Při širším zapojení drobných, a hlavně institucionálních investorů se můžeme dostat na cenu mezi 100 000 a 250 000 dolary za jeden bitcoin.

Bitcoin je jedna z mála asymetrických investic dostupných lidem kdekoliv na světě. Velmi podobně jako u kupní opce zde investor riskuje ztrátu pouze ve výši hodnoty vložených prostředků, zatímco získat může stále ještě stonásobek nebo i více. Bitcoin je první skutečně globální bublina, jejíž velikost a rozsah omezuje pouze to, nakolik si lidé přejí ochránit své úspory před vrtochy neschopných

vládních ekonomů. Zrodil se přece jako fénix z popela globální finanční krize v roce 2008 – krize, kterou svou politikou způsobily centrální banky, především americký Fed.

Kromě toho, že bitcoin má lidem co dát po finanční stránce, bude mít nástup tohoto nestátního uchovatele hodnoty dalekosáhlé geopolitické důsledky. Existence globální, neinflační rezervní měny přinutí státy, aby přestaly svůj chod financovat pomocí inflace a přešly na financování prostřednictvím přímého zdanění, které je politicky daleko méně stravitelné. Státní aparáty se začnou smršťovat úměrně tomu, jak bude přechod na financování výhradně z daní politicky bolestivý. A co víc, obchodování po celém světě se začne vypořádávat tak, jak si přál Charles de Gaulle, když prohlásil, že žádný národ by neměl být zvýhodňován oproti ostatním:

> *„Považujeme za nezbytné, aby mezinárodní obchod stejně jako předtím, než svět postihly těžké rány osudu, spočíval na nezpochybnitelném měnovém základě, jenž neponese značku žádné určité země.“*[52]

Za padesát let ode dneška bude tím měnovým základem bitcoin.

52 https://www.bullishcaseforbitcoin.com/references/degaulle-speech

EPILOG

VELKÁ DEBATA

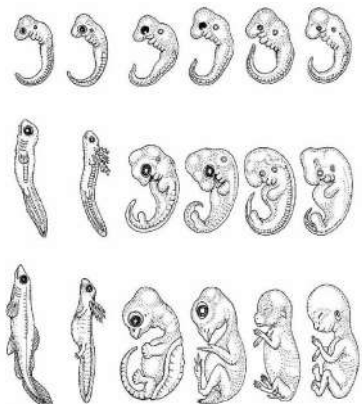
Co je bitcoin? Zdánlivě jednoduchá otázka, která však mezi vývojáři a investory vyvolala bouřlivou debatu, jež se táhla několik let a vyvrcholila rozkolem v komunitě a rozštěpením bitcoinové sítě k 1. srpnu 2017. Během prvních roků po vzniku Nakamotova vynálezu se totiž vynořily dvě myšlenkové frakce, z nichž každá prosazovala jiný pohled na budoucnost bitcoinu. První v něm viděla především platební systém srovnatelný s platformami Visa nebo PayPal, pouze bez centrální autority. Zaměřovala se na využití bitcoinu při transakcích a byla přesvědčena, že peníze jsou definovány v první řadě svou úlohou prostředku směny. Druhá frakce považovala za zásadní, že bitcoin není cenzurovatelný, a upozorňovala, že by bylo nebezpečné přenechat kontrolu nad protokolem jedné konkrétní zájmové skupině. Spatřovala v bitcoinu digitální obdobu zlata a kladla důraz na jeho úlohu coby nestátního uchovatele hodnoty.

Spory mezi oběma tábory se ještě prohloubily, když tvůrce bitcoinu nedlouho po oznámení svého vynálezu zmizel. Dne 12. prosince 2010, 772 dnů poté, co poprvé vystoupil na internetu, aby zveřejnil svůj návrh, Satoshi Nakamoto napsal poslední příspěvek do internetového fóra o bitcoinu. Jeho odchod měl pro rodící se projekt dalekosáhlé důsledky. Vývojáři bitcoinového softwaru museli pokračovat v práci bez prvotního hybatele, bez vedení a bez společné vize budoucnosti. Nejpřesnější vyjádření Nakamotových úmyslů nalezneme v zakladatelském dokumentu bitcoinu (whitepaperu), zveřejněném 31. října 2008. Ani tento krátký dokument však nedává jednoznačnou odpověď na otázku, zda bychom měli bitcoin považovat v první řadě za prostředek směny, nebo za uchovatele

hodnoty. Satoshi sice napsal stovky příspěvků do internetových fór a e-mailů bitcoinovým vývojářům, ale k peněžní podstatě svého vynálezu se nikdy jednoznačně nevyjádřil. V některých textech připodobňuje bitcoin ke zlatu a poukazuje na jeho využití při uchovávání hodnoty:

