Dominik Stroukal
Jan Skalický

Třetí rozšířené vydání

Bitcoin

a jiné kryptopeníze budoucnosti

HISTORIE, EKONOMIE
A TECHNOLOGIE KRYPTOMĚN

GRADA

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. 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. 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

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 ... 15

Předmluva ke třetímu vydání: Díky Bitcoinu ... 17

Předmluva k druhému vydání: Bitcoin už mění svět k lepšímu ... 18

Předmluva k prvnímu vydání: Bitcoin není peněžní systém ... 19

Úvod ... 23

Peníze budoucnosti ... 24
- Vynález, který změní svět k lepšímu ... 24
- Léčba šokem ... 25
- Budoucnost je krásná ... 26

Bitcoin: Příběh ... 27

2009: Genesis ... 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

2010: Nejdražší pizza dějin ... 42
- Ďobající programátor ... 42
- Chyby ze zlata ... 44

2011: Nahoru, nahoru a dolů ... 47
- Nahoru ... 47
- Dolů ... 48
- Kryptozloději ... 50

2012–2013: Raketou do budoucnosti ... 52
- Kostky jsou vrženy ... 52
- Žít Bitcoin ... 53
- Sjet si hedvábnou stezku ... 56
- Bitcoin a média ... 58

2014–2015: Dolů ke hvězdám ... 61
- Pád z hory Gox ... 61
- Regulace v Evropě ... 63
- Rok stimulujícího klidu ... 64

2016–2017: Hodl to the moon! ... 67
Sklízení úrody ... 67
Daň z úspěchu ... 68
2018–2021: Hodl to Mars! ... 70
Stabilizace výfukem ... 70
První krize ... 71
Mars a dál! ... 71

Příručka uživatele kryptoměn ... 75
Pořízení peněženky ... 76
První kroky ... 76
Úsporný software ... 77
Mince na webu ... 79
Mobilní Bitcoin ... 81
Kde bitcoiny koupit ... 83
První mince ... 83
Směnárny a burzy ... 86
Další možnosti ... 89
Jak bitcoiny vytěžit ... 90
Krumpáče do rukou ... 90
Horníci v bazénu ... 93
Jak bitcoiny ochránit ... 96
Bitcoin není jiný ... 96
Trezor ... 96
Jde to i na papíře ... 99
Jak a kde Bitcoin používat ... 102
První nákup ... 102
Příjem bitcoinů ... 103
Jak na něm vydělat ... 107
Experiment za všechny prachy ... 107
Algoritmus na štěstí ... 109
Nic jiného než poptávka ... 111
Chceš haš? ... 112
Daně :(... 113
Jak být anonymní ... 116
Nevidět nic ... 116
Vidět všechno ... 117

Ekonomie a technologie kryptoměn ... 119
Ekonomické základy Bitcoinu ... 120
Rakouské kořeny Satoshiho Nakamota ... 120
Svobodné bankovnictví ... 121
Bitcoin jako peníze ... 123
Hlasy z druhých břehů ... 125
Svět bez hospodářských krizí ... 127

Škálování Bitcoinu 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
Alternativní kryptoměny 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
Stablecoins 177
Pryč s volatilitou 177
Kryptodolar jménem Tether 178
Tokenizace komodit 179
Krypto na krypto – MakerDAO 180
Další stablecoiny 181
Blockchain 3.0 183
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 – puntíkovaná paralelizace 202

