

Dominik Stroukal
Jan Skalický

Bitcoin

a iné kryptopeniaze
budúcnosti



HISTÓRIA, EKONÓMIA A TECHNOLÓGIA KRYPTOMIEN

**Dominik Stroukal
Jan Skalický**

Bitcoin

**a iné kryptopeniaze
budúcnosti**

**HISTÓRIA, EKONÓMIA
A TECHNOLÓGIA KRYPTOMIEN**

 **GRADA®**

OBSAH

Predslovy	9
Predslov k tretiemu českému vydaniu: Vďaka Bitcoinu	10
Predslov k druhému českému vydaniu:	
Bitcoin už mení svet k lepšiemu	11
Predslov k prvému českému vydaniu:	
Bitcoin nie je peňažný systém	12
Úvod	15
Peniaze budúcnosti	17
Vynález, ktorý zmení svet k lepšiemu	17
Liečba šokom	18
Budúcnosť je krásna	19
Bitcoin: Príbeh	21
2009: Genesis	23
Kto je Satoshi Nakamoto?	23
Padajúce hviezdy	27
Digitálny terorista	28
Poučné príbehy	29
Dobré peniaze	30
Nekryté, ale vzácne	32
Peniaze bez tlačiarne	33
2010: Najdrahšia pizza v dejinách	37
Zobkajúci programátor	37
Chyby zo zlata	38
2011: Hore, hore a dole	41
Hore	41
Dole	42
Kryptozlodeji	44
2012–2013: Raketou do budúcnosti	47
Kocky sú hodené	47
Žiť Bitcoinom	48
Prejsť po hodvábnjej ceste	50
Bitcoin a médiá	52
2014–2015: Dole ku hviezdám	55
Pád z hory Gox	55

Regulácia v Európe	57
Rok stimulujúceho pokoja	58
2016–2017: Hodl to the moon!	61
Zber úrody	61
Daň z úspechu	62
2018–2021: Hodl to Mars!	65
Stabilizácia výfukom	65
Prvá kríza	65
Mars a ďalej!	66
Príručka používateľa kryptomien	69
Získanie peňaženky	71
Prvé kroky	71
Úsporný softvér	72
Mince na webe	74
Mobilný Bitcoin	75
Kde kúpiť bitcoiny?	79
Prvé mince	79
Zmenárne a burzy	81
Ďalšie možnosti	84
Ako vyťažiť bitcoiny?	85
Krompáče do rúk	85
Baníci v bazéne	89
Ako ochrániť bitcoiny?	91
Bitcoin nie je iný	91
Trezor	91
Dá sa to aj na papieri	94
Ako a kde používať Bitcoin?	97
Prvý nákup	97
Príjem bitcoinov	98
Ako na ňom zarobiť?	101
Experiment za všetky peniaze	101
Algoritmus na šťastie	103
Nič len dopyt	104
Chceš haš?	105
Dane :(.....	107
Ako byť anonymný?	109
Nič nevidieť	109
Vidieť všetko	110

Ekonomía a technológia kryptomien	113
Ekonomické základy Bitcoinu	115
Rakúske korene Satoshiho Nakamota	115
Slobodné bankovníctvo	116
Bitcoin ako peniaze	118
Hlasy z druhého brehu	120
Svet bez hospodárskych kríz	122
Škálovanie Bitcoinu	125
Ako zlepšovať Bitcoin	125
Čože? Vidličky a nože	127
Fork a zmena pravidiel	128
Vidličky z korundu	130
Forkovanie Bitcoinu	131
Bitcoin XT, Unlimited, Classic, Segwit	132
UASF, Segwit2x	134
UAHF, Bitcoin Cash	136
Škálovanie, neškálovanie a kolosálne poplatky	138
Lightning Network	140
Blesky v sieti	142
Alternatívne kryptomeny	145
Čo je to „altkojn“?	145
Zoológia altcoinov	145
Kto drží, má za troch	147
Čeríme s Ripple	148
Klasické deriváty – Namecoin, Litecoin, Peercoin	150
Chcete anonymitu?	152
CryptoNote nevidieť	153
CryptoNote je viditeľný, ak chce	155
CryptoNote v praxi – Bytecoin, Monero	156
Čarovanie s anonymitou	158
Od Zerocoin k Zerocash	160
A čo Dash?	161
Virtuálny stroj menom Ethereum	163
Ďalšie kryptoplatformy	164
Metacoins	165
Sidechains	166
ICO, letná láska roku 17	167
Dobrý, zlý a škaredý altcoin	168
Stablecoins	171
Preč s volatilitou	171