> *„[Bitcoin se] spíše podobá drahému kovu. Místo aby se měnila nabídka a hodnota zůstávala stejná, je nabídka dána předem a mění se hodnota. S rostoucím počtem uživatelů se tedy hodnota mince zvyšuje. Může tu vzniknout pozitivní smyčka zpětných vazeb – čím víc uživatelů, tím větší hodnota, což přiláká další uživatele, kteří budou chtít z jejího růstu těžit.“*[53]

Při několika jiných příležitostech Nakamoto psal o využití bitcoinu při platbách a zdůrazňoval úlohu peněz coby prostředku směny.



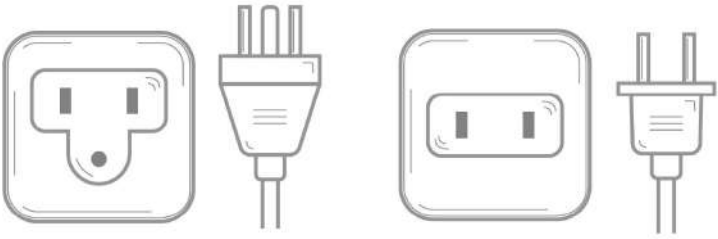
Embrya různých živočišných druhů vypadají podobně

53 https://www.bullishcaseforbitcoin.com/references/satoshi-gold-quote

Bitcoin v zárodečné podobě vypadal, že splní všechna očekávání stejnou měrou. Na jedné straně byly v jeho síti zpočátku nízké transakční poplatky, takže jej bylo možné levně posílat po celém světě a zdálo se, že v tom spočívá jeho výhoda oproti jiným platebním systémům, například kartám Visa. Na druhé straně postupem času velmi získal na ceně a začal se jevit jako nový způsob, jak uchovávat hodnotu. Stejně tak mnohé živočišné druhy jsou si v zárodečné formě podobné, a přitom mají v DNA vepsány příkazy, které v pravý čas odhalí jejich odlišnosti. DNA bitcoinu je tvořena dohodnutými pravidly jeho protokolu, a jak si ukážeme, tato pravidla jasně určují, že pouze jedna z představ o budoucnosti bitcoinu se může stát skutečností.

PROČ NEMĚNIT PROTOKOLY

Protokol je soubor pravidel, která musejí dodržovat všichni uživatelé daného systému. Jako příklad softwarového protokolu můžeme uvést TCP/IP, který stanoví způsob kódování dat a jejich přenosu po internetu, a SMTP upravující posílání elektronické pošty. Protokoly existují i ve fyzickém světě, například normy IEC 60906-2 a NEMA 5-15 se týkají elektrických zásuvek a definují tvar zástrček, napětí a maximální proudové zatížení.



Otvor pro zemnicí kolík je zpětně kompatibilní změna původního tvaru elektrické zásuvky

Jakmile jsou protokoly softwarového nebo hardwarového systému s mnoha uživateli jednou spuštěny, bývá většinou velmi obtížné je upravovat, a to z dobrého důvodu: všichni, kdo na nich postavili své podnikání nebo zařízení, spoléhají na jejich neměnnost. Modifikace obecně rozšířeného protokolu by pro uživatele znamenala vysoké náklady navíc. Představme si například, na kolik by domácnosti přišla změna tvaru elektrických zásuvek. Všechny do jedné by se musely modernizovat a každé zařízení postavené pro původní tvar by se muselo zlikvidovat nebo opatřit adaptérem. Vysokým nákladům se lze vyhnout jedině pomocí zpětně kompatibilní změny, jež nijak neovlivní systémy běžící na starších verzích protokolu. Příkladem je otvor pro zemnicí kolík, vynalezený v roce 1924. Jednalo se o zpětně kompatibilní modernizaci, která snižovala nebezpečí zasažení elektrickým proudem, ale do zásuvek nového tvaru se dala zapojit i starší zařízení s dvoukolíkovou zástrčkou.