Budoucnost Bitcoinu ... 211
Možné problémy ... 212
Je bitcoinů málo? ... 212
Není málo adres? ... 213
Většina útočí ... 214
Pálení elektřiny ... 215
Regulace ... 217
Úřad pro zničení Bitcoinu ... 217
Dějiny úřadu ... 218
První vlaštovky ... 219
EU pro, Čína proti ... 220
Postátnění Bitcoinu ... 222
Nové trhy ... 225
Víra v Bitcoin ... 225
Apoštolové blockchainu ... 225
Byznys jménem Bitcoin ... 227
Soukromé blockchainy ... 228
Válka o Bitcoin ... 230
První bitvy ... 230
Vítězná linie ... 231
Regulace coby koule u nohy kryptoměn ... 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
Ekonomie halvingu ... 239
2024 ... 239
Nabídka: Inflace 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
Je Bitcoin bezpečným přístavem? ... 244
Zachovejte paniku ... 244
Substituty a komplementy ... 244
Luxusní statek ... 245
První velká recese v historii Bitcoinu ... 246
Na vlně nových peněz ... 247
Bitcoin nemá problém s deflací. Fiat má ... 249
Zmatení pojmů ... 249
Bitcoin je deflační ... 250
Proč se bojíme deflace? ... 250
U dobrých peněz můžeme nechat ceny klesat ... 251

Odvrácená strana Bitcoinu ... 253
Do temnoty ... 253
Žádní nájemní vrazi ... 255
Dark Web nezastavíš ... 256
Rozvine se bitcoinová revoluce v rozvíjejících se ekonomikách? ... 258
Rozvíjející se problémy ... 258
Hledání jistoty ... 259
Budoucnost patří Bitcoinu ... 260
Rozvíjej se, poupátko ... 261
Tesla a další velcí hráči jsou pro Bitcoin dvousečnou zbraní ... 262
Velká radost z velkých hráčů ... 262
Fandové až za hrob? ... 263
Bitcoin nespálí planetu ... 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
Digitální peníze centrálních bank jsou opakem Bitcoinu ... 269
Centrální hrozba? ... 269
Inspirováno Bitcoinem ... 270
Jak budou CBDC fungovat? ... 271
Co to znamená pro nás smrtelníky? ... 272
Dává smysl naskakovat do rozjetého vlaku? ... 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
Nejlepší čas začít s Bitcoinem je právě dnes ... 277
Bitcoin existuje právě kvůli tomu, co se nyní děje ... 277
Co je silnější než bazuka? ... 278
Vyzkoušejte si Bitcoin. Dnes, ne zítra ... 279
Hlavně se z toho nezblázněte ... 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

Doslov ... 287
Tečka za tečkou, blok za blokem ... 288

Rejstřík technických pojmů ... 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 změní 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 změn 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. 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, 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.

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.

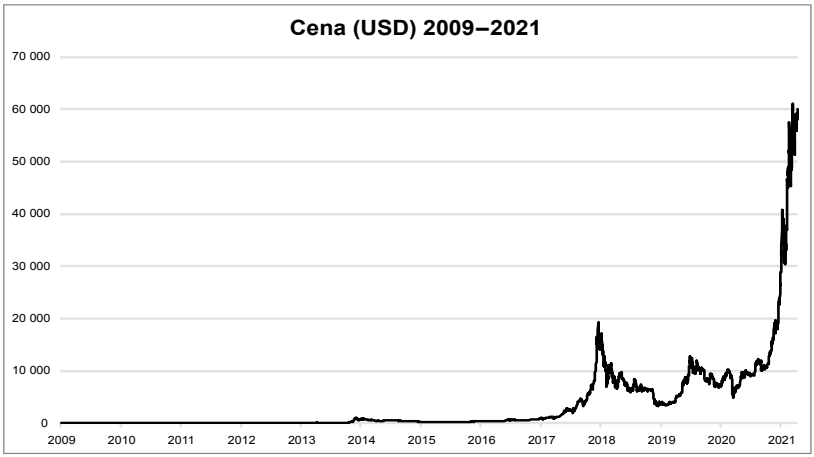
Nakonec to netrvalo dlouho a z Jeffreyho Tuckera se stal jeden z nejviditelnějších stoupenců Bitcoinu na světě. Ve svých přednáškách po celém světě vyvrací přesně to, co si sám kdysi myslel. Přijímá bitcoiny, platí bitcoiny, miluje Bitcoin. Dokonce je mu vyčítáno, že to s láskou k němu přehání.