Kryptodolár zvaný Tether	172
Tokenizácia komodít	173
Krypto na krypto – MakerDAO	174
Ďalšie stablecoiny	175
Blockchain 3.0	177
Blockchainové generácie	177
Generácia 1 – meny	178
Generácia 2 – platformy	179
Generácia 3 – ako to zlepšiť?	181
IOTA – keď blockchain nie je blockchain	186
Cardano – krypto z akadémie	189
Polkadot – bodkovaná paralelizácia	194
Budúcnosť Bitcoinu	201
Možné problémy	203
Je bitcoinov málo?	203
Nie je málo adries?	204
Väčšina útočí	205
Pálenie elektriny	206
Regulácia	207
Úrad pre zničenie Bitcoinu	207
Dejiny úradu	208
Prvé lastovičky	209
EU pre, Čína proti	210
Poštátnenie Bitcoinu	211
Nové trhy	215
Viera v Bitcoin	215
Apoštoli blockchainu	215
Biznis menom Bitcoin	217
Súkromné blockchainy	218
Vojna o Bitcoin	221
Prvé bitky	221
Víťazná línia	222
Regulácia sťa guľa na nohe kryptomien	225
Skratky za všetky peniaze	225
Rýchlokurz skratiek	225
Svet po roku 2001	226
Prečo by ma to malo zaujímať?	227
Čo bude ďalej?	228
Ekonomía halvingu	231

2024	231
Ponuka: Inflácia Bitcoinu padá na 0,8 %	231
Ponuka: Zabudnite na stock-to-flow	232
Dopyt: Halving priťahuje pozornosť...	233
Dopyt: ...ale pre niekoho len dočasne	233
Dopyt: Sú trhy efektívne?	234
Ponuka a dopyt: Miesto pre optimizmus	235
Je Bitcoin bezpečným prístavom?	237
Zachovajte paniku	237
Substitúty a komplementy	237
Luxusný statok	238
Prvá veľká recesia v histórii Bitcoinu	239
Na vlně nových peňazí	239
Bitcoin nemá problém s defláciou. Fiat má	243
Zmätok pojmov	243
Bitcoin je deflačný	244
Prečo sa bojíme deflácie?	244
Pri dobrých peniazoch môžeme nechať ceny klesať	245
Odvrátená strana Bitcoinu	247
Do temnoty	247
Žiadni nájomní vrahovia	249
Dark Web nezastavíš	250
Nastane bitcoinová revolúcia v rozvíjajúcich sa ekonomikách?	253
Rozvíjajúce sa problémy	253
Hľadanie istoty	254
Budúcnosť patrí Bitcoinu	255
Rozvíjaj sa, púpätko	255
Tesla a ďalší veľkí hráči sú pre Bitcoin dvojsečnou zbraňou	257
Veľká radosť z veľkých hráčov	257
Fanúšikovia až za hrob?	257
Bitcoin nespáli planétu	259
Ďalšia hrozba?	259
Prvý mýtus: Energia	259
Mýtus druhý: Bude to len a len horšie	260
Mýtus tretí: Porovnávanie neporovnateľného	261
Bonusový mýtus: Je to nanič	263
Digitálne peniaze centrálnych bánk sú opakom Bitcoinu	265
Centrálna hrozba?	265
Inšpirované Bitcoinom	265
Ako budú fungovať CBDC	266

