S předmluvou Jeffreyho Tuckera

Bitcoin

a jiné krypto peníze budoucnosti

Historie, ekonomie a technologie kryptoměn,
stručná příručka pro úplné začátečníky

Dominik Stroukal
Jan Skalický

GRADA®

GRADA®

Bitcoin

a jiné krypto peníze budoucnosti

Grada Publishing

Bitcoin

a jiné kryptopeníze budoucnosti

Historie, ekonomie a technologie kryptoměn,
stručná příručka pro úplné začátečníky

Dominik Stroukal
Jan Skalický

Praha 2018

Grada Publishing

Velice silnou stránkou knihy je, že popisuje, informuje a vysvětluje. Své si v ní tudíž najdou všichni, kteří chtějí vědět, ne si jen apriorně o Bitcoinu něco myslet. To je velmi cenná vlastnost textu v časech, kdy kdekdo má na cokoli názor, ale neobtěžuje se jej podepřít jakýmikoli faktickými znalostmi. Takže silné doporučení všem zájemcům o kryptoměny zní: tuhle knihu si určitě pořiďte.

Ing. Mojmír Hampl, MSc., Ph.D.
viceguvernér, Česká národní banka

Kniha je skvělým úvodem do světa Bitcoinu a souvisejících technologií. Dávno předtím, než jejich význam začala chápat širší veřejnost, autoři knihy byli schopni vysvětlit základní ekonomické přednosti decentralizovaných peněz a objasnit, jaké je technologické pozadí tohoto průlomového objevu. Druhé, rozšířené vydání navíc vysvětluje, co se děje, když se Bitcoin stává předmětem zájmu milionů lidí a investorů.

prof. Ing. Josef Šíma, Ph.D.
rektor, VŠ CEVRO Institut

Jak Bitcoin myšlenkově uchopit a kam jej zařadit? To je základní problém, který dnes vyvolává nápadné zmatení v médiích a mezi veřejností. Kniha Dominika Stroukala a Jana Skalického dává potřebnou odpověď – Bitcoin aspiruje na to být plnohodnotnou formou peněz, která v sobě kombinuje anonymitu hotovosti, pohodlnost elektronických peněz a neinflační povahu zlata. Zda už se v evoluci prosadí právě Bitcoin či jiná ze stovek kryptoměn, nemusí být rozhodující. Jako bankéři totiž nemusíme v Bitcoinu vidět jen spekulativní příležitost, ale také vstupní dveře do digitálního světa finančních inovací, který mnohým na první pohled může připadat jako bizarní svět za zrcadlem. Pak tato kniha může být klikou ke zmíněným dveřím.

Ing. Vlastimil Nešetřil, Ph.D.
výkonný ředitel, J&T Banka

Kniha je ideální pro první seznámení s Bitcoinem, neboť se dobře čte a je sympaticky útlá. Navzdory malému rozsahu pokrývá poměrně široký okruh témat, a kromě zájemců o kryptoměny ji doporučuji třeba i studentům ekonomie. Vysvětlivky technických detailů, kterými je kniha proložena, by si sice v publikaci pro začátečníka zasloužily větší prostor, jejich minimalistickou přesnost však ocení pokročilejší čtenáři.

Mgr. Vítězslav Línek, Ph.D.
matematik

Autoři jsou přední čeští odborníci na Bitcoin a kryptoměny obecně. Svou knihou se nesnaží lákat čtenáře k neuváženým investicím, ale pečlivě vysvětlovat samotnou technologii a její širší souvislosti.

Marek „Slush" Palatinus
tvůrce první hardwarové peněženky TREZOR, SatoshiLabs

Obsah

Předmluvy

Předmluva k druhému vydání: Bitcoin už mění svět k lepšímu

Když jsme s Honzou v roce 2015 vydávali tuto knihu, napsal jsem do úvodu, že doufám, že se kniha bude dát číst i za šest let. Uběhly dva roky a už víme, že to není tak úplně pravda. A je to dobře. Bitcoin se změnil. Vyvinul se. Celý ekosystém se proměnil. Je jednodušší bitcoiny koupit, je mnohem jednodušší je ochránit. Je více možností, jak je utratit. Bitcoin pronikl do médií. Změnilo se toho neuvěřitelně moc. V roce 2015 dokonce neexistovala většina z dnes největších kryptoměn.

Když jsem psal předmluvu v prosinci 2015, stál jeden bitcoin 400 dolarů, na které se propadl z 1300 dolarů. I na cenovém dně jsme pevně věřili, že jsme teprve na začátku. Věděli jsme totiž, co vše tato technologie znamená a co může světu přinést. Právě teď při psaní koukám, jak se cena jednoho bitcoinu opírá o 16 000 dolarů. Měli jsme pravdu. Čtyřicetkrát tolik, za dva roky.

