

BITCOIN: NÁVRAT ZDRAVÝCH PENĚZ

ESEJE O BITCOINIZACI ŽIVOTA,
SPOLEČNOSTI A SVĚTA

AUTOR: JOSEF TĚTEK
PŘEDMLUVA: DANIEL STEIGERWALD

BRAVNS Publishing

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**



STACKUJ.CZ

**Podcast o Bitcoinu,
penězích a svobodě**



citadeliscoming
 GRAFIKY A ORIGINALY NA STACKUJ.CZ/SHOP



OBSAH

PŘEDMLUVA	VI
ÚVOD	VIII
SLOVNÍK POJMŮ	XI
ČÁST PRVNÍ: PERSPEKTIVY	14
Úvod první části	14
Perspektiva dlouhodobá: U bitcoinu vám stále ještě neujel vlak	15
Perspektiva incentív: Fiatová mentalita: proč (nejen) ekonomové nechápou bitcoin	25
Perspektiva udržitelnosti: Bitcoin přežije euro	36
Perspektiva historická: Dějiny koruny: od zlaťáků k fiat	45
Perspektiva racionálního optimismu: bitcoin navrací do života naději	60
Perspektiva finanční: Nakamotův-Greshamův zákon aneb Proč na hodlování není nic špatného	69
ČÁST DRUHÁ: CTNOSTI	77
Úvod druhé části	77
Rozumnost aneb Jak na hardwarové peněženky	79
Prozíravost aneb Jak zanechat bitcoin příštím generacím	93
Obezřetnost aneb Jak o sobě neprozradit vše	100
Trpělivost aneb Jak přečkat medvědí trhy	110
Umírněnost aneb Jak být v pohodě	121

ČÁST TŘETÍ: NÁVRATY	126
Úvod třetí části	126
Návrat konfiskací: Stát bitcoin nezakáže; bude na něm parazitovat	128
Návrat úspor: Bitcoin jako konzervativní volba	146
Návrat zdravých peněz: Svět po hyperbitcoinizaci	153
Návrat pokory: Libertariáni vs. sociální inženýři	166
DOSLOV	170
BITCOINOVÉ DESATERO	171

PŘEDMLUVA

Vše, co lidé stvořili, vzniklo nejdříve v něčí hlavě. Bez myšlenky není žádného díla. Ale jak vznikají samotné myšlenky? Syntézou jiných myšlenek. Stejně tak ani bitcoin nevznikl zničehonic, ale je syntézou myšlenek již dříve existujících. Genialita Satoshiho Nakamota byla v tom, že volně poletující myšlenky spojil do jedné, pojmenoval ji a naprogramováním jí vdechl život. Tak vznikl bitcoin.

Nevznikl by ale, kdyby nebylo lidí, kteří dávají myšlenkám křídla. Jedním z takových je můj dávný kamarád Josef Tětek. I samotnému tvůrci bitcoinu musel kdysi dávno někdo říct A a někdo jiný zas B (nebo to A a B museli alespoň někam napsat), aby si Satoshi mohl A a B spojit dohromady, zamyslet se, hecnout se a stvořit evolučně novou inkarnaci peněz.

Proto je správné dobré myšlenky šířit a přesně tohle Josef dělá. Josef však ani náhodou není „hurá bitcoiner“. Na svou roli se dlouhé roky, aniž to věděl, poctivě připravoval. Studoval, zpracovával a pak publikoval právě ty myšlenky, které daly vzniknout bitcoinu. Proto se ostatně známe. Jako student ekonomické vysoké školy jsem byl výukou ekonomie zklamán. Mírně řečeno. Ačkoliv jsem kdysi četl nesmírně zajímavé ekonomické texty, tak to, co mi bylo servírováno školou, bylo jedním slovem otravné. Formou i obsahem. Minimálně polovina studentů prošla jen proto, že se z paměti naučili říct to, co učitelé chtěli slyšet. Mně to přišlo absurdní, proto jsem zoufale hledal i jinou ekonomii. V článkách, které Josef publikoval, jsem ji našel.

Aby totiž člověk mohl pochopit bitcoin, musí nejprve pochopit problém, který bitcoin řeší: peníze. Aby člověk pochopil peníze, musí chápat ekonomii. Aby člověk chápal ekonomii, musí rozumět tomu, proč se lidé chovají tak, jak se chovají. Proto se říká, že bitcoin je jako králičí nora, ve které je schován celý nový svět. Ten se však odkryje jen tomu, kdo je dostatečně pokorný a zvědavý. Kdo by se díval například pouze na zdrojový kód bitcoinu, tak bez kontextu

nepochopí nic. Pokora a zvědavost bitcoin chrání před namyšlenými hlupáky. Kdo není dostatečně pokorný a zvědavý, snadno se nechá zlákat přeludy bitcoinových napodobenin, tzv. altcoinů.

Bitcoin je jako trojský kůň. Lidé si přijdou pro rychlé zbohatnutí, ale odejdou s hlavou plnou otázek, o kterých je dříve nenapadlo přemýšlet. Co jsou to peníze? Kde se bere bohatství a kde chudoba? Co je to inflace? Kde bere stát svou moc? Je uchopení moci státem legitimní? Jaká je ideální výše daní? A proč? Má stát nějaké hranice moci? Co to vlastně vůbec je ten stát?

Žádná kniha nezodpoví vše, taková snaha by ostatně byla krajně podezřelá. Dobrá kniha toho zodpoví právě tak akorát. Chybět nesmí nic a přebývat také ne. Berte tuto knihu jako návod k pochopení a použití bitcoinu – zdravých peněz. Knihu, kterou můžete dát zvědavé kamarádce či kamarádovi, budou-li se ptát. Otázky si žádají odpovědi a tato kniha jich je plná. I to zbohatnutí tam je, ale není primární.

Přeji vám při čtení Josefovy knihy takové uspokojení, jaké mám z jeho textů já.

Daniel Steigerwald
30. července 2023, Praha

ÚVOD

V době psaní knihy oslavil bitcoin své čtrnácté narozeniny. Je to již čtrnáct let, kdy světem cloumala finanční krize a Satoshi Nakamoto publikoval výchozí Genesis blok se zprávou „Chancellor on brink of second bailout for banks“, který můžeme volně přeložit jako „Ministr financí zvažuje druhý bankovní bailout“. Jednalo se o titulky britských Timesů ze dne 3. ledna 2009. Satoshi tímto zápisem dokázal, že bitcoin nebyl předtěžený – nemohl totiž existovat před tímto datem – a také nám poodhalil motivaci k vzniku bitcoinu. Satoshi stvořil alternativní peníze, ve kterých neexistují privilegia, a nezodpovědnost je potrestána trhem, nikoli odměněna vládou. Proto pokud bych měl bitcoin charakterizovat třemi slovy, volil bych *peníze bez privilegií*. A pokud bych to měl zkrátit na pouhá dvě slova, byly by to *zdravé peníze*. Jedním slovem pak prostě *peníze*.

Jak se s postupem času ukazuje, vlastně se nejedná ani o kdovíjak „alternativní“ peníze; anomálií jsou spíše dnešní fiatové měny, zatímco bitcoin představuje návrat k principům, kterými se peníze řídily po tisíce let. Konzervativní povaha bitcoinu stojí v ostrém protikladu k nevypočitatelnosti fiatových měn. Zatímco bitcoin následuje od 3. ledna 2009 stále stejné základní principy, fiat čelí palčivé existenciální krizi a fiatoví ekonomové musí vymýšlet čím dál krkolomnější obhajoby pro státní peněžní monopol produkující měnové jednotky se stále horšími vlastnostmi.

Pravda ohledně fiatů je prostá: jedná se o nástroj pro přesun bohatství z kapes neprivilegovaných do kapes privilegovaných. S pomocí Cantillonova efektu (neboli inflační daně) si stát a zájmové skupiny udržují postavení, o které by v prostředí zdravých peněz musely soupeřit ve férové tržní soutěži. Až donedávna byla jediná obrana proti Cantillonově efektu hrát fiatovou hru: efektivně pracovat s dluhem, investovat do sektorů tyjících z konstantního přílivu nových peněz, spekulovat nad dalšími kroky centrálních bankéřů. Po roce 2009 se peněžní paradigma proměnilo a s důsledky

návratu zdravých peněz se teprve seznamujeme. Ambicí této knihy je pomoci čtenáři s orientací ve světě, ve kterém již nelze bitcoin ignorovat.

Jednotlivé kapitoly knihy vznikaly převážně v letech 2021–2022, kdy vycházely jako samostatné články v *Bitcoin Magazine*, *BTC Times*, *Alza.cz*. Ačkoli texty byly původně publikovány jako nezávislé články, v této knize podávají čtenáři ucelený návod na to, jak o bitcoinu přemýšlet, a to jak z pohledu logiky bitcoinu v rámci současných makroekonomických problémů a historie peněz, tak i z pohledu osobního přístupu. Po přečtení knihy by tak čtenář měl mít jasnější představu ohledně toho, proč se bitcoinem dále zabývat, a jak při tom minimalizovat riziko finanční i nervové újmy.

Knihy je členěna do tří částí. První část seznamuje čtenáře s různými pohledy na bitcoin: od perspektivy měnového vývoje v českých zemích a eurozóně, přes „fiatovou mentalitu“ dnešních mainstreamových ekonomů a všemožných kritiků bitcoinu, po vysvětlení racionality „hodlu“ – věřím, že čtenář obdrží v této části dostatek materiálu k přemýšlení o bitcoinu z více úhlů.

Druhá část představuje praktičtější přístup k bitcoinu ve formě základních čteností, které by si bitcoineři měli osvojit, chtějí-li cestu ke světové adopci bezpečně zvládnout. Čtenáři se zde seznámí s hardwarovými peněženkami, problematikou dědictví a dlouhodobé bezpečnosti seedu, otázkou soukromí, tržními cykly a nebezpečností finanční páky.

Třetí část knihy pojednává o dlouhodobém impaktu bitcoinu, a to jak na osobní úrovni (bitcoin jako úspory), tak i na úrovni celospolečenské (dopady hyperbitcoinizace). Důležitou kapitolou je i varování před vztahem státu k bitcoinu – navzdory rozšířené obavě ze zákazů je na místě mít se na pozoru spíše před konfiskacemi bitcoinu, a to buď úplnými – obdobně jako bylo konfiskováno zlato ve Spojených státech v roce 1933 – tak i před částečnými v podobě speciálních bitcoinových daní. Věřím, že bitcoin v dlouhém období v soutěži se státními penězi vyhraje, jelikož ekonomické zákony

zkrátka fungují se stejnou mírou spolehlivosti jako zákony přírodní. Nicméně než se tak stane, čekají nás turbulentní časy – fyzikální a ekonomické zákony sice fungují bez ohledu na lidské mínění, zpátečníci ale rádi upalují domnělé heretiky. Jedním z důležitých poselství knihy tudíž je: mějte se na pozoru a raději buďte lehce paranoidní než naivní. Koneckonců, bitcoin ztělesňuje kromě návratu zdravých peněz i odluku peněz od státu – a to se státu nemusí líbit.

Velké poděkování za realizaci knihy patří týmu Braiins Publishing, zejména neúnavnému editoru Jáchymovi. Děkuji Slushovi, že mi na jaře 2021 nabídl práci pro Trezor, v rámci které jsem získal možnost publikovat na Bitcoin Magazine a položit tak základy pro tuto knihu. Děkuji své rodině za dlouhodobou podporu a důvěru. A děkuji Satoshimu, že navrátil světu naději na lepší budoucnost.

SLOVNÍK POJMŮ

V knize se vyskytují termíny, se kterými se čtenář nemusel dříve setkat. Pro lepší orientaci si je na tomto místě vysvětlíme.

BIP – Bitcoin Improvement Proposal. Formalizovaný proces pro navrhování změn v bitcoinu (jak v protokolové oblasti, tak v oblasti implementace, např. peněženek). Proces BIP je založen na peer-review: všechny návrhy jsou veřejně dostupné a veřejně diskutované. I když je ale některý BIP schválen a změny zaneseny do referenční implementace Bitcoin Core, neexistuje proces, jakým změnu v síti prosadit – poslední slovo mají vždy provozovatelé bitcoinových uzlů, kteří se sami rozhodují, jakou verzi bitcoinového software budou provozovat.

Cantillonův efekt – Dopadu tištění nových peněz a jejich nerovnoměrnému šíření ekonomikou se říká Cantillonův efekt nebo také „inflační daň“. Nové peníze se nejprve dostávají do rukou státu, finančním institucím, korporacím. Tito první držitelé utrácejí peníze, dokud se v ekonomice ještě nezvýšily ceny. Jak se nové peníze postupně šíří ekonomikou, dochází ke zvyšování cen. Vlivem Cantillonova efektu dochází k přesunu kupní síly od chudších vrstev společnosti k bohatším.

CBDC – Central Bank Digital Currencies. Většina centrálních bank zkoumá možnosti zavedení digitálních měn založených na blockchainové technologii. V principu by CBDC neřešily žádné problémy fiatových měn, naopak by umožnily centrálním bankám a vládám ještě tužší kontrolu nad měnovým systémem a v kombinaci se zrušením hotovosti by v takovém systému neexistovalo žádné soukromí. CBDC v době psaní knihy již zavedly Čína a Nigérie.

DCA – Dollar Cost Averaging neboli strategie pravidelných nákupů bitcoinu nehledě na aktuální cenu.

Fiat – Státní peníze vznikající z příkazu (například dle legislativy o zákonném platidle). Z latinského fiat = budiž. Nejčastěji používán jako termín pro dnešní papírové a virtuální peníze nekryté drahými kovy.

FUD – Fear, uncertainty, doubt. FUD je termín, kterým bitcoineři označují záměrné vyvolávání pochyb o přínosu bitcoinu či jeho vyhlídkách na budoucí adopci. Mezi oblíbené FUD patří označování bitcoinové těžby za neekologickou či měnové politiky bitcoinu za neudržitelnou.

Hodl – Slangový termín pro dlouhodobou držbu bitcoinu. Vznikl díky překlepu slova „hold“ (anglicky držet) v nadpisu legendárního komentáře na fóru BitcoinTalk. Hodler je pak člověk, který dlouhodobě drží bitcoin.

KYC/non-KYC – *Know your customer* je požadavek kladený regulátory na poskytovatele finančních služeb. Poskytovatelé služeb (např. banky, burzy) mají povinnost identifikovat své zákazníky, uchovávat záznamy o identifikaci a předávat je státním orgánům. „KYC bitcoin“ je bitcoin získaný s doložením identity nakupujícího. Vzhledem k transparentní povaze bitcoinového blockchainu může burza (a další, se kterými osobní údaje nakupujícího burza sdílela) sledovat další transakce uživatele. „Non-KYC bitcoin“ je bitcoin získaný bez doložení identity nakupujícího, typicky v režimu peer-to-peer.

Lightning Network – je bitcoinová platební síť, která uživatelům umožňuje rychlé a levné bitcoinové platby. Na Lightning Network není zapotřebí čekat na zahrnutí transakce do bloku ze strany těžařů.

Lindy effect – Pravidlo popularizované Nassimem Talebem vyslovující tezi, že pokud určitá technologie či instituce existuje x let, bude pravděpodobně existovat ještě dalších x let. V kontextu bitcoinu Lindy effect znamená, že po 14 letech existence pravděpodobně jen tak nikam nezmizí; zlato má velmi silný Lindy effect, což bývá také hlavní argument ze strany kritiků bitcoinu.

P2P – Peer-to-peer. Označuje platební či komunikační styk mezi dvěma jedinci či softwarovými uzly bez účasti prostředníka. Bitcoinové uzly fungují v režimu P2P, ne každý však s bitcoinem nakládá v osobním životě ve stylu P2P: nákup bitcoinu přes burzu není P2P (burza hraje roli prostředníka mezi dvěma obchodníky), zatímco nákup přímo od jiných bitcoinerů je P2P. Používání bitcoinu v režimu P2P přináší zejména výhody v oblasti soukromí.

Satoshi – (zkráceně sats) Nejmenší jednotka bitcoinu. 1 bitcoin je 100 000 000 satoshi, 1 satoshi je 0,000 000 01 bitcoinu.

Stacking sats – Slangové synonymum DCA, doslova se jedná o „štosování satů“ neboli přikládání dalších a dalších drobných jednotek bitcoinu do vlastní peněženky. Oproti DCA nemusí být stacking pravidelný (stackovat se dá dobře při cenových propadech – tzv. buying the dip) a nemusí se ani jednat o nákupy (stackovat lze vyděláváním bitcoinu).

ČÁST PRVNÍ: PERSPEKTIVY

Úvod první části

Bitcoin existuje. To už je po čtrnácti letech fungování těžké zapřít a ani největší kritici tuto základní skutečnost nerozporují. Bitcoin tu zkrátka je a „šlape jako hodinky“ – každých deset minut sestaví těžaři nový blok a vybrané transakce dostanou své první potvrzení. Jak konstatují bitcoineři: *tick tok, nový blok.*

Bitcoin coby minivesmír protokolových pravidel, uzlů, peněženek a dalších technologických prvků není předmětem sporu. To, o čem se my, lidé, rádi hádáme, je spíše *význam* věcí. Někteří považují bitcoin za zbytečný, ba dokonce škodlivý; my bitcoineři jej naopak vnímáme jako milník lidského vývoje, s pomocí kterého se můžeme konečně zbavit přežitku státních peněz.

Bitcoin existuje – nikoliv však ve vakuu. Existuje po boku státních peněz, z čehož, jak si dále ukážeme, pramení velmi zajímavá dynamika; a především pak existuje v různých perspektivách.

Po mnoha letech s bitcoinem jsem dospěl k poznání, že bitcoin nelze zcela pochopit – vždy, když už si člověk myslí, že pochopil všechny aspekty a důsledky existence bitcoinu, objeví opět něco nového. Co je ale možné, je postupně se seznamovat s různými pohledy na bitcoin a dotvářet si tak mentální obraz ohledně toho, jaký dopad bude mít bitcoin na další vývoj lidstva. Perspektiva historického vývoje peněz odhalí jiné stránky než perspektiva osobních financí; konfrontace fiatové mentality s rakouskou školou ekonomie nám opět o povaze bitcoinu a jeho kritiků i příznivců odhalí něco nového.

Přimět čtenáře přemýšlet o bitcoinu z různých, možná i neintuitivních perspektiv, je ambicí první části *Návratu zdravých peněz.*

Perspektiva dlouhodobá: U bitcoinu vám stále ještě neujel vlak

Bitcoin Magazine, 21. 8. 2021

Když jsem před lety objevil bitcoin, myslel jsem si, že je už žalostně pozdě. Při zpětném pohledu je zřejmé, jak strašně jsem se mýlil. Stejně jako Jon Snow jsem nevěděl zhola nic. Většina cenového růstu, technologického vývoje, geopolitických důsledků – to vše bylo ještě přede mnou. A s odstupem let se domnívám, že to dnes platí ještě více. Pokud tyto řádky čtete, bitcoinový vlak vám rozhodně neujel. Jsme stále ještě na začátku.

„Jsem si jistý, že za 20 let bude objem transakcí buď velmi velký, nebo žádný.“

– Satoshi Nakamoto, 14. 2. 2010

Po letech zkoumání bitcoinu a jeho vlivu na svět je jasný jeden fakt: bitcoin nemůže uspět jen částečně. Nebude hrát druhé housle. Jak Satoshi předpověděl, adopce bitcoinu bude probíhat ve stylu „všechno, nebo nic“. Globální měnová evoluce, nebo bezvýznamnost.

Proč tomu tak je? Bitcoin jsou peníze vznikající a šířící se odspodu a jako takové konkurují fiat, což jsou naopak peníze „naordinované“ shora. Společnost potřebuje peníze k bezproblémové směně zboží a služeb a k uchování vytvořené hodnoty pro budoucí použití. Řečeno ekonomickým žargonem, peníze potřebujeme pro jejich funkci prostředku směny a uchovatele hodnoty. Nyní fiat peníze fungují docela dobře jako prostředek směny (zejména v západním světě), ale jako uchovatel hodnoty jsou v průběhu desetiletí stále horší.



Americký dolar je jednou z nejpevnějších fiat měn posledního století. Přesto však od roku 1913 ztratil přes 95 % kupní síly. Zdroj: Visual Capitalist.

Aby lidé toto selhání fiat peněz kompenzovali, hledají jiné nástroje pro zastoupení role uchovatele hodnoty, například cenné papíry nebo nemovitosti. Bitcoin tak konkuruje i těmto nástrojům. Ve srovnání s jinými uchovateli hodnoty nespadá bitcoin pod konkrétní jurisdikci (jako je tomu u akcií, dluhopisů, derivátů nebo nemovitostí) a nevyžaduje k úschově třetí stranu (jako je tomu u větších objemů zlata, diamantů nebo cenných uměleckých sbírek). Tyto dvě vlastnosti jsou někdy přehlíženy, přestože jsou stejně důležité (ne-li důležitější) jako jeho spolehlivá měnová politika, jejímž výsledkem je konečná nabídka 21 milionů bitcoinů.

Uchování hodnoty v instrumentech s jurisdikčním rizikem a u napadnutelných správců bude s postupem času stále těžší obhájit, protože rizikovost bitcoinu vyplývající nyní zejména z jeho novosti se bude s přibývajícím věkem výrazně snižovat.

Nástroje, které se v současnosti používají jako provizorní uchovatel hodnoty, nezmizí, pouze ztratí svou „peněžní prémii“ – která by, jak z termínu vyplývá, měla připadnout fungujícím penězům. Až bude problém peněz vyřešen prostřednictvím širokého přijetí bitcoinu, budou provizorní nástroje přeceněny na čistě tržní hodnotu a využity k účelům, kvůli kterým v prvé řadě vznikly: domy pro bydlení, dluhopisy pro zajištění předvídatelných peněžních

toků věřitelů, akcie pro alokaci kapitálu. Tyto nástroje jsou pro společnost užitečné, ale neměly by primárně sloužit jako uchovatel hodnoty. To je role zdravých peněz.

Bitcoinová generace

Uvažujme v dlouhodobém horizontu. Nemyslím teď vzdálenou budoucnost ve stylu „bitcoinové astronomie“ (mimořádně skvělé čtení – googlujte sérii textů *Bitcoin Astronomy*), spíše budoucnost stylu „dědo, co jsi dělal ve 20. letech?“ Pokud bitcoin uspěje a stane se globálními zdravými penězi, budeme patrně označováni za první bitcoinovou generaci. A lhostejno, zda jsme zažili kolaps Mt. Gox v roce 2014, účastnili se války o velikost bloku v roce 2017 nebo pozorovali velkou čínskou migraci hashratu v roce 2021. Průkopnický status získáme už jen proto, že jsme byli u toho, když bitcoin napravoval svět.

Možná vám to zní, jako bych při psaní kouřil kvalitní hopium, ale zkuste zvážit, zda na následujících řádcích vskutku něco není. Bitcoin se totiž dnes ani zdaleka neblíží svému potenciálu.

Posudme fakta:

Bitcoin má obří prostor pro růst. Bitcoin stále nedosahuje ani desetiny tržní kapitalizace zlata. Ve prospěch zlata sice hraje silný Lindy effect, ale není možné jej v mžiku oka teleportovat na druhou stranu planety, jako to můžeme udělat s bitcoinem přes Lightning Network. Zlato ke svému správnému fungování potřebuje důvěryhodné zprostředkovatele, zatímco bitcoin si může (a měl by) každý držet a spravovat sám. Bitcoin má zkrátka lepší vlastnosti pro plnění úlohy peněz a dlouhodobě nad zlatem zvítězí, a to včetně překonání jeho tržní kapitalizace.

Státy teprve objevují bitcoin jako zákonné platidlo. Bitcoin přijaly za své zákonné platidlo doposud pouze dvě země: Salvador a Středoafriká republika. Teorie her zde hovoří jasně: země, které nemají v otázkách finanční suverenity co ztratit, budou v 21. století

nakloněny adoptovat bitcoin, podobně jako v průběhu 20. století v obdobné situaci adoptovaly dolar.

Rapidní rozvoj Lightning Network. Většina lidí si neuvědomuje, jak masivní pokrok pro bitcoin představuje platební nadstavba Lightning Network. Jak často slyšíte FUD typu „bitcoin nedokáže zpracovat více než na čtyři transakce za sekundu“? Lightning funguje již dnes a tato platební nadstavba je každým rokem výrazně spolehlivější, použitelnější a robustnější.

Jednotkové zkreslení. Obdobně si mnozí lidé stále neuvědomují, že bitcoin lze dělit na sto milionů jednotek, tzv. satoshi či saty. Jednotkové zkreslení (*unit bias*) je rozšířený dojem, že bitcoin je již drahý a shitcoiny jsou naopak levné. Ve skutečnosti je to naopak, protože bitcoin je světem stále značně nedocenený, zatímco shitcoiny dlouhodobě vůči bitcoinu padají k nule. Je na čase přestat lamentovat nad tím, že jeden celý bitcoin je příliš drahý. Přepněte se do satoshi: za jeden dolar stále ještě dostanete tisíce satů! Směšně levné!

Opomíjení centrálními bankami. Centrální banky zatím bitcoin ani neakumulují, přestože bitcoin v rozvaze nabízí vysokou šanci na záchranu menších národních měn – alespoň v krátkém období; dlouhodobě veškerý fiat vymizí, jelikož neobstojí v konkurenci se zdravými penězi.

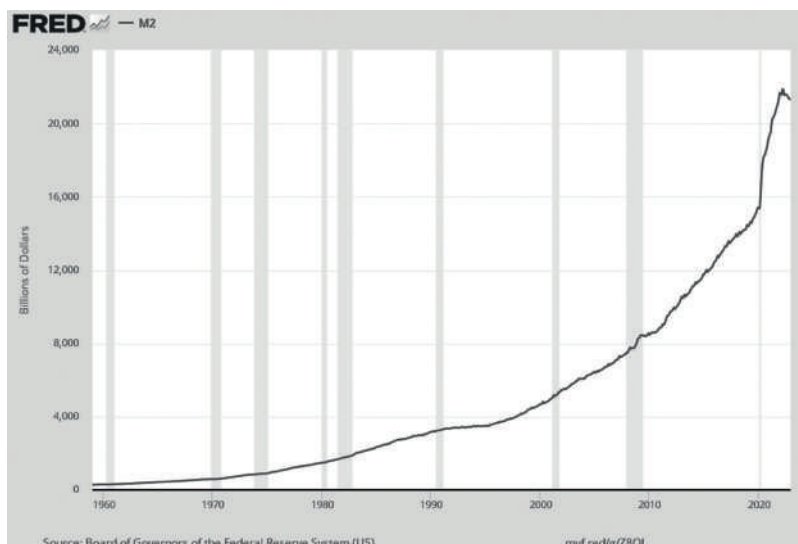
Alokace ze strany velkých investorů. Velcí investoři se již pozvolna probouzejí k poznání, že s dluhopisy, akciemi a dokonce i s penězi samotnými je něco fundamentálně špatně. Známí investoři Paul Tudor Jones, Stanley Druckenmiller, Ricardo Salinas či instituce jako Fidelity představují prozíravé první vlašťovky nového trendu: uznání, že nenulová alokace do bitcoinu by měla být součástí dlouhodobého portfolia.

Microstrategy a spekulativní útok na dolar. Doposud pouze jedna jediná korporace (Microstrategy) začala provádět spekulativní útok na americký dolar v podobě vytváření dluhových závazků ve fiat

a akumulace zdravých peněz do rozvahy. V průběhu medvědího trhu 2022–2023 jsou Microstrategy a její ředitel Michael Saylor zsměšňováni; až se však situace otočí, pak si mnozí uvědomí, že by je měli spíše následovat a akumulovat bitcoin všemi dostupnými prostředky.

Výše uvedené trendy, i když ne všechny měřitelné, nám o bitcoinu říkají více než krátkodobá cenová volatilita. Dočasná volatilita je svůdná pro gamblery, ale v dlouhém měřítku je zcela irelevantní. Nesejde na tom, zda je cena tři tisíce dolarů, třicet tisíc dolarů nebo tři sta tisíc dolarů. Na žádné fiatové cenovce ve skutečnosti nezáleží, protože fiatové měny nebudou v dlouhém horizontu relevantní. Dokud potřebujeme vyjadřovat hodnotu bitcoinu v některé z fiatových měn, je stále ještě příliš brzy; znamená to totiž, že bitcoin se ještě nestal univerzální účetní jednotkou.

Fiat s každým dalším rokem ztrácí na hodnotě. To je zkratka logický důsledek současného peněžního systému založeného na dluhu. Je třeba vytvářet stále více peněžních jednotek, aby se celý systém nezhroutil:



Graf měnové zásoby dolarového peněžního agregátu M2. Grafy ostatních světových měn vypadají velmi podobně. Peněžní tiskárna dělá „brrr“ všude na světě. Zdroj: Fred.

Všechny státní měny procházejí pozvolnou hyperinflací. Jediný rozdíl mezi nimi je tempo jejich úpadku.

Používání bitcoinu jako prostředku k hromadění dalšího fiat je známkou zásadního nepochopení toho, co se vlastně děje. Fiat není udržitelnou formou peněz. Hromadění fiat je bláhové, jelikož ho je limitně neomezené množství. Bez ohledu na to, kolik státních peněz nahromadíte, při dostatečném časovém odstupu bude vaše kupní síla rozředěna na nulu.

Z „Number go up“ se stane „Number go down“

Oceňování bitcoinu ve fiat tedy nedává z dlouhodobého hlediska smysl. Co ale pak dává smysl?

Oceňování všeho ostatního v bitcoinu.

Ano, dnes taková teze působí trochu absurdně, jelikož většina z nás má stále mzdy, výdaje a dluhy vyjadřované ve státních penězích. Ale jak se bude společnost bitcoinizovat, kalkulace v bitcoinu – či spíše v satoshi – se stane denní přirozeností.

Koneckonců dnes nepřemýšlíme o „ceně“ dolaru, ale spíše o tom, co si za dolar koupíme. A stejné to bude s postupující světovou adopcí s bitcoinem. Lidé se mentálně posunou od ceny bitcoinu ke *kupní síle* bitcoinu.

Vzhledem k tomu, že bitcoin se v dnešní době používá především jako úložiště hodnoty, dává smysl, abychom si nejprve osvojili zvyk přemýšlet o svém bitcoinovém jmění v satech místo v dolarech. Dolarová hodnota našeho bitcoinového jmění se může v průběhu času měnit, ale většina lidí nakonec dospěje k závěru, že **záleží pouze na navyšování množství bitcoinu v naší peněžence**. Mnozí na to přijdou až po špatné zkušenosti: prodají za cifru na cenovce, již považují za dostatečně vysokou, ale později se stanou svědky dalšího prudkého růstu ceny. Většina spekulantů časem zjistí, že má stále méně bitcoinů. Ti prozíravější následně přepnou svůj mentální model z dolarů na saty.

Dalším krokem je, když lidé začnou přijímat část či dokonce celou svou mzdu v bitcoinu. Kromě vášnivých bitcoinerů se možnost dostávat část mzdy v bitcoinu začne dříve či později šířit i mezi „normálními“ pracovníky – tento vývoj lze očekávat zejména v rozvojových zemích, kde je již nyní běžné vydělávat v zahraniční měně, nejčastěji v dolaru. Při vyplácení mzdy v bitcoinu bývá mzda vyjadřována ve fiat, pracovníci si však nevyhnutelně všimají, kolik satoshi každý měsíc obdrží. Jak bude cena bitcoinu ve fiatovém vyjádření stoupat, pracovníci budou pozorovat, že vydělávají stále méně a méně satoshi, ačkoliv tyto menší částky mají postupem času vyšší kupní sílu. Lidé si tak poměrně přirozeně začnou zvykat na cenově (a mzdově) deflační aspekt bitcoinové ekonomiky.

Přirozeným vývojem pak bude mentální přecenění velkých nákupů v satoshi. „Tři miliony satů za iPhone?! Padesát milionů satů za auto?!“ Každý dlouhodobý hodler ví, že tyto ceny časem klesnou. Bitcoin má silný vliv na snížení časových preferencí, tj. upřednostnění budoucího blahobytu před krátkodobým uspokojením. Mentální kalkulace věcí v satech se stane druhou přirozeností dávno předtím, než bude zboží v bitcoinu přímo naceňováno obchodníky.



Takto se postupně z „number go up“ stane „number go down“. Cena bitcoinu může v budoucnu ve fiatovém vyjádření stoupat do nekonečna, ale málokdo tomu bude věnovat pozornost, protože fiat bude již irelevantní. Nikoho dnes nezajímá, kolik stojí bitcoin v zimbabwských dolarech; obdobně nikoho nebude zajímat, kolik bude za několik desetiletí stát v amerických dolarech. Lidé na bitcoinovém standardu budou místo rostoucí fiatové cenovky vnímat konstantně klesající ceny.

Ale co ona pověstná volatilita? Jakmile se bitcoin stane všeobecně používanou účetní jednotkou, volatilita a míra zhodnocování se výrazně sníží. Bude to způsobeno několika faktory: nebudou existovat žádní spekulanti usilující o zisky ve fiat, namísto nich budou všichni provádět pravidelné DCA (jen se tomu bude říkat jednoduše „spoření“) a tržní kapitalizace bude tak obrovská, že bude prakticky nemožné, aby nějaký jednotlivý subjekt pohnul kupní silou bitcoinu. Místo náhlých růstů a propadů bude míra zhodnocování kupní síly po hyperbitcoinizaci jednoduše odpovídat míře růstu ekonomické produktivity. Bitcoinový standard je tak v souladu s přirozenou deflací vyvolanou technologickým růstem (v angličtině growth deflation).

„Technologie je deflační. To není jen má domněnka. Je to přirozenost technologie. A protože technologie je základem stále větší části světa kolem nás, znamená to, že vstoupíme do věku deflace, jaký svět ještě nezažil.“

– Jeff Booth, *The Price of Tomorrow: Why Deflation is the Key to an Abundant Future*

Možná si teď řeknete: „To všechno je sice hezké, ale je to vzdálené desítky let“. No, to je ale smyslem tohoto textu, ne? Dnes ještě není pozdě, protože hlavní sociálně-ekonomické důsledky nás teprve čekají. Zhodnocení možného – a podle mého názoru docela pravděpodobného budoucího vývoje – má silný vliv na dnešní chování. Vědomí, kam to všechno vede, nás motivuje k tomu,

abychom se dnes chovali ctnostně: osvojili si přístup s nízkými časovými preferencemi, trpělivě strádali a zároveň kalkulovali své úspory v satech místo ve fiat, ignorovali fiat maximalisty a shitcoinery.

Nikdy není pozdě, ale ranní ptáče dál doskáče

Na bitcoin nebude nikdy „příliš pozdě“. I poté, co se bitcoin stane globálními penězi a míra zhodnocování jeho kupní síly bude odrážet pouze růst produktivity, bude mít smysl uchovávat hodnotu v bitcoinech. Bude to zkrátka nejlepší možný spořicí instrument pozvolna zhodnocující kupní síly bez rizika protistrany či selhání investičního záměru (koncept bitcoinu jako spoření rozvádím v kapitole *Návrat úspor: Bitcoin jako konzervativní volba*).

Nic ale není stoprocentně jisté. Strádání a držení bitcoinu předtím, než dojde k hyperbitcoinizaci, má svá rizika. Bitcoin má stále hypotetická nebezpečí technického typu, bezrizikové není ani samotné držení (ať u správce, či ve vlastní peněžence), ačkoliv nástroje na bezpečnou úschovu se rychlým tempem zlepšují a jsou stále intuitivnější.¹ Další rizika jsou politické povahy; stát má stále legální monopol na peníze a bude si je chránit. Současní držitelé bitcoinů čelí riziku nespravedlivého zdanění, konfiskaci a dalším druhům obtěžování ze strany státu.²

Proto i když s přijetím bitcoinu se nikdo nikdy neopozdí, osobní adopce bitcoinu před hyperbitcoinizací má potenciálně značně vysoký výnos, který odpovídá zvýšenému riziku před celosvětovou adopcí.

1 O hardwarových peněženkách pojednáváme později v knize v kapitole *Rozumnost aneb Jak na hardwarové peněženky*.

2 O těchto tématech pojednává kapitola *Návrat konfiskací: Stát bitcoin nezakáže; bude na něm parazitovat*.

Poznatky z kapitoly

- V současnosti jsme stále na samotném počátku procesu bitcoinizace.
- Bitcoin je vhodným uchovatelem hodnoty, jelikož není libovolně tisknutelný tak jako fiat měny.
- Bitcoin je vhodným prostředkem směny, jelikož lze s pomocí Lightning Network „teleportovat“ po celém světě, okamžitě a s velmi nízkými poplatky.
- Svět teprve objevuje potenciál bitcoinu.
- V budoucnosti nebudeme oceňovat bitcoin ve fiat, ale spíše vše ostatní v bitcoinu (nebudeme mluvit o ceně bitcoinu, ale o *kupní síle* bitcoinu).
- Globální adopce bitcoinu nicméně není jistá a má své překážky; proto má brzká adopce vysoký potenciální výnos odpovídající nejistotě hyperbitcoinizace.

Perspektiva incentív: Fiatová mentalita: proč (nejen) ekonomové nechápou bitcoin

Bitcoin Magazine, 17. 5. 2021 a Finmag, 22. 10. 2021

Někteří lidé připodobňují bitcoin k tulipánové mánii či Ponzioho schématu s jasným závěrem, že se jedná o bublinu, která musí brzy splasknout. Takto se o bitcoinu vyjadřuje ne jeden slavný ekonom s Nobelovkou na krbové římse. Proč tito renomovaní odborníci nevidí v bitcoinu žádnou hodnotu? Myslím, že se nejedná až tak o nepochopení bitcoinu jako takového, ale spíše o diametrálně odlišný pohled na svět.

Vliv ekonomie hlavního proudu nelze podceňovat. Jak řekl John Maynard Keynes: „Praktičtí muži, kteří sami sebe považují za odolné vůči všem intelektuálním vlivům, jsou obvykle otroky některého ze zesnulých ekonomů. Blázní u moci destilují své šílenství z per polozapomenutých akademických pisálků.“ Tento citát hezky vystihuje současnou hospodářskou politiku. Podívejme se tedy, jak se na současnou ekonomiku – a tedy i na společnost samotnou – dívají vlivní šílenci a pisálci dneška.