Čo to znamená pre nás smrteľníkov?	267
Dáva zmysel naskakovať do rozbehnutého vlaku?	269
Výnimka z pravidla	269
Áno, dáva zmysel vyskúšať si úžasnú technológiu	269
Áno, dáva zmysel naskakovať priebežne	270
Áno, sme len na začiatku	271
Najlepší čas začať s Bitcoinom je práve dnes	273
Bitcoin existuje práve kvôli tomu, čo sa teraz deje	273
Čo je silnejšie ako bazuka?	274
Vyskúšajte si Bitcoin. Dnes, nie zajtra	274
Najmä sa z toho nezbláznite	277
Vážne. Ide o vaše zdravie!	277
Odzoomujte	277
NYK NYC	277
Nenaháňajte sviečky	278
Zdaňte to	279
Nie ste na tom najhoršie	279
Neextrapolujte	280
Natiehnite sa na gauč...	281
Doslov	283
Bodka za bodkou, blok za blokom	284
Register technických pojmov	286

PREDSLOVY



PREDSLOV K TRETIEMU ČESKÉMU VYDANIU: VĎAKA BITCOINU

Pred šiestimi rokmi sme po dokončení tejto knihy napísali, že by sa mala dať čítať aj v roku 2021. „Ak by to možné nebolo, bola by to najlepšia správa. Znamenalo by to totiž, že sa Bitcoin zmenil, že našiel lepšieho nástupcu alebo že už by všetko vypovedané v tejto knihe bolo všeobecne známe,“ tvrdili sme. A čas na tretie vydanie skutočne nastal.

Je práve Veľký piatok roku 2021, sme uprostred núdzového stavu a bitcoin sa dnes niekoľkokrát prehupol cez 60 tisíc dolárov za kus. Od 400 dolárov, ktoré stál pred šiestimi rokmi, urazil obrovský kus cesty a ten rast je zaslúžený. Cena je ale iba symptómom všetkého, čo sa odohráva pod pokrievkou. Je to para nad hrncom, v ktorom sa varí niečo kúzelné.

Bitcoin sa zmenil. To je tá najlepšia správa. Prešiel si svojou prvou hospodárskou krízou, vystúpilo proti nemu množstvo vyzývateľov, dostal sa na titulky novín a do ekonomického spravodajstva hneď vedľa kurzu eura a dolára. Tweetuje o ňom Elon Musk, najbohatší človek na svete. A jeho Tesla ho nakupuje. Už sa ho nebojí Visa ani PayPal, fandia mu niektoré banky. Aj politici.

Stále je to však ten istý Bitcoin, ktorého nikdy nebude viac ako necelých 21 miliónov kusov. Ten Bitcoin, ktorý zmení svet. K lepšiemu.

Aj vďaka tomu sme mohli jadro knihy ponechať len s menšími aktualizáciami. Je to stále náš starý dobrý Bitcoin a jeho kryptomenoví kolegovia. Zmien však nastalo toľko, že sme knihu mohli doplniť o desiatky strán diskusií, ktoré v priebehu rokov vyvstali a stále nie sú uzavreté. Pridať vysvetlenie toho, ako fungujú ďalšie zaujímavé kryptomeny. A dopísať kapitolu o rokoch, ktoré uplynuli medzi druhým a tretím vydaním. Boli to nádherné tri roky. Aj vďaka Bitcoinu.

Dominik Stroukal
2. apríla 2021

PREDSLOV K DRUHÉMU ČESKÉMU VYDANIU: BITCOIN UŽ MENÍ SVET K LEPŠIEMU

Keď sme s Janom v roku 2015 vydávali túto knihu, napísal som do úvodu, že dúfam, že sa kniha bude dať čítať aj o šesť rokov. Ubehli dva roky a už vieme, že to nie je tak úplne pravda. A to je dobre. Bitcoin sa zmenil. Vyvinul sa. Celý ekosystém prešiel premenou. Bitcoinov možno ľahšie kúpiť, je oveľa jednoduchšie ich ochrániť. Je viac možností, ako ich minúť. Bitcoin prenikol do médií. Zmenilo sa toho neuveriteľne veľa. V roku 2015 dokonca neexistovala väčšina z najväčších kryptomien dneška.