Byly to krásné dva roky.

I tuto knihu proměnily k lepšímu. Doplnili jsme text tak, aby odpovídal současnosti, kdekoliv to bylo jen možné. Vedle toho přibyly i některé celé kapitoly. V první části, která popisuje historii Bitcoinu, přibylo pár stran o letech 2016 a 2017. Druhá část, která je příručkou pro začátečníky, zůstaly kapitoly v původní podobě, byly pouze aktualizovány. V třetí části jsme doplnili několik aktuálních témat, která nově hýbala bitcoinovým světem. Největší změnou je pak celá velká kapitola o dalších kryptoměnách, které se Honza ujal s pečlivostí sobě vlastní. Přesvědčte se sami.

Změnilo se toho opravdu hodně. Ale evolučně, nikoliv revolučně. Bitcoin se vyvinul, zlepšil. Některé velké bitvy ho stále čekají, jiné už pomalu vyhrál. Pomalu se vyjasňují regulace, graduje debata o tom, jak zvýšit množství transakcí, které lze v síti uskutečnit, vznikají zajímavější alternativy. Stále více lidí bitcoiny přijímá a používá. Některým lidem doslova zachraňuje životy. Ale o tom všem se dočtete dále.

Dominik Stroukal
4. ledna 2018

Předmluva k prvnímu vydání: Bitcoin není peněžní systém

Od té doby, co jsem začal psát o kryptoměnách, se má e-mailová schránka změnila na shromaždiště otázek o Bitcoinu. Naprosto to chápu, dokonce i pro mne zní stále tento nápad jako přitažený za vlasy – že jakýsi bezejmenný, kódem se ohánějící geek mohl nějak vynalézt novou měnu stvořenou z jedniček a nul, vypustit ji na otevřeném internetovém fóru a že (za pouhých pět let) mohla získat na trhu hodnotu téměř 10 miliard dolarů.

Co to celé znamená? Zabralo mi skutečně hodně času pochopit, jak spolu celá ta technologie souvisí a proč. K pochopení Bitcoinu je zapotřebí znalost peněžní teorie, open-source programování, distribuovaných sítí a kryptografie – a to je docela velké sousto. Tím se vysvětluje, proč jsou lidé tak zmatení a jak se mohl základem nového peněžního řádu stát protokol.

Avšak ve skutečnosti si nemyslím, že by za tím, proč mají i skutečně chytří lidé obtíže úspěch Bitcoinu pochopit, stál nedostatek technologických znalostí. Vodítkem může být e-mail, ve kterém se mne tazatel ptal, jak budou fungovat smlouvy a účetnictví, až bude jednou Bitcoin „zaveden jako měna".

U výrazu „zaveden" jsem se zarazil. Právě toto slovo je jádrem klamu, avšak opět zcela pochopitelného. Hayek v roce 1974 napsal, že vlády vlastní a řídí peněžní systémy po mnoho staletí – dokonce i v dávném starověku byly mince celé říše chápány jako zodpovědnost dané vlády. V 19. století se od všech vlád čekalo zavedení takového systému, který bude nejlépe splňovat potřeby populace.

Ve 20. století dovedla vláda tuto myšlenku mnohem dál. Nestačilo pouze to, že tiskla peníze, že dozírala na celý systém a že určovala, co je podstatou peněz. Nikoliv – použila ještě „vědu" k nalezení optimálního tempa růstu tvorby peněz a ke kartelizaci celého bankovního systému, aby se ujistila, že to bude přesně tak, jak to být má. Na každý aspekt peněžního systému – a mluvíme o polovině veškerých ekonomických transakcí – bylo dohlíženo státem spojeným se soukromými partnery z průmyslu.

A takto to fungovalo po celá léta. Žádný dosud žijící člověk si nepamatuje doby, kdy ještě peníze existovaly v jakékoliv podobě mimo veřejnou správu. Ve výsledku všechny vlády na světě učinily z peněz socialisticky vlastněný statek. A co se nenadálo – peníze se staly nástrojem politiky a snížila se jejich kvalita, jelikož šlo jejich prostřednictvím zakoupit méně a méně zboží a služeb. V důsledku se staly hlavním prostředkem podpory růstu moci na úkor svobody.

Náhlý úkaz v podobě kryptoměn toto paradigma naprosto rozdrtil. „Satoshi Nakamoto" se nikdy nikoho neptal, jestli může zveřejnit svůj na kódu založený model ideální měny, neposílal odborný článek do National Bureau of Economic Research, nesetkal se s ekonomy z Federálního rezervního systému, nevystupoval před senátním bankovním výborem ani si ho nevyslechl žádný člen vedení Fedu. Šel s tím rovnou na veřejnost.