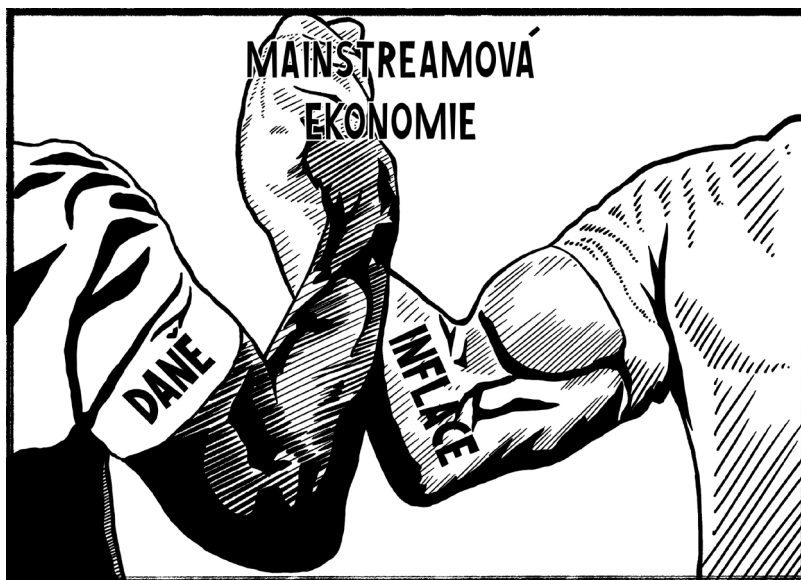
Co je to vlastně mainstreamová ekonomie?

Ekonomie hlavního proudu je směsicí dvou dominantních škol ekonomického myšlení: keynesiánství a monetarismu.

Keynesiánství v různých podobách (tj. postkeynesiánství, nové keynesiánství) je silně zaměřeno na ekonomické agregáty: HDP, míru nezaměstnanosti, spotřebitelské výdaje, inflaci měřenou prostřednictvím indexu spotřebitelských cen (CPI) apod. Tržní síly považuje za chronicky nedostatečné v důsledku různých údajných selhání trhu. Společnost neustále potřebuje veřejné statky poskytované státem. **Veřejné výdaje jsou v očích keynesiánských ekonomů všelékem a měly by se uskutečňovat i za cenu vysokých rozpočtových deficitů**, je-li to nutné. Zajímavé je, že sám Keynes předepisoval deficity veřejných financí pouze v období hospodářského poklesu – rozpočet USA byl nicméně v deficitu 46 z posledních 50 let, a to i v době silného hospodářského růstu.

Monetarismus se také zaměřuje na ekonomické agregáty, ale jeho recepty jsou, inu, monetaristické povahy: místo fiskálních opatření by měla ekonomice pomáhat centrální banka. **Nafukování peněžní zásoby, manipulace s krátkodobými úrokovými sazbami, zastávání role věřitele poslední instance, skupování hypoték, dluhopisů nebo dokonce akcií** – všechna tato opatření v očích monetaristů ochraňují ekonomiku před nevyhnutelným krachem, deflací a nezaměstnaností.

Dnešní ekonomičtí experti, poradci a vládní úředníci obvykle zastávají kombinaci těchto dvou pohledů na ekonomiku. Hospodářská politika by tedy měla využívat jak peníze daňových poplatníků, tak i jejich kupní sílu. Je důležité zdůraznit, že monetarismus začal hrát roli v hlavním proudu ekonomie v 70. letech 20. století – poté, co americký dolar ztratil svou směnitelnost, a celý svět se ocitl pod čistým fiatovým standardem bez jakékoliv vazby na zlato. V jistém smyslu přišel monetarismus na pomoc keynesiánství: s neustále rostoucím zadlužením bylo třeba najít argument pro stále nižší úrokové sazby.



Mainstreamoví ekonomové se shodnou, že vaše peníze nejlépe poslouží státu: ten si své uloupne nejprve prostřednictvím daní, poté s pomocí inflace.

Chronické deficity vyvolávají potřebu nafukovat dluh prostřednictvím politiky levných peněz. A politika levných peněz je zase silnou pobídkou k dalšímu zadlužování – pro vládu i ekonomiku jako celek.

Ačkoliv se může zdát, že hospodářská politika založená na mainstreamové ekonomii v posledních desetiletích uspokojivě funguje, z dlouhodobého hlediska spěje ke katastrofě. Nafukování dluhové bubliny s pomocí politiky levných peněz prostě není udržitelné a tak či onak tato bublina nakonec praskne: buď se dlužníci dostanou do insolvence, nebo se kupní síla fiat peněz vypaří. Jak to stručně okomentoval Dylan LeClair: „Ze současného ekonomického prostředí není žádné civilizované východisko.“³

Fiatová mentalita

„Namísto peněz vytvořených kliknutím myši máme peníze, které se musí těžit – vytvářet pomocí výpočtů náročných na zdroje. (...) Jinými slovy, nadšenci do kryptoměn ve skutečnosti oslavují využití nejmodernější technologie k tomu, aby vrátili měnový systém o 300 let zpět. Proč bychom to měli chtít? Jaký problém to řeší? “

– Paul Krugman⁴

Nyní zpět k úvodní otázce: Proč mainstreamoví ekonomové nenávidí bitcoin?

Výše uvedený citát renomovaného nobelisty nám pomůže na tuto otázku odpovědět. Je pozoruhodné, že to, co zastávce zdravých peněz považuje za hlavní přednost bitcoinu, odsuzuje mainstreamový ekonom jako jeho nevýhodu. Pro Paula Krugmana – typického představitele dnešního ekonomického mainstreamu – je bitcoin

3 Dylan LeClair: The Conclusion of the Long-term Debt Cycle and the Rise of Bitcoin, *Bitcoin Magazine*, 12. 4. 2021.

4 Paul Krugman: Transaction Costs and Tethers: Why I'm a Crypto Skeptic, *The New York Times*, 31. 7. 2018.

odsouzen k selhání, protože v něm nelze vytvářet nové peněžní jednotky kliknutím myši.

A to je právě ona *fiatová mentalita*: světonázor, podle něhož by stát a jeho experti měli mít možnost vytvářet peníze a intervenovat s nimi v ekonomice podle libosti. My si zde můžeme tento přístup nazvat pravým jménem: monetární socialismus. Stát definuje, co jsou peníze prostřednictvím zákonů, řídí měnovou politiku (tj. rychlost tvorby peněz), stát rozhoduje o tom, ke komu se nové peníze dostanou nejdříve, stát určuje úrokové sazby, stát demotivuje lidi od úspor a naopak je tlačí k zadlužování. Ačkoliv moderní centrální banky provádějí měnovou politiku nepřímými nástroji, jako jsou tzv. „operace na volném trhu“, pro působení tržních sil není v éře fiat peněz ponecháno mnoho prostoru.

Jednou ze základních funkcí peněz je (nebo by měla být) jejich role uchovatele hodnoty. Ta však jde stranou, když se do práce pustí fiatoví ekonomové. Vzhledem k tomu, že peníze lze pod fiatovým standardem vytvořit ze vzduchu, nemá smysl je dlouhodobě držet. Že by pro investování do budoucích projektů? Na to přece máme úvěry se stále nižšími úrokovými sazbami! A co rezerva pro nejistou budoucnost? K tomu zde máme sociální stát! Proto nikdy neuvídíte mainstreamového ekonoma uznat, že bitcoin může plnit funkci uchovatele hodnoty: je to jako chtít po barvoslepém, aby ocenil krásu duhy. Jednoduše nemá schopnost ji vidět.

Z pohledu mainstreamové ekonomie to dává smysl: jedinou cestou z keynesiánské dluhové pasti je kromě přímého bankrotu inflace. Myšlenka, že by peníze měly fungovat jako dlouhodobý uchovatel hodnoty, je pro nositele fiatové mentality absurdní, přežitá a nebezpečná. Peníze by podle tohoto světonázoru měly sloužit jako prostředek směny. Stačí, když krátkodobě nedojde k jejich hyperinflaci, ale dlouhodobě je žádoucí, aby postupně ztratily většinu své hodnoty.

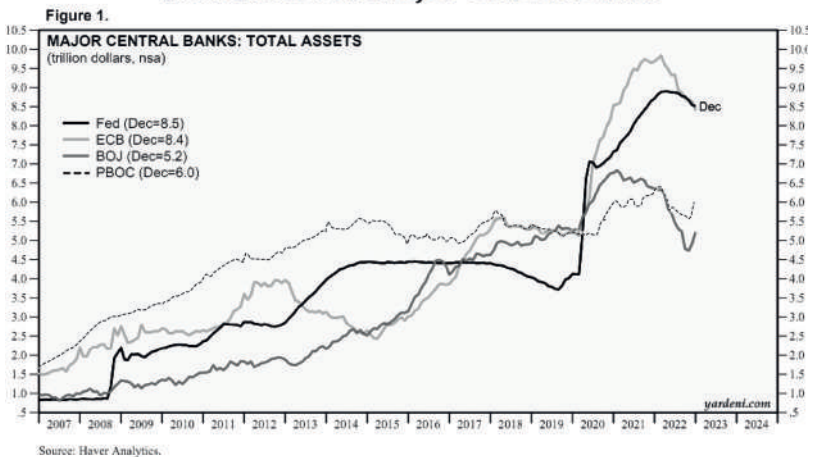
Rakouská alternativa

„Veškeré racionální jednání je ekonomické. Veškerá ekonomická aktivita je racionálním jednáním. Veškeré racionální jednání je v první řadě individuálním jednáním. Pouze jednotlivci jednají.“

– Ludwig von Mises, *Socialismus: Ekonomická a sociologická analýza*

Klíčovým problémem mainstreamového přístupu je obsese agregátními veličinami a minimální pozornost individuálnímu jednání a relativním silám, které působí v ekonomice. Je tak sice pravda, že vláda nebo centrální banka mohou stimulovat ekonomiku a vyvolat agregátní růst, ale struktura ekonomiky může být v důsledku státních zásahů nestabilní. Stačí si vzpomenout na finanční krizi v roce 2008: americká ekonomika po léta zdánlivě silně rostla, ale později se ukázalo, že tento růst byl značně toxický, a celý finanční systém se v důsledku téměř zhroutil. Řešením podle mainstreamového receptu bylo více téhož: ještě více deficitních výdajů, ještě nižší úrokové sazby a další způsoby tisku peněz, jako je kvantitativní uvolňování.

Total Assets of Major Central Banks



Rozvahy hlavních centrálních bank. Normalizace kvantitativního uvolňování po roce 2008 vedla k masivnímu nafouknutí rozvah, přičemž nákup aktiv do rozvahy = vytváření nových peněz. Zdroj: Yardeni Research.

Rakouská ekonomická škola se zaměřuje právě na to, co mainstream ignoruje: relativní změny cen, heterogenitu kapitálu, rozdílnost motivací v soukromém vs. veřejném sektoru, změny v časových preferencích prostřednictvím měnové politiky. Nevíte-li, co všechny tyto termíny znamenají, lze to zjednodušit na jednu klíčovou myšlenku: individuální lidské jednání. Vše, co se v ekonomice děje, vychází z toho, že jednotlivci jednají. Jednotlivec je motivován svými subjektivními preferencemi a incentivy, které ho pohání. Na hospodářskou politiku lze pohlížet jako na pokus o manipulaci se strukturou incentív: kupříkladu snížením úrokových sazeb jsou lidé motivováni k zadlužování a upřednostňování spotřeby před investicemi.

Na rozdíl od ekonomie hlavního proudu není rakouská škola ve své podstatě technokratická. Stoupenci rakouské ekonomie chápou, že ekonomika je v zásadě neovladatelná. Absence vědomého řízení však neznamená, že nastane chaos. Jak vysvětluje Hayek v článku *Využití znalostí ve společnosti*, individuální jednání je koordinováno prostřednictvím cenového mechanismu. Ekonomika je složitý systém v neustálém pohybu a relevantní údaje o nabídce, poptávce, nedostatku zdrojů a individuálních preferencích (a nikdy nekončících změnách těchto faktorů) jsou rozptýleny napříč miliony myslí. Obsáhnout každý datový bod v jeho úplné podobě je nemožné – místo toho je nejmenší potřebná informace komunikována prostřednictvím ceny. Cena je veškerou informací, kterou výrobci, obchodníci, investoři a spotřebitelé potřebují znát, aby mohli přizpůsobit své jednání tak, že bude lépe odrážet realitu.

Pokud jsou však peníze samy o sobě předmětem centrálního plánování, je cenový mechanismus zanesen šumem. Aby cenový mechanismus vysílal čisté ekonomické signály a ekonomika správně fungovala, musí být peníze odděleny od státu.

Je důležité si uvědomit, co jsou vlastně peníze. Peníze jsou v nejzákladnějším smyslu společenskou institucí – souborem pravidel a zvyklostí, které usnadňují spolupráci mezi lidmi. Jak

upozorňuje Nick Szabo v článku *Shelling Out*⁵, instituce peněz se v průběhu dějin objevuje všude, kam se podíváme, protože je logickým evolučním krokem vždy, když společnost dosáhne dostatečné komplexity a s ní spojené dělby práce. Peníze vznikly z potřeby uchovávat hodnotu vlastní práce pro pozdější použití a směňovat tuto hodnotu s ostatními. Obě role – uchovatel hodnoty a prostředek směny – jsou klíčové pro to, aby peníze mohly plnit svou roli ve společnosti. Není jistě náhodou, že bitcoin vznikl a prosadil se na vrcholu celosvětové finanční krize, během které byla funkce uchovatele hodnoty v dnešních penězích obětována, aby se systém nerozpadl.

Fiatovou mentalitu nezměníme; učiníme ji irelevantní

Všichni zastáváme nějaký světonázor. Autor těchto řádků je nakloněn nestátním řešením společenských problémů a tato náklonnost je jen částečně založena na ekonomických argumentech – velkou roli v adopci světonázorů hraje i politická filosofie; to je přirozené a neměli bychom se bát si to přiznat. Fiatová mentalita je jednoduše světonázor, který zpravidla zastávají ti, kteří jsou niterně přesvědčeni o své schopnosti řídit společnost (a za udržování statu quo bývají také celoživotně motivováni prostřednictvím vysokých pozic v akademické sféře, vysoké politice a finančním odvětví).

Myšlenka zbavit měnovou politiku lidských zásahů je zcela protichůdná způsobu, jakým dnes peníze fungují. To je hlavní problém mainstreamové ekonomie, která se zaměřuje na peníze jako na krátkodobý prostředek, který nelze ušetřit, pouze je možné je utratit, a to nevyhnutelně ve prospěch těch, kteří peníze za téměř nulové náklady tvoří.

Proto budou mainstreamoví ekonomové bojovat proti bitcoinu až do doby, dokud nebude hyperbitcoinizace klepat na dveře. Bitcoin jako nově vznikající peněžní fenomén je pro ně políčkem do tváře. Má potenciál zcela rozbít iluzi technokratického řízení. Když

⁵ Nick Szabo: *Shelling Out: The Origins of Money*, dostupné na nakamotoinstitute.org, původně publikováno v roce 2002.

stát ztratí schopnost řídit peníze, rozpadne se uspořádání, které fungovalo v minulých desetiletích: žádná monetární inflace, žádný Cantillonův efekt, žádné chronické deficity veřejných financí, žádné záchranné programy. Domeček z karet se zhroutí. Ale neobviňujte z toho bitcoin; fiat systém by se rozpadl, i kdyby bitcoin nikdy nevznikl, protože centrální plánování selhává vždy. Bitcoin může fungovat jako záchranný člun před kolapsem fiatů a jako nástroj obnovy po něm.

Fiatová mentalita v praxi: spící princezny, cantilionáři, shitcoineři

Ekonomie je ve velké míře věda o incentivách – pozitivních či negativních pohnutkách, které nás motivují k jednání. Lidé, kteří z určitého důvodu kritizují bitcoin a snaží se jej zesměšnit či přímo zničit, mají své specifické incentive. Lze je rozdělit do tří kategorií.

„Na fiatů netřeba nic měnit“ aneb Spící princezny. První početný tábor tvoří spíš vlažnější kritici bitcoinu. Jsou to lidé, kteří bitcoinu nerozumějí, nechápou, jak a proč může fungovat peněžní systém bez centrálního správce a k čemu lidstvo něco takového vůbec potřebuje.

Spadají sem zejména lidé ze Západu, kteří jsou se svými peněží spokojeni. Bankovní systém je pro ně funkční, debetní/kreditní karty a fintechové aplikace odvádějí svou práci bez zádrhelů, kupní síla se nevypařuje tempem dvaceti a více procent ročně.⁶ V globálním kontextu se ale jedná o relativně úzkou a privilegovanou skupinu. Pro mnohem větší část lidstva tohle neplatí – miliardy lidí žijí bez přístupu ke spolehlivým platebním metodám nebo v prostředí dvou- až třiciferné inflace.

Privilegovaní se o bitcoin nezajímají, jsou ukolébáni dojmem stability státních peněz. Finančně neprivilegovaní naopak chápou bitcoin téměř instinktivně, představuje pro ně záchranný žebřík z nefunkčního systému. Zajímá-li vás adopce bitcoinu v rozvojových

6 Tuto větu jsem napsal do původního článku v říjnu 2021. Ponechávám pro tragikomický efekt – v době psaní knihy (říjen 2022) dosahuje oficiální cenová inflace v ČR již téměř 20 procent.

zemích, doporučuji zejména sledovat výstupy Alexe Gladsteina z Human Rights Foundation.⁷

„Bez fiatů by se rozpadla společnost (a můj sen o páte vile)“ aneb Cantillionáři. Druhý tábor odpůrců bitcoinu tvoří ti, kteří jsou přímo zainteresováni na současném finančním systému a jeho zachování. Patří sem protagonisté výše rozebírané mainstreamové ekonomie jako Paul Krugman či Nouriel Roubini, komerční i centrální bankéři, většina politiků a nadnárodních byrokratů z organizací, jako jsou Mezinárodní měnový fond a Světové ekonomické fórum, jakož i množství investorů, kteří se naučili hrát fiatovou hru.

Znovu jde především o lidi ze Západu. Stávající peněžní systém pro ně funguje ještě daleko lépe než pro lidi z prvního tábora. Přímo totiž těží z Cantillonova efektu a odsávají kupní sílu z kapes nic netušících spoluobčanů. Jak si rozebereme dále v kapitole o světě po hyperbitcoinizaci, bitcoin je přímým ohrožením cantillionářů; kritika z řad tohoto tábora je z jejich pohledu vysoce racionální a do budoucna je třeba počítat s tím, že u kritiky nezůstanou. Ti hloupější se budou snažit bitcoin zakázat, ti chytřejší konfiskovat a kontrolovat.

„Bitcoin je zastaralý, mám něco lepšího“ aneb Shitcoiněři. A pak jsou tu tvůrci altcoinů a takzvaní bagholderi (ti, co mají plné bágly všelijakých nově vznikajících coinů). Z tohoto tábora nejhlučněji zaznívají zkazky o zastaralosti bitcoinu. Tvůrci altcoinů a jejich investoři se neustále potýkají s existenciální otázkou: Proč by se lidé měli zajímat zrovna o jejich projekt, jeden z tisíců jemu podobných? Jejich nejsnadnější odpověď je, že jsou inovativnější než bitcoin. Zpravidla to není pravda (zastánci tohoto směru většinou ignorují bitcoinovou platební nadstavbu Lightning Network), případná skutečná inovace je u altcoinů vždycky vykoupena jejich centralizací. Jenže právě schopnost fungovat bez *centrálního bodu selhání* je tou největší a těžko překonatelnou inovací, kterou přináší bitcoin.

⁷ Gladsteinova kniha *Check Your Financial Privilege* patří k tomu nejlepšímu, co jsem o bitcoinu četl.



Nejedná se o stejné odvětví, nejsme v tom spolu, není to diverzifikace. Shitcoiny jsou šum a zmatení, bitcoin je signál a to jediné, o co tu jde.

Naprostou většinu hlasitých kritiků bitcoinu můžeme zařadit do jednoho z výše jmenovaných táborů. Je mezi nimi jistý rozdíl, pokud se podíváme na jejich motivaci k odmítání bitcoinu.

Ti první ho odmítají, protože nemají pocit, že by jim mohl něco přinést, nechtějí do něj tedy investovat ani čas, i když to se v době maniakální měnové politiky může rychle změnit.

Druzí a třetí jsou pak silně motivováni proti bitcoinu bojovat všemi prostředky, jelikož ohrožuje jejich zájmy. Až příště narazíte na další řeči o zaručeném splasknutí bubliny nebo oznámení definitivní bitcoinové smrti, zkuste si nejdřív položit otázku, jestli se spíš nejedná o zbožné přání konkrétního hlasatele.

Poznatky z kapitoly

- Dnešní mainstreamová ekonomie je nejvíce ovlivněna keynesiánstvím a monetarismem; pro stát je to ideální kombinace, protože má z akademické sféry „dovoleno“ okrádat společnost jak prostřednictvím daní, tak i inflace.
- Zatímco mainstreamová ekonomie se zabývá hlavně agregátními ukazateli, rakouská škola ekonomie zakládá svou analýzu na jednání a motivacích jedinců.
- Rakouská škola ekonomie zdůrazňuje úlohu cen coby nenahraditelných přenašečů informací; státem řízené peníze zanášejí tento přenos šumem.
- Bitcoiněři nebojují proti fiat; fiat se rozpadá sám od sebe a bitcoin je možnost záchrany pro ty, kdo si jsou osudu fiatů vědomi.
- Bitcoin kritizují zpravidla lidé patřící do jednoho ze tří táborů: ti, kteří nechápou problém státních peněz (spící princezny); ti, kteří vydělávají na existenci státních peněz (cantillionáři); ti, kteří mají finanční zájem na úspěchu konkurenčních nestátních peněz (shitcoineři).

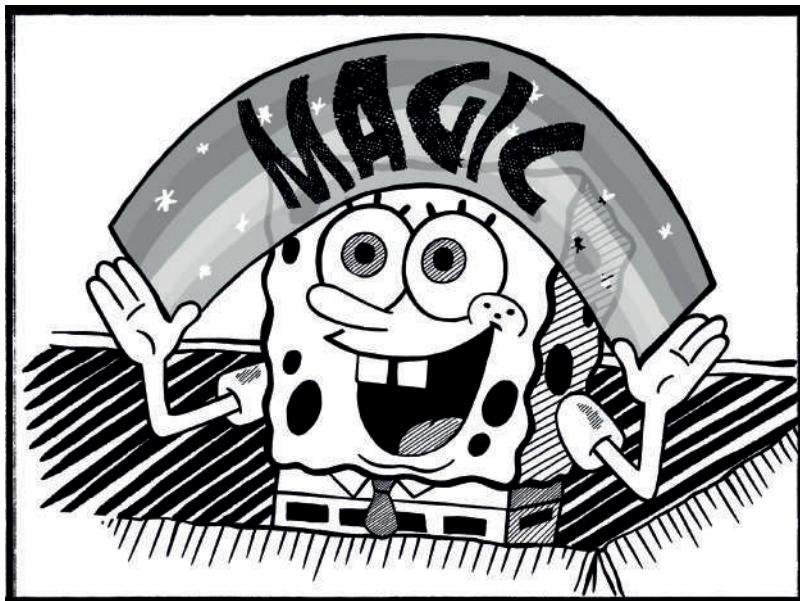
Perspektiva udržitelnosti: Bitcoin přežije euro

Bitcoin Magazine, 24. 8. 2021

Nedávno jsme byli vystaveni myšlenkovým pochodům jistého Eera Heinäluoma, socialistického poslance Evropského parlamentu. Ačkoliv do vážně míněného zákazu těžby bitcoinu zřejmě ještě pár let zbývá, lze předpokládat, že takový návrh dříve či později přijde.

Válka proti realitě

Progresivním nápadem pana Heinäluomy je „zastavit používání podkladové technologie bitcoinu“, což by v praxi znamenalo zakázat proof of work. Na tento neinformovaný postoj samozřejmě navazuje výzva, aby kryptoměny přešly na „klimaticky šetrnější“ konsensus v podobě proof of stake.



A proof of stake samozřejmě energii nepotřebuje, jelikož funguje na principech magie.

Ach jo.

Má vůbec smysl potísić opakovat, že proof of work je *tím* zásadním průlomem bitcoinu, jenž zajišťuje neutrální a předvídatelnou měnovou politiku, která v dnešním fiatem zamořeném světě tak chybí? Fakta nechávají Heinäluomu a jemu podobné jedince v klidu, neboť ti si vedou svůj džihád proti realitě.

Když se mudžáhedíni etatismu pustí do práce, fakta letí oknem. Potřebují prodat dobře vypadající příběh. A příběh v souvislosti s bitcoinem zní, že těžba je škodlivá pro životní prostředí a *někdo by s tím měl něco udělat*, což obvykle znamená, že by to vláda měla zakázat.

Ačkoliv politikům na pravdě nezáleží, čtenářům těchto řádek snad ano.

Podle průzkumu Bitcoin Mining Council (BMC) Michaela Saylora se věci mají takto:

- Energetický mix členů BMC, kteří disponují přibližně 32 % celosvětového hashratu, se skládá z 67 % z udržitelné výroby elektriny (udržitelná definovaná jako: obnovitelné zdroje a jaderná energie plus fosilní zdroje offsetované emisními povolenkami).
- Výše uvedenou metriku pak BMC extrapoluje na přibližně 56 % udržitelné energie pro celou těžební síť bitcoinu⁸.

Ostatní výzkumy udávají podíl obnovitelné/udržitelné energie při těžbě bitcoinu na 39 % (studie University of Cambridge⁹) a 36 % (studie Coinshares¹⁰). Můžeme tedy tvrdit, že spodní odhad je, že okolo jedné třetiny energie využívané k těžbě bitcoinu pochází

8 Bitcoin Mining Council Q2 2021 Briefing, dostupné na hope.com.

9 3rd Global Cryptoasset Benchmarking Study, dostupné na stránkách University of Cambridge – Judge Business School, jbs.cam.ac.uk.

10 The Bitcoin Mining Network 2021, dostupné na coinshares.com.

z ekologických zdrojů. Těžaři přirozeně hledají nejlevnější zdroj energie, kterým je často jinak nevyužitá obnovitelná energie (větrná, solární, větrná v době nadprodukce) nebo takzvaná uvízlá energie, například propálený zemní plyn z ropných plošin.

Jak si tedy Evropská unie stojí v porovnání s bitcoinem, pokud jde o udržitelnou energii?

Podle statistik Eurostatu využívá Evropská unie 15 % obnovitelných zdrojů a 13 % jaderné energie, celkem tedy 28 % udržitelné výroby energie.

Energetický mix těžby bitcoinu je tudíž ekologičtější než energetický mix Evropské unie.

Krásné na tom je, že zatímco v případě Evropské unie je zvyšování podílu obnovitelných zdrojů dosahováno prostřednictvím politicky motivovaného programu shora dolů, programu, se kterým se pojí obří náklady a zvýšená nestabilita sítě, v případě bitcoinu je to jen přirozený důsledek ekonomických incentív. Bitcoin je šetrný k životnímu prostředí jako vedlejší efekt, aniž by na těžaře musel kdokoliv tlačit.

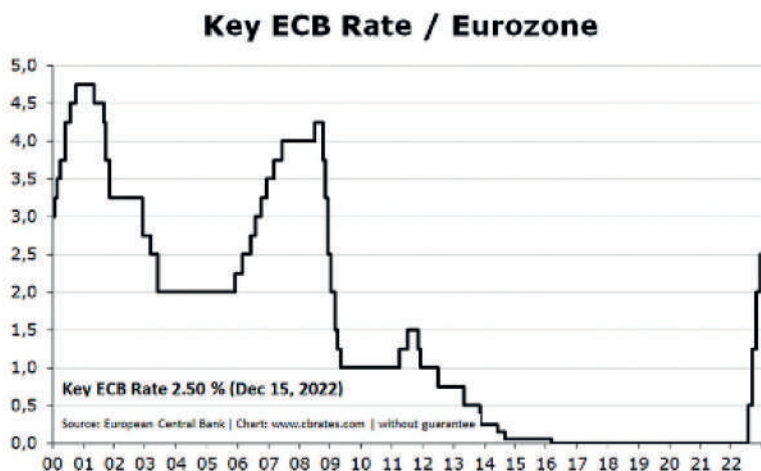
Euro – Frankensteinovo monstrum, jež musí zemřít

Jak často upozorňuje podcaster Marty Bent, o podíl obnovitelné energie při těžbě bitcoinu ale nakonec vůbec nejde. I kdyby se bitcoin těžil výhradně z vody, slunce, nevyužitého zemního plynu a sopek, stejně by byl kritizován za plýtvání energií. Nejedná se totiž o otázku energetických statistik, ale spíše o otázku samotné legitimacy bitcoinu. Politici a další lidé postižení fiatovou mentalitou prostě potřebují bitcoin vykreslit jako neužitečný a škodlivý a použijí k tomu jakýkoliv narativ, který toto zadání splní, ať už jde o plýtvání energií, financování terorismu, obchod s drogami, malware, nerovnost či cokoliv jiného.

Bitcoin nastavuje establishmentu nepřijemné zrcadlo. Navzdory stovkám předpovědí smrti se bitcoinu po 14 letech existence

daří, dvě země jej již přijaly jako zákonné platidlo, další to zvažují a uživatelé po celém světě mohou provádět globální, okamžité a téměř beznákladové transakce.

Bitcoin jsou peníze, které si Evropa zaslouží po dvaceti letech měnového režimu, jenž od samého začátku sotva drží pohromadě. Euro bylo zavedeno v roce 2002 a již v roce 2008 prošlo značnou krizí, když bylo třeba zachraňovat Řecko před krachem. Základním problémem eura je, že jednotná měnová politika funguje jako permanentní dotace fiskálně nezodpovědným zemím. Řecko spolu s dalšími zeměmi PIIGS (Portugalsko, Irsko, Itálie, Řecko, Španělsko) jsou dlužníci, kterým by mělo být velmi riskantní půjčovat, ale jednotná měnová politika jim umožnila se zadlužovat za uměle výhodných podmínek. Výsledkem tak již pár let po spuštění eura bylo, že Řecko fakticky zkrachovalo, když během finanční krize došlo ke zvýšení úrokových sazeb. Vzhledem k tomu, že německé banky byly hlavními věřiteli řecké vlády, bylo nutné celý systém zachránit v zájmu spásy eurozóny – a to necelých deset let po vzniku eura.

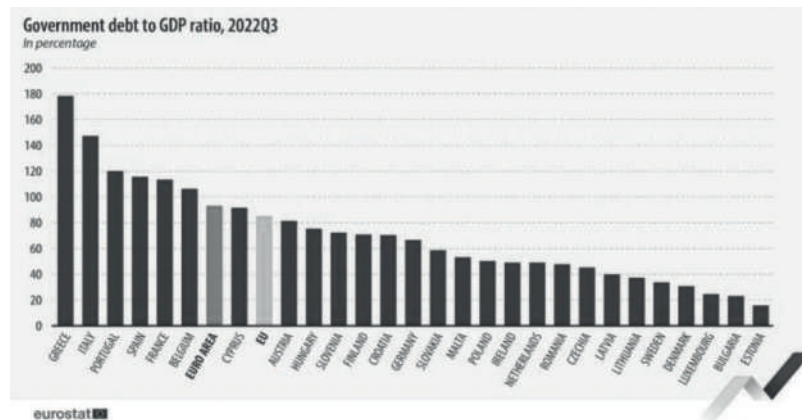


Zdroj: CBrates.com.

Od jara 2016 do léta 2022 byla eurozóna udržována na nulových úrocích. Politika trvale levných peněz měla katastrofální dopad

na veřejné finance členských zemí. Aby mohly kandidátské země původně přijmout euro, musely splnit maastrichtská kritéria, přičemž jedním z nich bylo udržet veřejný dluh pod 60 % hrubého domácího produktu dané země.

Takto vypadala metrika dluhu k HDP po třetím kvartálu roku 2022:



Zdroj: Eurostat.

Eurozónu tvoří dvacet zemí. Třináct z těchto zemí by dnes již nespĺnilo maastrichtská kritéria pro poměr dluhu k HDP, většina zemí také nespĺňuje „povinné“ požadavky Paktu o stabilitě a růstu.

Nejtipnější však je, že řecké státní dluhopisy byly donedávna oceňovány téměř stejně jako německé – to znamená, že řecký státní dluh zdánlivě nenesl větší riziko než německý, přestože země před deseti lety prakticky zbankrotovala a jedná se o jeden z nejzadluženějších států na světě.

Great Convergence

Spread on Greek 10-year bonds over bunds fell below 100 basis points

■ GREEK - GERMAN 10 YR SPREAD - Last Price



Spread mezi německými a řeckými dluhopisy koncem roku 2021 – nízký spread znamená, že řecký dluh je oceňován s podobnou mírou rizika jako německý dluh. Zdroj: Bloomberg.

Toto však není kritika samotného Řecka či jiné konkrétní země. Politici v těchto zemích jednají ekonomicky racionálně a v dnešní době je bohužel ekonomicky racionální se rychle zadlužovat a nehlédět na budoucnost. Z grafu znázorňujícího spread řeckých a německých dluhopisů vyplývá, že trh výše zadlužení příliš netrápí. V celé eurozóně totiž panuje atmosféra morálního hazardu: Řecko se již dříve dostalo do platební neschopnosti a bylo zachráněno. Současná měnová politika je ještě uvolněnější než před deseti lety a v případě problémů člena eurozóny lze opět čekat, že bude zachráněn ostatními.

Jak varovali kritici při zavádění eura, společná měna funguje spíše jako italská lira než německá marka. Bylo to nevyhnutelné, protože umělé politické konstrukty tohoto typu musí nutně vyhovět nejslabším členům, jinak by se rychle rozpadly.

Euro vytváří zombie země a zombie ekonomiky – jediné, co je udržuje naživu, jsou levné úvěry. **Všechny dluhy však nakonec musí být tak či onak vyrovnány – nebudou-li splaceny, pak k vyrovnání dojde prostřednictvím kaskádových bankrotů nebo uloupením kupní síly od stávajících držitelů eura prostřednictvím vysoké inflace, která může eskalovat v hyperinflaci.**

Zdá se tudíž, že je to především euro, které má problém s udržitelností.

Rovněž se také zdá, že si to mocní uvědomují. Když jsou konvenční nástroje měnové politiky jako úrokové sazby vyčerpány, musí být centrální bankéři kreativní. Záporné úrokové sazby či vrtulníkové peníze by mohly pomoci s dalším pumpováním peněz do ekonomiky, v současném systému jsou však neproveditelné. Proto Evropská centrální banka aktivně vyvíjí orwellovské digitální euro.



European Central Bank ✓
@ecb

...

(THREAD) We have decided to launch a project to prepare for possibly issuing a digital euro. We will look at how a digital euro could be designed and distributed to everyone in the euro area, as well as the impact it would have ecb.europa.eu/press/pr/date/... 1/3



1:35 PM · Jul 14, 2021 · Twitter Web App

Evropská centrální banka na Twitteru: „Rozhodli jsme se spustit přípravný projekt pro možné vydání digitálního eura. Budeme zkoumat, jakým způsobem by digitální euro mohlo být navrženo a jak jej distribuovat ke každému v eurozóně, a co by digitální euro přineslo.“

Digitální euro samozřejmě nijak nemění podstatu fiatové měnové politiky. V bitcoinovém žargonu by se digitálnímu euru právem

říkalo shitcoin: centralizovaná a nepředvídatelná měnová politika s limitně neomezeným počtem jednotek, vyžadující povolení státních orgánů a plně cenzurovatelné. Možná to o pár let prodlouží život Frankensteinovu monstrem, kterým je euro, ale přesto taková ohavnost dlouho nepřežije. A doufejme, že s eurem – ať stávajícím, či digitálním – zemře i celý koncept fiatů.

„Energetická náročnost infrastruktury [digitálního eura] by byla zanedbatelná ve srovnání se spotřebou energie a ekologickou stopou kryptoaktiv, jako je bitcoin.“

– Evropská centrální banka ¹¹

A právě v tom je jádro problému: fiat měnu lze vytvořit z ničeho. Potřeba energie je sice zanedbatelná, ale stejně tak i dlouhodobá hodnota takových „peněz“.

Fiat maximalisté nemají rádi konkurenci

Kdyby byly obavy o životní prostředí míněny upřímně, byla by těžba bitcoinu v Evropě vřele vítána, protože umožňuje ekonomické využití jinak promarněných zdrojů, a má potenciál stabilizovat energetickou síť okamžitým využitím nepředvídatelné nadprodukce obnovitelných zdrojů.

Skutečný záměr establishmentu je prozaický: ochrana vlastních zájmů. Peněžní monopol je pro stát posvátný a bude si jej chránit, zejména když nebude schopen obstát v konkurenci. Centrální bankéři již nyní prohrávají souboj idejí – stačí se podívat na komentáře k jakémukoliv tweetu Mezinárodního měnového fondu, Banky pro mezinárodní platby, Federálního rezervního systému nebo Evropské centrální banky; těžko najdete jedinou pozitivní reakci. Pokusy o pošpinění pověsti bitcoinu prostřednictvím falešných obav o životní prostředí mohou na chvíli fungovat jako rozptýlení, ale základní problémy eura nevyřeší.

11 Zdroj citátu je výše odkazované twitterové vlákno Evropské centrální banky.

Evropané budou v příštích letech svědky čím dál patrnějšího kontrastu: stále zoufalejších pokusů o záchranu měnové unie a stále spolehlivější měnové politiky bitcoinu. Očerňovací kampaň bude pokračovat a patrně nabude mnohem vyhocenějších rozměrů než dnes. Doufejme, že veřejnost bude schopna rozeznat fakta od fikce a že adoptuje zdravé peníze i navzdory oficiálnímu narativu.

