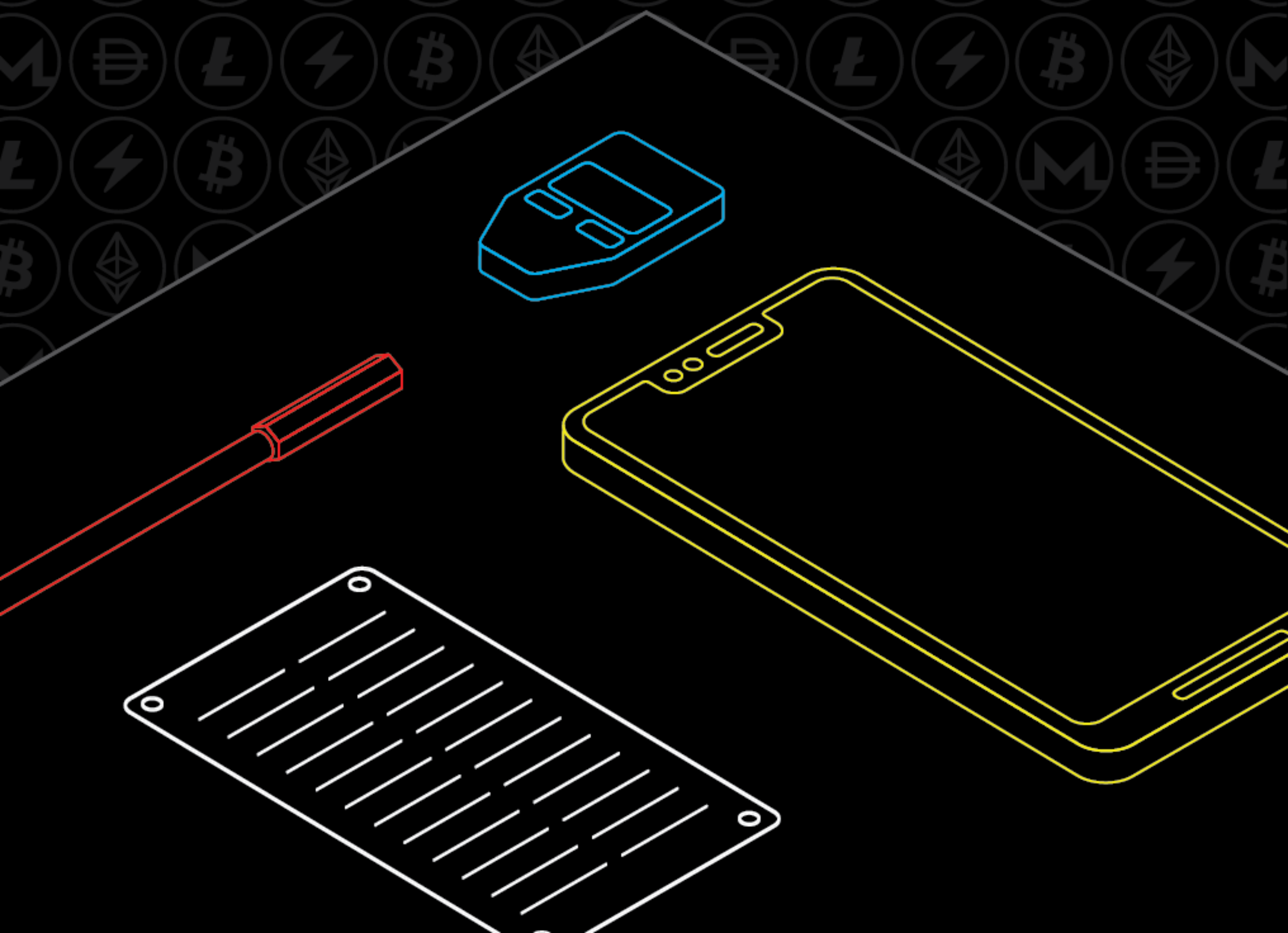


JURAJ BEDNÁR

KRYPTOMENY

VYHACKUJ SI LEPŠÍ ŽIVOT



ÚVOD

Kryptomeny sú inováciou, na akú sme niektorí čakali roky. Internet priniesol možnosť komunikovať, vymieňať si hudbu, obrázky, videá a iné typy súborov. Ďalším krokom bol nástup e-commerce, vďaka ktorému sme si mohli cez prehliadač stránok niečo objednať. Na rozdiel od obrázkov sme si cez internet nemohli poslať peniaze, aj keď ilúzia to bola pomerne veľká. Pomocou internetu sme ovládali len iné platobné siete - kreditné karty, bankové prevody alebo kuriéra, ktorý po nás vyžaduje hotovosť na dobierku pri doručení balíka. Tieto siete však nie sú natívnym internetovým protokolom a preto ľudia ako ja, ktorí veria v to, že Internet dokáže zásadným spôsobom zlepšiť spoločnosť k lepšiemu čakali na tzv. e-cash. Ten prišiel s vynálezom Bitcoinu.

V tejto knihe sa dozviete, čo je to Bitcoin, prečo si myslím, že je dôležitý pre spoločnosť. Prejdeme si rôzne platobné siete Bitcoinu a povieme si niečo o iných kryptomenách ako Bitcoin. Ale ak by kniha skončila pri tomto, bol by to len lepšie (dúfam) spísané to, čo nájdete v kníhkupectve hneď vedľa, v knižkách o kryptomenách. Iný autor má možno iný názor na Bitcoinový maximalizmus, preferuje iné kryptomeny, kritizuje niektoré aspekty alebo je pomýlený Keynesiánskou doktrínou tlačenia peňazí. Ale základné fakty o kryptomenách vám odrecituje každý.

Táto kniha by mala byť iná v tom, aby vám vysvetlila ako fenomén kryptomien použiť na zlepšenie svojho života. Nevyhnem sa filozofickým a ekonomickým témam ako prečo sú dobré neinflačné peniaze - pre jednotlivca aj pre spoločnosť. Pozrieme sa však aj na nové príležitosti na trhu práce, nové odvetvia, produkty a služby (napríklad úschova kryptomien, hardvérové peňaženky). Povieme si