Keď som písal predslav v decembri 2015, stál jeden bitcoin 400 dolárov, na ktoré sa prepadol z 1 300 dolárov. Aj na cenovom dne sme pevne verili, že sme ešte len na začiatku. Vedeli sme totiž, čo všetko táto technológia znamená a čo môže svetu priniesť. Práve teraz pri písaní pozerám, ako sa cena jedného bitcoinu dotýka 16 000 dolárov. Mali sme pravdu. Štyridsaťkrát toľko, za dva roky.

Boli to krásne dva roky.

Aj túto knihu premenili k lepšiemu. Doplňli sme text tak, aby zodpovedal súčasnosti, kdekoľvek to bolo možné. Okrem toho pribudlo niekoľko celých kapitol. V prvej časti, ktorá sa venuje histórii Bitcoinu, pribudlo pár strán o rokoch 2016 a 2017. V druhej časti, ktorá je príručkou pre začiatočníkov, zostali kapitoly v pôvodnej podobe, boli iba aktualizované. V tretej časti sme doplnili niekoľko aktuálnych tém, ktoré hýbali bitcoinovým svetom. Najväčšou zmenou je celá veľká kapitola o ďalších kryptomenách, ktoré sa Jan ujal so starostlivosťou, ktorá mu je vlastná. Presvedčite sa sami.

Zmenilo sa toho skutočne veľa. Ale evolučne, nie revolučne. Bitcoin sa vyvinul, zlepšil. Niektoré veľké bitky má stále pred sebou, iné už pomaly vyhral. Pomaly sa vyjasňuje regulácia, graduje debata o tom, ako zvýšiť množstvo transakcií, ktoré možno v sieti uskutočniť, vznikajú zaujímavejšie alternatívy. Stále viac ľudí bitcoiny prijíma a používa. Niektorým ľuďom doslova zachraňuje životy. Ale o tom všetkom sa dočítate ďalej.

Dominik Stroukal
4. januára 2018

PREDSLOV K PRVÉMU ČESKÉMU VYDANIU: BITCOIN NIE JE PEŇAŽNÝ SYSTÉM

Odkedy som začal písať o kryptomenách, moja e-mailová schránka sa zmenila na zhromaždisko otázok o Bitcoine. Úplne tomu rozumiem a dokonca aj mne pripadá za vlasy pritiahnutý nápad, že akýsi bezmenný, kódom sa oháňajúci geek mohol vynásť novú menu vytvorenú z jednotiek a núl, vypustiť ju na otvorenom internetovom fóre, a že (len za päť rokov) mohla získať na trhu hodnotu takmer 10 miliárd dolárov.

Čo to celé znamená? Trvalo mi naozaj dlho, než som pochopil, ako a prečo celá tá technológia spolu súvisí. Na pochopenie Bitcoinu je potrebná znalosť teórie peňazí, open-source programovania, distribuovaných sietí a kryptografie a to je pomerne veľké sústo. Vysvetľuje to však, prečo sú ľudia takí zmätení a ako sa mohol základom nového peňažného poriadku stať protokol.

V skutočnosti si však nemyslím, že by za tým, že aj skutočne múdri ľudia majú problém pochopiť úspech Bitcoinu, stál nedostatok technologických znalostí. Indikátorom je e-mail, v ktorom sa ma pisateľ pýtal, ako budú fungovať zmluvy a účtovníctvo, ak raz bude Bitcoin „zavedený ako mena“.

