

„Ak si chceš prečítať len jednu knihu  
o tomto novom globálnom fenoméne, je to práve táto.“

Dennis Jacobs, Angel Investor

# KRYPTO MENY

Bitcoin, Ethereum, Blockchain, ICO & Co.  
jednoducho a zrozumiteľne



DR. JULIAN HOSP

Juliana môžete poznať z:

FORBES CNBC BLOOMBERG INC.



TATRAN

70

ROKOV



# **KRYPTOMENY**

**JEDNODUCHO A ZROZUMITEĽNE**

**Dr. Julian Hosp**

TATRAN

Z nemeckého originálu Julian Hosp: Kryptowährungen einfach erklärt:  
Bitcoin, Ethereum, Blockchain, Dezentralisierung, Mining, ICOs & Co.

ktorý vyšiel vo vydavateľstve FinanzBuch Verlag, Mníchov 2018,  
preložili Miroslava Čelinská a Anna Harská.

Vyšlo v roku 70. výročia Vydavateľstva TATRAN, Bratislava 2018  
ako 5166. publikácia.

Vydanie I.

Obálku podľa pôvodného návrhu spracoval  
AldoDesign, Bratislava.

Odborná spolupráca s projektom Kryptotrejder, sprievodcom  
vo svete kryptomien.

Zodpovedná redaktorka Eva Melichárková

Jazyková redaktorka Daniela Šinková

Technická redaktorka Jozefína Novotná

Sadzba RS servis, Bratislava

Vytlačila Těšínská tiskárna, a. s., Český Těšín.

[www.slovtatran.sk](http://www.slovtatran.sk)

:: knihy pre **hodnotnejší** život

All rights reserved.

Copyright © Dr. Julian Hosp 2018

Translation © Miroslava Čelinská, Anna Harská

Slovak edition © Vydavateľstvo TATRAN 2018

ISBN 978-80-222-0945-8

*Túto knihu venujem svojmu otcovi  
Laurinovi Hospovi, pretože práve on  
prebudil vo mne záujem o technológie.*



# OBSAH

<b>PREDSLOV – Dr. Harald Mahrer</b> .....	13
<b>ČO ŤA ČAKÁ</b> .....	15
<b>PREČO PRÁVE TÁTO KNIHA A NIE INÁ</b> .....	18
<b>1. OD ZLATA KU KRYPTOMENÁM</b> .....	25
Čo sú peniaze? .....	25
Čo je mena? .....	25
Ako funguje zlato ako peniaze? .....	26
Aká je hodnota samotného zlata? .....	28
Čo sú papierové peniaze viazané na zlato? .....	29
Čo sú FIAT peniaze? .....	30
Čo je dôvera v peniaze? .....	30
Čo je centralizácia? .....	31
Čo je decentralizácia? .....	34
<b>2. ZÁKLADNÉ INFORMÁCIE O BLOCKCHAI NE</b>	
<b>A KRYPTOMENÁCH</b> .....	37
Čo znamená double spending? .....	37
Čo je blockchain? .....	38
V akom vzťahu je blockchain a digitálna mena? .....	39
Čo je kryptomena? .....	39
Ktorá bola prvá decentralizovaná mena? .....	40
<b>3. SÚKROMNÝ KĹÚČ A VEREJNÁ ADRESA</b> .....	43
Ako funguje decentralizovaný account management (správa účtov)? .....	43
Čo je súkromný kľúč a verejná adresa? .....	44
Čo znamená open source? .....	49
<b>4. ŤAŽBA</b> .....	52
Čo je ťažba (mining)? .....	52