Když Satoshi Nakamoto 9. ledna 2009 zveřejnil zdrojový kód bitcoinu, předložil v podstatě protokol pro přenášení hodnoty prostřednictvím internetu. Uvědomoval si, že jakmile se jeho návrh rozběhne ve skutečné síti, bude velmi obtížné, ne-li nemožné, provádět v protokolu zpětně nekompatibilní změny. Dne 17. června 2010 k tomu poznamenal: „Vydáním verze 0.1 byla natrvalo určena základní koncepce.“[54]

ROZKOL

Bitcoinový protokol je soubor pravidel určujících, které zprávy posílané v bitcoinové síti jsou platné. Na jeho dodržování dohlížejí počítače zapojené do sítě, na nichž běží příslušný software. Pokud počítač dohodnutá pravidla (konsenzus) porušuje, je ze sítě vyloučen.

54 https://www.bullishcaseforbitcoin.com/references/satoshi-protocol-quote

Nejznámější pravidlo stanoví, kolik nových bitcoinů může vzniknout v jednom bloku, jinými slovy určuje výši odměny za vytěžení bloku. Toto pravidlo udává časový průběh inflace na bitcoinu – omezuje celkovou zásobu na konečných 21 milionů mincí. Další důležité pravidlo se týká maximální velikosti bloku a omezuje počet transakcí v jednom těženém bloku. Vzniklo v roce 2010 ve snaze zabránit DoS útokům[55] na síť, která tehdy byla ještě v plenkách.[56]

Pravidlo o velikosti bloku se stalo hlavním sporným bodem mezi dvěma tábory názorů na budoucnost bitcoinu. Jeden prosazoval velké bloky a domáhal se změny protokolu ve smyslu jejich zvětšení, aby se do nich vešlo víc transakcí. Potíž spočívala v tom, že navrhovaná změna by nebyla zpětně kompatibilní, a pokud by ji jednomyslně a ve stejný okamžik nepřijali všichni účastníci, vedla by k rozštěpení sítě. Zastánci velkých bloků vnímali bitcoin prostě jako každý jiný software (například Word od Microsoftu) a byli toho názoru, že potřebuje časté aktualizace, aby vyhovoval potřebám obchodníků, kteří jej používají především k uzavírání transakcí. Druhý tábor trval na malých blocích, stavěl se proti změně a varoval, že by přenesla kontrolu nad bitcoinem do rukou společností, které tak nápadně usilují o aktualizaci protokolu. Zároveň upozorňoval, že zvětšením bloku by se oslabila decentralizace bitcoinu, protože by vyžadoval nákladnější hardware, což by ze sítě vytlačilo méně zámožné účastníky. Zastánci malých bloků vnímali bitcoin ne jako software, nýbrž jako protokol, a zdůrazňovali, jaké náklady by úprava pravidel znamenala pro jeho ekosystém. Především si ale uvědomovali, že podaří-li se snadno upravit jedno dohodnuté pravidlo, bude jednodušší změnit i ta ostatní, včetně pravidla o velikosti odměny za blok. Poptávka po bitcoinu coby uchovateli hodnoty je do značné míry dána důvěryhodností jeho měnové politiky,

55 Z anglického Denial-of-Service (odepření služby). Útok na internetovou službu pomocí soustředěného zahlcení požadavky tak, aby službu nemohli použít ostatní uživatelé. (pozn. red.)

56 https://www.bullishcaseforbitcoin.com/references/theymos-dos-quote

založené na předem stanovené nabídce, a změna velikosti bloku v bitcoinovém protokolu by tuto důvěryhodnost nepřímo narušila.

Bouřlivé spory mezi oběma tábory vyvrcholily 1. srpna 2017, kdy zastánci velkých bloků pozměnili software na svých počítačích tak, aby mohl zpracovávat větší bloky, čímž jej učinili nekompatibilním se zbytkem bitcoinové sítě. Původní síť ale počítače s novým softwarem odmítla a ty pak vytvořily vlastní síť. Tato událost se nazývá rozštěpení sítě (*fork*). Odštěpená síť dostala název bitcoin cash a vydávala vlastní tokeny obchodovatelné na trhu. Otázka budoucnosti bitcoinu se tak z debaty uvnitř komunity přelila na trh, kde se proti sobě obchodovaly jak původní bitcoiny pod označením BTC, tak tokeny bitcoin cash pod zkratkou BCH, a čekalo se, až ekonomika sama ukáže, která verze přiláká větší poptávku investorů. V následujících letech se převážná část trhu přiklonila k původní síti a k pojetí bitcoinu jakožto nestátního uchovatele hodnoty. Síť bitcoin cash upadla do bezvýznamnosti a její malá komunita se roztříštila v pokračujících vnitřních bojích a rozkolech.