ako môžeme neslávnu volatilitu nielen skrotiť, ale ju rovno zapriať do našich finančných plánov. Povieme si aké máme možnosti, keď zaútočí medveď (teda krypto trh padá oproti fiat). Vysvetlíme si prečo a ako prijímať kryptomeny vo vašom podnikaní. Zamyslíme sa nad tým ako môže Bitcoin pomôcť prechodu na obnoviteľné zdroje energie práve vďaka tomu, že používa proof of work. Pokúsím sa vás zoznámiť s mojimi víziami platobných sietí, kam sa Bitcoin dostane o niekoľko dekád, či sprístupnenie predikčných trhov, nových foriem odmeňovania autorov obsahu. Povieme si ako si vytvoriť komunitu ľudí, s ktorými môžeme spoločne kryptomeny používať, či už pri cestovaní alebo pri vzájomnom obchodovaní. Ako bonus si povieme ako môžeme bezpečne komunikovať, keď už máme tie súkromné peniaze bez tretích strán. Skritizujeme regulácie a povieme si, čo s nimi na globálnej úrovni (deregulovať!), ale aj ako je možné zareagovať na osobnej úrovni.

Ak ste čítali moje knihy Hackni sa alebo Veľký reštart, bude vám štýl písania knihy povedomý. Knihy píšem tak, aby boli zložené z článkov, ktoré sú viacmenej nezávislé. Cieľom väčšiny týchto textov je vytvoriť efekt otvorenia mysle. Najlepší výsledok po prečítaní jednej kapitoly by mal byť zamyslenie sa a zvedavý povzdych "takto som nad tým ešte nerozmýšľal". Verím, že tento efekt vyvolám pri viacerých kapitolách. Neznamená to, že sa máte hneď zamestnať v decentralizovanej autonómnej organizácii, ísť all-in do Bitcoinu, presťahovať sa na ostrov - do tropického (daňového raja) a vybudovať tam nezávislú sieť Lightning network na lokálne platby, ktoré fungujú aj keď nefunguje Internet. Nemusíte ani hneď začať prijímať Bitcoin, brať si fiatovú pôžičku, ktorá je ním krytá alebo vytvárať nové predikčné trhy na získavanie kvalitných informácií. Úplne mi postačí, ak sa nad týmito možnosťami zamyslíte a uvedomíte si tie obrovské možnosti, ktoré nám kryptomeny prinášajú už dnes.