Pri výraze „zavedený“ som sa zarazil. Práve toto slovo je jadrom klamu, avšak opäť úplne pochopiteľného. Hayek v roku 1974 napísal, že už mnoho storočí vlády vlastnia a riadia peňažné systémy a dokonca aj v dávnom staroveku boli mince celej ríše chápané ako zodpovednosť danej vlády. V 19. storočí sa od všetkých vlád čakalo zavedenie takého systému, ktorý bude najlepšie spĺňať potreby populácie.

V 20. storočí vláda doviela túto myšlienku oveľa ďalej. Už nestačilo len to, že tlačila peniaze, že dozerala na celý systém a že určovala, čo bude podstatou peňazí. Nie – použila ešte „vedu“ na nájdenie optimálneho tempa rastu tvorby peňazí a na kartelizáciu celého bankového systému, aby zabezpečila, že to bude presne tak, ako má byť. Na každý aspekt peňažného systému – a hovoríme o polovici všetkých ekonomických transakcií – dohliadal štát spojený so súkromnými partnermi z priemyslu.

A takto to fungovalo po celé roky. Žiadny dnes žijúci človek si nepamätá doby, keď ešte peniaze existovali v nejakej podobe mimo verejnej správy. Všetky vlády na svete tak prakticky urobili z peňazí socialisticky vlastnený statok. A čo sa nestalo – peniaze sa stali nástrojom politiky a znížila sa ich kvalita, pretože sa prostredníctvom nich dalo kúpiť menej a menej tovarov

a služieb. Stali sa prakticky hlavným prostriedkom podpory rastu moci na úkor slobody.

Náhly úkaz v podobe kryptomien túto paradigmu úplne rozdrvil. „Satoshi Nakamoto“ sa nikdy nikoho nepýtal, či môže zverejniť svoj model ideálnej meny založený na počítačovom kóde, neposielal odborný článok do National Bureau of Economic Research, nestretol sa s ekonómami z Federálneho rezervného systému, nevystupoval pred bankovým výborom Senátu a ani si ho nevypočul žiadny člen vedenia Fedu. Vyšiel so všetkým rovno na verejnosť.

Obišiel celú mocenskú štruktúru a umiestnil svoj model na distribuovanú sieť. A prizval svet, aby sa do jeho projektu zapojil. Inými slovami, nenavrhol vôbec žiadny systém, nejde o kompletný plán peňažnej reformy. Takých sme už videli hromadu – len za posledných sto rokov sa ich vynorili tisíce a tisíce. Žiadny z nich k ničomu nevedol. Môžeme sa baviť o peňažných pravidlách, reformách, auditoch a fixných úrokových mierach od rána do večera, ale smutná realita je takáto: vláda vlastní peniaze a bude ich využívať tak, aby slúžili jej vlastným záujmom.

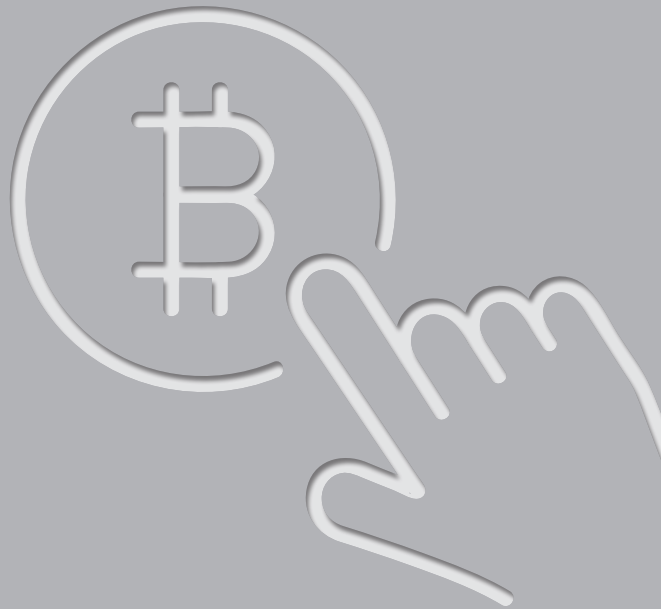
To je dôvod, prečo bol potrebný úplne iný prístup: slobodný trh. Slobodný trh nie je systém, nie je to politika diktovaná niekým konkrétnym, nie je to niečo, čo zaviedol Washington, neexistuje to v žiadnej legislatíve, zákone, návrhu zákona, regulácii alebo knihe. Je to to, čo získame, keď ľudia konajú sami za seba, úplne bez centrálneho riadenia, so svojím vlastným majetkom, v rámci spojenia svojich vlastných výtvorov a svojich vlastných záujmov. Je to krása, ktorá vzniká z neprítomnosti kontroly.