Poznatky z kapitoly

- Proof of work je zásadním průlomem bitcoinu, díky kterému nelze libovolně tisknout neomezené množství jednotek; proof of stake je pohádka o vytváření hodnoty bez vynaložení zdrojů.
- Proof of work motivuje těžaře hledat ty nejlevnější zdroje energie, které čím dál častěji spadají do kategorie vyplývaných či obnovitelných.
- Problém s udržitelností má spíše než bitcoin euro, které se již několik let po vzniku téměř rozpadlo; nyní drží pohromadě za cenu značně rozbujeleho tisknutí peněz a alarmujícího růstu zadlužení členských zemí.
- Státní dluhy musí být nakonec vyrovnány – varianty (řazeno od nejméně pravděpodobné) jsou splacení, bankrot a inflace.
- Evropská centrální banka zkoumá cesty pro zavedení měnové reformy v podobě digitálního eura, současně s tím lze očekávat zvýšenou míru boje proti bitcoinu, mimo jiné v podobě lživé argumentace ohledně jeho ekologické stopy.

Perspektiva historická: Dějiny koruny: od zlatáků k fiat

Alza, 13. 2. 2021

Historie státních peněz podtrhuje důležitost bitcoinu jakožto možnosti bránit se státním měnovým kejklím. Na českém území se během posledních 150 let vystřídal 7 různých státních měn. Budovat v takovém prostředí rodinné úspory je zhola nemožné.

Před korunou: stříbrné tolary, zlaté floriny (1754–1892)

Okolo roku 1750 byla v zemích střední Evropy ustanovena tzv. konvenční měna: vzájemná dohoda, že německé státy, české země, Rakousko a Uhry budou používat stejnou konvenci při ražbě mincí. Dohoda byla, že z jedné kolínské marky (váhová jednotka odpovídající 233,8 g) se bude razit 10 tolarů či 20 florinů. Od roku 1754 obíhaly ve střední Evropě tolary s obsahem stříbra 23,3 g a floriny s obsahem zlata 11,7 g. Stříbrný tolar by odpovídal zhruba dnešním 430 korunám, zlatý florin pak 14 500 korunám.

Důležité na této éře je skutečnost, že marky, tolary, forinty byly váhové jednotky, měny byly definovány jako mince s konkrétním obsahem zlata či stříbra. Deviace směnného kurzu mezi měnami různých zemí byla tudíž možná pouze tehdy, když panovník dané země zlehčoval mince či měnu jinak devalvoval (např. vydáváním papírových státovek, u kterých panovala pochybnost o směnitelnosti za podkladové zlato/stříbro). Pokud by do definic a obsahu mincí nezasahovali panovníci, pak by se jednalo o velmi stabilní období bez jakýchkoliv peněžních problémů. Tak tomu samozřejmě ale nikdy nebylo, a to ze dvou důvodů: z vnitřních problémů bimetalismu (současného oběhu zlata a stříbra se zákonem daným poměrem, který se liší od tržního poměru mezi kovy) a z důvodu pokusu peněžního perpetua mobile – tvorby peněz z ničeho.

Rakouské císařství (1804–1867) se zmítalo ve válkách s napoleonskou Francií a dalšími zeměmi, což řešilo zadlužováním, bankrotem (1811)

a vydáváním částečně krytých či nekrytých papírových peněz a státních dluhopisů, později došlo i k redefinici váhových jednotek a devalvaci měny.



Stříbrný tolar z roku 1822. Zdroj: Numista.com.

Zlatá koruna (1892–1918)

Rakousko-Uhersko (existující v letech 1867–1918) reformovalo roku 1892 peněžní systém a založilo novou měnu na zlatu. V té době však již byly populární a rozšířené papírové peníze a krytí bankovek nebylo stoprocentní: banky měly povinnost držet zlaté rezervy pouze ve výši čtyřiceti procent hodnoty vydaných bankovek. **Bankovky nebyly plně směnitelné pro běžné občany, jelikož se jednalo o tzv. devizovou zlatou měnu, kdy banky nemusely bankovky proplatit ve zlatě, nýbrž v zahraniční měně, která již přímo směnitelná za zlato byla (např. libra či frank).**

Poměr koruny vůči zlatu byl stanoven takto: z 1 kilogramu ryzího zlata se razilo 3 276 korun, tj. **jedna koruna měla obsah přibližně 0,3 g zlata** o dnešní hodnotě 370 Kč.

V oběhu byly i zlaté mince, kterými byla podporována důvěra ve zlaté krytí bankovek. Jak uvádí historik Jiří Hána v textu o historii rakousko-uherské koruny:¹²

„Pro oběh byly od r. 1892 z čistě demonstračních důvodů raženy zlaté 10 a 20 K, později od r. 1907 i 100 K, aby se obyvatelstvo přesvědčilo, že rakouská koruna je zlatá měna. Ale mince se brzy vracely do pokladen

¹² Text je dostupný na stránkách <https://www.mincelipka.cz/blog/2018/05/86-obdobi-rakousko-uherske-koruny>.

banky. Tezaurační činitel byl téměř nulový, v oněch idylických dobách lidé neměli důvod nedůvěřovat papírovým penězům či schovávat zlato na ‚horší časy‘. Základem tohoto posílení rakousko-uherské měny byla aktivní obchodní bilance se zeměmi se zlatou měnou a odstranění dříve chronických schodků státního rozpočtu.“

A ze stejného zdroje ocitujme ještě informaci o mincích nižších nominálních hodnot:

„Ze stříbra byly raženy mince v hodnotě 5, 2 a 1 K, z obecných kovů haléře (20, 10, 2 a 1). Stříbrná koruna vážila 5 gramů o ryzosti 0,835, zlatá dvacetikoruna vážila 6,775 067 g o ryzosti 0,900 (tj. obsahovala 6,097 56 g zlata) a desetikoruna o stejné ryzosti měla poloviční váhu.“

Rakousko-uherská „dvacka“ tudíž měla kupní sílu v ekvivalentu dnešních 7 400 Kč.

Po začátku války v roce 1914 bylo zlaté krytí okamžitě zrušeno, v oběhu byly hlavně nekryté bankovky, které rychle ztrácely hodnotu vůči zahraničním měnám, jež krytí měly.



Zlatá desetikoruna z roku 1898. Zdroj: Numista.com.

Koruna československá: stříbrné pětikoruny a standard zlaté devizy (1919–1939)

Prvním ministrem financí Československa se stal Alois Rašín, který byl seznámen s rakouskou ekonomickou školou (skrže svého učitele Albína Bráfa), a představuje tak čestnou výjimku mezi politiky a vladaři, jelikož nechtěl peněžní monopol zneužít

ke prospěchu státu, nýbrž k zajištění ekonomické prosperity celé společnosti.¹³ **Rašín si velmi dobře uvědomoval, v čem tkví nebezpečí papírových peněz a že produktivitu a funkční trh nelze nahradit papírovým bohatstvím.** V roce 1922 přednesl pro Českou národohospodářskou společnost přednášku *Inflace a deflace*, ze které ocitujeme několik zásadních myšlenek, jež dávají najevo jeho nekompromisní postoj vůči státem způsobené inflaci:

„Všechno toto národní jmění nahražováno bylo papírovými penězi a válečnými půjčkami. Výrobnost klesala a byla čím dále ve větším nepoměru ke spotřebě. Přes velikou záplavu peněz, věčného jmění, výrobních prostředků ubývalo. To, co generace nastrádaly prací, úsporami, podnikavostí, vynalézavostí a organisací výroby, bylo ničeno a sněděno. Národní hospodářství chudlo ve stejném poměru, jak přibývalo válečných dluhů a papírových peněz.“

(...)

„Podceněná koruna v zahraničí je svrchovaně nebezpečná pro vývoj hospodářský. Znamená sice usnadnění vývozu, ale současně zvýšení cen z dovozu a pozvolný vzestup cen, mezd a výrobních nákladů.“

(...)

„Není pochyby, že bude deflace probíhati daleko tíže než inflace, avšak pro dosažení normálních poměrů je nevyhnutelnou.“¹⁴

Deflace pod Rašínovým vedením vskutku přišla – a to v míře, která by dnes byla naprosto nemyslitelná. V roce 1922 se cenová úroveň snížila zhruba o 40 %, soukromé mzdy klesly až o 30 %, platy státních zaměstnanců o 10 %. Rašín za svou odvážnou politiku později zaplatil životem, když na něj v roce 1923 spáchal atentát anarchokomunista Josef Šoupal, jenž považoval deflacii za výpomoc kapitálu.

13 Prospěch státu a společnosti jsou často v protikladu, jak vysvětlují ve své předešlé knize *Bitcoin: Odluka peněz od státu*.

14 Alois Rašín: *Inflace a deflace*, dostupné na bibliothecaeconomica.cz.

Nyní se pojďme podívat, jakými penězi tedy naši předci v poválečné době platili a spořili.

Samostatná československá koruna byla nejprve ryzím fiatem – v oběhu byly mince z mědi a niklu a nesměnitelné bankovky. V roce 1926 vzniká Národní banka Československá; k založení československé centrální banky došlo až po tak dlouhé době po rozpadu monarchie proto, že panovaly čilé debaty ohledně konkrétní formy zlatého krytí.

V roce 1926 bylo stanoveno krytí zlatem a cizími měnami směnitelnými za zlato v objemu 20 % všech vydaných bankovek. Každý další rok se zlaté krytí mělo zvyšovat o 1 procentní bod, a to až do úrovně krytí ve výši 35 %. Jednalo se však o **standard zlaté devizy** – požádat o směnu koruny za zlato mohly pouze velké instituce, jako byly zahraniční centrální banky, a minimální výše směny byla v objemu 12 kg zlata (dnešních zhruba 15 milionů Kč). **V roce 1929 odpovídala jedna koruna 0,044 58 gramům ryziho zlata** a před německou okupací vlastnilo Československo celkem 96,6 tun zlata.

Ačkoli bankovky nebyly pro občany směnitelné za zlato, k dispozici měli alespoň stříbro: od roku 1928 byla ražena stříbrná pětikoruna dle návrhu Otty Gutfreunda. Mince měla zpočátku 50% obsah stříbra, v této ryzosti však byla ražena pouze do roku 1932 – poté byla ražena jen z výrazně levnějšího niklu.

V roce 1929 začala ve Spojených státech velká deprese a v následujících letech se krize rozšířila i do Evropy. V roce 1934 tak dochází k první prvorepublikové devalvaci, kdy je **koruna redefinována jako 0,037 15 gramů zlata** (devalvace o 17 %). Zajímavostí je, že kurz koruny vůči dolaru výrazně zpevnil: z předchozích 33,75 korun za dolar na 23,92 korun za dolar. Důvodem byly dvě americké události: konfiskace zlata americkým občanům v roce 1933 a následná devalvace dolaru o 41 %. S odstupem národních měn od zlata si tak mnozí národohospodáři začali uvědomovat jednu okolnost fiat měn: je

celkem jedno, jak mizerná je vaše měna, když jsou na světě měny ještě mizernější – jelikož pak vaše měna vůči těm ostatním posiluje. **Všechny fiatové měny devalvují, některé rychleji, jiné pomaleji; relativní rychlost devalvací pak určuje vzájemný kurz.**

V roce 1936 je koruna redefinována jako 0,031 21 gramů zlata (devalvace o dalších 16 %). K odstupu od zlatého krytí by pravděpodobně dříve či později došlo přirozenou cestou (tj. vlivem nepohodlnosti zlata při úvěrových expanzích a vládním zadlužování), nicméně v československém případě jej urychlila německá okupace.



Československé koruny. Vlevo vzácná pětitisícovka (byla v oběhu jen krátce) dle návrhu Alfonse Muchy. Vpravo stříbrná pětikoruna. Zdroj: iDnes, Lovec pokladů.

Protektorátní koruna (1939–1945)

Mezi lety 1939 a 1945 panovala doba temna, a to i v peněžních záležitostech. Československé bankovky byly nejprve pouze přetištěny protektorátním kolkem, později byly vytištěny nové státopvky a bankovky s dominantním německým popisem. Mince byly raženy ze zinku v továrně na nábytek.

Protektorátní koruna měla stanovený umělý kurz ve výši 10 korun za 1 marku. Reálný kurz byl okolo 6 : 1, tj. oficiální kurz korunu značně podhodnotil. To mělo za následek, že Němci vykupovali české obchody, jelikož jejich marky měly na území Protektorátu uměle vysokou kupní sílu. Následkem byla vysoká cenová inflace, mezi lety 1939 a 1945 vzrostla cenová úroveň o 60 % (inflace 7 % ročně), a to i přes silnou regulaci cen. Na černém trhu rostly ceny ještě rychleji.

Německé marky přijaté českými obchodníky byly odváděny do říšské centrální banky k vypořádání. To se však nedělo, na konci války držela česká centrální banka pohledávky vůči říšské centrální bance ve výši 15,3 miliardy korun. Velká část zboží byla tudíž prodána zadarmo, jelikož česká ekonomika obdržela výměnou za zboží dluh, jenž nebyl nikdy splacen. Ještě horší situace pak byla v dodávkách českého průmyslu a zemědělství do říše – celkový dluh na konci války za tyto dodávky činil 57,9 miliard korun, rovněž se tak jednalo o práci zadarmo. Tzv. „matrikulární příspěvek“ (příspěvek na válečné výdaje) činil poslední rok protektorátu 270 % ročního rozpočtu.

Jak jsme si již uvedli, před válkou disponovalo Československo 96,6 tunami zlata. Většina tohoto zlata byla uložena v zahraničí, i tak na něj však německá vláda dosáhla s pomocí nátlaku. **Celkem bylo během války uloupeno 45,5 tuny československého zlata. V rámci repatriací se mělo do Československa navrátit 24,5 tuny.** Tak se i stalo, ačkoli navrácení trvalo přes 30 let.



100 protektorátních korun (rub) a 1 protektorátní koruna (líc, rub). Zdroj: Wikipedie, Lovec pokladů.

Osud československého zlata

Roku 1938 disponovalo Československo 96,6 tunami zlata, z čehož okupační vláda uloupila 45,5 tun. Po válce byl vyjednáán příslib na navrácení 24,5 tuny (zbytek zlata se nepodařilo dohledat), v roce 1947 dostalo Československo zpět prvních 6 tun zlata. Zbýlých 18,4 tun zlata se do ČSSR dostalo až v roce 1982, a to kvůli sporům ohledně válečných úvěrů, odškodněním za komunistické zestátnování atd. Po rozdělení země na Českou republiku a Slovensko v devadesátých letech zůstalo České republice 70 tun zlata. Většinu z tohoto zlata prodala Česká národní banka (ČNB) v roce 1998 za cenu okolo 300 dolarů za unci. Nyní drží ČNB okolo 10 tun zlata, tj. téměř desetkrát méně než za první republiky.¹⁵ Dnešní koruna nicméně není žádným způsobem „kryta“ zlatem, jelikož není směnitelná za zlato ani pro občany, ani pro zahraniční instituce.

Poválečný chaos: přidělový systém a zestátnění (1945–1953)

Poválečný stav byl chaotický nejen v oblasti peněz. Česko a Slovensko se opět sjednotilo, nicméně v obou zemích ještě obíhaly separátní měny tištěné za války. Panoval přidělový systém, kdy lidé kupovali zboží nikoliv za měnu, nýbrž za přidělové lístky. Přídělový systém trval ještě osm let po válce, až do roku 1953. Tak dlouho přetrvával proto, že poválečná socialistická ekonomika se začala orientovat na těžký průmysl a zbrojení dle státního programu – nikoliv na spotřební zboží dle tržní poptávky. Lidé tak měli nominálně mnoho peněz, nicméně neměli co si za ně pořídit. Bujel černý trh, na kterém ceny rostly na násobky oficiálních socialistických cen. Toto následně „vyřešila“ reforma roku 1953, v rámci níž vláda peníze lidem prostě uloupila.

Poválečné ekonomické situaci také nepomohly Benešovy dekrety, v rámci kterých došlo k zestátnění bank, pojišťoven, průmyslových a potravinářských podniků. Zestátnění bylo přípravou na ovládnutí země Sovětským svazem – program zestátnování totiž prosadili českoslovenští komunisté dle instrukcí z Moskvy (konkrétně se jednalo o tzv. Košický vládní program).

¹⁵ Pro detailnější fakta o historii československého zlata navštivte stránku historie.cnb.cz.

V roce 1945 byla koruna redefinována jako **0,017 773 43 gramů zlata** (devalvace o 43 % oproti předválečné koruně). Mince byly raženy jen v hodnotě 20 a 50 haléřů, 1 a 2 koruny (z mědiniklu a tombaku, tedy mosazi s vysokým obsahem mědi).



Shora: předělové lístky, 1 000 Kčs. Zdroje: Wikipedie, ČNB.

Koruna socialistická: vyvlastnění úspor a státní bankrot (1953–1993)

„Naše měna je pevná a měnová reforma nebude, všechno jsou to fámy, které šíří třídní nepřátelé.“ Tak pravil socialistický prezident Antonín Zápotocký v rozhlasu v pátek 29. května 1953. O den později byla oznámena měnová reforma: dosavadní bankovky zůstaly platné pouze do nedělní půlnoci, v pondělí došlo k jejich zneplatnění a musely být měněny za nové. Jak se později ukázalo, měnová reforma byla nachystána již měsíce dopředu, nové bankovky a mince byly tajně zhotoveny v Sovětském svazu.

Měnová reforma roku 1953 měla následující rysy:

- Od 1. 6. 1953 probíhala výměna bankovek, a to dle různých poměrů (právě na rozdílných směnných poměrech bylo obyvatelstvo nejvíce ožebračeno).
- Hotovost do 300 Kčs se měnila v poměru 5 : 1, tj. za 300 Kčs starých jste dostali 60 Kčs nových, tedy pokud žadatel nepocházel ze státem perzekvované skupiny (např. bývalý majitel podniku, akcionář apod.).
- Hotovost nad 300 Kčs a hotovost perzekvovaných skupin a právnických osob se měnila v poměru 50 : 1 (za 50 Kčs starých 1 Kčs nová).
- Vklady fyzických osob do 5 000 Kčs v poměru 5 : 1.
- Vklady 5 000 až 10 000 Kčs v poměru 6,25 : 1.
- Vklady 10 000 až 20 000 Kčs v poměru 10 : 1.
- Vklady 20 000 až 50 000 Kčs v poměru 25 : 1 a vyšší vklady v poměru 30 : 1.
- Zůstatky na účtech státních organizací a JZD v poměru 5 : 1.
- Zůstatky na účtech soukromých podniků v poměru 50 : 1.
- Zrušeny bez náhrady byly některé typy vkladů, závazky z tuzemských cenných papírů a především tuzemský státní dluh = stát de facto vyhlásil bankrot.

Objem oběživa byl snížen z 52 miliard starých korun na 1,4 miliardy nových korun (poměr 37 : 1). Záměrem reformy bylo zničit nezávislou, produktivní část společnosti, a to se také povedlo. Došlo k přesunu značného bohatství od střadatelů, podnikatelů a řemeslníků ke komunistickým funkcionářům a státu.

Obyvatelé se nemohli měnové reformě nijak bránit – zlato a stříbro již nedrželi od konce monarchie a státem emitované koruny se staly ze dne na den neplatnými. Taková je povaha fiatové měny, jejíž hodnota se odvíjí čistě od státní libovůle.¹⁶

V době socialismu byly tištěny bankovky s budovatelskými motivy a podivnými nominály (nařízenými ze Sovětského svazu) například ve výši 3 Kčs či 25 Kčs. Mince byly raženy z levného hliníku.

S nemalým závanem ironie byla socialistická československá koruna nominálně kryta zlatem, a to v poměru **1 koruna = 0,123 426 gramu zlata. Tento kurz nicméně neměl žádný reálný dopad a oporu v realitě** – takový kurz by implikoval dolar za 7,20 Kčs, realita však byla výrazně jiná, kurz byl při výměně upravován koeficientem, „příspěvkem na turistický ruch“, a lidé mohli nakupovat jen na základě tzv. devizového příslibu, tj. oficiálního svolení k nákupu určitého objemu zahraničních měn.

Oficiální inflace byla v období socialismu nízká, jelikož ceny byly centrálně stanovené a udržované uměle nízko. To znamenalo, že se ekonomika nacházela ve stavu notorického nedostatku zboží a bujel černý trh (kde byly ceny několikanásobně).



Socialistická stokoruna. Zdroj: Wikipedie.

16 Arbitrární zneplatňování fiatů se děje po světě i nyní. V posledních letech patří mezi nejzávažnější případy zneplatnění některých bankovek v Indii v roce 2016, jejímž následkem došlo dle analýz ke ztrátě 1,5 milionu pracovních míst a několika úmrtím (lidé ušlapání v tlačenicích při chaotické výměně bankovek). Dalším příkladem je zneplatnění bankovek v Nigérii počátkem roku 2023, které bylo provedeno s úmyslem přinutit obyvatelstvo používat digitální měnu centrální banky (CBDC). Nigérijci nicméně podle rozličných průzkumů mohutně preferují bitcoin. Pro více informací o situaci v Nigérii doporučuji článek Abubakara Nur Khalila *The Nigerian Election And Naira Crisis Are Fueling Bitcoin Adoption*, vyšlo dne 1.3. 2023 na Forbes.com.

Koruna česká: fixování kurzu, inflační cílování (1993–?)

Po sametové revoluci v roce 1989 byla stále v oběhu socialistická koruna československá, a to až do roku 1993, kdy došlo k rozdělení Československa a vzniku dvou nových měn: české a slovenské koruny.

Česká národní banka (ČNB) do roku 1997 udržovala fixní kurz koruny a cílovala růst peněžní zásoby v podobě agregátu M2 (oběživo + běžné vklady + termínované vklady). Koruna však byla podhodnocená (do liberalizované země proudily zahraniční investice tlačící na růst kurzu oproti oficiálnímu) a ČNB od poloviny roku 1997 kurz uvolňuje. Od té doby **nastává éra inflačního cílování; od roku 2010 stanovuje ČNB cíl 2 % s pásmem 1 procentního bodu oběma směry**. Zlato již nehraje žádnou měnovou roli, tu převzaly devizové rezervy, zejména dolar a euro. V letech 2013–2017 se ČNB de facto vrátila k fixnímu kurzu, kdy cíleně oslabovala korunu na úroveň 27 Kč za 1 euro. Důvodem byl pokles úrokových sazeb na nulovou úroveň a snaha odvrátit případnou deflaci a zlevnit vývozy (jedním z dopadů však bylo zdražení dovozů – jak upozorňoval ve dvacátých letech Rašín).

Vývoj inflace, objemu peněz, rozvahy ČNB

Jak si za posledních dvacet let vedla koruna? Od roku 2002 zveřejňuje ČNB kromě údajů o inflaci i údaje o objemu peněz v agregátu M3 (tzv. široké peníze, tedy zásoba M2 + vybrané nástroje finančního trhu) a rozvahy (objem aktiv a pasiv držených ČNB). Rostoucí agregát M3 a rozvaha ve stručnosti znamená, že do ekonomiky se dostávají nové peníze, které způsobí inflaci – přiznanou, či skrytou (o skryté inflaci níže).

Inflace od roku 2002 až do roku 2021 činila v mediánovém vyjádření 1,9 % ročně. To se nezdá jako příliš, nicméně v praxi to znamená, že zboží, které v roce 2002 stálo 1 000 Kč, se v roce 2021 zdražilo na 1 473 Kč – došlo ke zvýšení cen o 47 %. Tyto výpočty jsou však po roce 2022 již pasé; inflace za rok 2022 činila dříve nepředstavitelných 15,1 %.

Objem peněz v agregátu M3 vzrostl z 1,428 bilionu korun v roce 2002 na 6,133 bilionu korun koncem roku 2022, což je nárůst o 329 %.

Rozvaha centrální banky (tj. převážně zahraniční měny a státní dluhopisy, které ČNB kupuje za nově vytvářené peníze) vzrostla z 788 miliard korun v roce 2002 na 3,2 bilionu korun koncem roku 2022, což je nárůst o 306 %.

Jak to, že se inflace po dvacet let držela na nízkých hodnotách, když bylo dlouhodobě vytvářeno tolik nových peněz? Protože tradičně měřená inflace zahrnuje jen definovaný koš spotřebního zboží. Jak uvádí Český statistický úřad: „Do spotřebního koše je zařazeno potravinářské zboží, nepotravinářské zboží a služby.“ Nefigurují tam nemovitosti či finanční instrumenty – což jsou oblasti, kam nové peníze zpravidla proudí nejčastěji a kde jsou nafukovány ceny, které občas přerůstají až do investičních bublin. Kupříkladu index cen bytů vzrostl mezi lety 2010–2022 o 124 %.¹⁷ Akciový index pražské burzy vzrostl mezi lety 2002–2022 o 180 % (největší spekulativní bublina na pražské burze byla v roce 2007).¹⁸

Dalším aspektem inflace je, že probíhá i tzv. **skrytá inflace**. Ta se může projevit třemi různými způsoby: **zprvé, ceny neklesají, ačkoliv by vlivem růstu produktivity klesat měly**. Inflace ve výši 0 % pořád znamená ochuzení spotřebitelů, pokud by ceny měly klesnout o 1 %. **Zadruhé, výrobci zachovají cenu a zmenší balení** – tento efekt se nazývá *shrinkflation* (česky smrskfance). **Zatřetí, výrobci zachovají cenu a sníží kvalitu** – v čokoládě je nižší obsah kaka, věci se vyrábějí z levnějších materiálů, služby se začnou dělit na základní a prémiové atd. – tento efekt můžeme nazývat šuntflance (*crapflation*).

Kombinací výše uvedených důvodů (úzká definice spotřebního koše + skrytá inflace) dochází k tomu, že tempo růstu nových peněz a tempo růstu oficiální měřené inflace není v souladu.

¹⁷ Zdroj: https://www.czso.cz/csu/czso/ceny_bytu.

¹⁸ Zdroj: <https://seekingalpha.com/symbol/PX:IND>.

Ve skutečnosti však každá nová koruna snižuje něčí bohatství a přerozděluje jej těm, kdo se k novým penězům dostanou jako první (Cantillonův efekt).

A konečně cílená devalvace koruny v letech 2013 až 2017 (tzv. „kurzový závazek“) ukázala, že dnešní situace se od padesátých let bohužel až tak neliší. Pro současné centrální plánovače v centrální bance je největším strašákem tzv. deflační spirála a pokud jsou sazby na nulové úrovni a hrozí pokles cen a vyfouknutí dříve nafouknutých bublin, pak udělají plánovači cokoliv pro to, aby tomu zabránili. Devalvaci koruny či nové nástroje jako kvantitativní uvolňování (nákupy státního dluhu centrální bankou – za nové peníze) tak můžeme klidně očekávat i do budoucna. Jeden z hlavních rozdílů oproti minulosti je, že máme možnost se státní peněžní politice bránit. **Máme k dispozici jak zahraniční měny, u kterých však funguje naprosto totožná politika centrálního plánování, tak i nestátní peníze. Máme k dispozici bitcoin, u něž je měnová politika jasně daná: 6,25 bitcoinů za blok, a to až do příštího halvingu, kdy opět dojde ke „kvantitativnímu zpevnování“.**



Má pravdu, klučina ušatej.

Historie koruny ukazuje, že státním penězům se nedá věřit. Ti, kdo se snažili jednat zodpovědně a spořit, o své peníze každou generaci přišli. Stát zkrátka mívá jiné zájmy než jeho občané. Můžeme si namlouvat, že v současnosti žijeme v civilizovanější době, nicméně povaha státních peněz je stále stejná. O kupní sílu přichází každý, kdo drží státní peníze. Existence nestátních peněz v podobě bitcoinu by v minulosti zachránila celé generace od svévole centrálních plánovačů. Minulost již nezměníme, můžeme však změnit svou budoucnost. Můžeme ignorovat centrální plánovače a zvolit si bitcoin.

Poznátky z kapitoly

- Během posledních 130 let se na českém území vystřídalo sedm různých měn – od skutečných peněz v podobě zlatých a stříbrných mincí až k dnešnímu čistému fiat.
- Naposledy bylo možné si v národní měně spořit – tj. odkládat peněžní jednotku bez ztráty kupní síly – za první republiky, kdy byly v oběhu stříbrné pětikoruny.
- Komunistická „měnová reforma“ v roce 1953 byla obzvláště krutá, jednalo se o cílenou likvidaci na státu nezávislých jedinců, rodin a firem a nastolení režimu totální závislosti na státu.
- Moderní politika inflačního cílování programově okrádá držitele státních peněz (nemluvě o tom, že inflace posledních let naznačuje, že centrální bankéři rozhodně nemají situaci pevně v rukou).
- Na současném měnovém uspořádání nám nic nezaručuje, že zde nynější forma koruny bude i za deset, dvacet či třicet let (to stejné platí i pro euro); naopak měnová politika čistého fiat je politika pozvolné hyperinflace – čím dál rychlejšího nafukování měnové zásoby a odpovídajícího rozkladu kupní síly.

Perspektiva racionálního optimismu: bitcoin navrací do života naději

Bitcoin Magazine, 27. 8. 2021

Vzhledem k událostem posledních let je chmurný pohled na budoucnost pochopitelný. Když se však na věci podíváme z širší perspektivy, zjistíme, že žijeme v nejlepším období v historii. A bude ještě mnohem lépe, protože díky bitcoinu máme šanci vyřešit „poslední velký problém“ lidstva.

Představte si, že byste se narodili ve dvacátých letech minulého století v Československu. Váš život by vypadal zhruba následovně.

Staré špatné dny

Dětství v optimistické éře po první světové válce by bylo radostné, ale tato krásná léta by trvala jen krátce.

V době dospívání byste byli svědky rostoucího strachu rodičů z celosvětové hospodářské krize a následného nástupu Adolfa Hitlera k moci v sousedním Německu. Během nacistické okupace v letech 1939 až 1945 byste byli zotročeni ve válečných továrnách. Někteří z vašich kamarádů – stále ještě děti – by v krutých podmínkách zemřeli.

Po válce by přišlo několik dobrých let. Ačkoliv byla země zpustošena a přišla o většinu zlata, které uloupili nacisté (za asistence Bank of England a Banky pro mezinárodní vypořádání), byla alespoň konečně svobodná. Veškerý optimismus byl však rychle rozdrčen pod tíhou komunistického škrpálu, když se v roce 1948 chopila moci Komunistická strana Československa řízená a financovaná z Moskvy.

I této nové realitě byste se přizpůsobili. Na začátku padesátých let byste měli práci, rodinu a v bance i nějaké úspory. Ty by vám byly zabaveny v rámci „měnové reformy“ v roce 1953 – což byl ve skutečnosti obrovský přerozdělovací program, který měl zadupat

do země zbytky střední třídy. Protože byste nebyli v komunistické straně, reforma by na vás dopadla plnou vahou a z vašich úspor by vám téměř nic nezbylo.

Padesátá a šedesátá léta by byla těžká. Pozorovali byste rozklad společnosti, kde se donašečství stalo normou. Po znárodnění a měnové reformě představovala kolaborace s režimem jedinou cestu vzhůru. Někteří vaši přátelé, kteří pronesli špatný názor ve špatný moment, by v horším případě zmizeli v uranových dolech, v lepším pak v nekvalifikované práci, ačkoli měli univerzitní vzdělání. V ekonomice řízené státem rozhoduje o úspěchu politika, ne schopnosti.

V druhé polovině 60. let byste spolu s ostatními nesměle doufali v lepší budoucnost. Zdálo se, že se věci mění. Přišlo pražské jaro a reformátoři upustili od cenzury médií a omezování cestování. Lidé se mohli opět svobodně nadechnout. Bohužel tyto naděje byly opět rozdraceny pod pásy sovětských tanků. Země zažila po necelých třiceti letech další okupaci, tentokrát z východu. Dopad na morálku lidí byl zničující. Stali byste se svědky toho, jak dvacetiletý Jan Palach spáchal protestní sebevraždu upálením.

Následovala by éra „normalizace“ – návrat k rutině sovětského typu. Lidé opět žili ve strachu. Ti, kteří mohli, utekli ze země, ti, kteří nemohli, volili „vnitřní exil“ – záměrné ignorování politické situace a věnování se neutrální činnosti, jako bylo zahrádkářství a chataření. Disidenti se pokusili oživit ducha roku 1968 prostřednictvím pamfletu nazvaného Charta 77, ale režim byl příliš silný a lidé příliš vystrašení – jediným efektem tak byla ztráta zaměstnání a svobody pro autory Charty a jejich sympatizanty.

V 80. letech byste se po životě plném zmařených nadějí stali zahořklými cyniky. Na smrtelné posteli byste asi neviděli budoucnost lidstva příliš optimisticky.



Recenze na život na území Československa, 1920–1989.

Nepopulární názor: máme se dobře a bude líp

Dvacáté století bylo pro ty, kteří se narodili v nesprávné části světa, velmi depresivní. Celý život jste mohli prožít pod etatistickou botou – nejprve nacistickou, poté komunistickou. Vskutku ubohá existence.

Po pádu Sovětského svazu a železné opony se svět stal optimističtější místem – a to nejen pro 400 milionů lidí osvobozených od nelidského socialistického režimu. Zastánci svobody na celém světě měli konečně nejen teoretický, ale i empirický důkaz obřích rozměrů, že centrální plánování jednoduše nefunguje.

Důvodů k optimismu ohledně budoucích vyhlídek lidstva je však mnohem více. Pád východního bloku, jakkoliv byl působivý, nebyl zdaleka největším krokem vpřed v nedávné historii. Prakticky veškeré podmínky lidského života se dlouhodobě zlepšují. Níže uvádím několik nejvýraznějších příkladů pokroku lidstva, které

citují z fakty nabitě knihy *Pokrok: Deset důvodů, proč se těšit na budoucnost* švédského ekonoma Johana Norberga.

Hlad. „*Hladomor byl natolik všudypřítomným a pravidelným fenoménem, pronásledujícím Evropu tak neústupně, že se podle slov francouzského historika Fernanda Braudela, začlenil do lidského biologického režimu a denního života. Francie, jedna z nejbohatších zemí světa, prožila dvacet šest celonárodních hladomorů v jedenáctém století, dva ve dvanáctém, čtyři ve čtrnáctém, sedm v patnáctém, třináct v šestnáctém, jedenáct v sedmnáctém a šestnáct v osmnáctém. V každém století se udály také stovky lokálních hladomorů.*“

Hladomory jsou dnes již převážně věcí minulosti a zbývající hladomory v minulých desetiletích byly způsobeny zásahem člověka – komunismem, válkou a embargy.

Čistá voda a hygiena. „*Během konce devatenáctého a začátku dvacátého století postavilo mnoho měst moderní vodovodní a kanalizační systémy a začalo se systematickým sběrem odpadu. Tyto nákladné projekty byly umožněny zvyšujícím se bohatstvím společnosti. Největší změna ale přišla s efektivním filtrováním a chlorováním vodních zdrojů v první polovině dvacátého století poté, co byla akceptována teorie nakažlivosti bakteriemi. Očekávaná délka života v USA vzrostla v této době rychleji než kdy jindy v americké historii a zavedení filtrace a chlorování vody dokázalo, že klíčovou proměnnou v tomto vývoji byla čistota vody.*“

Podle údajů Our World in Data má dnes 74 % světové populace přístup k čisté pitné vodě.

Očekávaná délka života. „*Průměrná světová délka života byla v roce 1900 jedenatřicet let. Dnes toto číslo vzrostlo na úžasných 71 let. ... Od konce devatenáctého století byla úmrtnost kojenců snížena z přibližně 25 mrtvých na dva až pět mrtvých na sto porodů.*“

Chudoba. „*Na začátku devatenáctého století byla míra chudoby i v těch nejbohatších zemích vyšší než v chudých zemích dnes. Ve Spojených státech, Británii a Francii žilo čtyřicet až padesát procent populace v podmínkách,*

keré dnes nazýváme extrémní chudobou a keré dnes můžeme najít pouze v subsaharské Africe. Ve Skandinávii, Rakousku-Uhersku, Německu a Španělsku bylo extrémně chudých mezi šedesáti a sedmdesáti procenty.“

Zbývající ohniska extrémní chudoby se dnes nacházejí převážně v autoritářských režimech a ve válkou zmítaných zemích. Extrémní chudoba již není výchozím stavem lidstva, ale spíše výjimkou.

Peníze: poslední velký problém lidstva

V kontextu výše uvedených historických skutečností je dnešní doba vskutku ta nejlepší, ve které můžeme žít.

Jeden závažný problém však zůstal nevyřešen. Je tak všudypřítomný, že bychom jej mohli dokonce nazvat *metaproblémem*: jedná se o problém, který je do značné míry příčinou všech ostatních problémů.

Fiat peníze.

Peněžní systém, který tvoří v posledních padesáti letech základní pilíř všech ekonomik na světě, je snem centrálních plánovačů. Bez jakékoliv vazby na zlato podléhá americký dolar a s ním i všechny ostatní měny totální státní kontrole.

Pokud vám přijde označení fiat peněz za centrálně plánovaný systém přitažené za vlasy, zvažte, jak jinak označit systém, kde:

- Vláda pomocí zákonů o zákonném platidle definuje, co jsou peníze.
- Vláda vydává dluhopisy, které jsou páteří peněžního systému.
- Státní úřad zvaný centrální banka vytváří peníze a stanovuje pravidla pro jejich tvorbu soukromými subjekty.
- Centrální banka uděluje privilegia ve formě licencí komerčním bankám, které se pak mohou podílet na procesu tvorby peněz.

- Centrální banka řídí úrokové sazby – kriticky důležitý signál pro objem a kvalitu úspor, investic a půjček v ekonomice.
- Pokud se objeví problémy, centrální banka mění pravidla hry a zavádí nová opatření, aby zabránila kolapsu systému.

Z jakéhosi podivného důvodu jsou v obecném povědomí moderní peněžní systém spolu s finančními trhy chápány jako produkty volného trhu. Kdyby však bylo výše uvedeným způsobem řízeno jakékoliv jiné odvětví, zřetelně bychom jej identifikovali jako subjekt centrálního plánování.