Čo je konsenzus? .....	52
Čo sú používatelia, uzly a ťažiar? .....	52
Ako vzniká konsenzus v blockchaine? .....	53
Aké sú mechanizmy pre konsenzus? .....	54
Proof of importance .....	56
Proof of stake .....	57
Proof of work .....	58
Ako vznikne z blokov blockchain? .....	61
Čo sú orphan blocks? .....	63
Čo je mining difficulty? .....	63
Čo je hash rate? .....	64
Rôzne druhy ťažobných počítačov .....	65
Je ťažba výnosná? .....	66
Existujú hospodársky významné riešenia ťažby? .....	68
Ako to celé vysvetliť desaťročnému dieťaťu? .....	69
Ako vyzerá blockchain v skutočnosti? .....	71
Čo je SPV (simple payment verification)? .....	73
Čo je problém škálovania? .....	74
Aké sú možné riešenia škálovania? .....	75
Čo je SegWit? .....	76
<b>5. AKO SA TVORIA KRYPTOMENY .....</b>	<b>78</b>
Čo je deflačná kryptomena? .....	79
Sú všetky kryptomeny limitované? .....	80
Čo znamená predbežná ťažba? .....	81
<b>6. PEŇAŽENKY .....</b>	<b>83</b>
Čo je peňaženka? .....	83
Čo je v peňaženke? .....	83
Papierové peňaženky .....	84
Pamäťové peňaženky .....	86
Softvérové peňaženky .....	86
Hardvérové peňaženky .....	87
Zmenárne .....	88
Osobná skúsenosť, z ktorej som sa poučil .....	89
Dá sa blockchain hacknúť? .....	91
Prečo sa verejná adresa stále mení? .....	91
Čo sú deterministické peňaženky? .....	92

Čo je seed? .....	92
<b>7. FORKY A ÚTOKY NA BLOCKCHAIN</b> .....	<b>95</b>
Čo je fork? .....	95
Čo je soft fork? .....	95
Čo je hard fork? .....	96
Čo sa deje s coinmi počas forku? .....	97
Prečo nevytvára každý fork nové coin? .....	98
Prečo nemôže blockchain forknúť jednoducho každý? .....	99
Čo sú replay attacks? .....	99
Čo robiť počas forku? .....	100
Čo sú útoky na blockchain? .....	100
Prečo by ťažiar zadržovali bloky? .....	101
Čo je 51-percentný útok? .....	102
Čo je útok Sybil? .....	103
<b>8. DÁ SA BLOCKCHAIN ZNIČIŤ?</b> .....	<b>104</b>
Kvantový počítač .....	104
Regulácia/Zákazy .....	105
Vypnutie/Cenzúra internetu .....	106
Veľkosť blockchainu .....	107
Centralizácia .....	108
<b>9. SÚKROMIE, ANONYMITA A TRANSPARENTNOSŤ</b> .....	<b>110</b>
Čo je súkromie? .....	110
Čo je anonymita? .....	110
Čo je KYC, KYB, AML a CTF? .....	111
Čo je transparentnosť? .....	111
Čo znamená pseudo-anonymný? .....	112
Sú kryptomeny vhodné na nezákonnú činnosť? .....	112
Rovnováha medzi intimitou a utajovaním .....	113
<b>10. ALTCOINY A BITCOIN</b> .....	<b>114</b>
Čo sú altcoiny? .....	114
Ako rozoznáš scam, snahu o okradnutie, podvod? .....	114
Aké dobré informačné zdroje existujú v oblasti blockchainov? .....	117
Čo je mastermindová skupina? .....	118
Bitcoin BTC .....	118
Kto je Satoshi Nakamoto a koľko BTC vlastní? .....	120
Aká je prognóza vývoja Bitcoinu? .....	121