Znie to ako anarchia? Tak to pripadalo aj Karlovi Marxovi. Nerozumel pohľadu liberálnej revolúcie 18. storočia: spoločnosť sa môže riadiť sama a vytvoriť vlastný nádherný poriadok bez akéhokoľvek centralizovaného dohľadu. Bitcoin je paradigmatický príklad, jeden z miliónov vyrastajúcich po celom svete.

Kto mapuje tieto revolučné pokroky a premýšľa, ako ich posunúť ďalej ako prostriedok na dosiahnutie väčšej slobody v našich vlastných životoch, a tým pádom aj v spoločnosti ako celku? Liberty.me. Naším cieľom je ponúknuť všetkým úzku spoluprácu v rámci týchto úžasných turbulencií, ktoré sa práve teraz odohrávajú.

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

ÚVOD



Peniaze budúcnosti

VYNÁLEZ, KTORÝ ZMENÍ SVET K LEPŠIEMU

V roku 2011 si ekonómovia začali všímať zaujímavú novú menu. Jeffrey Tucker o nej napísal v októbri toho istého roku na stránkach mises.org kritický článok a zmienil sa o nej na Facebooku.

Kládol si dobré otázky. Čo to je **Bitcoin**? Na čo je dobrá virtuálna mena? Navyše ničím nekrytá? Čo z toho, keď už jednu takú máme? Odpoveď je zlato. Dokonca aj papierové peniaze sa dajú priložiť do kachlí, keď je najhoršie, virtuálne peniaze sa nutne vyparia a nezostane nič. Bitcoin je hra, podvod, pyramídová hra. Kúpte si popcorn a sledujte, ako sa zruší.

Nič z toho nie je pravda.

Nič z toho nemôže byť viac vzdialené od pravdy.

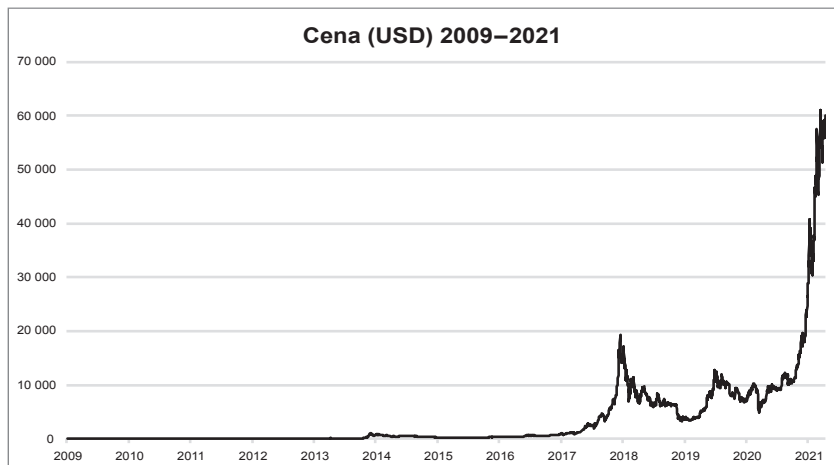
Netrvalo dlho a z Jeffreyho Tuckera sa stal jeden z najviditeľnejších zástancov Bitcoinu na svete. Vo svojich prednáškach po celom svete vyvracia presne to, čo si sám kedysi myslel. Prijíma bitcoiny, platí bitcoinmi, miluje Bitcoin. Dokonca sa mu vyčíta, že to s láskou k nemu preháňa.