Jaké jsou důsledky fiat peněz? Jelikož peníze tvoří polovinu každé transakce, jejich kvalita ovlivňuje ekonomiku ve všech ohledech:

Vadné signály. Fiatová měnová politika je příčinou vzniku výrazných hospodářských cyklů, spekulativních bublin a chronické misalokace kapitálu; je to způsobeno tím, že úrokové sazby stanovuje centrální plánovací výbor – bankovní rada centrální banky – místo toho, aby úrokové sazby odrážely tržní signály.

Inflační daň. Tvorba peněz je zdrojem Cantillonova efektu: ti, kdo jsou nejbližší penězvodům, bohatnou (vláda, finanční průmysl, bohatí investoři, věřitelé), zatímco ti, kdo jsou od nich nejdále, chudnou (pracovníci s fixními mzdami a důchody, lidé s úsporami). Cantillonovu efektu se také říká inflační daň, jelikož se jedná o velmi zákeřný způsob, jak vysát kupní sílu z peněženek těch, kdo se inflaci nedokáží bránit.

Dluhová koule. Neustálý tlak na snižování úroků pod přirozenou tržní míru vede k rostoucímu zadlužování všech sektorů (vlády, podniků, domácností): na začátku roku 2021 činil globální dluh 281 bilionů dolarů, tj. 355 % světového HDP – což je prudký nárůst oproti 67 bilionům dolarů, tj. 198 % světového HDP v roce 2000.

Celkový kombinovaný efekt je takový, že lidstvo plýtvá obrovským množstvím zdrojů. Miliony lidí jsou zbytečně udržovány v chudobě nebo nemohou plně využít svého potenciálu.

Zlo fiat peněz je obzvláště záladné, protože je pro většinu lidí neviditelné. Zdá se, že systém navenek funguje dobře, protože všechny negativní účinky jsou nepřímé, a k pochopení jejich příčiny je třeba pečlivě studovat ekonomii a peněžní historii. To vede mnohé k tomu, že z ničivých účinků fiat peněz obviňují volný trh, a vyvozují zdánlivě logický závěr, že potřebujeme více centrálního plánování, nikoliv méně.

V bitcoinových kruzích často zaznívá mantra *Fix the money, fix the world* – **Napravme peníze, napravme svět**. To je velmi výstižný příslib bitcoinu.



Před bitcoinem nebylo mnoho nadějí na nápravu peněz. Ti, kdo chápali problém fiat peněz, nedokázali nabídnout uspokojivou alternativu. Někteří se domnívali, že bychom se měli vrátit ke zlatému standardu – to však vyvolávalo neodbytnou otázku jeho praktičnosti.

Zlato je hmotné a neumíme jej teleportovat; pro jeho využití v moderním obchodním styku tudíž nutně potřebuje zprostředkovatele. Hypotetický návrat ke zlatému standardu by tak nutně koordinovala vláda a banky; tedy přesně ty instituce, které z existence fiat peněz výrazně profitují.

Bitcoin je nehmotný, můžeme jej tak posílat po celém světě se stejnou lehkostí, jako když posíláme e-maily. Nehmotnost bitcoinu však neimplikuje jeho bezcennost. Bitcoin má v očích čím dál většího počtu lidí hodnotu, jelikož představuje peněžní statek s kryptografickými zárukami, že jej nikdy nebude více než 21 milionů.¹⁹ Bitcoin je tudíž mnohem pragmatičtější alternativou k fiat penězům, než kdy může být zlato.

Nepřečenujme ale, jak daleko se nacházíme v závodě mezi bitcoinem a fiat měnami. Většina lidí je stále skeptická nebo zcela neznalá vyhlídek bitcoinu na vyřešení problému fiat peněz. Začít nyní spořit v bitcoinu a chránit své úspory s pomocí hardwarové peněženky je dost možná jedním z nejpřelomovějších rozhodnutí, které můžete ve svém životě učinit.

Budme optimisté

Vzhledem k událostem po roce 2020 má mnoho lidí pesimistický výhled do budoucnosti. Dobrým lékem na skleslost je vnímat vše v historickém kontextu. Ve skutečnosti totiž žijeme ve velmi optimistické době. Myšlenka centrálního plánování v oblasti výroby a distribuce zboží byla již dávno zdiskreditována. Většina největších problémů historie – hlad, voda, hygiena, chudoba – je téměř vyřešena. A nyní máme k dispozici i řešení přetrvávajícího metaproblému fiat peněz.

Ve srovnání s beznadějnou situací někoho, kdo se narodil před 100 lety, se máme báječně. Nešťastný protagonista ze začátku

¹⁹ Abychom byli přesnější, v případě bitcoinu nejsou záruky pouze kryptografické. Další důležitá záruka neměnnosti bitcoinu vyplývá ze sociálního konsensu držitelů bitcoinu a provozovatelů bitcoinových uzlů. Více o garancích měnové politiky bitcoinu v článku Parkera Lewise *Bitcoin is not backed by nothing*, vyšlo na unchained.com dne 27. 9. 2019.

kapitoly měl jen velmi omezené informace o tom, co se děje ve světě, a téměř žádnou naději vyhnout se důsledkům centrálně plánovaného hospodářství. Jedinou šancí na lepší život byl fyzický útek, který s sebou nesl značné riziko a velmi nejistý výsledek.

Dnes máme možnost se z monetárního centrálního plánování vymanit bez ohledu na to, kde žijeme. Můžeme doslova vzít peníze do vlastních rukou, zachovat si soukromí a na nikoho se přitom nespolehat.

A to je značný důvod k optimismu.

Poznanky z kapitoly

- Život na území dnešní České republiky nebyl během dvacátého století žádný med – státní a měnová uspořádání se měnila často, zpravidla k neprospěchu běžného občana.
- Z hlediska historických poměrů se v současnosti těšíme z nevídané prosperity a stability.
- Existence státních peněz je jedním z posledních velkých problémů lidstva; státní peníze do značné míry způsobují další velké problémy a zhoršují či znemožňují jejich řešení.
- Dnešní (fiatové) peníze jsou produktem centrálního plánování a selhávají obdobně jako jiné centrálně plánované sektory; pro nápravu je zapotřebí zcela odloučit peníze od státu.
- Na metaprobém státních peněz máme od roku 2009 elegantní řešení: bitcoin.

Perspektiva finanční: Nakamotův-Greshamův zákon aneb Proč na hodlování není nic špatného

Bitcoin Magazine, 27. 1. 2022

Bitcoin jsou peníze. To znamená, že otevřeně konkuruje stávajícímu peněžnímu uspořádání. Společný oběh dvou typů peněz není bezprecedentní; ekonomický princip, který dynamiku souběžného oběhu dvou typů peněz popisuje, je známý jako Greshamův zákon. Aplikujeme-li Greshamův poznatek na dynamiku bitcoinu a fiat, zjistíme, že hodlování je za současných podmínek ekonomicky racionální.

„Dobré a špatné mince neobíhají v ekonomice současně.“

– Thomas Gresham, 1558

Hierarchie peněžních potřeb

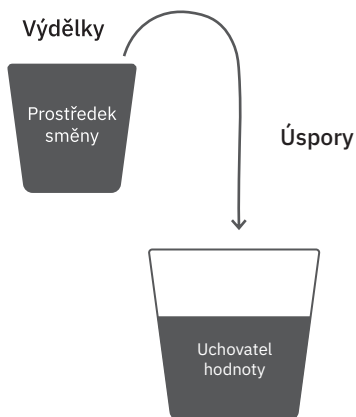
Abychom pochopili racionalitu hodlování, připomeňme si ve stručnosti, proč vyspělá civilizace potřebuje peníze.

Lidské jednání je účelové chování a prvořadým cílem každého člověka je nejprve uspokojit své nejnaléhavější potřeby. Vlastní-li člověk peníze a jeho základní potřeby přitom nejsou uspokojeny, s největší pravděpodobností se rozhodne vyměnit své peníze za jídlo, oblečení a přístřeší před čímkoliv jiným. Teprve po uspokojení svých základních potřeb může peníze spořit, aby v budoucnu dosáhl uspokojení složitějších potřeb.

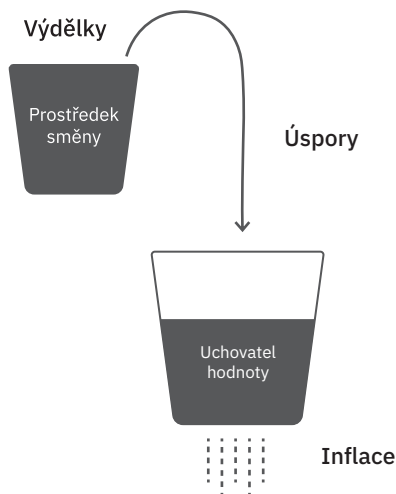
Peníze musí fungovat především jako prostředek směny. Jakmile je tato funkce satureována, k čemuž dochází poměrně brzy, je-li člověk schopen alespoň nějakou část svých výdělků uspořit a nežije takříkajíc „z ruky do huby“, druhá funkce peněz coby uchovatele hodnoty nabývá na významu.

Nejdřív směna, potom úspory

Obě funkce peněz a jejich vzájemný vztah můžeme znázornit na metafoře věder. Prostředek směny je první vědro, které musíme naplnit, abychom uspokojili své základní potřeby. Jakmile je toto vědro naplněno, přeteče přebytečná kupní síla do vědra pro uchování hodnoty. Vědro prostředku směny má omezenou kapacitu, protože existuje jen omezené množství zboží a služeb, které potřebujeme koupit a spotřebovat v krátkém časovém horizontu. Naproti tomu vědro uchovatele hodnoty má nekonečnou kapacitu, protože vždy můžeme navýšit objem svých úspor.



Dnešní fiatové peníze nicméně nejsou dobrým uchovatelem hodnoty. Jedná se o peníze s nekonečnou nabídkou, přičemž každý nový dolar oslabuje kupní sílu všech ostatních dolarů. Během turbulentních 24 měsíců mezi lednem 2020 a prosincem 2021 vzrostla peněžní zásoba amerických dolarů o 40 %, tedy o sčítaných 6 bilionu dolarů, neboli *šest tisíc miliard dolarů*. To vedlo k explozi cen ve všech oblastech: vysoká cenová inflace je nyní patrná v oblastech spotřebního zboží, výrobních statků, paliva, energií, nemovitostí, finančních nástrojů. Fiat je velmi děravé vědro, protože veškeré úspory čím dál rychleji ztrácejí svou kupní sílu.



Zásadní problém fiatů: jeho kupní síla nám protéká mezi prsty.

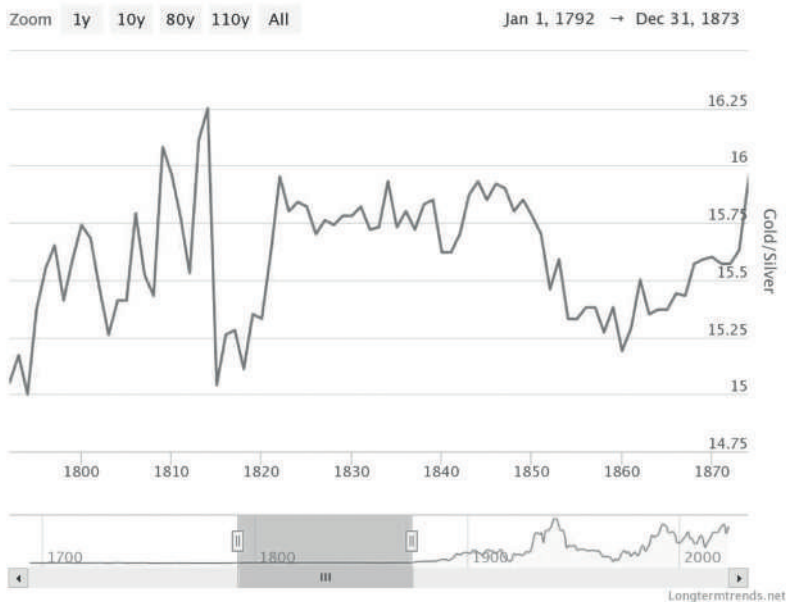
Nyní do těchto úvah zahrňme bitcoin.

Když pan Gresham potkal pana Nakamota

Mezi bitcoinery je populární argumentovat Greshamovým zákonem, nicméně ten popravdě není na situaci souběžného oběhu bitcoinu a fiatů aplikovatelný, alespoň ne ve své standardní formě.

Greshamův zákon popisuje současný oběh dvou měn, kdy nominální hodnotu obou měn definuje vláda. Nejlepším historickým příkladem Greshamova zákona je éra bimetalismu. Ve Spojených státech mezi lety 1792 a 1873 vláda stanovovala nominální hodnotu zlatých a stříbrných mincí. Zpočátku byl tento poměr udán na 15 : 1 – takže 15 uncí stříbra bylo ze zákona rovno jedné unci zlata. Problém však spočíval v tom, že poměr cen zlata a stříbra v průběhu času osciloval kolem této parity, což vedlo k tomu, že jeden kov byl neustále nadhodnocený a druhý podhodnocený. Vláda tento pevný poměr nominální hodnoty několikrát upravila, až se nakonec v roce 1873 nadobro vzdala myšlenky bimetalismu a přešla na čistý zlatý standard.

Gold / Silver Ratio since 1693



Tržní poměr mezi zlatem a stříbrem nedbal státních zákonů, naopak vláda se musela přizpůsobovat trhu – ačkoliv tak činila se zpožděním a s typickou byrokratickou rigiditou. Mezi lety 1792 až 1837 stanovila vláda poměr na 15 : 1, v letech 1837 až 1873 byl poměr upraven na 17 : 1. Stříbro bylo pevným poměrem podhodnoceno, bylo lidmi stahováno z oběhu a nakonec bylo opuštěno a Spojené státy adoptovaly zlatý standard. Zdroj: longtermtrends.net.

Jak upozorňuje Murray Rothbard v knize Peníze v rukou státu, správná formulace Greshamova zákona není často uváděné „špatné peníze vytlačují dobré peníze“, ale spíše „peníze uměle nadhodnocené vládou vytlačují z oběhu uměle podhodnocené peníze“.

Je zřejmé, že toto neplatí pro dynamiku bitcoinu a státních peněz, protože vláda nestanovuje nominální hodnotu bitcoinu. Abychom tedy mohli aplikovat poznatky Greshamova zákona v kontextu bitcoinu, musíme Greshamův poznatek upravit tak, aby byl aplikovatelný i na situaci, kdy jsou v oběhu jak státní, tak nestátní peníze.

Co vlastně znamená, že jeden typ peněz vytlačuje z oběhu druhý? Optikou peněžních funkcí to znamená, že jeden peněžní instrument přebírá roli prostředku směny a druhý roli uchovatele hodnoty.

Rozvinutá verze původního Greshamova zákona by tedy zněla takto:

„Nadhodnocené peníze se v ekonomice stanou dominantním prostředkem směny, zatímco podhodnocené peníze se stanou dominantním uchovatelem hodnoty.“

Přesně to se totiž stalo v éře bimetalismu, kdy se zlato stalo preferovaným prostředkem směny, zatímco stříbro bylo „hromaděno“ jako uchovatel hodnoty.

Abychom nyní tento poznatek konečně aplikovali na dynamiku bitcoinu a fiat, musíme se zbavit označení „nadhodnocený“ a „podhodnocený“. Nahradit je můžeme výhledovým hodnocením příslušných měnových politik. Fiat je typ peněz s potenciálně nekonečnou emisí, zatímco bitcoin je typ peněz s garantovanou pevnou emisí.

Lze tudíž předpokládat, že měnová politika státních peněz bude nadále inflační, tudíž že dosavadní peněžní jednotky budou neustále ztrácet svou kupní sílu tím, jak jsou do oběhu uvolňovány stále další a další peněžní jednotky.

Obdobně můžeme předpokládat, že bitcoin zůstane věrný své měnové politice, na konci které nebude v oběhu více než 21 milionů jednotek, takže kupní síla dosavadních jednotek nebude v budoucnu neustále ředěna novými bitcoiny.

Nyní můžeme Greshamův zákon přeformulovat tak, aby zohledňoval souběh státních a nestátních peněz.

Nakamotoův-Greshamův zákon

„Bitcoin vytlačuje fiat jako uchovatele hodnoty.“

„Fiat vytlačuje bitcoin jako prostředek směny.“

Jinak řečeno, je racionální utrácet fiat a hodlovat bitcoin. Fiat časem ztrácí hodnotu, takže přirozeně hledáme způsoby, jak se ho zbavit. Bitcoin v průběhu času získává na hodnotě, takže přirozeně hledáme způsoby, jak získat a dlouhodobě udržet co nejvíce bitcoinu.

Dopad Nakamotova-Greshamova zákona bude s postupem času sílit s tím, jak si více lidí začne uvědomovat, že zaprvé, fiat nadobro ztratil roli uchovatele hodnoty, a zadruhé, že bitcoin představuje očividné řešení tohoto problému.



Nakamotův-Greshamův zákon má však dvě podmínky:

1) Fiat je stále použitelný jako prostředek směny. Je-li fiat použitelný pro běžné platby, pak je logické jej k tomuto účelu v první řadě používat. V některých zemích je fiat nicméně nepoužitelný nad rámec prostých hotovostních plateb a lidé žijící v takových zemích pak přirozeně hledají cesty, jak provádět digitální platby. Bitcoin se jako prostředek směny čím dál více používá pro platební styk (domácí, remitenční, podnikatelský) v El Salvadoru, Argentíně, Nigérii a dalších zemích tzv. globálního jihu.²⁰

²⁰ Globální jih je termín používaný pro střední a jižní Ameriku a subsaharskou Afriku. Globální jih se v kontextu peněz vyznačuje vysokou mírou populace bez bankovních účtů, dlouhodobě vysokou mírou cenové inflace a často i neexistující infrastrukturou pro domácí a přeshraniční platby.

2) Jedinec nebo firma stále mají příjem ve státních penězích.

V případě příjmu ve fiat mají jedinci a firmy tendenci zbavit se fiat dříve než bitcoinu. Pokud je daný jednatel nebo firma již plně bitcoinizována a nakládá pouze s bitcoinem, pak se bitcoin přirozeně stává i prostředkem směny.

Bitcoin jako ochrana před civilizačním úpadkem

Ekonomové, komentátoři a mluvčí hlavy všeho druhu kritizují bitcoin za to, že není rozšířeným prostředkem směny, nechápou problém dynamiky souběžně obíhajících peněz. Čelíme-li „problému dřavého vědra“, nepotřebujeme další prostředek směny: roli platebního nástroje stále uspokojivě plní fiat a většina z nás doposud ve fiat pobírá mzdu. Bylo by iracionální utrácet přednostně bitcoin, máme-li nenulové zůstatky fiat. Hodlovat bitcoin je racionální; navrací penězům funkci uchovatele hodnoty, kterou fiat ztrácí alarmujícím tempem.

Až fiat přestane plnit roli prostředku směny nebo až jednotlivci budou dostávat plnou mzdu v bitcoinu, teprve pak bude mít smysl utrácet bitcoin za všední nákupy.²¹

Rozšíření bitcoinu coby obecně dostupného uchovatele hodnoty může představovat spásu naší civilizace. Vyspělé civilizace potřebují nástroj pro spolehlivou konzervaci vytvořených hodnot, pro nerušené budování a uchovávání bohatství. Když nejsme schopni vytvářet úspory a místo toho utrácíme vše, co vyděláme (a prostřednictvím dluhu mnohdy ještě více), pak se naše infrastruktura začne rozpadat, společenské hodnoty budou erodovat a přestaneme dbát na budoucnost. Kam taková cesta vede, vidíme na mnoha příkladech z historie: znehodnocování

21. Někteří bitcoineři s analýzou předloženou v této kapitole nesouhlasí a poukazují na to, že placení bitcoinem i v prostředí s funkčním fiatem má své výhody. Většinou se jedná o ochranu soukromí a podporu adopce. Soukromí vskutku může být relevantní důvod pro upřednostňování bitcoinu, je však třeba upozornit na to, že bitcoin není sám o sobě kdovíjak soukromý (více o soukromí v kapitole Obezřetnost aneb Jak o sobě neprozradit vše) a fiatová hotovost bývá pro průměrného jedince tou nejsoukromější metodou platby. Podpora adopce je záslužná, nicméně v takovém případě se jedná spíše o altruistický, nikoli ekonomický důvod pro používání bitcoinu. Mým cílem v této kapitole bylo analyzovat ekonomické pohyby lidí pro používání bitcoinu v různých peněžních funkcích. Protože v dlouhém období jsou to pouze ekonomické incentivy, které o budoucnosti bitcoinu rozhodnou.

mincí ve starém Římě vedlo ke kolapsu říše; epizody hyperinflace ve 20. a 21. století vedly k válkám, totalitě a hladomoru. Adopce bitcoinu jako uchovatele hodnoty nás před tímto osudem může ochránit, a to jak na úrovni jednotlivců, tak na úrovni společnosti.

Poznatky z kapitoly

- Peníze plní ve společnosti dvě hlavní funkce: prostředek směny a uchovatel hodnoty.
- Funkce prostředku směny je nejnaléhavější v krátkém období, jakmile jsou ale naše krátkodobé potřeby naplněny, potřebujeme, aby peníze fungovaly i jako uchovatel hodnoty.
- Státní peníze selhávají jako uchovatel hodnoty, jelikož v sobě mají zabudovanou trvalou peněžní inflaci, která eroduje kupní sílu všech držitelů.
- Bitcoin má předvídatelnou měnovou politiku, na konci které bude v oběhu 21 milionů mincí; má proto vhodné předpoklady k plnění funkce uchovatele hodnoty.
- Je ekonomicky racionální utracet státní peníze a bitcoin dlouhodobě držet – tj. používat státní peníze jako prostředek směny a bitcoin jako uchovatel hodnoty.
- Na světě jsou země, kde státní peníze nefungují uspokojivě ani jako prostředek směny; v takových zemích má smysl používat pro placení bitcoin.

ČÁST DRUHÁ: CTNOSTI

Úvod druhé části

Vnímání bitcoinu v rozmanitých perspektivách je důležité pro chápání jeho významu, samo o sobě však nezaručuje, že o svůj bitcoin tím či oním způsobem nepřijdete. Na bitcoinity číhá mnoho nástrah, ty nejzákeřnější se skrývají v nich samotných. Existují zástupy jedinců, kteří pochopili přelomový význam bitcoinu, avšak neučinili poslední důležitý krok ve formě držení vlastních klíčů či se nechali zlákat maniakálními předpověďmi o „supercycklu“, vstoupili do pákových pozic a následně o většinu svých bitcoinů přišli.

Proti nástrahám vnějšího i vnitřního světa zná lidstvo již tisíce let spolehlivý protilek: osvojení si jasných morálních a etických principů neboli ctností. Odvolávání se na ctnosti může znít poněkud archaicky, skutečnost je ale taková, že základní ctnosti jako obezřetnost či trpělivost jsou zásadním předpokladem pro dlouhodobý úspěch v libovolné oblasti života.

Ctnost můžeme chápat jako mentální pojistku, na kterou je spolehnutí v momentech nejistoty. Příklad: všichni okolo bohatnou na shitcoinech, NFT šutrech, pákových obchodech a vy nabýváte dojmu, že zůstáváte pozadu. V takových momentech je dobré si zhodnotit, zda jednání druhých odpovídá některé ze základních ctností, či jsou naopak strženi krátkozrakou chamtivostí a závistí. Spolehnutí se na trpělivost, obezřetnost a umírněnost by vás v takovém případě zachránilo před masivními ztrátami, které po shitcoinové mánii vždy přijdou – v roce 2022 přišlo u „kryptozbohatlíků“ vystrážlivění s kolapsem ponzi schémat Luna a Celsius či s působivým rozkladem shitcoinového kasina FTX.

Ctnosti jsou zkrátka nepostradatelnou součástí mentální výbavy každého bitcoinera a zároveň jsou s bitcoinem krásně synergické: ctnosti vám pomáhají přežít divokou fázi bitcoinizace a bitcoin

z vás na oplátku dělá lepšího a ctnostnějšího člověka (například ve formě dlouhodobého snižování časových preferencí).

Pojďme se tedy nyní seznámit se základními bitcoinovými ctnostmi.

Rozumnost aneb Jak na hardwarové peněženky

Bitcoin Magazine, 1. 7. 2022

Ať už uvažujete o koupi své první hardwarové peněženky nebo už ji léta používáte, vždy je dobré si osvěžit možnosti těchto úžasných zařízení. Navzdory rozšířenému přesvědčení není hardwarová peněženka nástroj typu „nastav a zapomeň“, který se o vše postará za vás. Hardwarová peněženka je spíše užitečný pomocník při nikdy nekončícím procesu starosti o vaše bitcoiny.

Kdy a proč si pořídit hardwarovou peněženku?

Vzhledem k tomu, že pořizovací cena hardwarové peněženky začíná na dvou tisících korunách, není zrovna lákavé si ji pořizovat, pokud s bitcoinem teprve začínáte. Dobrým pravidlem je pořídit si hardwarovou peněženku, jakmile její pořizovací cena činí desetinu zabezpečeného bitcoinu; jinými slovy, máte-li bitcoin v hodnotě alespoň dvacet tisíc korun, je na čase zbystřit.²²

Někteří lidé zastávají názor, že hardwarové peněženky jsou zbytečné a místo nich adekvátně poslouží starý telefon nebo notebook. Problém ale spočívá v tom, že na univerzálním hardwaru může běžet libovolný software, a pokud nejste pokročilý bezpečnostní expert, nemáte šanci s jistotou vědět, zda je zařízení skutečně bezpečné. A popravdě ani bezpečnostní experti nejsou někdy schopni vytvořit si skutečně bezpečné prostředí na svých počítačích – důkazem je nešťastný případ dlouholetého bitcoinového vývojáře Luka-jr, který v lednu 2023 přišel o více než 200 bitcoinů, jelikož měl privátní klíče k bitcoinům uložené přímo na svém počítači.²³

Hardwarové peněženky jsou účelová zařízení se specializovaným firmwarem, jehož funkce jsou omezeny na úzkou sadu procesů,

22 To ale neznamená, že pro menší částky je v pořádku držba na burze. Burza by nikdy neměla sloužit k dlouhodobému držení bitcoinu! Pro menší částky použijte mobilní peněženku, kde kontrolujete vlastní klíče (tj. musíte si opsat obnovovací seed). Důvěryhodné mobilní peněženky jsou Muun, Green, Blue Wallet.

23 Více se můžete dočíst v článku na CoinTelegraph.com s názvem *Bitcoin core developer claims to have lost 200+ BTC in hack*.

konkrétně generování klíčů a podepisování pomocí těchto klíčů – to vše v offline prostředí, vždy a za všech okolností.



Nedržel bitcoin na burze je první krok k finanční suverenitě. Držet je v hardwarové peněženke je hned následující krok.

Zapsání a ochrana seedu

Při nastavování hardwarové peněženky je jedním z prvních kroků vygenerování vašich soukromých klíčů. Abyste měli jistotu, že vám bitcoiny zůstanou i v případě ztráty nebo poruchy konkrétního zařízení, budete vyzváni, abyste si zapsali svůj obnovovací seed (v angličtině *recovery seed*): seznam anglických slov, který lze použít k obnovení vašich soukromých klíčů v kompatibilních peněženkách.²⁴

Pečlivé opsání slov, která tvoří obnovovací seed, je jedna z nejdůležitějších věcí při správě vašeho bitcoinu. Hardwarové peněženky obnovovací seed znovu nezobrazují – musíte si jej zapsat při prvotním nastavení.

²⁴ Většina hardwarových i softwarových peněženek používá stejný standard zvaný BIP39. Proto si můžete obnovit například seed z Trezoru v mnoha jiných peněženkách a nemusíte mít obavu o budoucí kompatibilitu.

Základní tipy pro ochranu seedu:

- Seznam slov opište vlastní rukou na kus papíru.
- Alternativně můžete použít robustnější řešení z oceli, kvalitní jsou výrobky firem Cryptosteel či Cryptotag.²⁵
- Neměňte pořadí slov seedu, pořadí slov je kriticky důležitý faktor.
- Nikdy si seed nefoťte ani neuchovávejte jeho digitální kopii – hackeři taková data aktivně vyhledávají.
- Seed uchovávejte na místě s kontrolovaným přístupem, v suchu, s minimálním rizikem požáru apod.
- Pro zvýšení bezpečnosti zvažte využití Shamir Backupu, jehož principy jsou detailněji popsány v následující kapitole.

Kontrola seedu

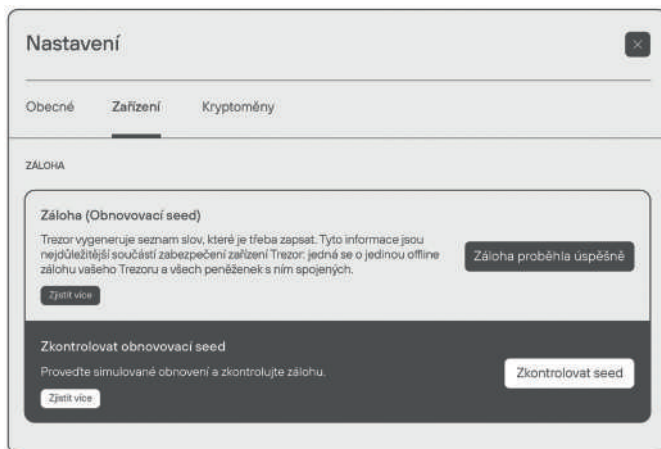
Jakmile si obnovovací seed zapíšete, je vhodné ověřit, zda vskutku funguje a zda opsaná slova obnoví vaši peněženku. Integritu seedu byste měli ideálně zkontrolovat ještě předtím, než na nové adresy pošlete bitcoiny.

Pro kontrolu seedu můžete resetovat hardwarovou peněženku do továrního nastavení a poté provést obnovu. Některé hardwarové peněženky nabízejí tzv. simulované obnovení (*dry run recovery*) – tato možnost vám bude vyhovovat více, pokud přece jen již v peněžence nějaké bitcoiny máte.

Chcete-li provést simulované obnovení v Trezor Suite, přejděte do Nastavení, vyberte možnost *Zkontrolovat seed* a postupujte podle displeje zařízení: připojený Trezor by měl po tomto kroku reagovat a podávat další instrukce – nikdy nezadávejte slova seedu

²⁵ Na stránkách blog.lopp.net naleznete desítky testů všemožných řešení pro fyzický backup seedu.

do počítače, pokud vám Trezor nedává pokyny ohledně pořadí jednotlivých slov!



Simulované obnovení naleznete v Trezor Suite v Nastavení→Zařízení→Zkontrolovat obnovovací seed.



Při simulovaném obnovení **NE**dochází k resetu zařízení do továrního nastavení – nemusíte se tudíž bát, že byste něco pokazili.



Veškeré operace se seedem vždy vyžadují instrukce od připojeného Trezoru. Pokud vám Trezor nepodává instrukce, nikam svůj seed nepište!

Je dobrou praxí kontrolovat seed pravidelně. Osvojte si zvyk zkontrolovat váš seed alespoň jednou za dvanáct měsíců, abyste měli jistotu, že je vše v pořádku a seed je připraven k obnově vašich prostředků v případě potřeby – předejdete tak nejčernějšímu scénáři, kdy ztratíte svůj Trezor, a následně zjistíte, že jste zároveň ztratili i obnovovací seed, aniž byste si toho všimli.

Nastavení PIN a Passphrase

Většinu hardwarových peněženek lze zabezpečit pomocí PIN. Dobrý PIN může zabránit útočníkovi v krádeži vašich prostředků, objeví-li vaše zařízení. PIN nicméně pouze zamyká samotné zařízení hardwarové peněženky, nechrání však před zneužitím obnovovacího seedu. Pokud by tedy útočník objevil jak vaše zařízení (chráněné kódem PIN), tak i váš obnovovací seed, stále vám může ukrást všechny bitcoiny, protože s obnovovacím seedem v ruce vlastně nepotřebuje samotné zařízení – jednoduše si obnoví přístup k bitcoinům v jiné kompatibilní peněžence.

Naštěstí existuje způsob, jak eliminovat riziko v případě, kdy útočník najde i váš obnovovací seed. Hardwarové peněženky jako Trezor nabízejí možnost chránit seed pomocí přístupové fráze

(*passphrase*). Nastavení přístupové fráze vám vytvoří zcela novou sadu peněženek, které jsou odvozeny z kombinace obnovovacího seedu a konkrétní *passphrase*. To znamená, že seed sám o sobě se pro útočníka stane nepoužitelný, protože bez *passphrase* není schopen odvodit správnou sadu peněženek.



U Trezoru Model T je možné zadávat passphrase přímo na zařízení. Tím eliminujete riziko jejího prozrazení při infekci počítače malwarem.

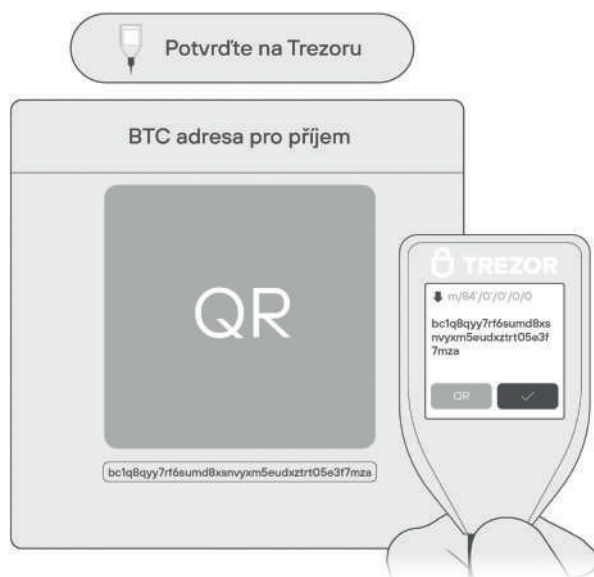
Jde-li vám z toho hlava kolem, stačí mít na paměti: **PIN odemká zařízení, passphrase chrání seed.** Pokud se rozhodnete používat *passphrase*, nespolehejte se na svou paměť. Zapomenete-li svou *passphrase*, již se ke svým bitcoinům nedostanete. *Passphrase* není možné resetovat – není totiž nikde uložena (pouze upravuje derivaci soukromých klíčů ze seedu). Je tudíž nutné, abyste si vytvořili zálohu *passphrase*, podobně jako jste to udělali pro seed. Udržujte seed a *passphrase* odděleně, znemožníte tak zlodějům krádež vašich prostředků, pokud najdou jednu z těchto záloh.

Proč má hardwarová peněženka vlastní displej?

Hardwarové peněženky jsou užitečné i nad rámec prostého hodlování. Jednou z hlavních výhod těchto zařízení je možnost přijímat a odesílat bitcoiny velmi bezpečným způsobem. Rozšířený virus zasahující kopírovací schránku na desktopovém počítači (tzv. *clipboard malware*) může změnit bitcoinovou adresu, kterou

kopírujete/vkládáte. Pokud je váš počítač takovým virem infikován, jedinou obrannou linií je porovnání adresy zobrazené na hardwarové peněžence s odesílající/přijímající protistranou (webovou stránkou burzy, peněženkou v telefonu vašeho kamaráda, zprávou v aplikaci Signal²⁶ atd.) To je jeden z důvodů, proč všechny hardwarové peněženky hodné svého označení mají vlastní displej.

Při přijímání bitcoinu zobrazí zařízení na displeji celou adresu, takže si můžete nezávisle ověřit, že adresa zobrazená v aplikaci na počítači je správná (tj. vskutku vygenerovaná hardwarovou peněženkou). Porovnejte adresu zobrazenou na počítači a na hardwarové peněžence. Po zkopírování a vložení do webové stránky/e-mailu/Signalu ještě jednou před odesláním ověřte adresu, abyste se ujistili, že nebyla změněna malwarem.



Přijímací adresu vždy ověřte na obrazovce zařízení! Poznámka: na tuto adresu nic neposílejte, jedná se pouze o ilustrativní adresu, autor textu k ní nemá klíče. Pokud byste přece jen chtěli autora potěšit bitcoinovým darem, můžete tak učinit prostřednictvím tlačítka Donate na stránkách Stackuj.cz.

²⁶ Aplikaci Signal doporučuji pro bezpečné posílání bitcoinových adres či QR kódů napříč zařízeními, jelikož se jedná o end-to-end šifrovaný komunikátor, kde obsah zpráv znají jen odesílatel a příjemce – nikdo tak nemůže vaši adresu přečíst a po cestě změnit. Signal doporučuji i k jakékoli další komunikaci, včetně telefonních hovorů.

Při odesílání bitcoinu se provádí několik kontrol: ověření adresy příjemce, transakčního poplatku a celkové částky, která má být odeslána. Nezapomeňte vše dvakrát zkontrolovat!



Při odesílání bitcoinu zkontrolujte odesílanou částku, cílovou adresu, výši poplatku.

S ověřováním nespěchejte. Pouze obrazovka zařízení vám může věrohodně zobrazit, co se uvnitř hardwarové peněženky skutečně děje, takže se ujistěte, že opravdu odesíláte nebo přijímáte prostředky tam, kam zamýšlíte.

Pozor na phishing

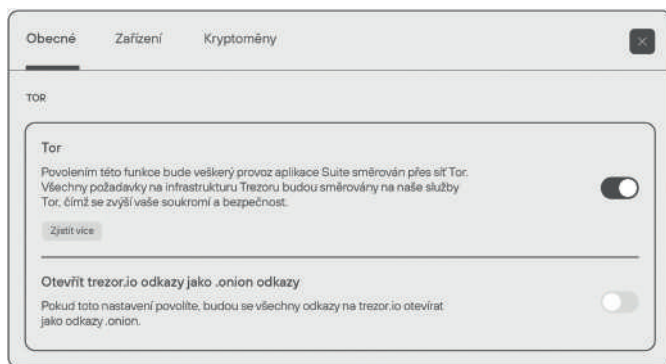
Světlem a zejména internetem se prohánějí zástupy zlounů, kteří by vám rádi ukradli bitcoinu. Někteří se rozhodnou šířit svá chapadla prostřednictvím malwaru, jiní se snaží zcizit vaše bitcoiny pomocí sociálního inženýrství – rozšířené jsou falešné webové stránky, phishingové e-maily nebo podvržené aplikace, které se vás snaží přimět zadat váš seed.

