

Dominik Stroukal  
Jan Skalický

Třetí  
rozšířené  
vydání

# Bitcoin

a jiné kryptopeníze  
budoucnosti

HISTORIE, EKONOMIE  
A TECHNOLOGIE KRYPTOMĚŇ



GRADA®



**Dominik Stroukal  
Jan Skalický**

# **Bitcoin**

a jiné kryptopeníze  
budoucnosti

**HISTORIE, EKONOMIE  
A TECHNOLOGIE KRYPTOMĚN**





# Bitcoin

## *a jiné kryptopeníze budoucnosti*

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

**Dominik Stroukal  
Jan Skalický**

**Praha 2021**

**Grada Publishing**



Velice silnou stránkou knihy je, že popisuje, informuje a vysvětluje. Svě 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 kdekoliv má na cokoli názor, ale neobtěžuje se jej podepřít jakýmkoli faktickými znalostmi. Takže silné doporučení všem zájemcům o kryptoměny zní: tuhle knihu si určitě poříďte.

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

Knihy 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. Kniha 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*

Knihy 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 přesností však ocení pokročilejší čtenáři.

*Mgr. Vítězslav Líněk, 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

<b>PŘEDMLUVY</b> .....	15
<b>Předmluva ke třetímu vydání:</b>	
<b>Díky Bitcoinu</b> .....	17
<b>Předmluva k druhému vydání:</b>	
<b>Bitcoin už mění svět k lepšímu</b> .....	18
<b>Předmluva k prvnímu vydání:</b>	
<b>Bitcoin není peněžní systém</b> .....	19
<b>ÚVOD</b> .....	23
<b>Peníze budoucnosti</b> .....	24
Vynález, který změnil svět k lepšímu .....	24
Léčba šokem .....	25
Budoucnost je krásná .....	26
<b>BITCOIN: PŘÍBĚH</b> .....	27
<b>2009: Genesis</b> .....	28
Kdo je Satoshi Nakamoto? .....	28
Padající hvězdy .....	32
Digitální terorista .....	33
Poučné příběhy .....	35
Dobré peníze .....	36
Nekryté, ale vzácné .....	38
Peníze bez tiskárny .....	38
<b>2010: Nejdražší pizza dějin</b> .....	42
Dobající programátor .....	42
Chyby ze zlata .....	44
<b>2011: Nahoru, nahoru a dolů</b> .....	47
Nahoru .....	47
Dolů .....	48
Kryptozloději .....	50
<b>2012–2013: Raketou do budoucnosti</b> .....	52
Kostky jsou vrženy .....	52
Žít Bitcoin .....	53
Sjet si hedvábnou stezku .....	56
Bitcoin a média .....	58
<b>2014–2015: Dolů ke hvězdám</b> .....	61
Pád z hory Gox .....	61
Regulace v Evropě .....	63
Rok stimulačního klidu .....	64

<b>2016–2017: Hodl to the moon!</b> .....	67
Sklízení úrody .....	67
Daň z úspěchu .....	68
<b>2018–2021: Hodl to Mars!</b> .....	70
Stabilizace výfukem .....	70
První krize .....	71
Mars a dál! .....	71
<b>PŘÍRUČKA UŽIVATELE KRYPTOMĚN</b> .....	75
<b>Pořízení peněženky</b> .....	76
První kroky .....	76
Úsporný software .....	77
Mince na webu .....	79
Mobilní Bitcoin .....	81
<b>Kde bitcoiny koupit</b> .....	83
První mince .....	83
Směnárný a burzy .....	86
Další možnosti .....	89
<b>Jak bitcoiny vytěžit</b> .....	90
Krumpáče do rukou .....	90
Horníci v bazénu .....	93
<b>Jak bitcoiny ochránit</b> .....	96
Bitcoin není jiný .....	96
Trezor .....	96
Jde to i na papíře .....	99
<b>Jak a kde Bitcoin používat</b> .....	102
První nákup .....	102
Příjem bitcoinů .....	103
<b>Jak na něm vydělat</b> .....	107
Experiment za všechny prachy .....	107
Algoritmus na štěstí .....	109
Nic jiného než poptávka .....	111
Chceš haš? .....	112
Daně :( .....	113
<b>Jak být anonymní</b> .....	116
Nevidět nic .....	116
Vidět všechno .....	117
<b>EKONOMIE A TECHNOLOGIE KRYPTOMĚN</b> .....	119
<b>Ekonomické základy Bitcoinu</b> .....	120
Rakouské kořeny Satoshiho Nakamota .....	120
Svobodné bankovníctví .....	121
Bitcoin jako peníze .....	123
Hlasy z druhých břehů .....	125
Svět bez hospodářských krizí .....	127