Nečudujem sa mu.

Bitcoin

decentralizovaná (**P2P**) sieť v internete, spravujúca históriu platobných **transakcií** medzi svojimi uzlami. Základnou jednotkou **transakcie** je bitcoin (**BTC**). Počet jednotiek tejto „kryptomeny“ je obmedzený a nové vznikajú procesom ťaženia (pozri **Ťažba**). Pri **ťažbe** dochádza okrem generovania nových bitcoinov tiež k **potvrdzovaniu** vlastných **transakcií** – prevodov jednotiek medzi bitcoinovými **adresami**.

Fungovanie siete je založené na konsenze pravidiel – informácie od ostatných uzlov sú akceptované, ak spĺňajú všetky očakávané pravidlá. Túto kontrolu vykonáva každý uzol samostatne – neexistuje žiadna centrálna autorita v nadradenej úlohe. Všetky **transakcie** spravovanej „účtovnej knihy“ (**ledger**) sú uložené v tzv. **blockchaine**, ktorého dáta sú k dispozícii všetkým uzlom.



Keď som v roku 2011 prvýkrát počul o Bitcoine práve od neho, považoval som ho tiež za nezmyselnú hru. Peniaze predsa nemožno naplánovať, učia nás ekonómovia. Nemožno ich úspešne centrálné riadiť, musia sa objaviť a trvá to stáročia, hodnota sa vytvára postupne, výmenou po výmene.

Dva roky nato som už stál pred preplnenou prednáškovou aulou na Vysokej škole ekonomickej na prednáške Students For Liberty a vysvetľoval, prečo je bitcoin vynález, ktorý zmení svet k lepšiemu.

LIEČBA ŠOKOM

V roku 2013 sa už Bitcoinu nedalo vyhnúť. Bol všade. V novinách, v televízii, hovorili o ňom všetci. Dôvodom bol najmä masívny nárast ceny, ktorý je vidieť na obrázku ukazujúcom vývoj ceny Bitcoinu k americkému doláru.

V čase, keď euro zažívalo jednu krízu za druhou, dávalo zmysel hľadať alternatívu. Hľadať peniaze budúcnosti. Krehké politické peniaze, či už národné alebo nadnárodné, sa začali vo svetle týchto kríz javiť ako rizikové. Po tom, čo sa kvôli euru zmrazili peniaze na cyperských účtoch, už nikto nepochyboval. Môže sa to stať komukoľvek. Kedykoľvek. Našťastie bola na obzore alternatíva. Bitcoin.

Ľudia sa chceli o ňom dozvedieť viac, teraz v tom bola už aj finančná motivácia, nielen záujem o technológiu. Navyše, myšlienka, že možno zaradiť stovky až tisíce percent za pár týždňov, je lákavá.

Zo skupinky jednotlivcov, ktorí vedeli o Bitcoine, sa stala počas krátkeho obdobia masa. Každý, kto si o Bitcoine začal zisťovať viac informácií, mu postupne prepadal. Bolo nesmierne ťažké zohnať protistranu do diskusií a prednášok. Ten, kto si Bitcoin vyskúšal alebo o ňom viac čítal, zistil, že ide o elegantný a jednoduchý systém. IT odborníci žasli nad jeho kódom, ekonómovia nad jeho ekonomickými vlastnosťami. Spolu začali organizovať konferencie, písať články, knihy, vystupovať v médiách a šíriť povedomie o alternatíve. Logo s veľkým, dvakrát prečiarknutým B sa objavilo na stovkách miest po svete.