Nejlepší ochranou je zapamatovat si jednoduché pravidlo: **nikdy nezadávejte svůj seed na webové stránky nebo do aplikace bez instrukcí na displeji připojené hardwarové peněženky**. Při obnově přístupu k bitcoinu pomocí hardwarové peněženky, jako je například Trezor, buď zadáváte slova seedu přímo na samotném

zařízení (Trezor Model T), nebo vám zařízení sděluje pořadí, ve kterém máte slova zadávat (Trezor Model One). Tím je zajištěno, že nedojde k úniku seedu ve správném pořadí případným keyloggerům nebo jiným špehovacím nástrojům.

Routing přes Tor, připojení vlastního full node

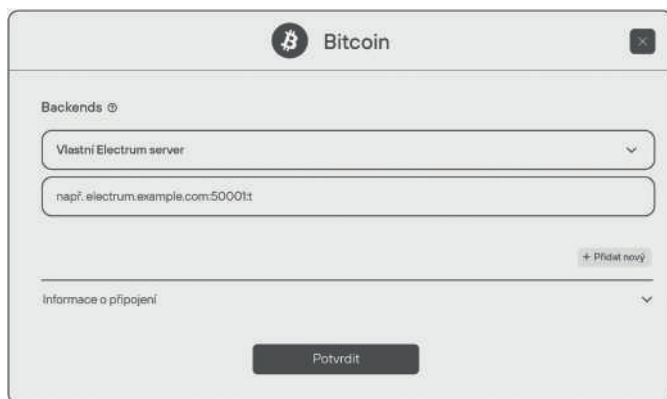
Pro zlepšení ochrany soukromí uživatelů a zabránění úniku IP adresy je vhodné směřovat veškerý provoz související s bitcoiny přes síť Tor. Tor je lepší než virtuální privátní síť (VPN), protože provozovatelé služeb VPN často uchovávají záznamy o aktivitách zákazníků, které mohou uniknout nebo být na požádání předány úřadům. S Torem je vaše IP adresa skutečně skrytá, takže vaše bitcoinové transakce zůstanou privátní (mějte však na paměti, že Tor sám o sobě vás neochrání, jsou-li vaše bitcoinové adresy spojeny s vaší identitou, pokud jste bitcoiny koupili na centralizované burze). V Trezor Suite je routování přes Tor již zapnuto v základním nastavení, tuto možnost podporují i jiné peněženky, například Bitcoin Core či Wasabi.



V Trezor Suite naleznete nastavení sítě Tor pod Nastavení→Obecné→Tor.

Chcete-li dále posílit své soukromí a suverenitu, můžete svou hardwarovou peněženku připojit k vlastnímu plnému uzlu (*full node*). Při provozování plného uzlu se nemusíte spoléhat na žádnou třetí stranu, která by zpracovávala vaše transakce a poskytovala vám nejnovější stav bitcoinového blockchainu. Plný uzel můžete spustit na svém domácím počítači, notebooku nebo zařízení Raspberry Pi

a připojit svou hardwarovou peněženku prostřednictvím Bitcoin Core HWI nebo Electrum.



V Trezor Suite si připojíte vlastní full node pod Nastavení→Kryptoměny→Bitcoin→Vlastní Electrum Server.

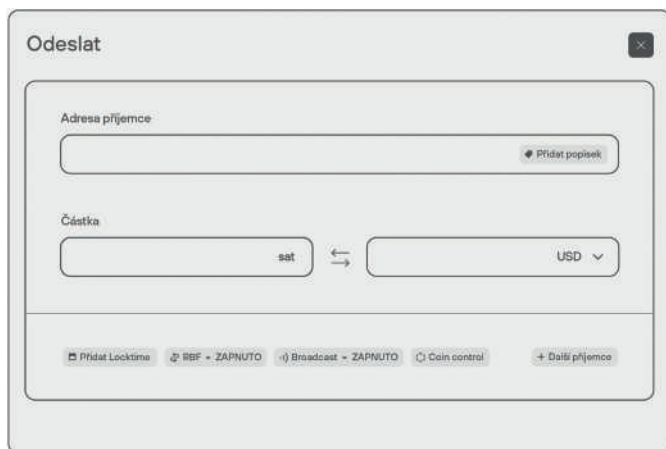
Coin control: vím, co utrácím

Každá bitcoinová transakce vám tvoří nový neutracený transakční výstup (*Unspent Transaction Output, UTXO*).²⁸ V Trezor Suite je možné (a doporučeníhodné) si každý výstup transakce pojmenovat, aby bylo na první pohled patrné, odkud daná transakce přišla (například „nákup v ATM“, „nákup na burze“, „Vexl“ atd.). Popisky k došlým transakcím si doplníte tak, že v seznamu příchodích transakcí najedete myší na bitcoinovou adresu transakce, načež se objeví tlačítko *Přidat popisek*; pro funkčnost popisků je zapotřebí připojit Dropbox či Google Drive (nemusíte mít obavu, že by se tím snižovala vaše úroveň soukromí, na cloudová úložiště jsou uploadována data v šifrované podobě, přičemž šifrujícím zařízením je přímo váš Trezor).

Při útratě je pak možné volit konkrétní UTXO – to je užitečné jak pro zachování soukromí, tak pro předcházení nepříjemným situacím: kupříkladu na centralizovanou burzu není dobré posílat UTXO, které prošlo Coinjoinem (burza pak může zmrazit účet, ptát

28 Více o konceptu UTXO v kapitole Opatrnost aneb Jak o sobě neprozradit vše.

se na transakční historii atd.). Volbu konkrétních UTXO naleznete v Trezor Suite při odesílání pod tlačítkem *Coin control*.



V dialogovém okně *Odeslat* si můžete volit konkrétní UTXO po rozkliknutí tlačítka *Coin control*.

Firmware pro minimalisty

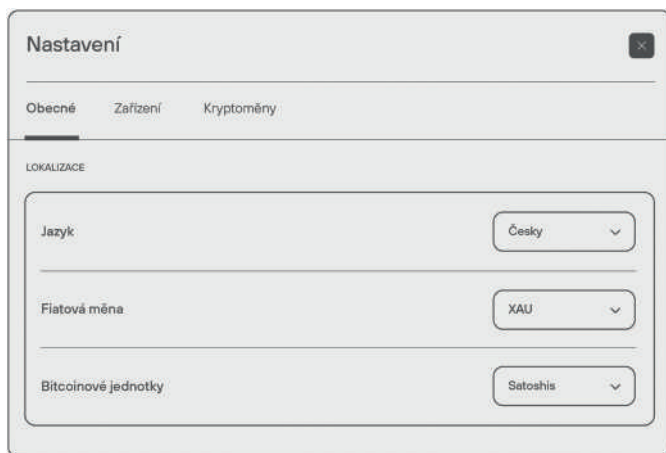
Pokud jste bitcoin maximalista (či výstižněji: bullshit minimalista), pak doporučuji si v Trezor Suite přepnout firmware na bitcoin-only verzi. Hlavní výhodou je nižší frekvence updatů (aktualizace firmware netýkající se bitcoinu budou ignorovány), dalšími výhodami pak rychlejší proces coin discovery při připojení Trezoru a menší prostor pro buggy. Potenciální nevýhodou tohoto firmware ovšem je, že nepodporuje využití Trezoru jako zařízení pro dvoufaktorovou autentizaci.



Bitcoin-only firmware si nainstalujete v *Nastavení*→*Zařízení*→*Firmware*.

Jsem milionář! Nastavení jednotek satoshi

S rostoucí hodnotou bitcoinu je do budoucna pravděpodobné, že plný bitcoin bude absurdně hodnotná jednotka; je tudíž dobré začít si zvykat na „bitcoinové drobáky“ neboli satoshi. V Trezor Suite si můžete nastavit zobrazení buďto v celých bitcoinech, nebo přepnout na satoshi:



Sats si nastavíte v Nastavení→Obecné→Bitcoinové jednotky. Bonus: můžete si vybrat i z velkého množství přepočtu do fiatových měn jako jsou koruny, eura, či dolary; fun fact: můžete si zde nastavit i unce zlata (XAU) či stříbra (XAG).

Chraňte se před reálnými riziky

Nejčastějším rizikem při nakládání s bitcoinem je náhodná ztráta. Vyhození obnovovacího seedu, odeslání nebo přijetí prostředků na špatnou adresu, nachytání se na phishingový podvod, zapomenutí passphrase nebo ponechání bitcoinu na burze, která je později hacknuta – to všechno jsou mnohem pravděpodobnější scénáře, než že vám bitcoin kupříkladu zabaví vláda. Nepříjemnou pravdou je, že bitcoineři jsou sami sobě těmi největšími nepřáteli.

Určitá míra obezřetnosti až paranoie je zdravá, příliš komplikovaným zabezpečením se však můžete střelit do nohy. Držte se ověřeného principu KISS: *keep it simple, stupid*.



Vypravěč: Charlie své bitcoiny taky nenašel.

Vše si otestujte. Po nastavení nové hardwarové peněženky vyzkoušejte, zda váš recovery seed skutečně funguje, a to buď vymazáním zařízení, nebo provedením simulovaného obnovení. Když posíláte svou první transakci pomocí hardwarové peněženky, přepošlete si nejprve mezi vlastními adresami pár korun, abyste si ověřili, jak vše funguje. Pravidelně kontrolujte svůj obnovovací seed. Pokud zvažujete použití passphrase, zkuste si do nové peněženky poslat jen drobné a pak se několikrát přihlásit a odhlásit s novou passphrase. Dobrá obeznamenost s tím, jak by měla hardwarová peněženka reagovat, je obří výhodou, ocitnete-li se někdy ve stresové situaci – do takových situací se vás totiž snaží četní podvodníci dostat v naději, že uděláte chybu.

Zopakujme si rovněž, že všichni hlavní výrobci hardwarových peněženek používají vzájemně kompatibilní standard obnovovacích seedů (standard BIP39 pro běžné seedy, SLIP39 pro Shamir Backup), takže i kdyby konkrétní výrobce zkrachoval, váš bitcoin bude vždy v bezpečí a přístup k němu budete moci obnovit v mnoha open-source peněženkách, hardwarových i softwarových.

Poznátky z kapitoly

- Hardwarové peněženky dávají smysl, máte-li bitcoin v hodnotě zhruba 20 tisíc korun; do té doby si vystačíte s mobilními peněženkami (Muun, Green, Blue Wallet).
- PIN zamyká zařízení hardwarové peněženky; pokud jej zapomenete, můžete si peněženku obnovit ze seedu.
- Passphrase mění derivaci klíčů ze seedu; pokud ji zapomenete, ztratíte přístup k vašim bitcoinům.
- Seed i passphrase je nutné si zapsat vlastní rukou či vyrazit do oceli; nikdy nepožizujte digitální kopie!
- Vyzkoušejte si obnovení ze seedu, než na novou peněženku pošlete bitcoiny.
- Nikdy nepište svůj seed do webové stránky.
- Pracujete-li s Trezorem, zařízení vás bude vždy instruovat o tom, jak provést obnovení ze seedu (pořadí zadávaných slov / zadávání slov přímo na displeji zařízení).
- Vždy zkontrolujte přijímací/odesílací adresu na displeji hardwarové peněženky.

Prozíravost aneb Jak zanechat bitcoin příštím generacím

Bitcoin Magazine, 21. 7. 2021

Na vrcholu cenové rally v roce 2017 jsem narazil na následující příběh. Jeden „známý známého“ si pořídil 20 bitcoinů v dobách, kdy stály pár tisíc korun. Když se v průběhu roku 2017 vyšplhala cena z jednoho na téměř dvacet tisíc dolarů, rozhodl se daný mládenec užít si svého nově nabytého bohatství a vyrazil na cestu po světě. Ubytoval se v Mexiku v pěkném hotelu a účastnil se párty na střeše. V průběhu párty se podnapilý mladík naklonil přes zábradlí, přepadl a zahynul. Pozůstalá rodina se následně snažila zjistit, zda se může k bitcoinům nějak dostat. Mladík však používal Trezor s nastavenou silnou passphrase, kterou si nikde nepoznamenal. Bitcoinů tak byly nadobro ztraceny.

S konkrétními bitcoiny mohou nakládat pouze ti, kdo mají adekvátní privátní klíče. Na rozdíl od většiny jiného majetku (akcie, dluhopisy, bankovní účty, nemovitosti) tak nestačí, aby pozůstalí o majetku věděli – musí být schopni podepsat bitcoinovou transakci správným klíčem.

Na druhou stranu málokdo chce, aby rodina měla neomezený přístup k osobnímu bitcoinu ještě za jeho života. Je proto zapotřebí mít nastavený postup pro správu přístupu: za života k bitcoinu může přistupovat pouze majitel, po smrti se bitcoin zpřístupní vybraným pozůstalým. K tomuto záměru může sloužit Shamir Backup, se kterým je možné pracovat v Trezoru Model T.

Než se však dostaneme k tomu, jak se Shamir Backup pracovat, pojďme si připomenout historii obnovovacího seedu a nastínit úskalí, která se s ním pojí.

Proč vznikl obnovovací seed a jaké má nedostatky?

V počátečních letech nebylo zálohování bitcoinu vůbec jednoduché. Bylo totiž nutné zálohovat všechny jednotlivé soukromé klíče – při

využívání nové adresy na každou transakci se mohlo jednat i o stovky jednotlivých klíčů. Není překvapením, že kvůli tomuto složitému procesu zálohování bylo ztraceno mnoho bitcoinů. V roce 2012 přišel Pieter Wuille s brilantním nápadem hierarchických deterministických peněženek (HD peněženky, standardizované pod BIP32), které zálohování výrazně usnadnily – uživatelé nově museli zálohovat pouze jeden hlavní seed, ze kterého se pak generovaly jednotlivé soukromé klíče. O rok později přišel BIP39, který standardizoval tzv. mnemonic seed – skupinu slov v určitém pořadí, dodnes nejrozšířenější způsob zálohy bitcoinových peněženek. S mnemonic seedem se zálohování stalo mnohem snazší, protože při zápisu obyčejných slov je jen malý prostor pro chybu ve srovnání se zápisem dlouhého řetězce písmen a číslovek.

V dnešní době tedy nezálohuje soukromý klíč jako takový, ale seed – obvykle v podobě 12 nebo 24 slov v konkrétním pořadí. Můžete ztratit telefon nebo rozbít hardwarovou peněženku, ale pokud máte seed bezpečně poznamenaný, přístup k bitcoinu neztratíte.

Dobrá, seed je tedy možné si správně a jednoduše zapsat; stále však musíme vyřešit otázku, kam s ním. Věci se komplikují, když si uvědomíme, že seed je třeba chránit před dvojím rizikem:

- Krádež – nalezený seed mohou zneužít cizí osoby.
- Ztráta – v případě ztráty, požáru, či jiné katastrofy můžete ztratit klíče k bitcoinům, jež se tak stanou navždy nedostupné.

Zatímco riziko krádeže vyžaduje co nejmenší počet kopií – nejlépe jen jednu u vás doma – riziko ztráty vyžaduje pravý opak. Mít jen jednu kopii seedu může být doslova zahrávání si s ohněm. Proto je třeba mít vícero kopií na několika geograficky vzdálených místech – čím více kopií seedu ale existuje, tím vyšší je riziko zneužití. Standardní seed založený na jednom seznamu slov nemůže ochránit před oběma riziky zároveň a je tak náchylný buďto ke ztrátě (v případě jedné kopie), nebo ke krádeži (v případě vícero kopií).

Talentovaný pan Shamir

Shamirovo sdílení tajemství (*Shamir Secret Sharing*, SSS) je kryptografický algoritmus, který v roce 1979 světu představil izraelský kryptograf Adi Shamir. Výhoda Shamirova vynálezu spočívá ve schopnosti zálohovat, sdílet a obnovit tajemství rozdělením daného tajemství na více částí, přičemž jednotlivé části jsou samy o sobě nepoužitelné a nesdělují nic o daném tajemství.

Pro SSS jsou důležité dva parametry: kolik částí celkem existuje a kolik částí musíme zkombinovat, abychom tajemství obnovili.

Například „Shamir 3 z 5“ znamená, že uživatel při nastavování schématu vytvořil pět částí a práh pro obnovení tajemství jsou tři podíly. Nezáleží na tom, které konkrétní tři části uživatel použije k obnovení tajemství, jednotlivé části jsou pro potřebu obnovy tajemství zaměnitelné.

To znamená, že Alice může zálohovat svůj seed například následujícím způsobem (za předpokladu Shamirovy zálohy 3 z 5):

- Dvě části doma
- Jedna část u nejlepší kamarádky
- Jedna část u matky
- Jedna část v bezpečnostní schránce

Jednotlivé části existují samozřejmě v analogové formě – ručně zapsané na papíře nebo vyražené do plechu (pomocí Cryptosteel, Cryptotag nebo jiných podobných řešení). Alice si je dobře vědoma toho, že by nikdy neměla části seedu či Shamirova schématu zapisovat do počítače připojeného k internetu nebo uchovávat jejich digitální kopii.

Díky tomuto uspořádání se Alice nemusí obávat, že by ztratila přístup ke svým bitcoinům, i kdyby jí shořel dům, protože si

bitcoinů v takovém případě může obnovit ze zbývajících podílů od kamarádky, matky a z bezpečnostní schránky. Nemusí se také obávat krádeže, protože žádná jednotlivá záloha nesplňuje potřebný práh pro přístup k bitcoinům.



Vyobrazeno: Alice, která pamatovala na zálohování bitcoinového seedu.

Shamirovo sdílení je tedy dokonalým řešením dilematu krádež/ztráta, protože jednotlivé části jsou samy o sobě k ničemu, a Alice může dokonce některé podíly ztratit, aniž by přišla o přístup ke svým bitcoinům.

Původní Shamirovo schéma existuje již od roku 1979, ale použití pro potřeby bitcoinového seedu bylo řádně standardizováno až koncem roku 2017 českou společností SatoshiLabs. Standard se nazývá SLIP39: Shamir's Secret-Sharing for Mnemonic Codes a je plně otevřený pro kohokoliv ke studiu, sdílení a implementaci ve vlastních produktech. Shamirovy zálohy založené na SLIP39 používá hardwarová peněženka Trezor Model T (pod názvem Shamir Backup), peněženka Hermit společnosti Unchained Capital a několik dalších bitcoinových peněženek.

Ochrana dědictví s pomocí Shamir Backupu

Zálohy dle Shamirova schématu jsou účinné nejen pro zabezpečení bitcoinu vůči ztrátě či zneužití, ale i pro bezpečné předání rodinného bohatství v případě smrti. Poté, co Alice rozdělila části Shamir Backupu do více lokalit, musí pro zajištění dědictví sepsat jasné pokyny pro pozůstalé.

Sepsání pokynů pro pozůstalé musí být provedeno s náležitou péčí. Zde je několik základních doporučení:

Vše sepište. Nepředávejte svým blízkým informace o Shamirově záloze pouze verbálně, raději jim napište dopis, který otevřou až po vaší smrti; když o záloze blízkým jen řeknete, podrobnosti s největší pravděpodobností zapomenou (v nejhorším případě může dotyčný zemřít s vámi při společné nehodě).

Žádné digitální kopie. Pokyny pište vlastnoručně na papír; stejně jako u seedu platí, že pokyny k přístupu k Shamirovým zálohám byste neměli psát na počítači a neměli byste je fotit.

Budte srozumitelní. Vysvětlete, co to vůbec Shamirova záloha je a proč by se obnova měla provádět s maximální opatrností (např. že seed nikdy nesmí být zapisován do webových stránek, nikdy se nesmí posílat cizím lidem atd.).

Předejte úplné informace. Uveďte celkový počet částí seedu, počet nutný k obnovení seedu a pokyny pro nalezení jednotlivých částí. Používáte-li passphrase, musí se o ní pozůstalí také dozvědět.

Za života mějte pokyny pod kontrolou. Uložte pokyny k předání dědictví na bezpečném a kontrolovaném místě, ke kterému budou mít vaši blízcí přístup v případě vaší smrti – dobré místo je kupříkladu domácí sejf; konkrétní místo však závisí na individuálních okolnostech.

Kontrolujte a aktualizujte. Jednou za rok si zkontrolujte, zda jsou pokyny na svém místě a zda jsou stále aktuální. Pokud se

v zabezpečení vašeho bitcoinu cokoli změní – například umístění částí seedu – musíte pokyny bez odkladu aktualizovat.

A samozřejmě, pokud máte nějaké bitcoiny na softwarových peněženkách, burzovních účtech nebo jiných službách, měli byste o nich informovat i své pozůstalé. Zkuste si představit scénář, ve kterém zítra umřete: měli by vaši příbuzní přístup ke každému vašemu satoshi? Je-li odpověď záporná, musíte to napravit.



Ten pocit, když vám nastupuje fatální infarkt, ale vy můžete umřít s klidným svědomím, protože jste zajistili dědictví bitcoinu.

Asi nejdůležitější radou je vžít se do situace nocoinera – tedy někoho, kdo se s bitcoinem nikdy nesetkal. Pokud totiž nemáte rodinu zapálených bitcoinerů, je pravděpodobné, že se v případě

zmatku po vaší smrti dopustí kritických chyb, a o bitcoin opět rychle přijdou. Snažte se tedy co nejsrozumitelněji informovat o tom, co jste po sobě zanechali, a jak se k dědictví bezpečně dostat, aniž byste vystavili pozůstalé riziku podvodníků, pokusů o phishing a podobných nepříjemností. Zvažte zanechání kontaktu na důvěryhodného kamaráda-bitcoina, který by vaší rodině pomohl. Buďte velmi opatrní v tom, koho doporučujete, ale také vězte, že pokud rodině nikoho nedoporučíte, mohou pak pozůstalí žádat o radu cizí lidi na internetu. A i když se váš přítel neprokáže jako důvěryhodný, vaše rodina bude mít možnost právního postihu vůči jim známé osobě, což by v případě, že by je podvedl někdo anonymní, nebylo možné.

Poznatky z kapitoly

- Dědictví bitcoinu není automatické, musíte jej sami zajistit.
- Základní seed o jednom seznamu slov čelí dvojímu riziku: ztrátě a krádeži.
- Shamir Backup výrazně snižuje rizika ztráty/krádeže bezpečným rozdělením seedu na více částí.
- Zvažte si sepsat vysvětlující instrukce pro rodinné příslušníky, jak se k bitcoinům v případě vaší smrti dostat.
- Instrukce pravidelně kontrolujte a v případě potřeby aktualizujte.

Obezřetnost aneb Jak o sobě neprozradit vše

Bitcoin Magazine, 28. 7. 2021

Prvního dubna roku 1933 byla jen hrstka Američanů dostatečně zdravě paranoidních, aby držela své dolary ve formě zlatých mincí u sebe doma. Zdálo se, že na uložení zlata v bezpečí bank přece není nic rizikového. To vše se změnilo o den později, kdy prezident Roosevelt vyhlásil exekutivní příkaz 6102 „zakazující hromadění zlata na území Spojených států“ a zlato americkým občanům zkrátka zabavil. Kdokoliv měl zlato v bance, o něj přišel. Pouze ti, kteří měli zdravou nedůvěru k vládě a bankovnímu systému, měli možnost volby: mohli se konfiskačnímu příkazu podřídit a držení zlata nahlásit, nebo si svůj majetek mohli v tajnosti ponechat.

„Soukromí je možnost selektivně se odkrýt světu.“

– Kryptoanarchistický manifest

Větu „soukromí je možnost selektivně se odkrýt světu“ napsal před 30 lety Eric Hughes v legendárním Kryptoanarchistickém manifestu. Soukromí nám ponechává volbu v tom, kdo o nás bude rozhodovat – bez soukromí se totiž snadno ocitneme v situaci, kdy o nás rozhodují druzí, a to často silnější a mocnější než jsme my; a jejich rozhodnutí zpravidla nebývají v našem nejlepším zájmu.

Ochrana před zvůlí

Koordinovaný útok na finanční soukromí začal ve 30. letech 20. století v době prohibice alkoholu v USA. Tato nesmyslná prohibice vytvořila nový typ podnikatele s vysokou tolerancí k riziku: gangstera. V oné době bylo obtížné stíhat gangstery konvenčním způsobem, a tak vláda tlačila na banky, aby se začaly zajímat o zdroj příjmů svých klientů. Ti, kteří své příjmy nedokázali vysvětlit, byli obviněni z daňových úniků. Právě za daňové úniky byl uvězněn gangster číslo jedna, Al Capone.



Představte si, že léta vedete kriminální organizaci, která rutinně vraždí své konkurenty a neposlušné zaměstnance, a soud vás odsoudí za to, že jste státu neodvedli adekvátní podíl.

Prohibice skončila v roce 1933, ale základy režimu finančního dohledu zůstaly. V následujících desetiletích byl systém špehování rozšířen ve jménu válek proti drogám a teroru (obě velmi pochybné svými výsledky a brutální z hlediska vedlejších škod a obětí). Ačkoliv se argumenty pro finanční dohled v průběhu let mění, existuje jeden základní motiv pro odstranění finančního soukromí: zajistit, aby nebylo možné uniknout daňovému režimu. Daňový leviatan je hladová bestie požírající vše, co jí přijde do cesty. A nehraje fair play.

Stát určuje pravidla a v případě potřeby je mění ze dne na den. Můžete se zaklínat tím, že „tady se to nestane“; vše se ale jednou stane poprvé. Kdo v roce 1933 čekal, že civilizovaný stát, jako jsou USA, své občany jednoduše okrade prostřednictvím exekutivního příkazu? Ve vyhrocené době se státní zákony mění rychle a obvykle v neprospěch občanů.²⁹ To, co je naprosto legální, například držení zlatých mincí nebo soukromých klíčů k bitcoinu, může být v budoucnu prohlášeno za nezákonné.

²⁹ Kdo by v roce 2019 čekal, že o rok později bude vláda plošně zakazovat vycházení z domu? Když společnosti cloumá strach, může si vláda dovolit naprosto cokoliv.

Ve vyhocené době žijeme právě dnes, na sklonku padesátiletého experimentu s čistým fiatem. Úrokové sazby největších centrálních bank se sotva mohou odlepit od nuly. Kvantitativní uvolňování, repo operace, stimulační dávky – to vše jsou jen různé termíny pro tisk peněz. Bez těchto programů se ekonomika závislá na dluhu rozpadne jako domeček z karet. Další krok pro zachování systému bude zřejmě orwellovský konstrukt zvaný digitální měny centrálních bank (CBDC).

Potom se váš bitcoin stane zaprvé nebezpečnou překážkou pro další monetární experimenty, zadruhé lukrativním cílem pro zdanění nebo konfiskaci (rozdíl mezi těmito termíny je však jen v míře zcizení).

Ochrana soukromí je pojistkou proti zvlůi, a to jak ze strany jednotlivců, tak celých veřejných subjektů, vlád a států. Avšak zatímco proti zlodějům se můžete legálně chránit, proti těm, kdož sami určují pravidla, to dost dobře nejde. Jediný způsob ochrany proti zlovůli státu je *ex ante*, před událostí.

Dosáhnout soukromí není snadné

Bitcoin sám o sobě je značně transparentní, i tak ale můžeme s trochou snahy dosáhnout dostatečné míry soukromí. Soukromí u bitcoinu funguje obdobně jako jeho zabezpečení – a to v tom smyslu, že záleží jen na nás, jak si věci zařídíme. Existuje množství nástrojů, vzdělávacích zdrojů a bitcoinerů připravených zodpovědět vaše dotazy; vy však musíte věnovat svůj čas a následně sami podniknout potřebné kroky.

V první řadě je třeba si uvědomit, že v rámci ochrany soukromí neexistuje žádný jednoduchý hack. Žádná aplikace, peněženka, nastavení nebo proces samy o sobě neochrání vaše soukromí na jedno kliknutí a na věčné časy. Ochrana soukromí je mentální nastavení. Musíte ji chtít a následně upravit své jednání.

Soukromí je také spektrum. Na škále mezi transparentností a anonymitou se nachází mnoho dílčích stavů. Je žádoucí udělat

alespoň malý krok směrem od úplné transparentnosti, i když nemůžete snadno dosáhnout úplné anonymity. Minimálně je totiž dobré nebýt „první na ráně“.

Otevřete svou mysl a zavřete pusu

Překvapivě tím nejsilnějším nástrojem pro posílení soukromí je vaše hlava a pusa.

Většina z nás v minulosti udělala řadu chyb, jež se týkají bitcoinu a soukromí: koupili jsme bitcoin na burze, která nyní uchovává naše osobní údaje; opakovaně jsme použili stejnou bitcoinovou adresu; spojili jsme transakční výstupy, které měly být oddělené, a tak dále. Uvědomit si tyto chyby a hledat způsoby, jak je napravit, je první krok. Uvědomit si, jak se vyhnout případným budoucím chybám, je ten další.

Je zásadní mít na paměti, že z technického hlediska můžete udělat všechno správně, ale vše následně pokazit tím, že o vašem zabezpečení budete vyprávět všude okolo. Můžete mít sebelepší Shamirovo schéma, ale co vám to bude platné, když o něm budete žvanit v hospodě.

Znamená to snad, že byste neměli o bitcoinu vykládat svým přátelům a rodině? Vůbec ne. Jen si pamatujte, že je obrovský rozdíl mezi vysvětlováním bitcoinu v obecné rovině a mluvením o *vašem* bitcoinu.

Vymezte si přísnou mentální hranici: debaty o vlastnostech bitcoinu a osvědčených postupech jeho získávání a držení (např. DCA) jsou relevantní, zatímco diskuse o vašem osobním nastavení, umístění seedů nebo množství držných bitcoinů nikoli.

Nyní se pojďme ponořit do několika praktických tipů pro zlepšení vašeho bitcoinového soukromí.

Vyhňte se KYC stopě

Udržovat bitcoin „čistý“ je trochu jako starat se o drahé oblečení; je sice dobré znát správné techniky praní, ale lepší je se v prvé řadě vůbec nezašpinit. V případě bitcoinu je pomyslnou skvrnou na kráse KYC – Know Your Customer. Jedná se o povinný proces identifikace, který musí poskytovatelé finančních služeb (např. burzy) provádět u svých klientů.

Pokud jde o KYC, potýkáme se s rizikem dvojího typu.

První riziko vyplývá z transparentní povahy bitcoinového blockchainu. Když nakoupíte bitcoinu na burze s KYC a vyberete si je do vlastní peněženky, provozovatelé burzy znají adresu, na kterou jste si vybírali, a mohou následně snadno sledovat vaše transakce. To platí i pro všechny třetí strany, s nimiž burzy tyto informace sdílejí, například analytické firmy a státní orgány. Toto konkrétní riziko lze zmírnit využitím postupu Coinjoin, což je kolaborativní transakce s jinými bitcoiny, jejímž účelem je ztížení sledování transakčních aktivit. Nejpoužívanějšími nástroji pro Coinjoin jsou peněženky Samourai či Wasabi Wallet; od jara 2023 je také možné coinjoinovat přímo z Trezoru. Mějte však na paměti, že pokud se rozhodnete zlepšit své soukromí prostřednictvím techniky Coinjoin, některé burzy to budou považovat za podezřelé a mohou vám zavřít účet.

Druhé riziko vyplývá již ze skutečnosti, že jste se nechali identifikovat. Pokud nakoupíte na burze s KYC, budete jednoduše známi jako někdo, kdo si v minulosti pořídil bitcoin. Toho mohou kupříkladu zneužít zločinci, kteří se na vás mohou zaměřit na základě uniklých uživatelských dat (a pro jistotu dopředu počítejte s tím, že všechna data uniknou). Tyto informace by v budoucnu mohla využít také vláda, pokud se změní zákony týkající se osobního držení bitcoinů či bude uzákoněna nová daň z držení bitcoinů apod. Jediný způsob, jak toto riziko skutečně odstranit, je prodat na burze stejné množství bitcoinů, které jste dříve nakoupili, a bitcoin znovu nakoupit anonymnějším způsobem (tj. vexlem či v bitcoinovém bankomatu). Tak budete mít oficiální záznam

o tom, že již žádné bitcoiny nadržíte. Tento proces samozřejmě může nést nepříjemnou daňovou povinnost, pokud mezi nákupem a prodejem došlo k růstu ceny bitcoinu. Potenciální alternativou je také výmluva na „nehodu na lodi“, kdy tvrdíte, že vám Trezor spadl přes palubu, pes vám sežral seed atd. – tento postup však na odrazení dostatečně motivovaných útočníků nebude fungovat.

Když už jsme zmínili rizika KYC, je na místě uvést i jednu potenciální výhodu. KYC jsou pro systém „čisté“ coiny, které vám ve vztahu s úřady (zejména tím daňovým) značně pomůžou a potenciálně ušetří nemalé prostředky. Máte-li k bitcoinům doklad o nákupu, můžete vždy doložit původ vašich prostředků a nemusíte při směně za fiat danit celou transakci jako čistý zisk. Ponechám nicméně na čtenářově uvážení, zdali tato výhoda stojí za to podstupovat výše zmíněná rizika.³⁰

UTXO hygiena

Z technického pohledu existuje bitcoin v podobě jednotlivých neutracených transakčních výstupů (UTXO). UTXO je konkrétní suma bitcoinu, která leží na vaší adrese jako výsledek předchozí transakce. UTXO je to, co pozorovatel – burza či burzou najatá analytická společnost – sleduje a analyzuje, kam se po výběru z burzy bitcoiny dále přesunují.

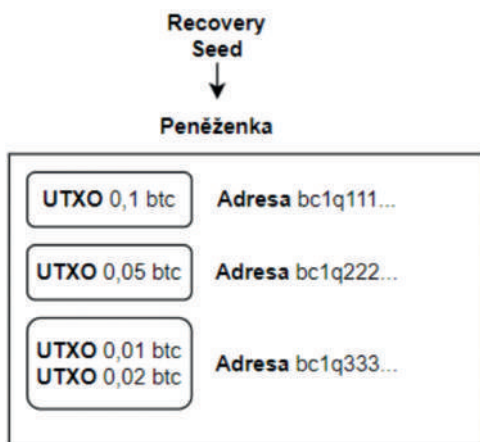
Správa UTXO může být na první pohled složitá; po pochopení základních pojmů to však bude snazší – důležité je znát vztahy a rozdíly mezi UTXO, *adresou* a *peněženkou*.

Adresy jsou místem, kde jsou UTXO uloženy. Na jedné adrese byste měli mít pouze jedno UTXO, což znamená, že byste nikdy neměli adresu používat opakovaně pro příjem více transakcí. Opakované použití adresy pomáhá pozorovateli propojit různé zůstatky s jedním držitelem. Vyhnout se opakovanému použití adresy je snadné: software peněženky ví, které adresy již přijaly UTXO

30 Stojí také za zmínku, že autor těchto řádek nemá žádnou odbornost v daňových otázkách – konzultujte prosím svou situaci s odborníky, například z firmy SimpleTax.

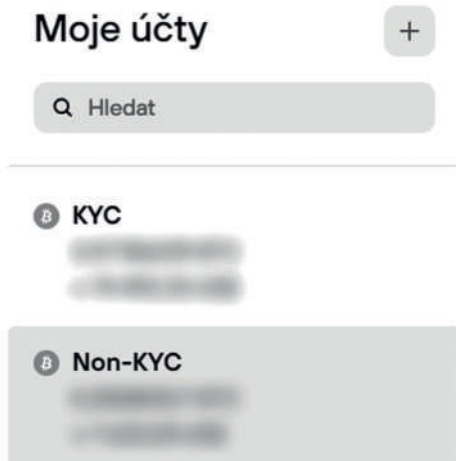
a které ne; když kliknete na „přijmout“, vždy vám dá nepoužitou adresu – vytváření čerstvých adres pro každou transakci je dnes již standardní funkcí každé peněženky. Přijímejte tudíž bitcoin vždy kliknutím na „přijmout“, nikoliv zkopírováním vaší staré adresy.

Peněženka uchovává váš unikátní soukromý klíč a odpovídající veřejné klíče, ze kterých se generují adresy ovládané touto peněženkou. Uvědomte si, že i když adresy nikdy nepoužíváte opakovaně a udržujete tak UTXO oddělené, můžete své UTXO neúmyslně propojit. Pokud se pokusíte odeslat platbu ve výši 0,1 BTC, ale žádné jednotlivé UTXO nemá takovou hodnotu, vaše peněženka automaticky spojí více UTXO, aby sestavila cílovou částku. Jakmile je tato transakce s více vstupy odeslána, pozorovatel vidí, že tyto separátní UTXO byly ve skutečnosti vlastněny jedním subjektem.



Ilustrativní obrázek: z obnovovacího seedu obnovíte svou peněženku se všemi adresami a UTXOs, které náleží k daným adresám. Pokud byste z této peněženky odeslali transakci o hodnotě 0,18 BTC, všechny UTXO se spojí jako vstupy transakce a pozorovateli tak bude jasné, že měly stejného majitele.

Ve své peněžence můžete pracovat s větším množstvím účtů, pokud peněženka podporuje BIP32 (např. Trezor). To je užitečné zejména v případě, že máte mince s KYC i bez KYC. Tím, že je budete mít oddělené na různých účtech, nikdy nedojde k jejich smíchání při transakci s více vstupy.



Rozlišení KYC a Non-KYC účtů v Trezor Suite. Strukturu účtů a možnost přidání nových účtů naleznete v této aplikaci po levé straně v sekci Peněženka.

Pokročilejším řešením je označení jednotlivých UTXO a výběr konkrétních UTXO pro každou transakci. Tomuto postupu se říká coin control. Tuto možnost dnes již nabízí většina populárních peněženek: Electrum, Samourai, Specter Desktop, Wasabi, Trezor Suite.

IP adresy

I když nenakupujete přes burzu s KYC a své UTXO udržujete čisté a voňavé, může být vaše identita odhalena prostřednictvím leaku IP adresy při provádění bitcoinových transakcí. K maskování IP adresy můžete použít službu VPN, nicméně tyto služby jsou založeny na důvěře (věříte poskytovatelům VPN služby, že neuchovávají záznamy).