Čo je ticker symbol?.....	122
Ktoré sú forky Bitcoinu? .....	122
Namecoin NMC .....	122
Litecoin LTC .....	123
Bitcoin Cash BCH .....	123
Ethereum ETH .....	124
Čo sú to smart contracts?.....	125
Čo je EVM (Ethereum Virtual Machine)? .....	125
Ako sa bude vyvíjať cena Etherea v budúcnosti? .....	126
Ako vzniklo Ethereum Classic? .....	126
Čo sú tokeny ERC20? .....	127
Čo je ICO? .....	128
Prehľad tokenov ERC20 (PAY, REP, ICN, MLN, DGD a iné) .....	128
Iné decentralizované platformy – NEM, Lisk, Stratis, Waves a iné ...	129
Tokeny pre aplikácie a aktíva .....	129
Čo je tokenizácia? .....	130
Čo sú súkromné coins .....	130
Čo sú tainted coins? .....	131
Ring signatures: Monero XMR .....	132
Mixéry (DASH a iné) .....	132
Zero knowledge proofs: ZCash, Ethereum a iné .....	133
Sú súkromné coins dobré alebo zlé? .....	135
Banking coins: Ripple a iné .....	136
Decentralizované riešenia konsenzu bez blockchainu:	
IOTA Tangle & Hashgraph .....	137
Blockchainové konektory: Lightning, Raiden, Interledger a iné .....	138
COMIT .....	138
Platobné kanály .....	139
Atomic swaps .....	140
HTLC (hashed time lock contracts) .....	140
<b>11. INVESTOVANIE DO KRYPTOMIEN .....</b>	<b>142</b>
Mal by človek vôbec investovať do kryptomien? .....	142
Nachádzajú sa kryptomeny v bubline? .....	143
Aký je pomer zisku a rizika? .....	144
Koľko by si mal investovať do kryptomien? .....	146
Kedy je najlepší čas do kryptomien investovať? .....	147
Aká je najlepšia stratégia investovania do kryptomien? .....	147

Čo znamená „HODL“? .....	149
Ako správne počítať zisk? .....	149
Ako vyzerá moje osobné kryptomenové portfólio? .....	150
Zima príde! .....	151
Ako sa nakupujú kryptomeny? .....	152
OTC (over the counter) .....	152
Zmenárne .....	152
Čo sa stalo s burzou MtGox? .....	153
Kde sa dajú kryptomeny uchovávať? .....	154
Kedy kryptomenu predat? .....	155
Ako sa kryptomeny zdaňujú? .....	156
Ako sa dá kryptomenami platiť? .....	156
<b>12. BUDÚCNOSŤ KRYPTOMIEN</b> .....	<b>158</b>
Ako budú vyzeráť platby o 5 – 7 rokov? .....	158
Čo je price discovery? .....	158
Ako budú vyzeráť platby o 10 rokov? .....	158
Ako budú vyzeráť platby o 15 – 20 rokov? .....	159
<b>BONUSOVÁ KAPITOLA: INITIAL COIN OFFERINGS (ICO)</b> .....	<b>160</b>
Čo je ICO? .....	160
Ako sa odlišuje ICO od IPO (vstup na burzu)? .....	160
Čo je predaj tokenov/možnosť generovania tokenov? .....	161
Prečo robia firmy ICO? .....	161
Vďaka čomu je ICO úspešné? .....	162
Mal by človek investovať do ICO? .....	163
<b>A ČO TERAZ?</b> .....	<b>164</b>
<b>REGISTER</b> .....	<b>167</b>
<b>O AUTOROVI</b> .....	<b>171</b>



# PREDSLOV

Dr. Harald Mahrer

Spolkový minister pre vedu, výskum a hospodárstvo

Rakúska republika

Ludia už od nepamäti snívajú o lepšom svete. Na podnet slávneho humanistu Erazma Rotterdamského zverejnil anglický štátnik Thomas More dielo s názvom Utópia. Tento spis, v ktorom opísal ideálnu spoločnosť, sa dodnes považuje za jedného z najdôležitejších predchodcov sociálne utopistických koncepcií, ktoré sa stále vracajú k spravodlivému rozdeleniu tovarov a často aj zrušeniu peňazí. Dnes, o 500 rokov neskôr, niektorí prognostici spochybňujú prevládajúce spoločenské modely založené na vysoko dynamickom technologickom vývoji, najmä ich vhodnosť pre budúcnosť. Individuálna sloboda verzus nátlak a kontrola zo strany štátu, alebo viac osobného pohodlia a ľahší život za cenu straty súkromia? Toto všetko sú metafory pre základné otázky digitalizácie nášho sveta a spoločného vývoja človeka a stroja.