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

Bitcoin: Příběh

2009: Genesis

Kdo je Satoshi Nakamoto?

Bitcoin je digitální **P2P** měna. Kryptoměna. Na rozdíl od současných peněz, jako jsou české koruny nebo americké dolary, nemá Bitcoin žádnou centrální autoritu, která by se za něj zaručovala nebo měla možnost „tisknout" nové peníze. Mimo této vlastnosti jde však o peníze se všemi standardními charakteristikami dobrých peněz. A mnohem více.

P2P

„peer-to-peer" – označení typu počítačových sítí, kde všechny uzly jsou si rovnocenné a jednotliví klienti spolu komunikují přímo bez existence centrálního uzlu – serveru. Na rozdíl od asymetrického modelu klient-server, v **P2P** s rostoucím množstvím uživatelů roste i přenosová kapacita sítě. Nevýhodou symetrie **P2P** je naopak obtížnost počátečního navázání komunikace.

Bitcoin byl vytvořen v roce 2009 anonymním vývojářem pod pseudonymem Satoshi Nakamoto na základě průvodního článku, který publikoval v říjnu roku 2008. Na internetovém fóru sám tento fenomenální a tajemný zakladatel tvrdil, že na Bitcoinu pracoval již od roku 2007. Krátce po rozšíření Bitcoinu Nakamoto předal internetovou doménu bitcoin.org fanouškovi celého projektu a později hlavnímu vývojáři celého projektu Gavinu Andresenovi. Následně se úplně odmlčel a dodnes se neví, kdo se za tímto zvučným japonským jménem skrývá nebo skrýval. Přestože o sobě na internetu tvrdil, že mu tehdy bylo 34 a je Japonec, vzhledem k perfektní angličtině a úplné absenci jakéhokoliv japonského slova v komunikaci i samotném protokolu se spekuluje, že jde o někoho z anglicky mluvící země. Pravděpodobně nikoliv z USA, protože je v jeho textech několikrát špatně použit americký dialekt, a naopak používá dialekt Velké Británie.

Nakamoto patrně chtěl skrýt svoji identitu. Je dokonce možné, že ani nešlo o jednotlivce, ale o skupinu odborníků na informatiku, kryptografii a ekonomii. Je totiž velmi nepravděpodobné, že by dokázal během tak krátkého času s natolik sofistikovanou technologií přijít jeden samotný člověk.

Kdo je Nakamoto, zajímalo samozřejmě i novináře, a tak se ho vydali hledat. Japonci začali spekulovat o tom, že autorem je geniální matematik Shinichi Mochizuki. Magazín Fast Company hledal spojení mezi jistým patentem z oblasti **kryptografie** a průvodním článkem Nakamota. Neal King, Vladimir Oksman a Charles Bry v něm použili stejnou část věty a texty jsou si nápadně podobné. Navíc patent přihlásili 15. srpna 2008 a jen o tři dny později byla zaregistrována stránka bitcoin.org, ke které se hlásil Nakamoto. Všichni tři však explicitně toto spojení odmítli.

Kryptografie (Cryptography)

matematická disciplína zabývající se šifrováním – převodem zpráv do/z utajené podoby, která je čitelná jen se znalostí šifrovacího klíče. Pokud klíč k dešifrování zprávy není stejný jako klíč k jejímu zašifrování (resp. pokud jsou tyto dvě informace oddělitelné), hovoříme o **kryptografii** asymetrické. **Bitcoin** využívá poznatků **kryptografie** ke svému bezpečnému fungování, a to zejm. hashovací funkce (viz **Hash**) a digitální **podpis** (viz **Asymetrická kryptografie**).