Nie je pri tom ani tak podstatné, či by sa tieto inovácie mohli udiť aj bez kryptomien. Veľa kritikov kryptomien tvrdí, že ak by nevznikol podcasting 2.0 nad kryptomenami, určite by sa našiel iný spôsob. Filozofovanie "čo by bolo keby" nie je však moja obľúbená činnosť a radšej sa pozerám na to, čo ľudia naozaj robia. Fascinujúci svet Bitcoinu a kryptomien otvoril toľko možností, že neverím, že tieto inovácie by vznikli vo vákuu alebo v izolovanom prostredí nejakých "fintech" startupov.

Kryptomeny sú revolúciou v rozmýšľaní nad peniazmi, nie sú trochu lepším dolárom alebo rýchlejším a lacnejším SWIFTom. Existencia digitálnych peňazí založených na správnej ekonomickej teórii (tzv. rakúskej ekonomickej škole), správnych hodnotách (sloboda, open-source, decentralizácia) a technologickej inovácii prilákal množstvo ľudí, ktorí sa elektronickým peniazom dovtedy nevenovali. Medzi Bitcoinermi nájdeme právnikov, účtovníkov, daňových poradcov, programátorov, umelcov, podnikateľov, ale aj farmárov, bezdomovcov, mamičky na materskej a dokonca aj policajtov, politikov a úradníkov. Spoločne majú najmä to, že majú otvorenú hlavu a sú ochotní experimentovať s úplne novými prístupmi k usporiadaniu spoločnosti.

Prajem vám príjemné čítanie, veľa "aha" momentov a dostatok energie na to, aby ste si vďaka tejto knižke a kryptomenám vyhackovali lepší život.

UPOZORNENIE

Nič v tejto knihe nie je právnym, daňovým, účtovným, životným ani iným poradenstvom. Chcem vám ukázať sféru možného s technickými nástrojmi, ktoré podporujú skutočnosť, že je to možné. Netuším, v ktorej krajine žijete, aké sú vaše miestne zákony. Táto kniha nebola prispôsobená žiadnej konkrétnej jurisdikcii - v priestore ani v čase. Aj keď túto knihu čítate v Slovenčine, nepredpokladám, že žijete pod Tatrami, môžete žiť v Čechách, vo Švajčiarsku, USA alebo v Paraguaji. Mám vás všetkých rád, ale prosím pochopte, že pravdepodobne nežijem v rovnakej krajine ako vy a už vôbec nepoznám pravidlá, ktoré sa vzťahujú na vás a vašu životnú situáciu.

Aj keby som rozumel rozsiahlemu súboru pravidiel, ktoré platia vo fyzickom priestore, kde žijete (nazývanom aj krajina alebo jurisdikcia), pravdepodobne by boli zastarané v čase, keď by na tejto knihe zaschol atrament. A to dokonca aj keby to bol rýchly elektronický atrament na vašej čítačke elektronických kníh. Statická kniha nemôže držať krok s prívalom nových zákonov a "reforiem", ktoré sa menia rýchlejšie ako predpoveď počasia.

Najmä v prípade právneho, daňového a účtovného poradenstva vám odporúčam vyhľadať odborníkov. Väčšina ľudí, ktorí vôbec čítajú takéto upozornenia, to nerobí, ale aj tak to odporúčam. Obzvlášť dôležité je, aby ste sa nepýtali na právne, účtovné alebo daňové rady na internetových fórach (Facebookových skupinách, Telegram alebo Signal chatoch a podobne). Väčšina rád tohoto typu, ktoré som videl, je jednoducho nesprávna. Nejaký náhodný človek na internete vám dá ďalekosiahlu právnu a daňovú analýzu (ešte k tomu zadarmo) po prečítaní článku na internete (alebo naštudovaní troch paragrafov nejakých zákonov), či po rozhovore s „kompetentným priateľom“.

Právne a daňové situácie sú špecifické a na detailoch záleží. To, čo platí pre znalého priateľa, sa na vašu situáciu pravdepodobne nevzťahuje.