Pre apologetu a prognostika kryptoekonómie predstavuje táto nová forma decentralizácie systémov cestu k novej utopii, k svetu založenému na blockchaine a zároveň k lepšej a spravodlivejšej spoločnosti. Kniha Juliana Hospa prináša vyhladky a názory na tieto nové možnosti, ponúka príležitosť pochopiť základné technické spôsoby fungovania kryptoekonómie a rozoznať jej potenciál. Autor v nej predstavuje celý podsystem kryptomien, pričom ako prvý približuje kryptoekonomický ekosystem širokej verejnosti.

Ďakujem Julianovi Hospovi za toto dielo a verím, že sa čitateľky a čitatelia budú vďaka získaným vedomostiam a osobnej reflexii aktívne podieľať na debate o svetlých a tienistých stránkach kryptoekonomického vývoja, ktorá je pre túto spoločnosť nevyhnutná. Stále nebola zodpovedaná otázka, ako môže svet založený na blockchaine ekologicky udržateľne, resp. na základe princípov trhového hospodárstva prispieť k súťaži, ktorá podporuje blahobyť. Práve naopak, existuje viac otázok než odpovedí, a viac cestičiek, než si dokážeme predstaviť. Máme teda, v duchu hesla osvietenstva, odvahu začať používať vlastný rozum? *Sapere aude!* Aj táto kniha k tomu významne prispieva.

Dr. Harald Mahrer

## ČO ŤA ČAKÁ

Už si si niekedy položil otázku, čo je to Bitcoin, kryptomena alebo blockchain? A čo slovo „decentralizácia“? Možno si už niekde počul, že „to prichádza“ a „bude to dominovať svetu“. Je však úplne jedno, či si sa s „tým“ už stretol, je „to“ totiž pravda – prichádza „to“ a zohrá „to“ rovnako dôležitú úlohu, akú za posledných 20 rokov zohral internet.

Vieš, kto z internetu profitoval najviac? Ľudia, ktorí sa naň pripravili včas a začali ho využívať na svoje osobné či obchodné účely medzi prvými, skôr než ich nasledovali ostatní. Patriš aj ty k prvým používateľom internetu, alebo si prvú vlnu premeškal? Možno však poznáš ľudí, ktorí ju stihli a dostali sa na čelo, či už vďaka investovaniu, rozumným obchodným rozhodnutiam, alebo mali jednoducho náskok pred prichádzajúcim trendom. S novou technológiou s názvom blockchain teraz prichádza podobná príležitosť.

Ak ani len netušíš, čo je to blockchain, kryptomena alebo Bitcoin, netráp sa – zatiaľ o nich počulo len málo ľudí. Ak však vieš, o čo ide, vedel by si to vysvetliť desaťročnému dieťaťu za menej ako jednu minútu? Pravdepodobne nie. Viem to, pretože na túto tému robím každý rok asi sto prednášok. Môžem byť v Európe, Ázii, Amerike alebo Afrike, môžem mať miestnosť plnú tvorcov blockchainu, no keď sa ich opýtam, kto by vedel vysvetliť, čo je to blockchain, a ešte dodám, že „desaťročnému dieťaťu za menej ako minútu“, takmer nikto sa neprihlási. Keď sa človek pozrie na tieto fakty, pýta sa, ako môže takéto priekopnícke koncepty priblížiť širokej verejnosti tak,



aby ich dokázali pochopiť milióny ľudí. Jednou z najväčších výziev pre každého, kto sa chce zoznámiť s témou blockchainu, decentralizácie, Bitcoinu a ďalších kryptomien, je otázka: „Kde mám začať?“. Bohužiaľ, existuje priveľa zlých zdrojov, a tie, ktoré by v podstate mohli byť dobré, sú väčšinou určené softvérovým vývojárom s bohatými skúsenosťami s programovaním.