Použití sítě Tor je bezpečnější. Tor je něco jako VPN bez důvěry v prostředníka, jelikož vaše internetové packety jdou přes několik náhodně volených uzlů, které provozují dobrovolníci po celém světě. Pokročilé peněženky obsahují možnost automaticky směřovat veškerý provoz přes Tor. V Trezor Suite stačí pouze zapnout funkci Tor Switch, která se o vše postará na pozadí.

Utajení vaší IP adresy je obzvláště důležité, provozujete-li vlastní bitcoinový uzel, protože tento uzel prozrazuje světu vaši IP adresu.

Provozování vlastního uzlu a blockchainového exploreru

Když se připojíte k uzlu někoho jiného, pak tento uzel eviduje všechny transakce, které přes něj posíláte a přijímáte. Když kontrolujete zůstatky svých adres nebo podrobnosti o transakcích ve veřejném block exploreru, vidí tuto aktivitu i provozovatel dané služby. V kombinaci s nezakrytou IP adresou to může mít vážné důsledky pro soukromí.

Nejlepším řešením je provozovat vlastní uzel a v ideálním případě nad ním mít i vlastní block explorer. Vše si můžete nastavit sami ruční instalací Bitcoin Core a Mempool.space, anebo můžete zvolit hotový balíček jako je Umbrel či MyCitadel, s pomocí kterých je snadné provozovat i další bitcoinové služby, jako jsou platební brána BTCPay či lightningový uzel a platební kanály.

Soukromí na Lightning Network

Lightning Network si v kapitole o soukromí zaslouží alespoň stručnou zmínku. Běžná, leč mylná představa je, že lightningové platby jsou anonymní, protože nezanechávají žádnou stopu v blockchainu. Předpokladem pro platbu přes Lightning je nicméně platební kanál, který pro otevření vyžaduje blockchainovou transakci. Pokud tedy pozorovatel má již spárované konkrétní UTXO s vaší identitou, pak také ví, kdo vlastní daný platební kanál.

Když pomineme otevření kanálu, ani samotné lightningové transakce nemusí být plně soukromé. Odesílatelé lightningových plateb mají slušnou úroveň ochrany soukromí, avšak příjemci toho o sobě prostřednictvím node ID a vystavených lightningových invoices odhalují poměrně hodně.

Pokud vás soukromí v síti Lightning Network zajímá hlouběji, doporučuji stránky [LightningPrivacy.com](https://lightningprivacy.com).

Z hlediska soukromí v bitcoinu obecně doporučuji také sledovat měsíčník *This Month in Bitcoin Privacy*, který píše autorka vystupující pod pseudonymem That One Privacy Girl.

Soukromí je stav mysli

Soukromí při používání bitcoinu má mnoho aspektů, které je třeba mít na paměti. Tato kapitola rozhodně není vyčerpávajícím výčtem všech možností, mým záměrem je spíše přimět čtenáře k zamyšlení nad tím, co by mohli při svých aktivitách zlepšit. Neexistuje jediné řešení, které by ochránilo vaše soukromí, ale spíše si každý z nás musí klást otázku, zda kroky, které podniká, nebudou mít negativní dopad na jeho soukromí. Je nebezpečné být v této otázce zpohodlnělý – jakákoliv informace, kterou sdílíte, může být použita k útoku na vás nebo vás jinak omezit bez ohledu na to, jak bezpečně se nyní cítíte. Klíčové je uvědomit si potřebu ochrany vlastního finančního soukromí, vytvořit si návyk přemýšlet o dopadech jednání na soukromí a využívat nástroje, které slouží k jeho ochraně.

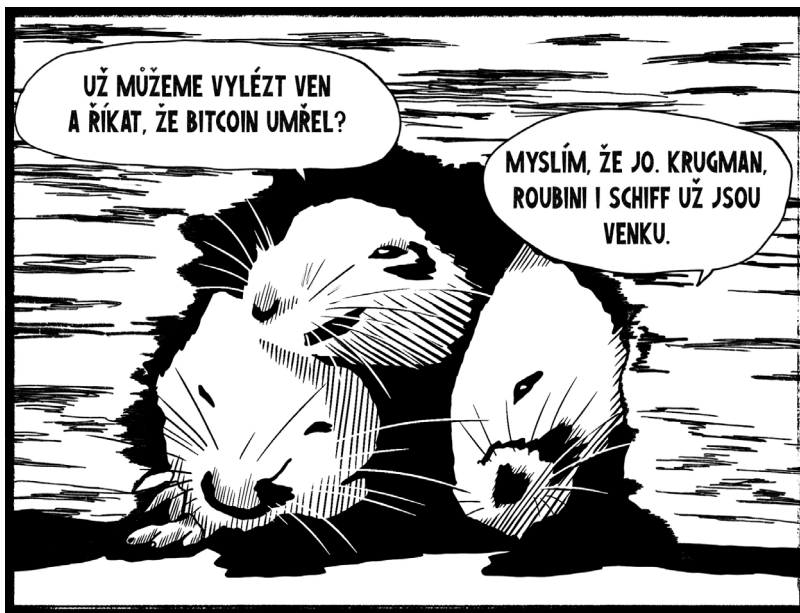
Poznátky z kapitoly

- Soukromí poskytuje svobodu rozhodovat se podle vlastního uvážení.
- Veškerá data, která o sobě poskytnete, dříve či později uniknou.
- Data spojená s držbou bitcoinu jsou obzvláště citlivá a vyhledávaná jak privátními, tak veřejnými zločinci.
- Jedno z nejčastějších rizik je nákup bitcoinu na burzách a směnárnách s KYC.
- Staré přešlapy nevrátíte zpět, ale můžete se z nich poučit a začít se napříště chovat obezřetněji.

Trpělivost aneb Jak přečkat medvědí trhy

Bitcoin Magazine, 15. 1. 2022

Cesta k hyperbitcoinizaci není přímá cesta „doprava a nahoru“; trajektorie spíše připomíná horskou dráhu, která navzdory mnoha infarktovým propadům dlouhodobě nabírá na nadmořské výšce. Při každém propadu je proto dobré napanikařit; nejedná se totiž o nic nového, ba ani neočekávaného.



V každém bear marketu vylézají na povrch krysy proklamující tentokrát již definitivní smrt bitcoinu.

Jak si ukážeme v této kapitole, v historii bitcoinu jsou patrné minimálně tři velké cenové cykly. Bitcoin se z cenového krachu doposud vždy vzpamatoval a vyšel z daného cyklu výrazně posílen se zástupy zocelených hodlerů za zády.

Medvědí trh 2011–2012

Cena bitcoinu klesla z 29 dolarů (8. června 2011) na 2 dolary (18. listopadu 2011), poté následovaly měsíce pohybu do strany:



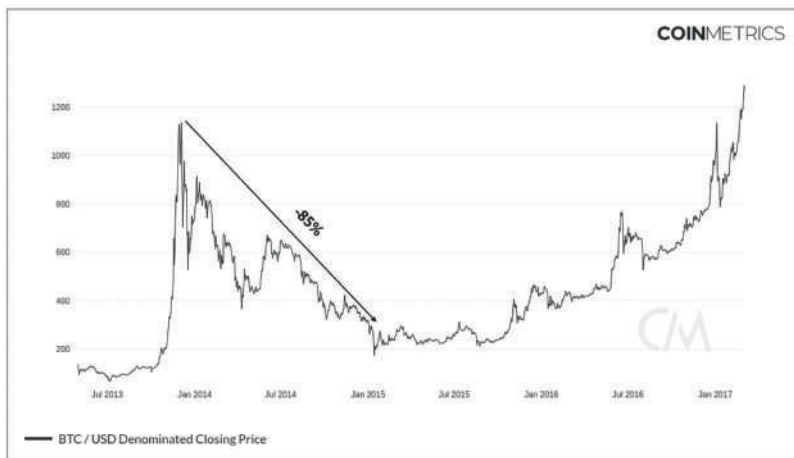
První medvědí trh bitcoinu, 2011–2012. Zdroj dat: CoinMetrics.io

Nejbolestivější medvědí trh se odehrál ještě předtím, než většina z nás vůbec tušila, že něco jako bitcoin existuje. Před více než deseti lety dosáhla cena bitcoinu na tehdy populární burze Mt Gox téměř 30 dolarů, aby pak následovalo „schodiště do pekel“, které během několika měsíců srazilo cenu na 2 dolary.

Bitcoin se propadl o neuvěřitelných 93 %. Ale uvědomme si následující: nákup bitcoinu při tehdy historicky nejvyšší ceně (ATH) třicet dolarů by byl z dnešního pohledu pohádkový. Kdo by si nechtěl stacknout celý bitcoin za sedm stovek, že? Samozřejmě jen málokdo tehdy mohl předpokládat, že za deset let bude bitcoin stát desítky tisíc dolarů; proto po tomto počátečním propadu trvalo více než rok, než se cena zotavila a vyšplhala do nových výšin. Chápání bitcoinu se v průběhu deseti let značně posunulo: od geekovského experimentu přes přes darknetovou měnu až k dlouhodobé obraně proti zvlí centrálních bank. A čím dál častěji je brán seriózně i coby základ nového globálního peněžního systému.

Medvědí trh 2014–2016

Cena bitcoinu se propadla z 1 135 dolarů (4. prosince 2013) na 175 dolarů (14. ledna 2015), poté následovaly měsíce pohybu do strany:



Druhý medvědí trh bitcoinu, 2014–2016. Zdroj dat: CoinMetrics.io

Na přelomu let 2013 a 2014 došlo ke dvěma zásadním událostem: bylo uzavřeno tržiště Silk Road³¹ zkrachovala burza Mt Gox. Tyto události byly spouštěčem několikaletého medvědího trhu. Silk Road a Mt Gox představovaly celý tehdejší vesmír bitcoinové ekonomiky; po jejich krachu se mnozí domnívali, že bitcoin již k ničemu není a že jej čeká pouze hanebný zánik. Po propadu o 85 % bylo napsáno mnoho nekrologů bitcoinu, obvykle se samolibým podtextem „však já vám to říkal“.

Ale ti, kteří zažili předchozí medvědí trh z let 2011–2012, již věděli své: bitcoin jen tak něco nezabije, a pokud se mu opět povede pozvednout se do nových výšin, bude to stát za to. Vývojáři pokračovali v práci a některé z nejvýznamnějších bitcoinových technologií spatřily světlo světa právě během druhého medvědího trhu: světově první hardwarová peněženka Trezor One byla uvedena na začátku roku 2014, v lednu 2016 pak byl zveřejněn whitepaper Lightning Network.

31 Provozovatel tržiště Silk Road jménem Ross Ulbricht si nyní odpykává dvojnásobný doživotní trest bez možnosti podmíněného propuštění.

Medvědí trh 2018–2020

Další spektakulární propad ceny bitcoinu se odehrál mezi 16. prosincem 2017, kdy stál bitcoin 19 640 dolarů, a 15. prosincem 2018, kdy našel své dno na cenovce 3 185 dolarů.

A opět následovaly měsíce pohybu do strany:



Třetí medvědí trh bitcoinu, 2018–2020. Zdroj dat: CoinMetrics.io

Tomuto medvědímu trhu se občas přezdívá „kryptozima“, zřejmě proto, že k velkému otřesu a poklesu na minimum poblíž 3 000 dolarů došlo v zimě 2018/2019. Tento medvědí trh byl nepříjemný kvůli falešné rally na jaře/létě 2019, kdy cena dosáhla 12 000 dolarů, jenže v březnu 2020, kdy naplno udeřila covidová panika, poklesla zpět na 4 000 dolarů.

Bitcoin se však opět vzchopil a následně vystoupal až k ceně převyšující 60 000 dolarů. V tomto období bylo opět uvedeno mnoho přelomových projektů – Trezor Model T se značně vylepšeným zabezpečením seedů v podobě Shamir Backup, platební brána BTC Pay Server, většina peněženek a nástrojů pro Lightning Network, projekt Spiral Jacka Dorseyho, firma Strike Jacka Mallerse a mnoho dalších nástrojů a služeb, které se staly nedílnou součástí bitcoinového ekosystému.

Milion obchodníků u milionu počítačů

V průběhu let vzniklo celé odvětví tzv. onchain analýzy, které se snaží predikovat převládající náladu na trhu. Problémem takových metrik je však to, že jsou samy o sobě postaveny na subjektivních interpretacích toho, co se děje:



Jameson Lopp ✓
@lopp



Bitcoin balances on exchanges ended 2021 higher at 1.56M BTC according to @coinmetrics, but they ended the year lower at 2.55M BTC according to @glassnode.

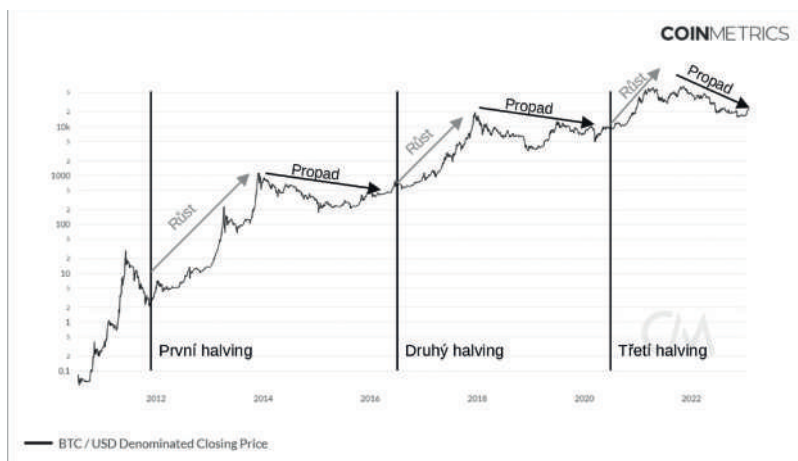


„Koncem roku 2021 vzrostl objem bitcoinů na burzách na 1,56 milionu BTC podle Coinmetrics a poklesl na úroveň 2,55 milionu BTC podle Glassnode.“

– Jameson Lopp

Poznámka překladatele: jak praví Kiccom, všichni ví ho*no, a to i když si říkají datoví analytici.

Někteří analytici se snaží předpovídat krátkodobé a dlouhodobé cenové dění poukazováním na korelaci mezi cenovými rally a bitcoinovými halvingy – čtyřletým cyklem, který snižuje na polovinu míru emise bitcoinů. A vskutku, na první pohled se zdá, že tato korelace existuje:



Bitcoinové halvingy a cena bitcoinu 2010–2023, logaritmické měřítko. Zdroj dat: CoinMetrics.io

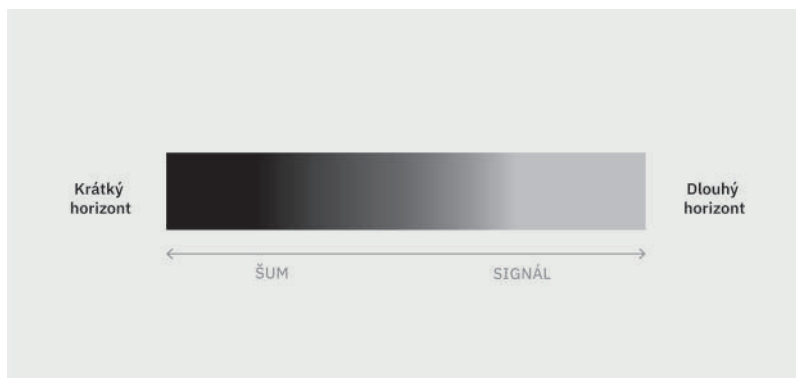
Problémem hypotézy o halvingovém cyklu je, že zatím máme k dispozici pouze tři datové body: období po prvním, druhém a třetím halvingu. Doposud se zdá, že cenový trend kopíruje i ve třetím období stejný vzorec, stále to však nemusí nic znamenat. Podle hypotézy efektivního trhu³² nemohou předvídatelné a všeobecně známé skutečnosti, jako je halving, ovlivnit cenu tak závratným způsobem – existují jiné neviditelné faktory (například postupný rozklad fiat měn, které čím dál více selhávají jako spolehlivý uchovatel hodnoty). Lidská mysl ráda hledá vzory v šumu a krátkodobě volatilní, dlouhodobě vzestupný graf je v tomto ohledu velmi svůdný.

Bitcoin je jediná skutečně globální peněžní jednotka. Můžete ho nakupovat, prodávat, posílat a přijímat v USA i Rusku, Norsku i Jihoafrické republice, Argentíně i Vietnamu. Neexistuje jediný „oficiální trh“ s bitcoiny – není žádná bitcoinová burza se sídlem na Manhattanu v budově s impozantními mramorovými sloupy a pracovní dobou od devíti do pěti. Bitcoin je obchodován celosvětově, velmi organickým způsobem: 8 760 hodin ročně, a to jak peer-to-peer způsobem, tak na regulovaných burzách.

Není proto divu, že v krátkých časových intervalech je cena bitcoinu náhodnou procházkou. V ceně se odráží milion myslí s milionem přání a milionem názorů na to, kam bude cena směřovat v příštích hodinách a dnech. Někteří usilují o prodej, jiní o nákup; v centru toho všeho se nachází prchlivá rovnováha zvaná spotová cena.

To však neznamená, že by cena bitcoinu byla náhodná. Ano, krátkodobě se jedná o šum vyplývající z organické povahy bitcoinového trhu; dlouhodobě však nad šumem převládá signál: bitcoinové fundamenty v podobě peněžních vlastností. Vzácnost, dělitelnost, durabilita, převoditelnost, ověřitelnost; bitcoin je dle tisíce let definovaných peněžních vlastností těmi nejlepšími penězi současnosti. A jak svět tuto skutečnost postupně objevuje, tak roste i směnný poměr vůči dnešním méněcenným penězům ve formě fiat. Chce to ale trpělivost.

32 Pro kvalitní pojednání o teorii efektivních trhů doporučuji článek Nica Cartera *An Introduction to the Efficient Market Hypothesis for Bitcoiners*, vyšlo 4. 1. 2020 na Medium.com.



Zkrátka a dobře: uděláte mnohem lépe, když se na výkyvy v ceně připravíte, než když se je budete snažit předpovídat.

Pravidla pro medvědí trh

Jak jsme si popsali výše, medvědí trh roku 2022 není ničím bezprecedentním. Jedná se již minimálně o čtvrtý výrazný propad z předchozího ATH a je dost možné, že bude trvat dva roky i více let. To nicméně neznamená konec bitcoinu; naopak pro jedince se může jednat o životní příležitost, jak si dostatečně „nastackovat“. Stačí následovat základní pravidla vyplývající z klasické ctnosti trpělivosti.

Neobchodujte. Začínající obchodníci si vždy myslí, že se jim podaří nakupovat nízko a prodávat vysoko. Nakonec však dělají pravý opak, protože se jim do cesty postaví emoce. Obchodování je velmi stresující hra s nulovým součtem, při které většina lidí přichází o své peníze: analýza na Business Insideru kupříkladu poukázala na to, že 70–97 % denních obchodníků utrpí ztrátu!³³ Pouze zkušené obchodníky (kteří se již poučili a umí ovládat své emoce) a burzy jsou dlouhodobě v zisku.

Nepoužívejte páku. Existují dva typy obchodníků využívajících páku: ti, kteří zažili duši drásající oznámení o likvidaci, a naivové, kteří si myslí, že mají vše pod kontrolou. Obchodování s bitcoinem za využití páky je snadný způsob, jak skončit v chudobinci nebo v blázinci.

33 Článek *If You're Day Trading, You Will Probably Lose Money: Here's Why*, vyšel na businessInsider.com dne 30. 7. 2021.



Taky možnost.

Nenechávejte bitcoin na burze / u správců. V bouřlivém období medvědího trhu krachují burzy a rozličné služby slibující zhodnocení vašeho vkladu. V minulosti došlo ke krachům velkých burz Mt Gox, Quadriga a Cryptopia; v roce 2022 je pak následovaly Celsius, BlockFi, FTX. Jediné bezpečné místo pro váš bitcoin je vaše vlastní peněženka. „Nemáte klíče, nemáte bitcoin“ zkrátka platí za všech okolností.

Neshitcoinujte. Na stránkách coinmarketcap.com máme možnost zobrazit řazení coinů v minulosti (*Cryptocurrencies* → *Historical snapshots*). Když se podíváme například na rok 2017, zjistíme, že tehdejších top 20 coinů vypadá dost jinak než dnes. Čistě ze spekulativního pohledu spočívá problém se shitcoiny v tom, že jich je prostě příliš mnoho a že denně vznikají další a další. Shitcoinů řeší jediný problém: málo peněz v peněženkách zakladatelů a jejich promotérů. Bitcoin jsou globální nestátní peníze a jako takové řeší problém fiat měn. Bitcoin je onen solidní coin s obrovským potenciálem, který hledáte!

Odzoomujte. Z hlediska cenových grafů i fundamentů se vyplatí udělat krok zpět a zvážit věci z širší perspektivy. Bitcoin si vede svou již 14 let a bez ohledu na to, jak špatně to s ním někdy vypadalo, vždy se zotavil. Bitcoin je antifragilní – volatilita, útoky, rozkoly a pokusy o jeho zákaz nebo regulaci jej nakonec vždy posílí. Abyste však mohli plně využít jeho výhod, musíte mít dostatečné přesvědčení jej udržet (či ještě lépe si v bitcoinu dlouhodobě spořit) v těžkých i dobrých časech.

Studujte. Zásadní díla, jako například *The Bullish Case For Bitcoin* od Vijaye Boyapatiho, Bitcoinový standard od Saifedean Ammous nebo *Gradually, Then Suddenly* od Parkera Lewise, byla vydána během medvědího trhu v letech 2018–2020. A zůstávají skvělým čtením za příznivého i bouřlivého počasí. Studium těchto děl vám pomůže dohlédnout za krátkodobý propad a pomůže vám učinit správné rozhodnutí pro vaši budoucnost.

A konečně, nebuďte posedlí cenovými vrcholy – zajímavý příběh vyprávějí i bitcoinová roční minima:



Každý propad nakonec nalezne své dno. Okolo něj zocelení hodleři již prodávají i své židle a vše vkládají do bitcoinu (toto není investiční doporučení).

Šťěstí přeje přesvědčeným

Když opustíte fiatovou mentalitu a místo toho se naladíte na perspektivu hyperbitcoinizace, medvědí trhy se vlastně stanou příjemnými: za fiat dostáváte mnohem více satoshi, buzzwordová mánie utichá a inovátoři pracují na převratných technologiích, jejichž plný potenciál se projeví až v dalších letech.

Medvědí trhy nabízejí pro mnohé životní příležitost. Bitcoin je potenciálně jedním z největších průlomů v dějinách lidstva a mít možnost získat větší množství bitcoinu na nízkých cenových úrovních může pro miliony lidí znamenat únik z chudoby či ubíjejících pracovních pozic v „křečkoidním“ korporátu.



A pro ostřílené hodlery jsou medvědí trhy zdrojem náramné zábavy.

Allen Farrington v knize *Bitcoin is Venice* pokládá skvělou otázku týkající se bitcoinové volatility. „Jak by to mělo vypadat, kdyby se na světě objevila nová forma peněz a začala nastupovat cestu světové adopce?“ A Farringtonovou odpovědí dále v knize je, že „Kdyby se globální, digitální, zdravé, otevřené, programovatelné peníze monetizovaly z absolutní nuly, pak by to vypadalo přesně takto.“

Poznatky z kapitoly

- Chcete-li si udržet bitcoin dlouhodobě, je trpělivost vašim nejlepším pomocníkem.
- Krátkodobá cena bitcoinu je náhodný šum; dlouhodobá cena odráží bitcoinové fundamenty ve formě kvalitních peněžních vlastností.
- Fáze trhu nelze spolehlivě předpovídat.
- Medvědí trh 2022–2023 je již čtvrtý v pořadí – nejedná se o nic nového a nepředvídatelného; monetizace nového typu peněz od nuly je zkrátka volatilní.
- Neobchodujte, nepákejte, neshitcoinujte, držte si klíče u sebe, žijte svůj život a občas si přečtěte kvalitní knihu či poslechněte dobrý podcast – učiníte tak mnohem více než stresujícím sledováním cenového grafu.

Umírněnost aneb Jak být v pohodě

Bitcoin Magazine, 19. 11. 2022

Události roku 2022 dokládají, že jedinci a instituce s vysokou reputací mohou být ve skutečnosti jen gambleři, kteří se těší dočasnému štěstí – realita však dříve či později i takové „propleskne“.

Bitcoin je neúprosná kotva do reality. Již samotný fakt jeho konečné zásoby 21 milionů bitcoinů a nemožnost vytisknout jej více by měla umlčet ego každého; čas od času se přesto objeví domýšlivci, kteří si myslí, že bitcoin bude skákat tak, jak pískají. Zhu Su a Kyle Davies (Three Arrows Capital), Alex Mashinsky (Celsius), Do Kwon (Luna), Sam Bankman-Fried (FTX). Všechny tyto gamblery spojoval sebevražedný instrument zvaný finanční páka.

Finanční páka (anglicky *leverage*) zní jako sofistikovaný finanční žargon, ale v principu jde jen o vypůjčení peněz za účelem nákupu finančních aktiv. Protože věřitelé v takových transakcích podstupují riziko – hodnota nakoupených aktiv může klesnout a dlužník nemusí být schopen splácet – obvykle požadují nějakou formu zajištění neboli kolaterál. A to je jádro problému: jmenované osoby měly jen velmi málo vlastního kolaterálu, což se snažily obejít jedním ze dvou způsobů: zaprvé vykouzlením vlastního finančního aktiva čili „tokenu“ a přesvědčením dostatečného množství lidí, že takový token má skutečnou hodnotu a lze jej použít jako zástavu. Druhým způsobem je využití vkladů klientů jako zástavy pro další půjčky neboli politika částečných rezerv – odvěké pokušení všech bankéřů.

V případě FTX udělal Sam Bankman-Fried obojí: využil token FTT jako zástavu k obřím půjčkám a následným „investicím“ do pochybných shitcoinových projektů a zároveň provozoval svou burzu jako klasickou banku s částečnými rezervami. Poté, co Changpeng Zhao (Binance) propíchl bublinu jménem FTX jediným tweetem, přišli na mizinu jak držitelé tokenu FTT, tak i klienti burzy FTX, kteří na burze drželi prostředky. O peníze přišli také investoři

do akcií FTX, a to včetně kanadského penzijního fondu. Čachry s pákovými obchody zkrátka mívají velmi nepřijemné konce.

Fiatové instituce bez fiatové tiskárny

Kryptoměnové instituce znovuvytvářejí toxické fiatové prostředí, ve kterém se gambluje s cizími prostředky, aniž by si majitelé těchto prostředků byli vědomi. Burzy, poskytovatelé půjček, fondy a další institucionální držitelé jsou v principu banky provozující politiku částečných rezerv – tudíž přesně to, co zásadně přispělo k masivní finanční krizi po roce 2007 a co také velmi pravděpodobně bylo impulzem pro spuštění bitcoinu počátkem roku 2009.³⁴

Tyto instituce nad sebou nicméně nemají ochrannou ruku „věřitele poslední instance“, tj. centrální banky, která může v případě potřeby natisknout libovolný objem peněz. To znamená, že nadměrná páka se v tomto prostředí pročistí přirozeným tržním způsobem, bankrotem. Jedná se o výtečnou ukázkou toho, že bitcoin je skutečně jiný než současný finanční systém, ve kterém se nezodpovědnost vyplácí, jelikož v případě problémů přispěchá na záchranu centrální banka. Systematické zachraňování gamblerských degenerátů v prostředí bitcoinu není možné, jelikož bitcoinu zkrátka nelze natisknout více, než dovolí protokol. Jak upozorňovali již před sto lety ekonomové rakouské školy, bankrot je v tržním prostředí velmi kýžený, jelikož zabraňuje nafouknutí mylných investic do katastrofálních rozměrů.

Jak přežít kolaps shitcoinového kasina

Impozantní kolaps FTX ovlivnil i bitcoinové trhy, což naznačuje, že tyto hrátky mohou tvrdě zasáhnout nejen ty, kteří se jich přímo účastní. Pár dní po kolapsu FTX klesla fiatová cenovka bitcoinu o 14 %; což nemusí mít vliv na dlouhodobé hodlery, ale krátkodobé spekulanty a pákové obchodníky to pěkně „vypláchno“.

34 Satoshi sice nikdy explicitně neodkryl svou motivaci pro spuštění bitcoinu, existují však četné náznaky, že motivací byla právě nespokojenost s existujícím peněžním uspořádáním. Patří mezi ně zpráva v genesis bloku („Kancleř zvažuje druhý bankovní bailout“), Satoshiho udaný termín narození na diskusním fóru P2P Foundation (5. dubna – datum vydání Exekutivního příkazu 6102, kterým Roosevelt konfiskoval zlato americkým občanům), a Satoshiho kritika systému částečných rezerv v jeho publikovaných komentářích.

Kolaps shitcoinových kasin jako FTX vás může zasáhnout různými způsoby:

Když držíte burzovní shitcoin. Očividné. Kdokoliv drží token burzy jdoucí ke dnu, bude vážně poškozen. Na burzovních shitcoinech není nic decentralizovaného, jedná se o pseudoakcie, které však nepodléhají regulaci a uživatelé nemají žádnou ochranu. Toto se týká i populárního shitcoinu BNB od Binance.

Když držíte prostředky na burze. Držitelé zůstatků na FTX přišli o vše – ať už na burze drželi bitcoin, fiat či shitcoiny. Kdokoliv si myslel, že „vlastní bitcoin“ a přitom měl pouze zůstatek na FTX, již nyní chápe staré dobré pořekadlo „nemáte klíče, nemáte bitcoin“.

Když provádíte pákové obchody s bitcoinem. Kdykoliv padne velká burza či „krytofond“, volatilita bitcoinu se zvýší. Během nejistoty okolo osudu FTX kurz bitcoinu nejprve stoupl o 5 %, následoval pokles o 13 %; to vše v rozmezí hodin. Obchodování na páku by v té době velmi pravděpodobně vedlo k likvidaci obchodní pozice.

Když držíte příliš mnoho bitcoinu. Pro některé bitcoiny to může znít kacířsky, ale skutečně je možné držet *příliš mnoho* bitcoinu. Přiznejme si to: bitcoin může být krátkodobě velmi volatilní, a pokud držíte v bitcoinu všechny své prostředky, nemusíte zkrátka vyjít s penězi a budete nuceni prodávat bitcoin v tu nejhorší dobu, na samém dně. Zůstat za všech okolností solventní je pro dlouhodobé držení stejně důležité jako držba vlastních klíčů!

Zkrátka a dobře, jediný způsob, jak se vyhnout následkům podobných krachů, je trpělivě držet bitcoiny ve vlastní peněženice a vést produktivní život: mít pozitivní peněžní toky z práce či podnikání a pravidelně stackovat. Kromě značného finančního komfortu, který vám tato strategie v příštích letech podle mého názoru přinese, si budete užívat klidu mysli, jelikož takto nemůže váš bitcoin být nikdy zmrazen, zlikvidován nebo zcizen, a poklesy směnného kurzu budou přinášet místo stresu vítanou příležitost získat více satoshi za váš fiat.



Aby to medojedovi bylo vskutku jedno, musí mít dostatečnou pokoru: držet si klíče u sebe, nepoužívat páku, nevěřit na pohádky o „supercycklu“ a rychlém zbohatnutí.

Bitcoin je neúprosný fenomén a čím déle je mu člověk vystaven, tím je vůči němu pokornější. Čas od času bitcoin připomíná živý organismus, který si sám volí, u koho se zdrží a kdy půjde dál. Zhu Su a Kyle Davies, Alex Mashinski, Do Kwon a nyní Sam Bankman-Fried – ti všichni si mysleli, že jim bitcoin patří, ale bitcoin usoudil jinak. Spolu se svými následovníky nebyli schopni bitcoin dlouhodobě udržet.

Budete toho schopni vy?

Poznatky z kapitoly

- Nevěřte nikomu, kdo chce držet váš bitcoin – ani když se jedná o velké burzy s dobrou reputací; i takové často končí hanebným krachem.
- Kryptoměnové burzy často podléhají pokušení politiky částečných rezerv; jelikož nad sebou ale nemají centrální banku, vede jejich jednání ke kolapsům a značným ztrátám.
- Snahy o namnožení bitcoinu s pomocí shitcoinů, časování trhu, využívání páky, půjčování si na nákup – vše s velkou pravděpodobností povede k tomu, že nakonec budete mít bitcoinu spíš méně.
- Dlouhodobě nejlepší výhled má umírněná strategie průběžného spoření do bitcoinu, který si spravujete sami – jedině tak se totiž vyhnete veškerým rizikům krátkodobé volatility a institucionálních krachů.
- Sláva, bohatství, podnikatelský úspěch ani brzká adopce bitcoinu nijak negarantují, že daný jedinec o bitcoin nepřijde. Dlouhodobá držba bitcoinu vyžaduje především chladnou hlavu a pokoru.

ČÁST TŘETÍ: NÁVRATY

Úvod třetí části

Co pro svět znamená návrat zdravých peněz? To je otázka, nad kterou patrně budeme filosofovat ještě pěkných pár let. Hyperbitcoinizace sice klepe na dveře, ale na uvítání s otevřenou náručí si bude muset ještě počkat. Naopak lze očekávat, že státy budou proti procesu bitcoinizace bojovat. Ty méně prozíravé tupými a nefunkčními zákazy, chytřejší pak daněmi, regulací a konfiskacemi. Hrstka osvícených zemí bitcoinu a bitcoinerům možná půjde vstříc, bude se však jednat spíše o výjimky, jež nemají v monetárních otázkách co ztratit. O tomto nepřiliš optimistickém výhledu na budoucnost pojednává kapitola *Návrat konfiskací: Stát bitcoin nezakáže; bude na něm parazitovat*.

Je důležité si uvědomit, jak důležitý bude monetární konflikt nadcházejících let. Na jedné straně bude stát bitcoin – globální, nestátní, zdravé peníze – na straně druhé CBDC a bezhotovostní společnost, kde má stát plný dohled, kontrolu a právo veta nad veškerými transakcemi v ekonomice. Plnohodnotný návrat zdravých peněz má potenciál nastolit éru nové renesance, zatímco alternativou je dystopický návrat všemocného státu.

Přečkáme-li ale turbulentní dobu odluky peněz od státu, dočkáme se kýženého návratu zdravých peněz a s ním i nevidaného rozmachu plného potenciálu lidstva, jehož obrysy jsem načrtl v kapitole *Návrat zdravých peněz: Svět po hyperbitcoinizaci*.

Bitcoineři často po začlenění bitcoinu do svých životů pozorují prodloužení rozhodovacího horizontu; a ultimátním projevem dlouhodobého rozhodovacího horizontu je nemyslet na sebe, nýbrž na budoucí generace. I přes četné krátkodobé překážky tudíž zůstaňme dlouhodobými optimisty, jelikož události příštích let a dekád jsou významné pro samotný osud lidstva. Peníze jsou

katalyzátor rozvoje a v prostředí zdravých peněz lze očekávat explozi kreativity, produktivity a prosperity.

Bitcoin na mnoho lidí zpočátku působí jako zcela převratná technologie. Ve skutečnosti je však bitcoin návratem k peněžním principům, které lidstvu uspokojivě sloužily tisíce let. Můžeme tak i docela obstojně predikovat, k čemu návrat zdravých peněz povede: k nápravě rozbitého cenového mechanismu, k návratu funkčních úspor, návratu všeobecného optimismu vůči budoucnosti, posílení společnosti a uměnění role státu.

Bitcoin je naděje a je naší odpovědností vůči budoucím generacím tuto naději v co nejvyšší míře naplnit.

Návrat konfiskací: Stát bitcoin nezakáže; bude na něm parazitovat

Bitcoin Magazine, 16. 9. 2021

„Myslím si, že pokud bude [bitcoin] opravdu úspěšný, tak se státy budou snažit jej zničit. A myslím, že se jim to povede.“

– Ray Dalio v rozhovoru o bitcoinu³⁵

Zakázat bitcoin je prakticky nemožné. Ekonomické zákony povedou k tomu, že bitcoin dlouhodobě převládne jako nejpopulárnější způsob spoření; to však neznamená, že se stát vzdá svého peněžního monopolu bez boje. Bystřejší mozky establishmentu se pokusí vyjít z probíhajících peněžních turbulencí neporaženy.

Vládní zákazy nefungují

Jednu z nejlepších definic státu zformuloval Max Weber, když jej označil za subjekt, který disponuje „monopolem na násilí“. Stát tento monopol využívá k dalšímu upevňování moci nad společností. Přímé státní monopoly jsou dnes již zdiskreditovány četnými případy hospodářského rozkladu, který nastal všude, kde byla ekonomika centrálně řízena. Moderní přístup státu k ovládnutí různých odvětví je proto nepřímý. Dva oblíbené způsoby, jak takové nepřímé kontroly nad ekonomikou dosáhnout, jsou buď zákaz určitého odvětví, nebo nepřímé řízení odvětví prostřednictvím kombinovaného efektu daní, regulace a dohledu.

Zákazy nebývají účinné. Existuje-li silná poptávka po určitém statku, ani vládní zákaz ji nepotlačí.

Ukázkovým příkladem je americká alkoholová prohibice, která platila v letech 1920–1933. Studie Marka Thorntona z roku 1991 shrnuje dopady prohibice následovně:

³⁵ CNBC: *Ray Dalio says if bitcoin is really successful, regulators will 'kill it'*, 15. 9. 2021.