Týdeník New Yorker pátral tak dlouho, až se dostal k mladému irskému studentovi Trinity College v Dublinu jménem Michael Clear. Clear psal o P2P, v roce 2008 byl označen za nejlepšího studenta kryptografie na škole, vyznal se v ekonomii a byl zaměstnán irskými bankami, kterým měl pomoci vylepšit software na obchod s měnami. I ten však nakonec popřel, že by za Bitcoinem stál. Což samozřejmě nic neznamená. Naopak, podíváme-li se na problémy, které čekaly na zakladatele jiných alternativních měn, potom je to zcela pochopitelné.

Spekulace se začaly šířit. Za autory byli označeni i následní vývojáři Bitcoinu Hal Finney, Gavin Andresen, Jed McCaleb, zakladatel ilegálního tržiště Silk Road Ross Ulbricht, bezpečnostní analytik Dustin D. Trammell, a dokonce i americká vláda. Švýcar Stefan Thomas prozkoumal více než 500 příspěvků Satoshiho Nakamota na bitcoinovém fóru bitcointalk.org a ukázal, že pokud chodil spát v obvyklém čase, potom je pravděpodobné, že žil v oblasti s časovým posunem –5 nebo –6 hodin proti Greenwichskému času (tzn. GMT–5h/6h – např. východ a střed USA/Kanady).

V březnu 2014 se strhla mediální lavina, když časopis Newsweek našel Japonce žijícího v Kalifornii Doriana Nakamota, jenž se narodil pod jménem Satoshi Nakamoto. Nakamoto pracoval jako systémový inženýr pro finanční instituce a dle slov své dcery se považoval za libertariána. Konečné rozuzlení mělo přijít, když Dorian Nakamoto prohlásil za přítomnosti policie, že už se „tomu" nevěnuje, že „to" předal dalším lidem a už s „tím" nemá nic společného. Od té doby před jeho domem stály zástupy novinářů prahnoucích po senzaci. Dorian Nakamoto však pravděpodobně skutečným Satoshim také není. V následných rozhovorech bylo zjevné, že o Bitcoinu neví a když mluvil o „tom", měl na mysli jistý kontrakt pro armádu Spojených států. Díky Dorianovi se ale po letech probudil skutečný Satoshi a na svém internetovém profilu napsal od vzniku Bitcoinu první a jedinou větu: „Nejsem Dorian Nakamoto."

Vedle těch, které za Nakamota považujeme my, se za něj začali i někteří sami označovat. Nejhlasitějším z nich byl australský podnikatel Craig Wright. V květnu 2016 to o sobě veřejně prohlásil, přestože nebyl schopen dodat jediný důkaz. Ten by byl snadný, stačilo by odeslat transakci z jedné z adres, o kterých víme stoprocentně, že jsou jeho. Důkazů by mohlo být mnohem více, ale žádný nedoložil. U většiny domnělých Nakamotů existuje pořád malá šance, že by jimi mohli být, jen to nechtějí přiznat. Craig Wright jím není. Přesto dodnes velká média po celém světě jeho velkohubé prohlášení považují za důkaz a ve svých zprávách rádi zmiňují, že je tvůrcem Bitcoinu.

Zatím nejpravděpodobnějším Satoshim Nakamotem je americký programátor maďarského původu Nick Szabo. Bloger Skye Grey pomocí stylometrie poukázal na používání obdobných slov v textech Szaba a Nakamota. Později se objevil Szabův dřívější článek o „bit gold", časté používání pseudonymů a jeho vlastní výrok, že pouze on, Wei Dai a Hal Finney přemýšleli nad Bitcoinem, ještě než se na scéně objevil Nakamoto. Navíc mají stejná písmena v iniciálách a Nick Szabo je bezpochyby génius. I on však vše popřel.

Podstatné ale je, že znalost tvůrce Bitcoinu je pro samotné fungování měny úplně bezpředmětná. Je to zajímavá detektivka, ale nic víc. Přestože Satoshi Nakamoto, ať už je to kdokoliv, měnu vytvořil, nemá nad ní absolutně žádnou moc.