Práve preto som napísal túto knihu. Celú problematiku sa v nej budem snažiť vysvetliť čo najjednoduchšie, aby to pochopilo aj desaťročné dieťa. Uvediem aj niekoľko technických detailov, aby si získal nielen celkový prehľad, ale priblížim ti aj niektoré detaily. Ak si teraz myslíš, že keď ti to chcem vysvetliť ako desaťročnému dieťaťu, diskriminujem alebo podceňujem tvoju inteligenciu, spomeň si na výrok Alberta Einsteina:

*„Ak to nevieš vysvetliť jednoducho, potom tomu dobre nerozumieš.“*

Pravdepodobne si už niekedy musel niečo vysvetľovať dieťaťu (možno svojmu vlastnému). Nemohol si použiť rovnaké výrazy a slová ako pri dospelých. Nebolo to jednoduché, ale keď sa ti to podarilo, sám si celú tému pochopil úplne nانو. Spomínaš si na tú chvíľu? Vôbec nešlo o „podceňovanie inteligencie“, ale práve o jej zvýšenie. Na základe tohto princípu by som chcel vysvetliť nové technické pojmy súvisiace s blockchainom rečou, ktorej porozumie naozaj každý – dokonca aj desaťročné dieťa. Nielenže ti to pomôže všetko lepšie pochopiť, ale budeš môcť šíriť tieto informácie ďalej – ak budeš chcieť. Hlavným cieľom je, aby boli ľudia na celom svete #CRYPTOFIT – fit pre novú vlnu decentralizácie a blockchainu.

Okrem jednoduchého jazyka a niekoľkých grafík predsa len použijem aj zopár technických detailov. V podstate to budú tie isté informácie, len na komplexnejšej úrovni. Tieto pasáže sú

vyznačené, takže keď budeš chcieť, môžeš ich rovno preskočiť. Neboj sa, nič podstatné ti neunikne, iba vysvetlím to, čo už raz bolo povedané, v jazyku čísiel, matematiky a kryptografie.

Tento ekosystém je plný anglických výrazov. Termíny ponechám v angličtine a preložím len tie, pri ktorých si myslím, že to má význam. Neboj sa, vždy im budeš rozumieť. Aj pre teba to bude oveľa jednoduchšie, veď keď budeš čítať nejaký blog alebo pozerat' videá, nebudeš počuť slovenské, ale anglické odborné výrazy. Blockchain nikdy nikto nenazve „refazcom blokov“, aj keď je to správny preklad.

**[TIP]**

Skôr ako začneme, ešte jedna dôležitá vec: Vypracoval som dvadsaťstranové zhrnutie, ktoré patrí k tejto knihe a určite by si si ho mal stiahnuť. Tento PDF dokument ti pomôže pochopiť konkrétne myšlienky a koncepty ešte lepšie a získať lepší prehľad. Je v digitálnej forme a môžem ho kedykoľvek aktualizovať, čo je v tomto dynamickom ekosystéme veľmi dôležité. Stačí navštíviť [www.cryptofit.community/arbeitsbuch](http://www.cryptofit.community/arbeitsbuch), kde si ho môžeš zadarmo stiahnuť.

**[DÔLEŽITÉ]**

Kniha síce má jasnú štruktúru, ALE ak ťa niektorá téma zaujíma viac, môžeš niektoré kapitoly samozrejme preskočiť. Ak sa chceš napríklad dozvedieť najmä niečo o investovaní do kryptomien, môžeš prejsť priamo na túto kapitolu. Napriek tomu ti odporúčam, aby si kapitoly čítal v poradí, v akom sú napísané.

