

OBSAH

PREDSLOV - Dr. Harald Mahrer.....	13
ČO ŤA ČAKÁ.....	15
PREČO PRÁVE TÁTO KNIHA A NIE INÁ.....	18
1. OD ZLATA KU KRYPTOMENÁM.....	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
2. ZÁKLADNÉ INFORMÁCIE O BLOCKCHAINED	
A KRYPTOMENÁCH.....	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
3. SÚKROMNÝ KĹÚČ A VEREJNÁ ADRESA.....	43
Ako funguje decentralizovaný account management (správa účtov)?.....	43
Čo je súkromný kľúč a verejná adresa?.....	44
Čo znamená open source?.....	49
4. ŤAŽBA.....	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 vysvetlí 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
5. AKO SA TVORIA KRYPTOMENY.....	78
Čo je deflačná kryptomena?.....	79
Sú všetky kryptomeny limitované?.....	80
Čo znamená predbežná ťažba?.....	81
6. PEŇAŽENKY.....	83
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
7. FORKY A ÚTOKY NA BLOCKCHAIN	95
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
8. DÁ SA BLOCKCHAIN ZNIČIŤ?.....	104
Kvantový počítač.....	104
Regulácia/Zákazy.....	105
Vypnutie/Cenzúra internetu	106
Veľkosť blockchainu.....	107
Centralizácia.....	108
9. SÚKROMIE, ANONYMITA A TRANSPARENTNOST	110
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
10. ALTCOINY A BITCOIN.....	114
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
11. INVESTOVANIE DO KRYPTOMIEN	142
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 portfolio?.....	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
12. BUDÚCNOSŤ KRYPTOMIEN.....	158
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
BONUSOVÁ KAPITOLA: INITIAL COIN OFFERINGS (ICO).....	160
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
A ČO TERAZ?.....	164
REGISTER	167
O AUTOROVI	171