Obešel celou mocenskou strukturu a umístil svůj model na distribuovanou síť. A přizval svět, aby se do jeho projektu zapojil. Jinými slovy, nenavrhnul vůbec žádný systém, nejedná se o kompletní plán peněžní reformy. Takových jsme už viděli fůry – jen za posledních sto let se jich vynořily tisíce a tisíce. Žádný z nich k ničemu nevedl. Můžeme se bavit o peněžních pravidlech, reformách, auditech a fixních úrokových mírách od rána do večera, ale tady je smutná realita: vláda vlastní peníze a bude je využívat k tomu, aby sloužily jejím vlastním zájmům.

To je důvod, proč bylo potřeba naprosto jiného přístupu: svobodného trhu. Svobodný trh není systém, není to politika diktovaná někým konkrétním, není to něco, co zavedl Washington, neexistuje to v žádné legislativě, zákoně, návrhu zákona, regulaci nebo knize. Je to něco, co dostanete, když lidé jednají sami za sebe, naprosto bez centrální direktivy, se svým vlastním majetkem, v rámci spojení svých vlastních výtvorů a svých vlastních zájmů. Je to krása, která vyvstává z nepřítomnosti kontroly.

Zní to jako anarchie? Takto se to zdálo i Karlu Marxovi. Co nechápal, byl náhled liberální revoluce 18. století: společnost se může řídit sama a vytvořit vlastní nádherný řád bez jakéhokoliv centralizovaného dohledu. Bitcoin je paradigmatický příklad, byť jeden z milionů nyní vyrůstajících po celém světě.

Kdo mapuje tyto revoluční pokroky a promýšlí, jak je posunout ještě dále jako prostředek k dosažení větší svobody v našich vlastních životech, a tím pádem i ve společnosti jako celku? Liberty.me. Naším cílem je nabídnout všem úzkou spolupráci v rámci těchto úžasných turbulencí, které se právě teď odehrávají.

Jeffrey Tucker
Chief Liberty Officer, Liberty.me
3. ledna 2014

Úvod

Peníze budoucnosti

Vynález, který změní svět k lepšímu

V roce 2011 si ekonomové začali všímat zajímavé nové měny. Jeffrey Tucker o ní napsal v říjnu stejného roku na stránky mises.org kritický článek a zmínil se o tom na Facebooku.

Kladl si dobré otázky. Co je to **Bitcoin**? K čemu je dobrá virtuální měna? Navíc ničím nekrytá? Co z toho, když už jednu takovou máme? Zlato je odpověď. Dokonce i papírové peníze se dají použít do kamen, když je nejhůř, virtuální peníze se nutně vypaří a nezbude nic. Bitcoin je hra, podvod, pyramidové schéma. Kupte si popcorn a sledujte, jak se zhroutí.

Nic z toho není pravda.

Nic z toho není pravdě více vzdálené.

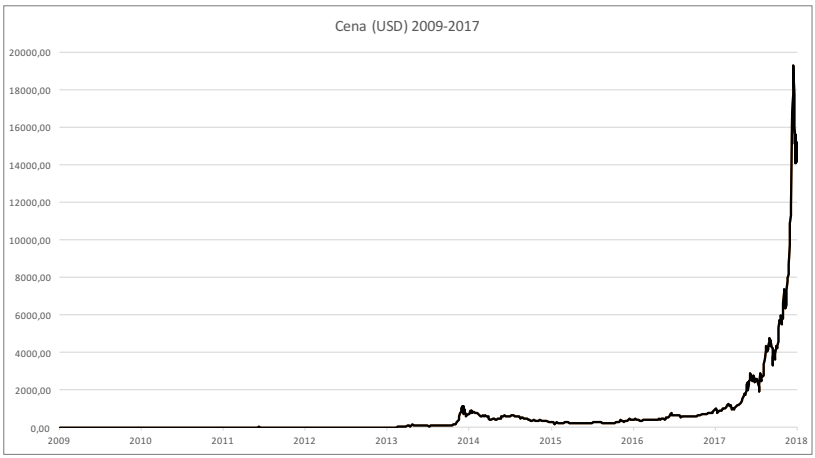
Nakonec to netrvalo dlouho a z Jeffreyho Tuckera se stal jeden z nejviditelnějších stoupenců Bitcoinu na světě. Ve svých přednáškách po celém světě vyvrací přesně to, co si sám kdysi myslel. Přijímá bitcoiny, platí bitcoiny, miluje Bitcoin. Dokonce je mu vyčítáno, že to s láskou k němu přehání.

Nedivím se mu.