<b>Škálování Bitcoinu</b> .....	130
Jak zlepšovat Bitcoin .....	130
Cože? Vidličky a nože .....	132
Fork a změna pravidel .....	133
Vidličky z korundu .....	134
Forkování Bitcoinu .....	136
Bitcoin XT, Unlimited, Classic, Segwit .....	137
UASF, Segwit2x .....	139
UAHF, Bitcoin Cash .....	141
Škálování, neškálování a kolosální poplatky .....	143
Lightning Network .....	145
Blesky v síti .....	147
<b>Alternativní kryptoměny</b> .....	150
Co je to „altkojnt“ .....	150
Zoologie altcoinů .....	150
Kdo drží, má za tři .....	152
Čeříme s Ripple .....	154
Klasické deriváty – .....	155
Namecoin, Litecoin, Peercoin .....	155
Je libo anonymitu? .....	158
CryptoNote není vidět .....	159
CryptoNote je vidět, když chce .....	161
CryptoNote v praxi – Bytecoin, Monero .....	162
Kouzla s anonymitou .....	164
Od Zerocoin k Zerocash .....	165
A co Dash? .....	167
Virtuální mašina jménem Ethereum .....	168
Další kryptoplatformy .....	170
Metacoins .....	171
Sidechains .....	172
ICO, letní láska roku 17.....	173
Dobrý, zlý a ošklivý altcoin .....	174
<b>Stablecoins</b> .....	177
Pryč s volatilitou .....	177
Kryptodolar jménem Tether .....	178
Tokenizace komodit .....	179
Krypto na krypto – MakerDAO .....	180
Další stablecoiny .....	181
<b>Blockchain 3.0</b> .....	183
Blockchainové generace .....	183
Generace 1 – měny.....	184
Generace 2 – platformy .....	185
Generace 3 – jak to zlepšit?.....	188
IOTA – když blockchain není blockchain.....	193
Cardano – krypto z akademie .....	196
Polkadot – puntíkováná paralelizace.....	202

<b>BUDOUČNOST BITCOINU</b> .....	211
<b>Možné problémy</b> .....	212
Je bitcoinů málo?.....	212
Není málo adres?.....	213
Většina útočí.....	214
Pálení elektřiny.....	215
<b>Regulace</b> .....	217
Úřad pro zničení Bitcoinu .....	217
Dějiny úřadu.....	218
První vlaštovky.....	219
EU pro, Čína proti.....	220
Postátnění Bitcoinu.....	222
<b>Nové trhy</b> .....	225
Víra v Bitcoin .....	225
Apoštolové blockchainu .....	225
Byznys jménem Bitcoin.....	227
Soukromé blockchainy .....	228
<b>Válka o Bitcoin</b> .....	230
První bitvy.....	230
Vítězná linie.....	231
<b>Regulace coby koule u nohy kryptoměn</b> .....	234
Zkratky za všechny peníze.....	234
Rychlokurz zkratek .....	234
Svět po roce 2001.....	235
Proč by mě to mělo zajímat?.....	236
Co bude dál? .....	238
<b>Ekonomie halvingu</b> .....	239
2024 .....	239
Nabídka: Inlace Bitcoinu padá na 0,8 % .....	239
Nabídka: Zapomeňte na stock-to-flow .....	240
Poptávka: Halving přitahuje pozornost.....	241
Poptávka: ...ale pro někoho jen dočasně.....	242
Poptávka: Jsou trhy efektivní?.....	242
Nabídka a poptávka: Místo pro optimismus.....	243
<b>Je Bitcoin bezpečným přístavem?</b> .....	244
Zachovejte paniku.....	244
Substituty a komplementy .....	244
Luxusní statek.....	245
První velká recese v historii Bitcoinu.....	246
Na vlně nových peněz.....	247
<b>Bitcoin nemá problém s deflací. Fiat má</b> .....	249
Zmatení pojmů.....	249
Bitcoin je deflační.....	250
Proč se bojíme deflace? .....	250
U dobrých peněz můžeme nechat ceny klesat.....	251