OBSAH

ÚVOD	5
ČO SÚ TO KRYPTOMENY?	1
PREČO NIE LEN BITCOIN AKO PLATOBNÝ PROTOKOL	5
TVRDÉ PENIAZE	6
FIAT A NETWORK EFFECT	7
BITCOIN AKO PLATIDLO	8
HIPSTERSKÁ KÁVIČKA ZA ALTCOINY	9
VISA VS DOLÁR	10
AKO DOSIAHNUŤ SIEŤOVÝ EFEKT	12
EXISTUJÚCE ALTERNATÍVNE PLATOBNÉ SIETE	15
ALTCOINOVÉ PLATOBNÉ SIETE	17
LITECOIN	18
ETHEREUM	20
MONERO	21
BITCOINOVÉ PLATOBNÉ SIETE	23
BITCOIN ON-CHAIN	24
LIGHTNING NETWORK	26
LIQUID	29
POUŽÍVANOSŤ	31
21-MILIÓNTINA Z NEKONEČNA	
- STÁLE NIE JE NESKORO ZAPOJIŤ SADO BITCOINOVEJ EKONOMIKY	35
JE 21 MILIÓNOV SPRÁVNE ČÍSLO?	36

ČO JE TO BOHATSTVO?	37
DIGITÁLNE ZLATO	39
NIE SME NESKORO - BITCOIN MÔŽE BYŤ DOBRÁ KÚPA AJ KEĎ STE NEBOLI PRI JEHO ZAČIATKU	39
“KRYPTOMENY” NIE SÚ TVRDÁ MENA	41
DEFLÁCIA NEVADÍ - POKROK A ŠETRENIE	42
PARETOVO ROZDELENIE	46
HRANIE SA S PARETOVÝM ROZDELENÍM	47
ZÁVER	48
PREČO NENAKUPUJEM ALTCOINY	51
SÚKROMIEA NO-KYC	55
PREČO JE KYC RIZIKO?	58
RIZIKÁ NO-KYC ZMENÁRNÍ	60
SÚKROMIE JEDNOTLIVÝCH KRYPTOMIEN	61
POROVNANIE SO SÚKROMÍM INÝCH PLATOBNÝCH SIETÍ	64
TRAVEL RULE	67
DYSTOPICKÁ VÍZIA ZAVEDENIA FINANČNÉHO SLEDOVANIA DO KRYPTOMIEN	70
KEDY SÚ KRYPTOMENY NAJLEPŠIE RIEŠENIE	71
UNBANKED POPULÁCIA	72
MEDZINÁRODNÉ TRANSAKCIE MEDZI ĽUĎMI	73
PRODUKTY A SLUŽBY, KTORÉ SA NEDAJÚ BEZPEČNE POSKYTOVAŤ CEZ KLASICKÚ PLATOBNÚ SIETĚ	75
KEDY JE DÔLEŽITÉ SÚKROMIE	76
ŠPECIALIZOVANÉ OBCHODNÉ OPERÁCIE	77

POPLATKY.....	77
VÍZIA PLATOBNEJ SIETE	
- AKÁ JE TEDA MOJA VÍZIA KRYPTOMIEN AKO PLATOBNEJ SIETE?.....	79
VÍZIA ZJEDNOTENIA PLATOBNÝCH POŽIADAVIEK.....	82
VÍZIA ZJEDNOTENIA PLATOBNÝCH SIETÍZ POHLADU OBCHODNÍKOV.....	84
VÍZIA - ZÁVER.....	84
PLATBY MEDZI ZNÁMYMI A RODINOU	87
PREČO PRIJÍMAŤ KRYPTOMENY VO FIRME	91
MARKETINGOVÁ VÝHODA	92
CESTOVATELIA.....	93
SÚKROMIE.....	94
FIRMA AKO TECHNOLOGICKÝ LÍDER.....	94
FINANČNÁ REZERVA A FIREMNÝ KRYPTO ROZPOČET.....	95
RÝCHLOSŤ A BEZPEČNOSŤ PLATBY - ZABUDNITE NA CHARGEBACKS.....	95
ROZŠÍRENIE GEOGRAFICKEJ PÔSOBNOSTI.....	96
KONEKTIVITA DO PLATOBNEJ SIETE.....	97
SÚKROMIE A OCHRANA OSOBNÝCH ÚDAJOV.....	98
NICHE TRHY.....	98
BOHATÍ ZÁKAZNÍCI.....	99
ZÁVER.....	99
AKO PRIJÍMAŤ KRYPTOMENY	101
PRIAMO DO PEŇAŽENKY.....	102
SLUŽBA MENIACA NA EURÁ.....	103
VLASTNÁ BRÁNA.....	104
ZARIADENIA NA PRIJÍMANIE (TERMINÁLY).....	105