## PREČO PRÁVE TÁTO KNIHA A NIE INÁ

Teraz pravdepodobne čítaš, o čom táto kniha je, nevieš, kto som a prečo by si mi mal vôbec dôverovať. Vynára sa otázka: „Prečo by si ma mal vlastne počúvať? Prečo práve táto kniha a nie iná?“ Viem sa vcítiť do tvojej kože – čo mi dáva právo hovoriť o blockchaine, kryptomenách, Bitcoine, ICO atď.? Na svete je toľko ľudí, ktorí šíria informácie o blockchaine a kryptomenách, tak prečo by si mal veriť práve mne? Správna otázka. Dovoľ mi najskôr pár slov o sebe a o tom, ako som sa dostal k ekosystému kryptomien.

Po šesťročnom štúdiu medicíny v Rakúsku som sa v rámci svojej klinickej praxe začal pripravovať na povolanie úrazového chirurga. Počas štúdia som bol vo svetovej top desiatke profesionálnych kitesurferov, ako športovec som precestoval prakticky celý svet, a to, že som mal byť zrazu celý čas zatvorený v jednej nemocnici, sa mi nepozdávalo. V roku 2012 som sa rozhodol, že sa práci lekára nebudem venovať, ale využijem svoje vedomosti z profesionálneho športu a medicíny, aby som mohol pre ľudí robiť koučing, tréningy pre špičkový výkon a pomáhať im pri rozvoji osobnosti. Prestahoval som sa do Hongkongu, aby som tam získal skúsenosti v oblasti biznisu, financií a marketingu. Vždy som totiž veril, že pri učení je dôležitá prax, nielen čisto teória. Zmena prostredia mala pre môj život obrovský význam. Pokus usadiť sa v meste medzi západným a východným svetom mi priniesol veľmi ťažký rok, no naučil ma veľa o predaji, verejných prejavoch, odmietaní a mnoho iného.

V roku 2014 som cítil, že už mám Hongkongu dosť, a opäť som sa rozhodol cestovať a ponúkať svoje školenia skôr na diaľku. Úplnou náhodou som na medzizastávke v Bangkoku stretol Tobyho, krajana z Rakúska, a jeho kamaráta Paula z Thajska. Od začiatku sme si dobre rozumeli a začali sme sa baviť o niečom, čo som počul už v roku 2011 od jedného pacienta: kryptomeny, Bitcoin a spol. Vtedy som tejto téme nevenoval veľa pozornosti, no vzhľadom na fakt, že kurz Bitcoinu bol v roku 2011 približne 1 americký dolár, ma šokovalo, keď som sa dozvedel, že práve v roku 2014 stúpol na približne 1 000 amerických dolárov: „Vau, keby som v roku 2011 investoval 1 000 dolárov, zarobil by som za tri roky milión dolárov.“ V roku 2011 by som to okamžite odpísal ako podvod, no po rozhovore s Tobym a Paulom ma to začalo nesmierne zaujímať a začal som túto novú tému skúmať. Vyhľadal som si všetky dostupné informácie o blockchaine, kryptomenách a Bitcoine. Pochopiť to nebolo síce ľahké, no stále to bolo jednoduchšie ako väčšina medicínskych materiálov, ktoré som predtým musel roky študovať. Vždy, keď sa ma ľudia opýtajú, či niekedy ľutujem, že nepracujem ako lekár, keďže som vyštudoval medicínu, som si istý, že práve štúdium mi umožnilo pochopiť technické veci okolo kryptosveta.

Toby, Paul a ja sme zostali v kontakte a niekoľko mesiacov po našom prvom stretnutí v Bangkoku sme ďalej rozmýšľali, ako by sme mohli kryptomeny sprístupniť širokej verejnosti. DBS, jedna z najväčších bánk v Singapore, usporiadala v máji 2015 v Singapore tzv. Blockchain Hackathon. V podstate išlo o víkend, počas ktorého sa niekoľko tímov pokúšalo presvedčiť porotu o svojom projekte. Rozhodol som sa, že spolu s Tobym a Paulom využijeme príležitosť, a pripravili sme prezentáciu, aby sme hlavnú cenu vo výške 15 000 amerických dolárov vyhrali práve my. Video odtiaľ vrátane našej prípravy si môžeš pozrieť na YouTube: „Julian Hosp Hackathon Singapur“.