<b>Odvrácená strana Bitcoinu</b> .....	253
Do temnoty.....	253
Žádní nájemní vrazi.....	255
Dark Web nezastavíš.....	256
<b>Rozvine se bitcoinová revoluce v rozvíjejících se ekonomikách?</b> .....	258
Rozvíjející se problémy.....	258
Hledání jistoty.....	259
Budoucnost patří Bitcoinu.....	260
Rozvíjej se, poupátko.....	261
<b>Tesla a další velcí hráči jsou pro Bitcoin dvousečnou zbraní</b> .....	262
Velká radost z velkých hráčů.....	262
Fandové až za hrob?.....	263
<b>Bitcoin nespálí planetu</b> .....	264
Další hrozba?.....	264
První mýtus: Energie.....	264
Mýtus druhý: Bude to jen a jen horší.....	265
Mýtus třetí: Srovnání nesrovnatelného.....	267
Bonusový mýtus: Je to k ničemu.....	268
<b>Digitální peníze centrálních bank jsou opakem Bitcoinu</b> .....	269
Centrální hrozba?.....	269
Inspirováno Bitcoinem.....	270
Jak budou CBDC fungovat?.....	271
Co to znamená pro nás smrtelníky?.....	272
<b>Dává smysl naskakovat do rozjetého vlaku?</b> .....	274
Výjimka z pravidla.....	274
Ano, dává smysl vyzkoušet si úžasnou technologii.....	274
Ano, dává smysl naskakovat průběžně.....	275
Ano, jsme teprve na začátku.....	276
<b>Nejlepší čas začít s Bitcoinem je právě dnes</b> .....	277
Bitcoin existuje právě kvůli tomu, co se nyní děje.....	277
Co je silnější než bazuka?.....	278
Vyzkoušejte si Bitcoin. Dnes, ne zítra.....	279
<b>Hlavně se z toho nezblázníte</b> .....	280
Vážně. Jde o vaše zdraví!.....	280
Odzoomujte si.....	280
NYKNYC.....	281
Nehoňte svíčky.....	282
Zdaňte to.....	283
Nejste na tom nejhůř.....	283
Neextrapolujte.....	284
Natáhněte se na gauč... ..	285
<b>DOSLOV</b> .....	287
Tečka za tečkou, blok za blokem.....	288
<b>REJSTRÍK TECHNICKÝCH POJMŮ</b> .....	291



# PŘEDMLUVY







# PŘEDMLUVA KE TŘETÍMU VYDÁNÍ: DÍKY BITCOINU

Před šesti lety jsme po dokončení této knihy napsali, že by se měla dát číst i v roce 2021. „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,“ tvrdili jsme. A čas na třetí vydání skutečně nastal.

Je zrovna Velký pátek roku 2021, jsme uprostřed nouzového stavu a bitcoin se dnes několikrát přehoupl přes 60 tisíc dolarů za kus. Od 400 dolarů, které stál před šesti lety, ušel obrovský kus cesty a ten růst je zasloužený. Cena je ale pouze symptomem toho všeho, co se odehrává pod pokličkou. Je to pára nad hrncem, ve kterém se vaří něco kouzelného.

Bitcoin se změnil. To je ta nejlepší zpráva. Prožil si svou první hospodářskou krizi, našel řadu vyzyvatelů, dostal se na přední stránky novin a do ekonomického zpravodajství hned vedle kurzu eurodolaru. Tweetuje o něm Elon Musk, nejbohatší člověk na světě. A jeho Tesla ho nakupuje. Už se ho nebojí Visa ani PayPal, fandí mu některé banky. I politici.

Stále ale zůstal tím stejným Bitcoinem, kterého nikdy nebude více než necelých 21 milionů kusů. Tím Bitcoinem, který změnil svět. K lepšímu.

I díky tomu jsme mohli jádro knihy ponechat jen s menšími aktualizacemi. Je to pořád náš starý dobrý Bitcoin a jeho kryptoměnoví kolegové. Nicméně změň bylo tolik, že jsme knihu mohli doplnit o desítky stran diskuzí, které v průběhu let vyvstaly a stále nejsou uzavřené. Přidat vysvětlení toho, jak fungují další zajímavé kryptoměny. A dopsat kapitolu o letech mezi druhým a třetím vydáním. Byly to nádherné tři roky. I díky Bitcoinu.

*Dominik Stroukal  
2. dubna 2021*

# 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. Nestálo 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 nenadalo – 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.

Náhly 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, nenavrhl 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.