„Ačkoliv spotřeba alkoholu na počátku prohibice klesla, v dalších letech se opět zvýšila. Konzumace alkoholu se stala nebezpečnější, byla provázena vysokou mírou zločinu, který se navíc stal ‚organizovaným‘, soudní a vězeňský systém byl napjatý až k prasknutí a korupce veřejných činitelů byla všudypřítomná. Nedošlo k žádnému měřitelnému zvýšení produktivity ani ke snížení absencí v práci. Prohibice odstranila významný zdroj daňových příjmů a výrazně zvýšila vládní výdaje. Vedla k tomu, že mnoho pijáků přešlo na opium, marihuanu, léky na předpis, kokain a další nebezpečné látky, s nimiž by se bez prohibice pravděpodobně nesetkali.“

– Mark Thornton: *Alcohol Prohibition Was a Failure* ³⁶

Válka proti drogám, která začala v 70. letech 20. století, měla podobné výsledky. Podle analýzy Cato Institute z roku 2017 jsou důsledky 50 let drogové prohibice ve Spojených státech následující:

- Počet úmrtí na předávkování se zvýšil z 1/100 000 v roce 1971 na 12/100 000 v roce 2008.
- Zvýšila se síla drog a spotřeba se přesunula od měkkých, jako je marihuana, k tvrdým drogám, jako jsou opioidy.
- Objevily se nové syntetické drogy, jako je crack a fentanyl, které mají zničující dopad na uživatele a jejich komunity.
- Vymáhání opatření spojených s válkou proti drogám stojí americké daňové poplatníky 50 miliard dolarů ročně; původní rozpočet schválený v roce 1972 na protidrogovou politiku počítal s rozpočtem 1 miliardy dolarů na tříletý program.
- Padesát let trvající válka dala vzniknout nelítostným mexickým drogovým kartelům a násilné reakci vlády – mexická drogová válka si od roku 2006 vyžádala odhadem 300 000 životů.

³⁶ Mark Thornton: *Alcohol Prohibition Was a Failure*, dostupné na cato.org.

- Bylo normalizováno opatření „zabavení civilního majetku“ (*civil asset forfeiture*), v rámci kterého mohou policejní orgány zabavit majetek podezřelého z drogové trestné činnosti. Objem takových konfiskací je ohromující: „V roce 1986, tedy ve druhém roce své činnosti, zabavil Fond ministerstva spravedlnosti pro zabavování majetek v hodnotě téměř 94 milionů dolarů. Do roku 2011 se toto číslo vyšplhalo na přibližně 1,8 miliardy dolarů [ročně]. Státní a municipální konfiskace měly obdobně růstový trend.“
- Mezi další důsledky patří militarizace policie, rozsáhlá korupce, zvýšený útlak menšin a zahraniční vojenské intervence.

Drogová prohibice je také hlavním zdrojem tzv. špinavých peněz, přičemž opatření proti praní špinavých peněz (AML) jsou čím dál vtíravější a dotýkají se každého, kdo přichází do styku s finančním sektorem.

Účelem této kapitoly však nyní není rozsáhle analyzovat alkoholovou nebo drogovou politiku. Smyslem těchto úvodních poznatků je ilustrovat, že vládní zákazy jsou neúčinné, pokud jsou zaměřeny na omezení aktivit, po nichž panuje vysoká poptávka. Tam, kde existuje trvalá poptávka, si nabídka najde cestu.

Neúspěšné pokusy o totální zákaz určitého odvětví se během času postupně transformují do druhého typu státní kontroly: kontroly nepřímé, a to prostřednictvím daní, regulací a dotací. Tento vývoj jsme viděli v případě alkoholového průmyslu a totéž se děje i v oblasti nelegálních drog; užívání konopí a obchod s ním jsou legální již v 18 státech USA a v Oregonu jsou od roku 2020 dekriminlizovány všechny typy drog.

Alternativou k zákazům pro stát není vyhlášení volného trhu, ale spíše ovládnutí odvětví prostřednictvím regulací a vybírání renty prostřednictvím daní.

Budete dobrý občan, nebo podvratný živel?

Nehledě na to, co si myslí Ray Dalio, je již nyní jasné, že bitcoin nebude zakázán ve stejném duchu, jako byl zakázán alkohol a drogy. Vlády nebo spíše odborníci v příslušných agenturách si již udělali domácí úkol a chápou, že bitcoin nemohou žádným praktickým způsobem zakázat.

Stát tudíž nevyhlásí žádnou válku proti bitcoinu ve snaze jej vymýtit.

Místo toho bude stát usilovat rovnou o nastolení prostředí nepřímé kontroly, dokud to ještě jde. Jinými slovy dokud proces bitcoinizace nedosáhne horizontu událostí, dokud se plně nerozšíří bitcoinová cirkulární ekonomika a běžné výplaty v bitcoinu a dokud se většina nových bitcoinerů neobejde bez burz a směnáren.

Bitcoin samotný zakázat sice nelze, ale jeho držitele lze sledovat, stíhat, pokutovat, zavřít. Navíc většinu obrovské hodnoty, která se do bitcoinu v příštích letech pravděpodobně přelije z ostatních aktiv, lze od držitelů odčerpat. Toho lze dosáhnout rozdělením potenciálních bitcoinerů do dvou kategorií:

- 1. Dobří občané:** každý, kdo chce získat expozici vůči ceně bitcoinu, tak může učinit na plně regulované burze. Dobří občané nepřicházejí do přímého kontaktu s bitcoinovým protokolem a jsou odrazováni od výběru bitcoinů do svých peněženek. Transakce mezi regulovanými poskytovateli služeb jsou povoleny; dobří občané například mohou posílat bitcoiny mezi Coinbase a PayPal. Všichni uživatelé jsou plně identifikováni a klíče drží poskytovatelé služeb, nikoliv samotní uživatelé. Vláda může libovolně zdaňovat zisky z takto „vlastněného“ bitcoinu, hackeři zase mají radost z ohromného množství citlivých dat, které leží exponované na burzovních serverech.
- 2. Podvratné živly:** kdokoliv chce provádět opravdové bitcoinové transakce (tj. ne pouze účetní převody mezi regulovanými službami) či držet vlastní klíče, je automaticky sprostý podezřelý.

Požadavky regulátorů na KYC a AML budou aplikovány i na jedince, kteří je nemohou plnit. Dostanou se tak do situace, kdy prostým používáním bitcoinového protokolu porušují četná nařízení, přičemž penalizace bude mít formu zabavení soukromě držných bitcoinů.

Domnívám se, že nastolení takového prostředí je hlavní motivací politiků a úředníků, kteří v EU a USA projednávají budoucí podobu regulace bitcoinu a kryptoměn. Kupříkladu v roce 2021 padl v americkém Infrastructure Bill návrh na definici „makléřů“ (*brokers*), který byl technicky nesmyslný a nezohledňoval fungování bitcoinového protokolu. Přesto nebyla vůle tyto nedostatky uzнат a ustanovení přiblížit realitě.



Bitcoin is Saving
@BitcoinsSaving

...

As written, the amendment excludes passive node operators who are just validating transactions but not broadcasting or relaying transactions.

It also does not exclude miners because they are providing another function / service.

It does not exclude free open source software.

„Podle znění dodatku jsou z něj vyloučeni pasivní provozovatelé uzlů, kteří jen ověřují transakce, ale nevysílají je ani nepředávají dál. Zákon nevylučuje těžaře, protože ti poskytují jinou funkci/službu. Nevylučuje ani open source software.“

– Pierre Rochard alias Bitcoin is Saving

Tato právní úprava by znamenala, že každý, kdo provozuje vlastní uzel nebo těží na území USA, by porušoval zákon.

Nemyslím si, že by se jednalo o neschopnost zákonodárců. Z pohledu státu není regulace tohoto druhu problém – je to řešení.

Cílem státu není „regulatorní jistota“ ani zajištění ochrany spotřebitele či omezení praní špinavých peněz. Cílem je zastrašit uživatele, vývojáře

a bitcoinové firmy, aby nakládali s bitcoinem pouze posvěceným způsobem prostřednictvím sledovaných míst, z nichž nebude úniku; a následně odčerpávat hodnotu, a to jak z bitcoinů držných na burze prostřednictvím daní, tak od suverénních bitcoinerů prostřednictvím konfiskací.



„V krajním případě může být regulace vykládána jako zákaz psaní kódu, který umožňuje end-to-end šifrování. Jinak řečeno, nutí poskytovatele komunikačních služeb psát kód se zadními vrátky. Paralely s oblastí kryptoměn by měly být zřejmé.

Regulační orgány zjišťují, že finanční zprostředkovatelé, které jsou zvyklé regulovat, rychle mizí, protože transakce lze nyní realizovat formou peer-to-peer bez potřeby prostředníků.“

– Jerry Brito, ředitel think tanku Coin Center

Odčerpávání bitcoinové hodnoty

Podle nedávného průzkumu společnosti NYDIG vlastní bitcoin asi 46 milionů Američanů, tedy 22 % dospělé populace USA.³⁷ Není zřejmé, kolik jich vskutku drží bitcoin ve vlastní správě a kolik má pouze účet na burze; předpokládejme ale, že alespoň polovina z nich má pod kontrolou privátní klíče (což je značně optimistický odhad). To by znamenalo, že zhruba 10 % dospělé populace USA skutečně vlastní bitcoin.

³⁷ Banking + Bitcoin Survey, 13. 1. 2021, dostupné na nydig.com.

Za předpokladu, že bitcoin bude i nadále vítězit nad fiatem jako dlouhodobý uchovatel hodnoty, je přirozené, že se větší část americké populace bude snažit v příštích letech získat expozici vůči bitcoinu. **A právě o způsob, jakým onu expozici získá, se dnes hraje. Stát má stále šanci nahnat většinu nových uživatelů do přeregulovaného panoptikonu centralizovaných burz.** Je to trochu podobné legalizaci konopí prostřednictvím licencovaných výdejen (*dispensers*), kde obchod probíhá pod dohledem, s trvalými záznamy a s vysokou mírou zdanění.³⁸

Prozaickou skutečností je, že většině populace bude stačit, když bude mít pouze expozici vůči ceně bitcoinu jakožto aktivu, aniž by měla cokoli společného s bitcoinem jako protokolem. Většině nebude ani příliš vadit, když bude proces výběru bitcoinu z burzy značně omezen nebo zakázán v rámci „ochrany uživatelů“. Menšina pravověrných bitcoinerů by podléhala trestnímu stíhání, protože by vždy porušovala zákon – provozováním vlastního uzlu či těžbou bez plnění požadavků na KYC/AML nebo používáním anonymních peněženek s otevřeným zdrojovým kódem.

Jakmile by většina populace byla chycena na centralizovaných burzách a zbývající menšina perzekvovaná podle libosti, mohl by stát přikročit k samotnému odčerpávání hodnoty:

1. Bitcoin na burzách by podléhal roční dani z nerealizovaných kapitálových výnosů. Nyní to může znít pobuřujícím způsobem, ale existují možnosti, jak takové zdanění propagandisticky prosadit. V současné době pravděpodobně míříme do největší hospodářské recese od velké deprese. Po každém může být požadován „jeho podíl“ v těžkém období – a zdanění čtvrtiny či poloviny ročního zisku by pravděpodobně prošla (zvláště pokud by v prostředí pokračujícího rozkladu fiatů výrazně rostla

³⁸ Jednotlivé americké státy uvalují na pěstování a prodej marihuany daně dle váhy, prodejní ceny a obsahu THC. V době psaní textu jsou nejnižší daně v Michiganu a Vermontu (žádné speciální daně), nejvyšší ve Washingtonu (daň ve výši 37 %). Více na *How Do Marijuana Taxes Work?*, dostupné na taxpolicycenter.org.

fiatová cenovka bitcoinu). Daň by se automaticky odečítala ze zůstatku na burzovním účtu uživatele.

2. Bitcoin v držení suverénních hodlerů by podléhaly civilnímu zabavení majetku – procesu, který se již široce používá ve válce proti drogám a kterému dobří občané fandí. Každý se přece může svobodně rozhodnout, že bude dodržovat zákon.



Konfiskace bitcoinu/kryptoměn není pro americký daňový úřad nic nového, naopak se pro erár začíná jednat o velmi lukrativní zdroj příjmů. Kromě skutečných zločinů, jako jsou krádeže či podvody, konfiskuje daňový úřad bitcoin například i za P2P obchodování bez licence.

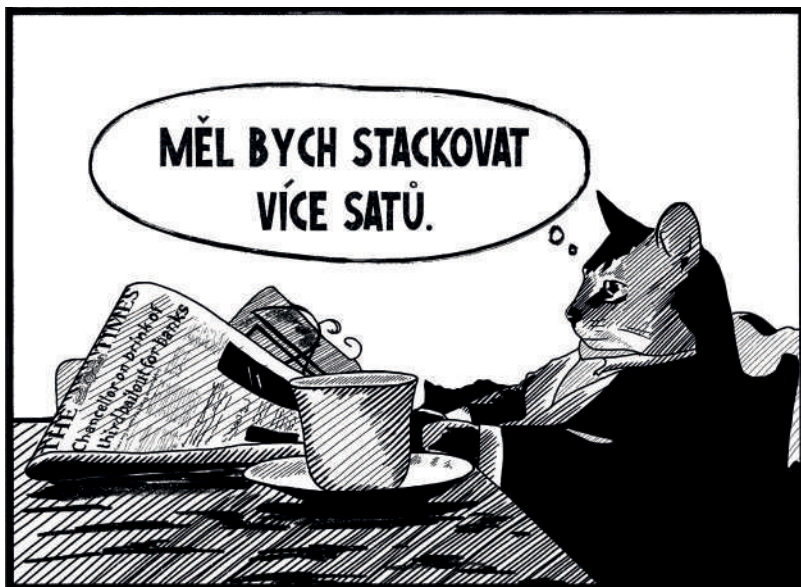
Cíl: maximální stacking

Je pravděpodobné, že lidé v establishmentu začínají chápat, co bitcoinoví hodleři chápou již několik let – důležitá není fiatová hodnota bitcoinu, nýbrž počet vlastněných bitcoinů. Zatímco fiat lze vytvořit limitně nekonečno, bitcoin je skutečně vzácný a v budoucnu může hrát kriticky důležitou geopolitickou roli.³⁹

Prozíraví politici a úředníci tak dost možná tuší, že musí něco udělat, a zároveň chápou, že zakazovat bitcoin je marná snaha. Nastolením

³⁹ Na strategickou důležitost bitcoinu v posledních letech poukazuje major Jason Lowery, člen amerických Vesmírných sil (Space Force). Lowery označuje bitcoin za druh zbraně. V únoru 2023 publikoval Lowery své myšlenky v knize *Softwar: A Novel Theory on Power Projection and the National Strategic Significance of Bitcoin*.

prostředí plně regulovaných a sledovaných pastí v kombinaci s demotivací lidí od suverénního přístupu k bitcoinu představuje docela dobrou šanci, jak může stát přežít hyperbitcoinizaci.



Vítězným scénářem pro stát není usilovná snaha o zákaz bitcoinu, ale spíše kontrola jeho toků a možnost pohodlné konfiskace. To neznamená, že tak učiní *všechny* státy; lze předpokládat, že některé postaví svou strategii přežití spíše na vstřícném přístupu k bitcoinerům prchajícím před predátorskými režimy. Z pohledu jedince je kriticky důležité zůstat ostražitý, kontrolovat vlastní klíče, starat se o své soukromí a být otevřený možnosti relokace do země, která je vůči bitcoinerům pohostinná.

Poznatky z kapitoly

- Státní zákazy vysoce poptávaných věcí zpravidla nefungují, trh si vždy najde cestu.
- Největším rizikem není zákaz bitcoinu, nýbrž jeho podmanění regulacemi.
- Na burzách a obdobných službách nejste majitelem bitcoinu a burza může na povel státu „váš“ bitcoin zadržet či předat státním složkám.
- Státní aparát v USA již nyní konfiskuje velké množství bitcoinu a kryptoměn; objem konfiskací se bude nadále zvyšovat, a tak tomu patrně bude i v jiných zemích.
- Je pravděpodobné, že na bitcoin budou kromě regulací uvalovány i speciální daně – ačkoliv lze očekávat, že čím více predátorský přístup budou mít určité státy (např. EU), tím přívětivější budou jiné státy (např. v Latinské Americe či Africe) v zájmu přilákání bitcoinového a lidského kapitálu.

Návrat cenových signálů: Fiat je babylon, bitcoin je univerzální jazyk

Bitcoin Magazine, 3. 10. 2021

„Hospodin si řekl: ‚Hle, lid je zajedno a všichni mají jednu řeč. A toto je jen začátek jejich díla. Nic jim už nezabrání vykonat, cokoliv si předsevzali. Nuže, sestoupíme a zmateme tam jejich řeč, aby jeden nerozuměl řeči druhého.‘“

– Genesis 11:7

„Zvláštním úkolem ekonomie je lidem předvést, jak málo ve skutečnosti vědí o tom, co považují za vědomě zkonstruovatelné.“

– Friedrich Hayek

Cenový systém slouží ke vzájemné výměně informací. Nejlépe funguje, je-li postaven na celosvětově sdíleném neutrálním peněžním podkladu. Čím je společnost složitější, tím naléhavější je potřeba peněžního standardu, jenž nevnaší do ekonomických signálů šum.

Znalosti mají rády společnost

Jeden z nejvýznamnějších poznatků ekonomie je Hayekův výklad podstaty cen. V krátkém a čtivém článku *Využití znalostí ve společnosti*⁴⁰ Hayek vysvětluje, proč by bez existence cen neexistovala žádná směna – a ani komplexní společnost.

Moderní ekonomika generuje miliardy informačních signálů o preferencích lidí, ochotě investorů riskovat, vzácnosti zdrojů,

40 V českém prostředí je tento text dostupný například v knize *Osudná domyšlivost*.

podmínkách výroby zboží atd. Tyto poznatky musíme neustále sdílet, abychom mohli koordinovat své úsilí. Jak upozornil velký ekonom Leonard Read, žádná jednotlivá mysl neví, jak vyrobit i tak jednoduchou věc, jako je tužka.⁴¹ Ekonomická realita prochází neustálými změnami. Když ceny vznikají nerušeně a odrážejí realitu, tak můžeme nerušeně spolupracovat. Když je cenám bráněno ve volném vzniku nebo přizpůsobování – a tudíž již neodrážejí realitu – je naše schopnost spolupracovat omezena.

Jak říká Hayek, ceny odrážejí „znalost konkrétních okolností v daném čase a místě“. Proto dominantní „využití znalostí ve společnosti“ neprobíhá prostřednictvím knih, televizorů nebo učeben; je to právě cenový systém, který představuje hlavní síť výměny znalostí lidstva. A je úžasně efektivní.

Jednoduchý příklad. V Turecku se pěstuje přibližně 80 % světové produkce lískových oříšků. Představte si, že se v Turecku něco přihodí: občanská válka, lískooříškový mor, dopad meteoritu. Jak se zbytek světa dozví, že se něco stalo a že by se nyní měly používat vlašské ořechy nebo arašidy, kdykoliv je to možné? Výrobci, obchodníci a spotřebitelé se to nedozví z televize či z novin; nejdůležitější a nejrychlejší signál ohledně změny okolností jim podá prudce rostoucí cena lískových oříšků. Cena sděluje jen tu nejpodstatnější informaci: že lískových oříšků relativně k ostatním statkům ubylo. Nezáleží na tom, kde ve světě se lískové oříšky vyrábějí nebo co konkrétního se stalo, důležité je, že oříšky jsou nyní vzácnější, tím pádem i dražší a lidé jimi musí šetřit.

„Zkrácenou formou, prostřednictvím jakéhosi symbolu, se pouze nejpodstatnější informace předává dál, a to pouze těm, kteří o ni mají zájem.“

– Friedrich Hayek, *Využití znalostí ve společnosti*

41 Esej *Já, tužka* naleznete na stránkách Mises.cz.

Cenový systém je elegantně minimalistický způsob přenosu znalostí. Umožňuje nám globální spolupráci, i když nesdílíme společný jazyk, kulturu nebo světonázor; tyto faktory nemají na ekonomickou spolupráci téměř žádný vliv. Ceny jsou objektivním vodítkem v našem společném boji o přežití a prosperitu.

Existují miliardy kusých informací, které mohou být relevantní pro jakýkoliv výrobní proces, spotřebitelské rozhodnutí nebo investiční příležitost. Bez cen, které pro nás agregují a zprostředkovávají znalosti místních poměrů, bychom tápali ve tmě. A přesně tak i dopadly společnosti s uměle řízeným cenovým systémem: od Incké říše až po Sovětský svaz, ekonomiky bez přirozeného cenového mechanismu se vždy promění v otrokářské státy, v nichž stagnuje pokrok.

Zašuměné peníze

Již jsme zjistili, že aby ceny správně vyjadřovaly ekonomické signály, musí odrážet podkladovou ekonomickou realitu. Bohužel tomu stát často aktivně brání. O tom, do jaké míry ceny plní svou úlohu, rozhodují následující tři faktory: jak ceny vznikají, jak se ceny šíří a kvalita cenového nosiče (tj. peněz).

Jak ceny vznikají: Ceny musí vycházet ze soukromého vlastnictví, tj. soukromě kontrolovaných peněz a kapitálu, pozemků a budov, strojů a technologií. Kde je vlastnictví v soukromých rukou, tam je i motivace k jeho efektivnímu využívání, jelikož odměny za dobrá rozhodnutí i ztráty plynoucí z těch špatných připadají těm, kteří jsou k nim nejcitlivější. Na druhou stranu ochrana soukromých vlastníků před negativními dopady vlastních mylných rozhodnutí – jako je tomu v případě bailoutů nebo dotací – je zaručeným způsobem, jak ochromit cenový systém, protože ceny pak již neodrážejí riziko. Dobré zpracování tohoto takzvaného „morálního hazardu“ naleznete ve filmu *The Big Short*.



Ano, někteří dokáží takto zkorumpovaný systém včas shortovat a vydělat majlant, ale vy to nebudete – raději stackujte.

Jak se ceny šíří: I v případě, že ceny vznikají nerušeně na základě soukromého vlastnictví, regulace cen může tento signál zničit dříve, než se rozšíří. V průběhu 20. století byla jednou z četných forem potlačování cenových signálů regulace nájemného. Výsledky této cenové regulace dobře ilustruje populární vtip švédského ekonoma Assara Lindbecka, který její účinky přirovnal k bombardování měst. Zastropování výše nájemného vede k degradaci kapitálu: s cenami udržovanými pod jejich skutečnou tržní hodnotou se majitelům již nevyplatí opravovat a kultivovat svůj majetek.

Mnoho lidí je překvapeno, když se setkají s názorem, že manipulace s úrokovými sazbami ze strany centrálních bank je rovněž druh cenové regulace. Skutečnost je vskutku taková, že mezibankovní úroková sazba (na kterou se centrální banka obvykle zaměřuje) je druhem ceny a centrální banky dělají vše pro to, aby tuto cenu ovládaly až do nejmenšího detailu jednotlivých bazických bodů (1 bazický bod = 0,01 %).

Kvalita cenového nosiče: Ceny neexistují samy o sobě, vyjadřujeme je v peněžním nosiči. Povaha peněžní jednotky proto hraje rozhodující roli v tom, jak dobře může cenový systém plnit svou funkci.

Řekněme, že kilogram lískových oříšků stál dříve 10 dolarů, ale pak se cena zvýšila na 11 dolarů. Pokud k této změně došlo v tržní ekonomice bez jakéhokoliv státního zásahu, pak existují dvě potenciální příčiny růstu ceny: buď se snížila nabídka oříšků, nebo se zvýšila poptávka po oříšcích. Ať tak či onak, účastníky trhu detaily nijak zvláště nezajímají; hlavní je, že jim cena podává signál ohledně zvýšené vzácnosti lískových oříšků.

Pokud však samotné peníze nejsou neutrální, existuje třetí potenciální příčina růstu cen: zvýšení peněžní zásoby a následně rozmělnění kupní síly neboli inflace. Problém pak spočívá v tom, že ekonomická realita se nezměnila (oříšky jsou stále stejně vzácné), takže ceny by neměly šířit žádnou změnu signálu. V případě inflace je však cenový mechanismus narušen šumem a účastníci trhu přizpůsobují své chování, jako by signál byl skutečný.

Peníze s elastickou nabídkou (tj. takové, které lze libovolně vytvářet) jsou jako gumový metr: nic pořádně nezměří, jelikož jej lze donekonečna natahovat.

Aby ceny odrážely realitu, musí být peněžní nosič neutrální; dnešní fiat měny jsou ale všechno, jen ne neutrální. Jejich nabídka je řízena státním orgánem – centrální bankou – za účelem dosažení arbitrárně definovaného cíle, jako je míra inflace u úzkého výběru spotřebního zboží a služeb. Peněžní zásoba i těch nejstabilnějších fiat měn se každoročně zvyšuje o pět až dvacet procent, což do cenového systému vnáší značný chaos.

Je-li cenový systém elegantním systémem pro přenos čistého signálu, pak je fiatová měnová politika zákeřná rušička, která do ekonomiky zavádí generátor náhodných čísel. Není proto divu, že

měnová politika ovlivňuje doslova vše v naší společnosti: povahu našich pracovních míst, náš sklon ke spotřebě namísto vytváření úspor, dokonce i naši kulturu.⁴²

Narušení neutrality peněžního nosiče je mnohem závažnější než omezení soukromého vlastnictví nebo regulace cen, protože se jedná o globální jev. V současné době na světě obíhá přibližně 180 národních měn a všechny fungují na principu centrálně řízené měnové politiky.

Zatímco v přístupu k soukromému vlastnictví či cenové regulaci máme srovnání a můžeme analyzovat dopady různých politik, v případě cenového nosiče takové srovnání neexistuje. **Všude na světě obíhá centrálně plánovaný fiat, přičemž všechny fiat měny postupně spějí k hyperinflaci a rozdíl spočívá jen v časovém měřítku, v němž k ní dochází.**

Globální povaha fiatového standardu je patrně hlavním důvodem, proč problém neutrality peněz ignoruje většina dnešních ekonomů, kteří zpravidla trpí nedostatkem představivosti. V dnešní době je pro mnohé složité si představit peněžní prostředek, který není kontrolován státem; s takovou formou peněz jsme se koneckonců nesetkali již více než 50 let. Současnou peněžní realitu můžeme přirovnat k hypotetické situaci, kdy by před rokem 1989 na celém světě panoval komunismus. Neexistovalo by praktické srovnání s lepším uspořádáním, a tak by všichni danou situaci považovali za normální.

Když jsou peníze definovány jako „to, co nařizuje a spravuje stát“, pak bude samozřejmě za peníze uznáván pouze fiat. Z tohoto úhlu pohledu lze všechny problémy současných měnových systémů zdánlivě vyřešit zaváděním dalších a dalších experimentálních politik, jako je nekonečné kvantitativní uvolňování, intervence na mezibankovním trhu, záporné úrokové sazby, CBDC atd.

42 Dopady fiatů na současnou kulturu glosuje ekonom Saifedean Ammous v podcastu *The Bitcoin Standard Podcast* a také v knize *The Fiat Standard*.

Výsledek lidského jednání, nikoliv lidského záměru

„Cenový systém je toliko jednou z formací, které se člověk naučil využívat poté, co na ni narazil, aniž by jí porozuměl.“

– Friedrich Hayek

Cenový systém je výsledkem lidského jednání – milionů lidí využívajících svůj majetek a řídících se incentivy – nikoliv však výsledkem lidského záměru. Pokusy tento systém řídit selhávají, ať už mají podobu omezování soukromého vlastnictví, přímé kontroly cen nebo manipulace se samotnými penězi.

Je samozřejmě naivní věřit, že významná část lidstva pochopí význam cenového systému a bude jej bránit proti státním zásahům. Mnohem realističtější je vyhlídka, že lidé, kteří budou chtít chránit své soukromé zájmy, se z fiatového systému vymaní a zvolí bitcoin, neboť ten v průběhu let potvrdí svou roli spolehlivého uchovatele hodnoty a neutrálního platebního prostředku.

Bitcoin začne napravit cenový systém, jak bude dále postupovat jeho adopce z uchovatele hodnoty na prostředek směny. To může chvíli trvat, protože lidé budou mít vždy motivaci utracet raději fiat než bitcoin, dokud budou vydělávat mzdu ve fiat. Ale přesto k tomu dojde a lokální kolapsy fiat po světě budou následovány přirozenou bitcoinizací, která vyvrcholí globální hyperbitcoinizací.

Bitcoin jako neutrální peněžní médium umožní cenovému systému konečně nerušeně fungovat a stát se supravodivou informační dálnicí lidstva.

Poznatky z kapitoly

- Ceny jsou kriticky důležitý koordinační mechanismus, přenášejí signály o relativní vzácnosti všech statků v ekonomice.
- Pro správné fungování cen je zapotřebí, aby bylo podkladové médium, tedy peníze, neutrální.
- Fiatové peníze vnášejí do cen značný šum, jelikož nelze rozpoznat, zda změny cen vyplývají ze skutečných jevů v ekonomice či z manipulace s měnovou zásobou.
- Bitcoin je neutrální peněžní médium, jelikož jeho měnovou zásobu nelze libovolně a donekonečna nafukovat, a jeho měnová politika je dopředu známá.
- Rozšíří-li se bitcoin jako peněžní standard, dojde i k návratu skutečných cen přenášejících čisté signály odrážející ekonomické jevy.

Návrat úspor: Bitcoin jako konzervativní volba

BTC Times, 3. 4. 2022

Mainstreamoví komentátoři rádi vykreslují bitcoin jako hypervolatilní, spekulativní záležitost, se kterou může mít co do činění jen zdegenerovaný gambler. Investování na akciovém trhu je naopak zpravidla propagováno jako zodpovědné a konzervativní nakládání s penězi. Je tomu ale skutečně tak?

*„Popsat bitcoin pro široké publikum je zatraceně těžké.
Není nic, k čemu by se dal přirovnat.“*

– Satoshi Nakamoto

Cesta k pochopení bitcoinu je pro nováčky často náročná – jak Satoshi podotkl, je těžké jej k něčemu přirovnat. V některých ohledech se bitcoin podobá fenoménům, které již známe: hotovosti, zlatu, bankovním a platebním systémům, někteří jej dokonce připodobňují k elektrické baterii. Tato srovnání však plně nevystihují, proč je bitcoin tak zásadní. Domnívám se, že nejlepší charakteristika bitcoinu je, že se jedná o peníze. Bitcoin jsou peníze, které sice fungují na zcela nových principech (proof of work, kryptografie, uzly), jsou ale zároveň dokonale kompatibilní s odvěkými peněžními vlastnostmi (vzácnost, zaměnitelnost, trvanlivost, ověřitelnost a přenositelnost).

Teze, že bitcoin je novou iterací klasického pojetí peněz, se postupně stává přijatelnou i mimo úzkou skupinku zapálených bitcoinerů a stoupenců rakouské ekonomické školy. Ricardo Salinas Pliego (třetí nejbohatší muž Mexika), Ross Stevens (zakladatel NYDIG a zkušený investor) a společnost Fidelity (jeden z největších správců aktiv na světě) jsou jedni z mnoha významných osobností a institucí, kteří se v posledních letech veřejně přihlásili k pojmání bitcoinu jako peněžního instrumentu.

	 Durabilita	 Dělitelnost	 Zaměnitelnost	 Převoditelnost	 Ověřitelnost	 Vzácnost	 Lindy effect
 Zlato	+	-	+	-	-	+	+
 Bitcoin	+	+	+	+	+	+	-
 Fiat	-	+	-	+	-	-	-

Tabulku s obdobným srovnáním jednotlivých peněžních komodit naleznete ve studii *Bitcoin First: Why investors need to consider bitcoin separately from other digital assets*, publikováno na stránkách fidelitydigitalassets.com.

Investice, spekulace, úspory

Je-li bitcoin skutečně penězi, pak nelze v jeho kontextu mluvit o spekulaci či investici, nýbrž o úsporách.⁴⁴ Je důležité mezi těmito pojmy rozlišovat, protože každý z nich má jiný rizikový profil a mělo by se k nim přistupovat s jinými očekáváním.

	Investice	Spekulace	Úspory
Zdroj návratnosti	Cash flow	Růst ceny	Zachovaná či zvýšená kupní síla
Časový horizont	Dlouhý	Krátký	Dlouhý
Rizika	Riziko protistrany Riziko selhání záměru Riziko měnové politiky	Riziko protistrany Riziko selhání záměru Riziko měnové politiky	Zlehčování měny Měnová reforma
Příklady	Dividendové akcie Dluhopisy s pozitivním výnosem Nemovitost k pronájmu	Akcie bez dividend Dluhopisy s negativním výnosem Obchodování s nemovitostmi	Prasátko Rezerva na horší časy Zakopaný poklad Bitcoin v Trezoru

Investice je vložení peněz do záměru, od kterého očekáváme pozitivní peněžní toky. Investice s sebou zpravidla nese riziko protistrany (například akciové certifikáty obvykle nedržíte sami, ale u makléře) a riziko neúspěchu celého záměru. Zajímavé je, že i moderní vkladové účty jsou vlastně formou investice, protože peníze vložené do banky jsou okamžitě rozpůjčovány a my

⁴⁴ Uznávám rovněž, že i peníze mohou sloužit i ke spekulativním účelům, nicméně ve funkční ekonomice se zdravými penězi se jedná o okrajovou záležitost.

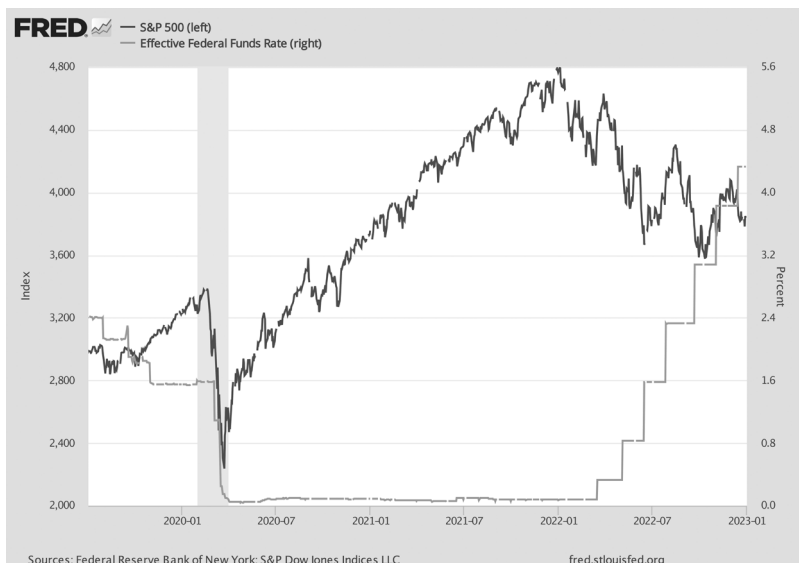
dostáváme část výnosu v podobě úroku (jakkoliv je dnes nepatrný a ani zdaleka nepokrývající cenovou inflaci).

Spekulace je vkládání peněz do projektů s očekáváním rychlého opětovného prodeje. Jediný očekávaný výnos plyne z krátkodobého růstu ceny nástroje. Mnoho dříve rozumných investičních příležitostí se prostřednictvím inflační měnové politiky postupně změnilo v čistou spekulaci: dluhopisy s nulovým nebo záporným výnosem, rychlé „otáčení“ nemovitostí, gambling s akciemi na platformách jako je Robinhood; to vše je důsledkem „financionalizace“ způsobené rychle rostoucí peněžní zásobou a dlouhým obdobím nulových úroků. Obchodování s „kryptem“ je rovněž čistou spekulací prováděnou v očekávání rychlých zisků.



Spekulace je velmi riskantní, protože je citlivá na měnící se nálady na trhu a rychlost tisku peněz; se spekulací se také pojí riziko protistrany – obchodníci s kryptoměнами obvykle potřebují držet coiny a tokeny na burze, aby mohli rychle reagovat. Ve srovnání s investováním nebo spořením je spekulace hrou s nulovým součtem, kde zisk jednoho člověka je ztrátou druhého.

Masivní tisk peněz (kdy mezi lety 2020 a 2022 bylo vytvořeno více než 40 % existujících dolarů) výrazně nafoukl ceny aktiv, takže fundamenty a očekávané peněžní toky již nehrají roli. Pro ceny aktiv jsou nyní důležité pouze kroky centrálních bank, investoři a spekulanti se namísto analýzy trhu a zdraví firem čím dál více zabývají odhadováním dalších opatření centrálních bankéřů. Proto i akcie velkých, ziskových korporací od přelomu let 2021/2022 zažily výrazný propad, který byl reakcí na restriktivní měnovou politiku Fedu:



Akciový index S&P 500 (levá osa) a referenční úroková sazba Federal Funds Rate (pravá osa). Zdroj: Fred.

Spoření znamená, že si odkládáme část výplaty na neurčitou dobu. Spoříme proto, abychom si uchovali nebo zvýšili kupní sílu. Uchování či zvýšení kupní síly nevyplývá z žádných peněžních toků a uspořené prostředky neprodáváme za jinou měnu; spoříme totiž přímo v penězích, které můžeme použít k přímému nákupu zboží a služeb.

Efektivně spořit bylo možné v době, kdy obíhaly zlaté a stříbrné mince. Až do první světové války mohli lidé držet své mince po celé generace, aniž by mince ztratily kupní sílu. Ba naopak, po průmyslové revoluci na konci 18. století se kupní síla peněz postupně zvyšovala, jelikož růst produktivity vedl k dlouhodobému snižování nákladů, rozšiřování nabídky statků na trhu a zvyšování jejich kvality.

Zdravé peníze a tradice konzervativního rodinného spoření padly za obět v první světové válce. Většina evropských zemí během války či krátce po ní opustila drahé kovy ve prospěch papíru, přičemž USA se zlatého standardu definitivně vzdaly až v roce 1971 (američtí občané nicméně měli zakázáno vlastnit zlato již od roku 1933).

Spoření v rámci současného fiatového standardu je nemožné, jelikož současné peníze jsou každý rok programově znehodnocovány. Pro ochranu kupní síly tak lidé hledají alternativní přístupy – zejména investice, které se však intenzivním tiskem peněz čím dál více proměňují ve spekulativní bláznovství.

Hodlování bitcoinu s cílem nikdy jej neprodat za fiat, nýbrž přímo utratit za zboží, služby a bydlení, se velmi podobá starému dobrému spoření.

Skutečný hodler nečeká na to, až prodá bitcoin za hromadu fiat; spíše ukládá současnou kupní sílu do zdravých peněz, za které v budoucnu uspokojí svou spotřebu.



Morpheus vysvětluje podstatu úspor.

Spoření: jedině do vlastního!

Šetrnost je další ze ctností, kterou si bitcoineři často osvojují. Mezi základní projevy šetrnosti v historii patřilo odkládání části příjmu pro zabezpečení v nejisté budoucnosti, výpomoc dětem při narození jejich prvních potomků, vybudování kapitálového polštáře pro rozjezd vlastního podnikání a podobně. O tradici úspor nás připravil současný peněžní systém, který šetrné trestá a rozhazovačné odměňuje.