BUDÚCNOSŤ JE KRÁSNA

Odvtedy sa veľa zmenilo. Vývoj je ale stále rovnaký a ide stále vpred. Čím ďalej, tým viac ľudí Bitcoin používa, čím ďalej, tým viac ľudí ho pozná a čím ďalej, tým viac ľudí ho obdivuje. Stále však prežívajú mýty a stále je ťažké sa zorientovať, ak chce človek vedieť viac.

Preto vznikla táto kniha. Ak viete, že Bitcoin existuje, ale máte otázky, potom ste na správnom mieste.

Je však ťažké písať knihu o niečom, čo sa mení každý deň. Bitcoin je nový a je to živý ekosystém, kde dochádza neustále k inováciám. Táto kniha pokrýva prvých 6 rokov od vzniku Bitcoinu až po koniec roku 2015. Bola napísaná tak, aby sa dala čítať aj za ďalších 6 rokov. Ak by to možné nebolo, bola by to najlepšia správa. Znamenalo by to totiž, že sa Bitcoin zmenil, že našiel lepšieho nástupcu alebo že už by všetko vypovedané v tejto knihe bolo všeobecne známe.

Budúcnosť je nevyspytateľná, ale už teraz vieme, že bude lepšia vďaka vynálezom minulosti. Za lepšiu súčasnosť i budúcnosť vďačíme nielen parnému stroju a automobilu, ale aj počítačom a internetu, o čom pochybuje dnes málokto.

Bitcoin je ďalšia technológia, ktorá zmení budúcnosť. A pretože ju zmení k lepšiemu, môžeme sa na budúcnosť tešiť. Budúcnosť je krásna.

Dominik Stroukal
10. decembra 2015

BITCOIN: PRÍBEH



2009: Genesis

KTO JE SATOSHI NAKAMOTO?

Bitcoin je digitálna **P2P** mena. Kryptomena. Na rozdiel od súčasných peňazí, ako sú americké doláre alebo eurá, nemá Bitcoin žiadnu centrálnu autoritu, ktorá by sa zaň zaručovala alebo mala možnosť „tlačiť“ nové peniaze. Okrem tejto vlastnosti však ide o peniaze so všetkými štandardnými charakteristikami dobrých peňazí. A ešte oveľa viac.

P2P

„peer-to-peer“ – označenie typu počítačových sietí, kde sú všetky uzly rovnocenné a jednotliví klienti spolu komunikujú priamo, bez existencie centrálného uzla – servera. Na rozdiel od asymetrického modelu klient-server, v **P2P** s rastúcim množstvom používateľov rastie aj prenosová kapacita siete. Nevýhodou symetrie **P2P** je naopak náročné počítačové nadviazanie komunikácie.

Bitcoin vytvoril v roku 2009 anonymný vývojár vystupujúci pod pseudonymom Satoshi Nakamoto, ktorý publikoval v októbri roku 2008 sprievodný článok. Na internetovom fóre tento fenomenálny a tajomný zakladateľ sám tvrdil, že na Bitcoine pracoval už od roku 2007. Krátko po rozšírení Bitcoinu Nakamoto odovzdal internetovú doménu bitcoin.org fanúšikovi celého projektu a neskôr hlavnému vývojárovi celého projektu Gavinovi Andresenovi. Následne sa úplne odmlčal a dodnes sa nevie, kto sa za týmto zvučným japonským menom skrýva alebo skrýval. Hoci o sebe na internete tvrdil, že mal vtedy 34 rokov a je Japonec, vzhľadom na perfektnú angličtinu a úplnú absenciu akéhokoľvek japonského slova v komunikácii aj samotnom protokole existuje domnienka, že ide o človeka z anglicky hovoriacej krajiny. Pravdepodobne nie z USA, pretože v jeho textoch je niekoľkokrát zle použitý americký dialekt a naopak používa dialekt Veľkej Británie.

Nakamoto chcel zrejme skryť svoju identitu. Je dokonca možné, že nešlo o jednotlivca, ale o skupinu odborníkov na informatiku, kryptografiu