ROZUZLENÍ

Trh tedy podpořil síť s původními pravidly, čímž jasně ukázal, že hodnota bitcoinu nespočívá v možnosti aktualizovat jeho software, nýbrž mnohem spíše v nemožnosti manipulovat jeho protokol. Pokud se na dohodnutých pravidlech ani v budoucnosti nic nezmění, zůstane i nadále omezena jak velikost bloku, tak počet transakcí, které lze v jednom bloku zpracovat. Zároveň bude do bitcoinu vstupovat stále více lidí, takže poroste poptávka po umístění transakcí v omezeném prostoru bloku, tudíž se časem budou muset zvýšit transakční poplatky. Vypořádávat na bitcoinové síti drobné platby například při koupi kávy nebo chleba začne být nehospodárné, ale stále bude vhodná pro převody větších hodnot, na nichž ostatně

stojí světový finanční systém. Menší platby v bitcoinech budou probíhat na vrstvách postavených nad bitcoinovou sítí, například na Lightning Network, nebo na vypořádacích vrstvách správců, mimo jiné bank. Geniální kryptograf Hal Finney, který jako první rozpoznal potenciál Nakamotova vynálezu, napsal v roce 2010:

> *„Samotný bitcoin nelze škálovat tak, aby se každá transakce na světě posílala všem uzlům a zapisovala se do blockchainu. Potřebujeme platební systémy druhé vrstvy, které budou méně náročné a efektivnější.*
> *...*
> *Jsem přesvědčen, že posláním bitcoinu je stát se ‚mocnými penězi', které budou banky využívat jako rezervní měnu při vydávání vlastní digitální hotovosti."* [57]

Finney tedy v důsledku uznal, že bitcoin se nejdříve potřebuje etablovat jako uchovatel hodnoty neboli jeho slovy jako rezervní měna, abychom jej poté mohli naplno využívat při běžných platbách v nadstavbových vrstvách. Chápal, že smyslem bitcoinu není sloužit jako platební systém přímo konkurující například platformám Visa nebo PayPal, nýbrž že jde o něco mnohem významnějšího: o nestátní uchovatel hodnoty, o měnový základ, na němž vyroste nový celosvětový finanční systém. Tak je to od samého začátku zapsáno v DNA bitcoinu – v jeho dohodnutých pravidlech.

57 https://www.bullishcaseforbitcoin.com/references/finney-second-layer-quote

PODĚKOVÁNÍ

Když jsem se začátkem roku 2017 pouštěl do psaní dlouhého článku s názvem „The Bullish Case for Bitcoin“, kolísala cena bitcoinu okolo jednoho tisíce dolarů a já doufal, že díky mému výkladu snad pár přátel a možná dokonce i nějací investoři z Wall Street pochopí, jak je tato převratná technologie pro ekonomiku významná. Nečekal jsem, že jej nakonec budou číst statisíce lidí na celém světě a že ho dobrovolníci přeloží do dvaceti jazyků. Zčásti to lze vysvětlit rostoucím počtem zájemců, kteří si přejí bitcoinu porozumět a zjistit, proč je tak důležitý, ale zároveň za tuto popularitu vděčím neocenitelné pomoci, díky níž se podařilo vytvořit text přístupný a srozumitelný i laikovi. V této souvislosti bych rád vyjádřil poděkování všem, kteří mi pomáhali při psaní původního článku a při sestavování této knihy, která jej rozpracovává do mnohem větší šíře.

Za prvé chci poděkovat Michaelu Saylorovi za předmluvu k této knize a za velkorysost, s níž mi prostřednictvím své nadace Saylor Academy zdarma zpřístupnil studijní materiály. Za druhé bych rád poděkoval umělci s pseudonymem @BitcoinUltras, s nímž jsem se seznámil na Twitteru a který jako dobrovolník vytvořil ilustraci na obálku a krásné obrázky, které zdobí každou kapitolu. Za třetí bych rád poděkoval svému příteli Sanjayovi Mavinkurveovi za to, že pro tuto knihu velkoryse vypracoval grafy dokládající pravdivost rčení, že jeden obrázek vydá za tisíc slov. Rád bych poděkoval Danielu Colemanovi, Michaelu Hartlovi, Benu Davenportovi, Matu Balezovi a Stephanu Kinsellovi za péči, kterou věnovali redakčnímu zpracování mého rukopisu. Mnoho lidí poskytlo zpětnou vazbu, díky níž je mé dílo srozumitelnější. Za to bych chtěl poděkovat Alexovi Morcosovi, Johnu Pfefferovi, Pierrovi Rochardovi, Koenu Swinkelsovi, Rayovi Boyapatimu, Michaelu Angelovi, Patri Friedmanovi, Ardianu Tolovi a Michaelu Flaxmanovi.