Bitcoin je konzervativní volbou jak v „kryptosvětě“, tak stále více i v širším světě konvenčních financí. Investice a spekulace jsou rizikové činnosti, kterým by se měli věnovat zkušení specialisté, nikoliv běžní lidé snažící se vyjít s penězi. Obyčejní lidé by měli mít možnost ochránit svou kupní sílu a podstupovat při tom co nejmenší riziko; tak tomu bylo po stovky let, kdy stačilo, aby si rodina tu a tam odložila stříbrňák či zlaťák.

Bitcoin představuje návrat úspor. Mějme však na paměti, že bitcoinový protokol sice chrání vaše úspory před devalvací či

měnovou reformou, ale riziko protistrany si musí eliminovat každý sám za sebe. **Bitcoin vám skutečně patří jen tehdy, držíte-li jej ve vlastní peněženke.** Vzhledem k samosprávné podstatě bitcoinu máte nad svými penězi plnou kontrolu a značnou šanci, že vaše dlouhodobá kupní síla bude nejen zachována, ale i výrazně navýšena jako důsledek střetu protikladných měnových politik: fixního bitcoinu a vysoce inflačního fiat.

Poznátky z kapitoly

- V systému inflačních fiat peněz je prakticky nemožné spořit, i běžní lidé jsou nuceni investovat či spekulovat a podstupovat přitom nemalé riziko.
- Vlivem vysoce inflační fiatové měnové politiky se z mnohých investic stávají spekulace (kdy zhodnocení pochází namísto dlouhodobého cashflow z krátkodobého vypumpování ceny).
- Pravidelné odkládání do bitcoinu není ani investice, ani spekulace; jedná se o spoření.
- Spoření znamená, že si odkládáme peněžní jednotky pro použití v budoucnosti, a to s vyhlídkou dlouhodobého udržení kupní síly a bez rizika protistrany; ukládání fiatové měny v bance proto není spoření (fiat je programově znehodnocován a vklad v bance s sebou nese riziko protistrany).
- Při spoření nepředpokládáme, že v budoucnu bitcoin směníme za fiat; bitcoin budeme přímo utrácet za zboží a služby.

Návrat zdravých peněz: Svět po hyperbitcoinizaci

BTC Times, 17. 2. 2022

„Hyperbitcoinizace je dobrovolný přechod od podřadných peněz k lepším penězům...

...Hyperbitcoinizaci by mělo doprovázet rychlé zvýšení produktivity a bohatství...

...Hyperbitcoinizace bude pravděpodobně pro všechny zmatečným obdobím, něco jako druhá puberta. Jakmile však proběhne, nikdo si nebude umět představit, jak jsme mohli žít v předchozím systému. “

– Daniel Krawisz, *Hyperbitcoinization*⁴⁵

Hyperbitcoinizace je v bitcoinových kruzích již zažitý termín – poprvé ho v roce 2014 použil Daniel Krawisz (zakladatel Nakamoto Institute)⁴⁶ a toto téma je od oné doby podnětem mnoha intelektuálních spekulací. Hyperbitcoinizace je proces nahrazování fiatové měny bitcoinem. Krawisz tvrdí, že jakmile proces hyperbitcoinizace začne, pak, obdobně jako u hyperinflace, jej již nebude možné zastavit a události naberou rychlý spád.

Tento text nerozebírá pravděpodobnost scénáře hyperbitcoinizace. Na téma cesty k hyperbitcoinizaci doporučuji následující články:

⁴⁵ Daniel Krawisz: *Hyperbitcoinization*, vyšlo 29. 3. 2014 na nakamotoinstitute.org.

⁴⁶ Osobní příběh Daniela Krawisze je pozoruhodný: ačkoli se zdá, že bitcoin velmi dobře chápal již v počátečních letech a jím založený Nakamoto Institute je dodnes jedním z nejhodnotnějších zdrojů ke studiu bitcoinu, po roce 2017 se Krawisz přidal ke kultu Craiga Wrighta alias „Faketoshiho“ a nyní je zapáleným zastáncem shitcoinu BSV. Hodnotu dřívějších Krawiszových myšlenek však tento podivuhodný vývoj podle mého názoru nesnižuje.

- *The Roads to Hyperbitcoinization* od Fulgur ventures a Alexandra Bussutila⁴⁷
- *Game Theory in Bitcoin: The Dominoes Have Begun to Fall* od Williama Clementa III⁴⁸
- *On Hyperbitcoinization* od Richarda Johnsona⁴⁹

V našem pojednání přeskočíme proces hyperbitcoinizace, místo toho si rozebereme její pravděpodobné dopady. Pro lepší stravitelnost rozdělují její dopady do dvou epoch:

Krátké období: počátky hyperbitcoinizace, kdy pouze několik zemí oficiálně přijalo bitcoin jako své zákonné platidlo. Chápající jednotlivci a jejich komunity již žijí v bitcoinovém standardu (v bitcoinu si spoří, částečně či úplně v něm provádějí transakce). Domnívám se, že v současnosti stojíme na prahu této epochy.

Dlouhé období: naprostá většina světa je již hyperbitcoinizovaná, fiat se stává kuriózní historickou poznámkou pod čarou, na planetě možná živoří pár zaostalých národů, které fiat stále využívají.⁵⁰

Krátkodobé dopady hyperbitcoinizace

Trvalo dvanáct let, než první stát oficiálně nastoupil cestu hyperbitcoinizace. Poté trvalo rok, než se k první zemi (Salvadoru) připojila druhá (Středoafriická republika). Třetí bude patrně záhy následovat. Pak již asi přestaneme počítat, protože malé země, nemajíce co ztratit⁵¹, se v obavách, že opět zůstanou pozadu, rychle připojí.

47 Vyšlo 22. 10. 2021 na bitcoinmagazine.org.

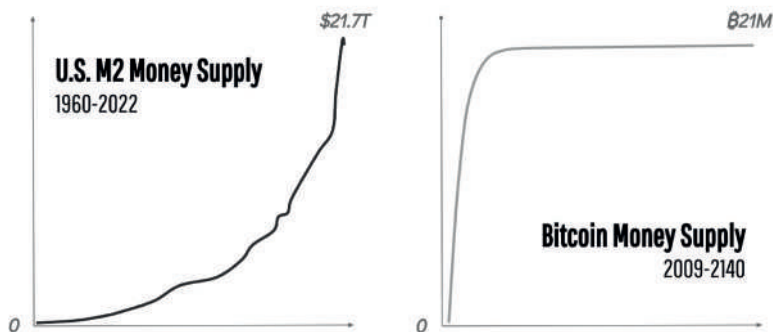
48 Vyšlo 27. 2. 2021 na bitrawr.com.

49 Vyšlo 13. 6. 2021 na hwessays.com.

50 Jsem přitom toho názoru, že „neprivilegované“ země globálního jihu promění svou dosavadní nevýhodu ve výhodu a budou jedny z prvních, kde hyperbitcoinizace proběhne. Naopak Spojené státy, Británie, Japonsko, Čína a země eurozóny se budou snažit držet fiat u co nejdéle.

51 Nemají co ztratit ve smyslu monetární suverenity a Cantillonova efektu, jelikož si vlastní fiat netvoří. El Salvador byl před přijetím bitcoinu dolarizovanou zemí, Středoafriická republika je nucena používat CFA frank, kterým Francie dodnes vykořisťuje čtrnáct svých „bývalých“ kolonií. Vedle Středoafriické republiky se jedná o: Benín, Burkínú Faso, Guineu-Bissau, Pobřeží slonoviny, Mali, Niger, Senegal, Togo, Čad, Gabon, Kamerun, Konžskou republiku a Rovníkovou Guineu.

Prvním významným důsledkem hyperbitcoinizace tak bude **nová forma měnové substitute**: namísto *dolarizace* 20. století budeme v 21. století svědky *bitcoinizace*, která postupně zachvátí celý svět. V doprovodu tohoto fenoménu budou fiat měny rychle ztrácet důvěru – a to jak obskurní malé měny, jako je libanonská libra (v posledních letech procházející hyperinflací a kolapsem důvěry), tak i majoritní měny včetně amerického dolaru, jenž na konci tohoto procesu přijde o své výsadní postavení zdánlivě nejbezpečnější měny světa. Dolar tento status ztratí následkem dvou vzájemně se posilujících faktorů: měnové politiky permanentní inflace fiatů a čím dál zjevnější role bitcoinu coby záchranného člunu, plynoucí z přesně opačné měnové politiky, než jakou má dolar.



Druhým významným důsledkem této éry bude **ztráta peněžní přírážky u investičních nástrojů**, jež v současnosti suplují funkci uchovatele hodnoty, kterou fiat peníze postrádají. Zlato, nemovitosti, dluhopisy, akcie – tyto nástroje mají v ekonomice zajisté své využití, ale jakmile se ocitneme pod zdravým peněžním standardem, nebudou zapotřebí jako uchovatelé hodnoty. Zde je stručné nastínění toho, jaké nevýhody mají tyto nástroje oproti bitcoinu:

Zlato: má své využití v elektronice, průmyslu a šperkařství; má silný *Lindy effect*, ale ve srovnání s bitcoinem má horší peněžní vlastnosti. Nelze jej teleportovat po celém světě, vyžaduje důvěryhodné třetí

strany pro transakce, pro ověřování pravosti a pro bezpečnou úschovu při vlastnictví většího množství.

Nemovitosti: v současnosti notně těží z Cantillonova efektu (který v hyperbitcoinizovaném světě nebude existovat). Nemovitosti jsou nejnáze zdanitelný a konfiskovatelný typ majetku⁵², v případě nejistoty na trhu jsou nelikvidní, jejich hodnota je silně závislá na měnové politice, jurisdikci a politikaření ve formě územního plánování.

Dluhopisy: v podstatě již vyhořelý nástroj, který se stal obětí měnové politiky státu: s reálnými výnosy hluboko pod inflací neexistuje racionální důvod, proč držet dluhopisy dlouhodobě. Z klasického investičního nástroje se stal nástroj spekulativní, jelikož dluhopisy nyní drží jen ti, kteří spekulují na krátkodobé cenové pohyby. A pak samozřejmě ti, kdo mají povinnost dluhopisy držet (finanční instituce, penzijní fondy, apod.).

„Naučte se počítat a pak prodejte dluhopisy a raději nakupujte bitcoin.“

– Greg Foss v podcastu *Bitcoin Bottom Line*⁵³

Akcie: jsou v dnešní době značně provázané s působením Cantillonova efektu. Jak jsme si nastínili v předešlé kapitole, v dnešní ekonomice akcie rostou, když centrální banky drží úrokové sazby uměle nízko. Ukončení Cantillonova efektu v důsledku vypaření důvěryhodnosti a hodnoty fiat měn přiblíží akcie jejich skutečnému tržnímu ocenění a namísto dnešních derivátů závislých na rozhodnutí centrálních bank se opět stanou investicí do produktivních firem. Dlouhodobě by akcie měly generovat zisky vyšší než zhodnocení peněžní jednotky, a to s odpovídajícím rizikem

52 Ve Spojených státech činí daň z nemovitosti v průměru 1 % ročně z tržní hodnoty. To znamená, že pokud vlastníte dům v hodnotě 10 milionů korun, musíte státu odvést 100 tisíc korun ročně – jen za to, že žijete ve vlastním domě. S rostoucími cenami nemovitostí výše daně adekvátně roste.

53 Greg Foss je kanadský obchodník s více než 30 lety praxe na dluhových trzích

a bez příslibu státní záchrany ve formě levných úvěrů a výkupních programů centrální banky. Investice do akciových trhů nebudou v hyperbitcoinizovaném světě dominantním způsobem ochrany kupní síly; tou budou prosté úspory, které mají v ekonomice se zdravými penězi prakticky nulové riziko.

Žádný z těchto nástrojů tudíž nezanikne, pouze přestanou plnit roli uchovatele hodnoty, která se navrátí zdravým penězům – bitcoinu. Bitcoin nad těmito nástroji vítězí, protože není závislý na žádné konkrétní jurisdikci nebo státní autoritě, lze jej ověřovat a chránit nezávisle na veřejných či soukromých institucích a pro dlouhodobé zvyšování hodnoty nespolehá na Cantillonův efekt, nýbrž na prostou nabídku a poptávku po penězích a jejich funkcích.

Dlouhodobé dopady hyperbitcoinizace

Ukončení experimentu s fiat měnami přinese do naší společnosti obrovské změny. Ve světě, kde se „DCA“ nazývá jednoduše *spoření* a platba bitcoinem je všední záležitost, můžeme očekávat následující vývoj.

Konec cenové inflace. Měnová politika fiat měn je nutně politikou trvalé inflace – peníze se vytvářejí stále rychleji a ceny neustále rostou, přestože růst produktivity v důsledku technologického rozvoje by měl náklady a ceny naopak snižovat. S pevnou peněžní zásobou dojde k růstové deflaci a kupní síla našich peněz se bude v průběhu času postupně zvyšovat. To však nevyvolá „deflační spirálu“, stejně jako jsme nikdy nezaznamenali deflační krizi v odvětvích s dlouhodobým růstem produktivity – naopak firmy vyrábějící počítače a mobilní telefony o stále vyšším výkonu za stále nižší ceny jsou jedny z nejlépe prosperujících.⁵⁴ Cenová deflace je známka prosperující společnosti.

⁵⁴ Pokud vás zajímá podstata růstové deflace a proč je snaha o její zamezení zcela absurdní, doporučuji knihu Jeffa Boothy *The Price of Tomorrow: Why Deflation is the Key to an Abundant Future*, 2020.



Konec investičních bublin. Co mají všechny velké investiční bubliny v historii společného? Tisk peněz a levné úvěry. Jihomořská bublina, Panika roku 1819, bouřlivá dvacátá léta, Dot Com bublina, krize subprime hypoték – všechny tyto bubliny byly nafouknuty s pomocí uměle levných úvěrů a často i přímým zapojením vlády a/nebo centrální banky. Mylné investice a krachující podniky budou samozřejmě existovat i v éře zdravých peněz, ale jejich eskapády už nepřerostou do krizí ohrožujících celou ekonomiku, protože všechny ztráty budou muset nést samotní investoři a měnová politika nebude nafukovat mylné investice až do absurdních rozměrů vyžadujících následně záchranné balíčky ve formě tisku dalších peněz.

Konec výrazného hospodářského cyklu. Založení Fedu v roce 1913 předcházela propagandistická kampaň volající po měnové autoritě, jež by ukončila cyklickou povahu ekonomiky.⁵⁵ Ve skutečnosti se stal pravý opak a od vzniku Fedu se výrazný hospodářský cyklus stal nedílnou součástí našich ekonomik. Je to proto, že právě

⁵⁵ Více o okolnostech vzniku Fedu najdete ve skvělé knize G. Edwarda Griffina: *The Creature from Jekyll Island: A Second Look at the Federal Reserve* (2010).

zásahy centrálních bank do peněžní zásoby a úrokových sazeb jsou příčinou silného cyklu, jak již více než sto let argumentují stoupenci rakouské ekonomické školy.⁵⁶

Během 109 let od vzniku Fedu došlo ve Spojených státech k 20 recesím. K těm sice může docházet i v prostředí zdravých peněz, ale bez centrálních bank a vládních zásahů by hospodářské propady rychle skončily tržní realokací kapitálu a pracovních sil a brzy by se na ně zapomnělo. Tedy stejně jako tomu bylo ve Spojených státech na počátku 20. let, kdy došlo k rychlému pročištění trhu, a na tuto recesi si dnes již nikdo nevzpomene – na rozdíl od velké deprese z let 1929–1939, kdy Rooseveltova administrativa nastoupila cestu centrálního plánování a depresi tím značně prodloužila.⁵⁷

Menší očištné korekce jsou prospěšné, jejich potlačování vede pouze k nafouknutí problému a vyšší oscilaci ekonomiky jak v horní, tak spodní fázi cyklu. Jak vysvětlují Aleks Svetski a Mark Moss v knize *UnCommunist Manifesto*:

„Podobně jako jsou malé, pravidelně se opakující lesní požáry nezbytné k tomu, aby se zabránilo rozsáhlým katastrofickým lesním požárům, jaké se vyskytují jednou za desetiletí a které mohou zničit svrchní vrstvu půdy, i výrobní cykly mají přirozeně své korekce.

Můžeme je nazývat krizemi, ale jedná se o cenné signály trhu o krátkodobé nadprodukci. Můžeme je přirovnat k drobným lesním požárům, které jsou pro zachování integrity komplexního systému zapotřebí.

Bez kontinuálních korekcí, bez nezbytné zpětné vazby může nadprodukce nebo podprodukce bujet tak dlouho, dokud se společnost nezhroutí nebo nedojde k vyčerpání zdrojů. O tom jsme se již nesčetněkrát mohli přesvědčit v centrálně plánovaných zemích po celém světě.“⁵⁸

56 Detailní, přitom velmi srozumitelný výklad tzv. rakouské teorie hospodářských cyklů, sepsal před lety pro stránky Mises.cz autor Jan Mašek – googlujte „Jan Mašek: Rakouská teorie hospodářských cyklů“.

57 Zmiňované recese a vliv vlády na jejich průběh analyzuje Murray Rothbard v knize *America's Great Depression* (1963), dostupné v e-book formátech na Mises.org.

58 Aleksandar Svetski, Mark Moss: *The UnCommunist Manifesto. A Message of Hope, Responsibility, and Liberty for All*, 2022.

Vymizení Cantillonova efektu. Tvorba peněz ve fiat systému neobnáší téměř žádné přímé náklady. Stát a finanční sektor – tedy ti, kteří jsou peněžním kohoutkům nejbližší – jsou prvními příjemci nových peněz, obvykle prostřednictvím úvěrů s velmi výhodnými sazbami. Jak první příjemci nové peníze utrácejí, dochází k nafukování cen a růstu hodnoty aktiv, čímž se zboží a aktiva stávají méně dostupnými pro všechny ostatní. Cantillonův efekt je velmi zákeřným způsobem přerozdělování bohatství od produktivních vrstev k těm neproduktivním: znehodnocuje reálné mzdy a tržby, eroduje úspory a odčerpává kupní sílu ve prospěch monetárních parazitů.

Bitcoin brání vzniku Cantillonova efektu, protože těžaři musí vynakládat reálné prostředky na vydávání nových peněžních jednotek; nemohou měnit monetární politiku bitcoinu ve prospěch sebe a spřátelených zájmových skupin. Bez fiatů Cantillonův efekt zanikne a moc státu a finančního sektoru adekvátně klesne.

Eliminace forexových fríkcí. Na světě obíhá 180 měn. Transakční náklady vyplývající z tohoto měnového babylonu jsou tak obrovské, že devizový trh je označován za největší trh na světě s ročním objemem kolem 2,4 biliardy dolarů – přitom tento trh před sto lety ani neexistoval! Nutnost neustále směňovat mezi jednotlivými měnami při zahraničním obchodu a cestování přináší obrovské náklady a nemalá rizika (která lze zmírnit zajištěním s pomocí měnových derivátů, jež s sebou však nesou další náklady).

V předfiatové éře rovněž existovalo mnoho měn, ale pouze jedny peníze: zlato, potažmo stříbro. V rámci zlatého standardu se směnné kurzy mezi národními měnami, jako byly dolary a marky, odvíjely od vzájemného poměru obsahu zlata a stříbra v daných měnových jednotkách. Potřeba devizových trhů vznikla teprve tehdy, když v průběhu 20. století vznikl čistý fiat s „volně plovoucími“ kurzy, které vesměs odrážejí různé tempo devalvace fiatových měn. Jak ve

svých textech popisují Parker Lewis⁵⁹ či Oleg Andreev⁶⁰, v průběhu historie můžeme pozorovat konvergenci k jedinému peněžnímu standardu. Hyperbitcoinizace ukončí současný chaos a navrátí řád globálního standardu, čímž dojde k odbourání masivní mrtvé váhy forexových trhů.

Zmenšení role státu. Fiat umožnil, že se téměř ze všech států světa postupně staly chroničtí dlužníci, utrácající každý rok více, než kolik vyberou na daních. Jedná se o důsledek Cantillonova efektu a trvalé poptávky po státních dluhopisech.⁶¹ Za posledních 50 let byl rozpočet USA přebytkový pouze pětkrát a americký státní dluh nedávno překročil 30 bilionů dolarů. V roce 2000 činil americký dluh 55 % HDP, v roce 2022 to bylo 125 %. Katastrofální rozsah světových válek 20. století byl přímým důsledkem snadné tvorby peněz – v předchozích konfliktech se vlády musely uchýlit k nepopulárnímu zdanění, zatímco po roce 1913 tiskařské stroje elegantně a nepozorovaně vysály kupní sílu občanů. Není ani náhoda, že dvacáté století bylo érou totalitních režimů, neboť moc státu byla kvůli tiskárnám na peníze posílena až na úroveň všemocného otrokáře. Koneckonců byl to Lenin, kdo prohlásil, že pro zničení kapitalismu stačí pouze zničit měnu. Bez inflační daně a možnosti nekonečného zadlužování by stát mnohem obtížněji ospravedlňoval své přebujelé výdaje, protože každý vydaný satoshi by musel být ukraden přímo z kapes produktivních jedinců a firem.

Celospolečenské snížení časových preferencí. Časová preference vyjadřuje, jak moc upřednostňujeme uspokojení potřeb v přítomnosti oproti budoucnosti. Lidé a společnosti s vysokými časovými preferencemi se zaměřují na uspokojování současných potřeb, zatímco lidé a společnosti s nízkými časovými preferencemi

59 Parker Lewis: *Bitcoin Obsoletes All Other Money*, 24. 1. 2020, dostupné na nakamotoinstitute.org.

60 Oleg Andreev: *Vesmír chce jedny peníze*, 28. 6. 2013, dostupné na bitperia.cz.

61 Přičemž trvalá poptávka po státních dluhopisech vyplývá ze tří hlavních faktorů: zaprvé, finanční společnosti jako banky a penzijní fondy mají zpravidla povinnost státní dluhopisy držet. Zadruhé, stát má moc okrádat produktivní sektory ekonomiky prostřednictvím daní, je proto považován za velice spolehlivého dlužníka, jelikož si na splátky dluhu může na rozdíl od ostatních ekonomických aktérů jednoduše nakrást. Zatřetí, při propadu poptávky finančních trhů po státních dluhopisech vykupuje státní dluhopisy centrální banka za nově vytvořené fiat peníze.

se vzdávají současného uspokojení ve prospěch vyšší budoucí prosperity. Trvalá inflace v prostředí fiatových peněz zvyšuje časové preference, jelikož jsme okolnostmi hnáni k tomu utratit své peníze dříve, než ztratí svou kupní sílu – a ideálně se ještě zadlužit, jelikož dluhy naopak s časem ztratí svou váhu.

Extrémní příklad vysokých časových preferencí je pak jednání v prostředí hyperinflace, kdy lidé přemýšlejí v horizontu nejvýše několika dní, jelikož v delším období nemají peníze – a tím i v penězích uložené lidské úsilí – žádnou hodnotu.

U zdravých peněz se kupní síla v čase zvyšuje, což vede ke snížení časových preferencí. Rakouský ekonom Hans-Hermann Hoppe popisuje nízkou časovou preferenci jako „civilizační proces“⁶² a je pravda, že zdravé peníze korelují s orientací společnosti na budoucnost: vrcholné civilizace jako Římská republika, Byzantská říše, Benátská republika, Florentská republika, Britské impérium byly vybudovány na základech zdravých peněz – a naopak jakmile se vydaly cestou znehodnocování peněz, velmi rychle došlo k jejich zániku. Bitcoin jako globální peněžní standard má potenciál přeorientovat naše zaměření z přítomnosti na budoucnost, a to v dosud nevídaném měřítku.⁶³

Od dluhové ekonomiky k ekonomice úspor. Současný peněžní systém je založený na dluhu: peníze vznikají prostřednictvím nových úvěrů, manipulace s úrokovými sazbami motivuje ke stále hlubšímu zadlužování, trvalá inflace odrazuje od spoření peněz a napomáhá dlužníkům erodit reálné hodnoty jejich závazků. Ačkoliv fiatoví ekonomové tvrdí, že jen na těchto základech může ekonomika fungovat, při analýze lidského jednání a dělby práce nenalezneme k takovým domněnkám žádný důvod. Ano, investice

62 Hoppe: *Democracy, The God That Failed*, 2001.

63 Někteří bitcoineři jdou dokonce tak daleko, že považují vynález bitcoinu za nutný předpoklad rozvoje na další civilizační stupeň na Kardašovově škále. Zajímá-li vás spekulativní sci-fi s oranžovým nádechem, doporučuji článek Aleksandara Svetskiho *Bitcoin and the Great Filter*, který vyšel 2. 6. 2022 na Bitcoin Magazine.

vyžadují kapitál; ten však ani zdaleka nemusí být vypůjčený. Kapitál vzniká v prvé řadě akumulací, tj. úsporami a odkládáním spotřeby. Vytváření peněz z ničeho naopak kapitál eroduje.⁶⁴

Za zmínku zde stojí také skutečnost, že největší půjčkou v životě většiny lidí je dnes hypotéka neboli půjčka na nemovitosti, které jsou kvůli své současné roli náhradního uchovatele hodnoty značně nafouknuté.

V hyperbitcoinizovaném světě by došlo k vyfouknutí nemovitostní bubliny a zároveň by docházelo k pozvolnému zvyšování kupní síly úspor v průběhu času. Nemovitosti poptávané pouze pro svůj primární účel – bydlení a prostor pro podnikatelské aktivity – by se tak staly mnohem dostupnější bez nutnosti celoživotního zadlužení.

Nebude to snadné

Jak jsme načrtli v kapitole *Návrat konfiskací*, cesta k hyperbitcoinizaci nebude hladká a establishment bude svůj monopol za každou cenu bránit. Čekají nás lživé kampaně⁶⁵, konfiskace a neférové zdanění, všudypřítomný dohled a pokusy o ovládnutí bitcoinového ekosystému regulátory. Pokud chceme dospět k hyperbitcoinizaci bez úhony, musíme používat bitcoin v maximální míře bez prostředníků. Trezor, BTC Pay Server, Vexl, Muun, Phoenix a mnoho dalších open-source nástrojů máme volně k dispozici; použijme je a vyhýbejme se centralizovaným pastem, jako jsou KYC burzy a instituce slibující výnos z vašich bitcoinů.

Zaujmete-li nyní maximálně obezřetný a konzervativní přístup ke svému bitcoinu, budete moci na stará kolena s úsměvem vzpomínat na divoké a vzrušující počátky hyperbitcoinizace.

64 O tom, že současný systém není kapitalismus a akumulaci kapitálu nepodporuje, nýbrž jí naopak zamezuje, pojednává skvěle Allen Farrington v knize *Bitcoin is Venice* (2022), zejména v kapitole *The Capital Strip Mine*. K přečtení i na Farringtonově blogu na stránkách medium.com.

65 Aktuálním příkladem takové kampaně je Change the Code organizace Greenpeace, která nabádá ke změně bitcoinového konsensu na proof of stake. Kampaň je financovaná společností Ripple, která stojí za shitcoinem XRP a usiluje o spolupráci s centrálními bankami na zavedení CBDC.



Poznatky z kapitoly

- Hyperbitcoinizace je proces, na jehož konci se bitcoin stane globálním peněžním standardem; jedná se o návrat zdravých peněz, podobající se dřívějšímu celosvětovému zlatému standardu.
- Instrumenty, které dnes plní zástupnou roli uchovatele hodnoty (zlato, nemovitosti, dluhopisy, akcie), v průběhu hyperbitcoinizace nezaniknou, přestanou však být ceněny jako náhrada úspor.
- Ve světě po hyperbitcoinizaci nebude existovat Cantillonův efekt, což povede k výraznému zmenšení role státu; v ekonomice zdravých peněz s fixní zásobou a bez manipulace s úrokovými sazbami rovněž vymizí neustálý růst cen a cyklické investiční bubliny střídající se s recesemi.
- Dalšími pozitivními důsledky budou eliminace forexových trhů, přeorientování společnosti na budoucnost a zejména přechod od dluhové ekonomiky k ekonomice úspor.
- Stát si bude svůj monopol chránit, proto je zapotřebí vždy mít bitcoin pod vlastní kontrolou.

Návrat pokory: Libertariáni vs. sociální inženýři

Finmag, 25. 9. 2013

Politické filozofii libertarianismu se dostalo v pokrizové dekádě nevídaného zájmu, a to jak mezi novými příznivci, tak i nelítostnými kritiky. Kde byly libertariánské postoje dříve zcela ignorovány, tam jsou dnes zesměšňovány a vláčeny blátem. Na tom by nebylo ani tak nic špatného – na poli myšlenek neexistuje nic jako špatná publicita; jen myšlenky, o kterých se mluví, jsou skutečně živé. Mnozí z kritiků však tuto filozofii zjevně nechápou, ačkoliv její základ je velice jednoduchý. Pojďme si jej osvětlit.

Zeptáte-li se typického libertariána na to, proč přijal za svou filozofii svobody, pravděpodobně si vyslechnete přednášku o ekonomické efektivnosti tržního uspořádání, o přirozeném právu na svobodu každého jedince či o banalitě zla úředního aparátu. Ačkoliv jsou všechna tato témata nedělitelnou součástí libertarianismu, jeho podstata leží v něčem jiném. Základním stavebním kamenem libertarianismu je především pokora. Pokora tváří v tvář složitosti lidské společnosti.

Palčivé otázky a nejisté odpovědi

Jakými penězi by měli lidé platit? Jak nejlépe vzdělávat děti? Jak se nejlépe připravit na penzi? Kde má sociální inženýr jasno, libertarián upřímně odpoví, že neví; chápe totiž, že tisíce a miliony vzájemně nezávislých jedinců přijdou na všestranně nejvhodnější řešení rychleji a za nižších nákladů než úzká skupinka vládních expertů. Existuje koneckonců na položené dotazy jediná správná odpověď?

Paradoxní je, že kritici libertariánům často vytýkají, že vidí svět černobíle a že nabízejí jednoduché až primitivní recepty na neduhy dnešní doby. „Pro vás je to jen samá privatizace a deregulace, neznáte snad jiná řešení? Komplexní problémy si žádají komplexní přístupy, například v podobě partnerství veřejného a soukromého sektoru,“ argumentují zdánlivě rozumně. Při potyčce s problémem

však není zrádnějšího řešení než některé způsoby jeho řešení předem vyloučit. Libertariánský přístup spočívá v ponechání otevřených možností – již zmíněná privatizace a deregulace totiž neznamená nic jiného než uvolnění dříve svázaných rukou řešitelů všemožných problémů.

Snaha o organizaci společnosti „shora“ je odsouzena k selhání právě v důsledku neuchopitelné složitosti. Dílčí selhání obdobných snah můžeme pozorovat v podobě takzvaných neočekávaných důsledků – vyšší nezaměstnanost vlivem regulace pracovního trhu, kriminalita spojená s drogovou prohibicí či nafukování investičních bublin jako důsledek monetární politiky.

Předlistopadová éra nás poučila o problémech plynoucích z centrálního plánování spotřebního zboží, jako jsou chronický nedostatek a nízká kvalita. Záhadou ovšem zůstává, proč jsou někteří stále přesvědčeni, že v jiných oblastech – a to oblastech mnohem důležitějších a složitějších – tento způsob organizace funguje a fungovat může, ba dokonce musí. Centrální plánování selhává, ať je jeho cílem výroba bot, pravidel či peněz. Nesehává proto, že by byl prováděn špatnými lidmi či na základě špatných motivací, nýbrž proto, že potlačuje informace v podobě tržních signálů, které jsou k racionálnímu rozhodování klíčovým prvkem. Ludwig von Mises trefně označil systém státních intervencí jako „plánovaný chaos“; ničím jiným nebyl v době Sovětského svazu – a není ani v době Evropské unie.

Pošetilost mocných

Politici, centrální bankéři a vysocí úředníci pokorou rozhodně netrpí. Čím dál intenzivnější snaha o regulaci každého aspektu společenského uspořádání svědčí o jejich pošetilé domýšlivosti, kterou neotrásly ani cyklické krize způsobené jejich manipulacemi.



Ve slovnících mocných byla pokora nahrazena expertními komisemi, analýzami, statistikami a „dynamickými stochastickými modely všeobecné rovnováhy“. Snaží se přesvědčit sami sebe i všechny okolo, že s moderními metodami je centrální plánování uskutečnitelné; a ačkoliv reálné výsledky svého snažení zlepšit nedokážou, zdání o své důležitosti se jim daří budovat skvěle. Jejich úspěch v této druhé kategorii je koneckonců pochopitelný – důvěra v abstraktní řád „neviditelné ruky trhu“ je mnohem méně intuitivní než uspokojivá jistota ztělesněná konkrétními jedinci a institucemi majícími řešení společenských problémů v popisu práce.

Absence pokory představuje v kombinaci s mocí zbraň hromadného ničení. Jen během krátkého období posledních sta let bylo lidstvo několiknásobným svědkem katastrofy, která nastane, když ve svých rukou nahromadí moc jedinec či úzká elita přesvědčená o svém oprávnění řídit životy druhých.

Společnost dvacátého prvního století je bezpochyby tou nejsložitější v historii lidstva. Nikdy dříve nebyl svět tak malý ve smyslu vzdáleností a komunikačních možností a zároveň tak velký ve smyslu neomezených příležitostí ke vzájemnému obchodnímu, kulturnímu a informačnímu obohacení. Nikdy dříve nebyla společnost tak křehká a nikdy nevyžadovala tolik pokory jako dnes.

Poznatky z kapitoly

- Libertarianismus je politická filosofie vycházející z teze, že lidé jsou schopni spolu uspokojivě vycházet bez státního donucení a že není možné pojmout komplexitu společnosti v socialistických plánovacích výborech.
- Pravým opakem libertarianismu je sociální inženýrství zastávající pozici, že společnost musí být centrálně řízena.
- Sociální inženýrství se vyznačuje zpupností; libertariánství se vyznačuje pokorou před společenskou komplexitou.
- Čím více je společnost komplexní, tím větší škodu mohou mocenské zásahy napáchat.

DOSLOV

*„Stay humble and stack sats“
(Budte skromní a štosujte saty)*

– Matt Odell

Bitcoin mění svět. Nemění jej však nějakým abstraktním, neviditelným způsobem; bitcoin mění svět prostřednictvím lidí, kteří bitcoin používají. Staré moudro praví, že nikdo nedokáže změnit bitcoin, ba naopak bitcoin mění každého, kdo s ním pracuje, přemýšlí o něm či jej prostě drží ve své peněžence. Bitcoin mění nás. A mění nás výrazně k lepšímu.

Fiat je experiment, jenž zcela selhal. Produktivita, úspory, dlouhý rozhodovací horizont, funkční ekonomika a racionální optimismus – to jsou prvky, které jsou v současnosti na ústupu, jelikož jsou v nesouladu s fiatovými penězi. S pomocí bitcoinu se k nim však můžeme rychle vrátit – zpočátku jako jedinci, postupně jako celá společnost.

Návrat zdravých peněz je sice možná na spadnutí, není však samozřejmý. Je jen na nás, zda a jak rychle k němu dojde, za jakých okolností a jaký dopad bude mít na konkrétní jedince a jejich rodiny. Pro plné využití potenciálu bitcoinu v osobním životě je zapotřebí k němu přistupovat konzervativně: dbát na soukromí, kontrolovat vlastní klíče, chápat jej jako průběžné a dlouhodobé úspory, vzdělávat sebe a ostatní. Doufám, že tato kniha přispěla k tomu, aby se takový přístup k bitcoinu stal pro ctěného čtenáře přirozenou součástí života.

Mé další knihy, podcasty a ostatní tvorbu naleznete na stránkách Stackuj.cz.

BITCOINOVÉ DESATERO

1. Klíče, seed a Shamira bližnímu svému neukážeš.
2. Své satoshi v hardwarové peněžence uschováš.
3. V mobilní peněžence pouze drobné přechovávatí budeš.
4. Z burzy okamžitě po nákupu satoshi své vyvedeš.
5. Upřednostňovat DCA před snahou předvídat tržní pohyby budeš.
6. Stackovat tak silně, že dostaneš strach z propadu ceny, jest zapovězeno (cenové propady kupovati – ne prodávati – budeš).
7. Pokušení altcoinů odoláš, jedná se o lest ďáblu, usilující o tvé saty.
8. Při odesílání pořádně kontrolovat adresu budeš, jelikož malwaroví démoni číhají za každým rohem.
9. Velikostí svého stacku chlubit se nebudeš.
10. Upřednostňovat hodl před obchodováním budeš.

BRAIINS Publishing

Josef Tětek

Bitcoin: Návrat zdravých peněz

Jazyková redakce: Daniela Hozdová

Odpovědný redaktor: Jáchym Černý

Grafická úprava a sazba: Sabina Heyová

Design obálky: Jiří Chlebus

Design konzultace: Robert Blecha

Marketingová strategie: Kristian Csepcsar

Vytiskla tiskárna Havlíčkův Brod

184 stran, první vydání

Vydalo nakladatelství Braiins Systems, 2023

braiins.com/publishing

ISBN 978-80-908709-8-7

BITCOIN: NÁVRAT ZDRAVÝCH PENĚŽ

ESEJE O BITCOINIZACI ŽIVOTA,
SPOLEČNOSTI A SVĚTA

0
0 0
1 0
1 1
0 1
0 0
1 0
0 0
Bitcoin 1
Bitcoin

„Aby člověk mohl pochopit bitcoin, musí nejprve pochopit problém, který bitcoin řeší: peníze. Aby člověk pochopil peníze, musí chápat ekonomii. Aby člověk chápal ekonomii, musí rozumět tomu, proč se lidé chovají tak, jak se chovají. Proto se říká, že bitcoin je jako králičí nora, ve které je schován celý nový svět. Ten se však odkryje jen tomu, kdo je dostatečně pokorný a zvědavý.“

DANIEL STEIGERWALD

Předchozí knihy autora:

Nepřátelé státu, přátelé svobody

Bitcoin: Odluka peněz od státu

BRAVNS Publishing