Bitcoin

decentralizovaná (**P2P**) síť v internetu, spravující historii platebních **transakcí** mezi svými uzly. Základní jednotkou **transakce** je bitcoin (**BTC**). Počet jednotek této „kryptoměny" je omezen a nové vznikají procesem těžení (viz **Těžba**). Při **těžbě** dochází kromě generování nových bitcoinů rovněž k **potvrzování** vlastních **transakcí** – převodů jednotek mezi bitcoinovými **adresami**.

Fungování sítě je založeno na konsensu pravidel – informace od ostatních uzlů jsou akceptovány, pokud splňují všechna pravidla, která jsou očekávána. Tuto kontrolu provádí každý uzel samostatně – neexistuje žádná centrální autorita v superiorní roli. Všechny **transakce** spravované „účetní knihy" (**ledger**) jsou uloženy v tzv. **blockchainu**, jehož data jsou k dispozici všem uzlům.



Když jsem právě od něj slyšel v roce 2011 o Bitcoinu poprvé, považoval jsem ho také za nesmyslnou hru. Peníze přece nelze naplánovat, učí nás ekonomové. Nejde je úspěšně centrálně řídit, musí se objevit, trvá to staletí a hodnota se ustavuje postupně, směnu po směně.

Dva roky nato už jsem stál před přeplněnou přednáškovou aulou na Vysoké škole ekonomické na přednášce Students For Liberty a vysvětloval, proč je Bitcoin vynález, který změní svět k lepšímu.

Léčba šokem

V roce 2013 už se Bitcoinu nedalo vyhnout. Byl všude. V novinách, v televizi, mluvili o něm všichni. Důvodem byl zejména masivní nárůst ceny, který je vidět na obrázku ukazujícím vývoj ceny Bitcoinu k americkému dolaru.

V době, kdy euro zažívalo jednu krizi za druhou, dávalo smysl hledat alternativu. Hledat peníze budoucnosti. Křehké politické peníze, ať už národní či nadnárodní, se začaly ve světle těchto krizí jevit jako rizikové. Poté, co se kvůli euru zmrazily peníze na kyperských účtech, už nikdo nepochyboval. Může se to stát komukoliv. Kdykoliv. Naštěstí na obzoru alternativa byla. Bitcoin.

Lidé se o něm chtěli dozvědět víc, nyní už v tom byla i finanční motivace, nikoliv jen zájem o technologii. Navíc, myšlenka, že lze vydělat během pár týdnů stovky až tisíce procent, je lákavá.

Ze skupinky jednotlivců, kteří o Bitcoinu věděli, se stala během krátkého období masa. Kdokoliv si o Bitcoinu začal zjišťovat více informací, mu postupně propadal. Do diskuzí a přednášek bylo nesmírně obtížné sehnat protistranu. Ten, kdo si Bitcoin vyzkoušel nebo o něm více četl, zjistil, že jde o elegantní a jednoduchý systém. IT odborníci žasli nad jeho kódem, ekonomové nad jeho ekonomickými vlastnostmi. Dohromady začali pořádat konference, psát články, knihy, vystupovat v médiích a šířit povědomí o alternativě. Logo s velkým, dvakrát přeškrtnutým B se objevilo na stovkách míst po světě.

Budoucnost je krásná

Od té doby se změnilo mnoho. Vývoj je ale stále stejný a stále jde kupředu. Čím dál více lidí Bitcoin používá, čím dál více ho zná, čím dál více ho obdivuje. Stále však přežívají mýty a pořád je složité se zorientovat, pokud chcete vědět více.

Proto vznikla tato kniha. Pokud víte, že Bitcoin existuje, ale máte otázky, potom jste na správném místě.

Je však obtížné psát knihu o něčem, co se mění každý den. Bitcoin je nový a je to živoucí ekosystém, kde dochází neustále k inovacím. Tato kniha pokrývá prvních 6 let od vzniku Bitcoinu až po konec roku 2015. Byla napsána tak, aby se dala číst i za dalších 6 let. Pokud by to možné nebylo, byla by to ta nejlepší zpráva. Znamenalo by to totiž, že se Bitcoin změnil, že našel lepšího nástupce nebo že už by vše zde řečené bylo všeobecně známé.

Budoucnost je nevyzpytatelná, ale už nyní víme, že bude lepší díky vynálezům minulosti. Za lepší současnost i budoucnost vděčíme nejen parnímu stroji a automobilu, ale i počítačům a internetu, o tom dnes pochybuje málokdo.

Bitcoin je další technologie, která změní budoucnost. A protože ji změní k lepšímu, můžeme se na budoucnost těšit. Budoucnost je krásná.

Dominik Stroukal
10. prosince 2015