Nakonec a především děkuji své manželce Lise, že mi pomohla dotáhnout tento projekt do konce a že mi dala tři děti, které jsou největší inspirací mého života.

UPOZORNĚNÍ

V této knize předkládám vlastní názory a také případné chyby jdou na vrub mně. Tato kniha slouží pouze pro informaci. Není míněna jako investiční poradenství. Své investice konzultujte s řádně licencovaným profesionálním poradcem.

O AUTOROVI

Vijay Boyapati se narodil v Austrálii. V roce 2000 se kvůli postgraduálnímu studiu počítačové vědy přestěhoval do Spojených států amerických, ale místo aby směřoval ke získání doktorátu, nastoupil do malého startupu jménem Google a několik let tam uplatňoval své znalosti strojového učení a zdokonaloval vyhodnocovací algoritmy pro Zprávy Google. V roce 2007 z lukrativního zaměstnání odešel, aby se mohl podílet na občanské kampani před prezidentskými volbami 2008. Pomohl vybrat miliony dolarů a získat stovky dobrovolníků, kteří v New Hampshire zajišťovali podporu pro Rona Paula. V roce 2011 Boyapati objevil bitcoin a vydal se dolů onou pověstnou králičí norou ve snaze odhalit, jak mohou nové internetové peníze, nepodložené žádnou komoditou ani státní zárukou, mít vůbec nějakou ekonomickou hodnotu. Vyzbrojen znalostmi rakouské ekonomické školy, sepsal v roce 2017 dlouhý článek s názvem „The Bullish Case for Bitcoin“, aby laikům poskytl ekonomický základ, na němž budou schopni bitcoinu porozumět.

Vijay Boyapati získal na Australské národní univerzitě titul bakalář přírodních věd s vyznamenáním první třídy a tamtéž obdržel Univerzitní medaili jako nejvyšší možné ocenění pro studenty. Je ženatý a je milujícím otcem tří dětí, které se jmenují Addie, Will a Vivi. Žije s rodinou v Seattlu ve státě Washington.

BRAIINS Publishing

Vijay Boyapati
Bitcoin je budoucnost

Z anglického originálu *Bullish Case for Bitcoin* přeložila Klára Ježková
Jazyková redakce: Daniela Hozdová
Odpovědný redaktor: Jáchym Černý
Grafická úprava a sazba: Sabina Heyová
Úprava obálky: Jiří Chlebus
Design konzultace: Robert Blecha
Marketingová strategie: Kristian Csepcsar
Zvláštní poděkování: Marek Šelmeci, František Šimek

Vytiskla tiskárna Havlíčkův Brod
124 stran, první vydání

Vydalo nakladatelství Braiins Systems, 2023
braiins.com/publishing
Pochvaly či připomínky posílejte na publishing@braiins.cz

ISBN 978-80-908709-2-5

NAŠE DALŠÍ TITULY

Bitcoin: Odluka peněz od státu

Fascinující sonda do historie peněz z pera českého ekonoma Josefa Tětka. Proč by se po církvi, vzdělávání a médiích měla ze státního monopolu vymanit i tvorba peněz? Jaká jsou úskalí používání státem vydávaných a kontrolovaných oběživ? Kniha o roli bitcoinu coby nástroje, který navrací lidem možnost být pány svých peněz.

Bitcoin: Návrat zdravých peněz

Ve volném pokračování *Odluky* se Josef Tětek ve třech částech se věnuje *perspektivám* bitcoinu po 14 letech jeho existence, *ctnostem*, jež by měly zdobit každého bitcoinera a *návratům*, které bitcoin ztělesňuje. Čtenář na jednom místě najde pronikavou kritiku neduhů současného fiatového systému, historické sondy do fungování peněz, ale i praktické návody, jak s bitcoinem zacházet.

Tyto a mnohé další tituly naleznete ke koupi i ke stažení zdarma na našem webu **bitperia.cz/knihy**