PRÍLEŽITOSTI (OBCHODNÉ A PRACOVNÉ).....	107
PRE SPRÁVCOV IT SYSTÉMOV.....	108
PREVÁDZKOVATELIA INFRAŠTRUKTÚRY.....	110
VÝVOJÁRI INFORMAČNÝCH SYSTÉMOV.....	111
ANALÝZA VEREJNÝCH PLATOBNÝCH SIETÍ.....	112
BEZPEČNOSŤ KRYPTOMIEN.....	113
VÝROBCOVIA ŠPECIALIZOVANÉHO HARDVÉRU.....	114
CUSTODIAN.....	114
ESCROW (ZÁBEZPEKA).....	115
STABLECOINY.....	116
SPOTOVÉ A DERIVÁTOVÉ BURZY.....	117
PLATOBNÉ BRÁNY.....	118
ARBITRI A ŠPEKULANTI.....	119
FINANČNÍ KONZULTANTI.....	120
EDUKÁTORI.....	121
PREDAJCOVIA KRYPTOMIEN.....	121
OSTATNÉ POVOLANIA (ÚČTOVNÍCI, PRÁVNICI...).....	121
AKO SPOZNAŤ PLATOBNÚ SIETŤ?	123
FORMÁTY ADRIES.....	125
FORMÁTY PLATOBNÝCH URL (PAYMENT REQUEST).....	127
INÉ PLATOBNÉ SIETE.....	127
MONERO.....	129
BITCOIN CASH.....	129
ETHEREUM.....	129
AKO FUNGUJE SIETĽ LIGHTNING NETWORK	131

ROZDIELY OPROTI BITCOIN BLOCKCHAIN A NETECHNICKÝ ÚVOD	132
PLATOBNÉ KANÁLY	133
OBOJSMERNÁ PREVÁDZKA	135
BITCOIN BLOCKCHAIN AKO RIEŠITEĽ SPOROV	135
SÚKROMIE PLATOBNÉHO KANÁLA	137
Z KANÁLA SIETĚ	137
NA ČO SI DAŤ POZOR PRI LIGHTNINGU	139
ZÁVER.....	140
BITCOIN, ENERGETIKA A PLANÉTA.....	141
ELASTICITA VÝPOČTOVEJ KAPACITY BITCOINOVEJ SIETE.....	143
AKO SA POČÍTA OTEPLENIE O PÁR STUPŇOV?	143
VNÚTORNÁ ŠTRUKTÚRA	
- NAOZAJ NIEKTO PÁLI ZUHOLNATENÉ TRILOBITY V Peci?	146
BITCOIN JE PEER TO PEER - STABILIZÁCIA ELEKTRICKEJ SIETE.....	147
STABILIZÁCIA SIETE VO VÄČŠOM MERÍTKU.....	148
A ČO PROOF OF STAKE?	150
BITCOINOVÉ STRATÉGIE - AKO SI VYBRAŤSPRÁVNÝ MINDSET	155
BARBELL STRATÉGIA.....	157
ÚČTOVNÉ INTERVALY A BOJ PROTI VOLATILITE	160
NETOLERANTNÁ MENŠINA MENÍ SVET	165
ZNÍŽENIE NÁKLADOV	167
ZÁKON KRYPTOMENOVÉHO IZOMORFIZMU	168
ČO ROBIŤ, KEĎ ZAÚTOČÍ MEDVEĎ	169
FUTURE KONTRAKTY	177
DECENTRALIZOVANÝ DOLÁROVÝ ÚČET	183

DOLLAR COST AVERAGING BEZ KYC.....	184
ZÁVER.....	187
DEFI - DECENTRALIZOVANÉ FINANCIE.....	189
CENTRALIZOVANÝ FINANČNÝ SYSTÉM	190
ZMENÁRNE	191
DECENTRALIZOVANÉ STABLECOINY	196
INÉ FORMY PÔŽIČIEK	201
DERIVÁTOVÉ PLATFORMY A SYNTETICKÉ DERIVÁTY	203
STÁVKY A PREDIKČNÉ TRHY	204
POISTENIE	204
AKO ZAČAŤ S DEFI	204
ZÁVER.....	207
AKO VYUŽIŤ HODNOTU BITCOINU BEZ TOHO, ABY SME HO MUSELI PREDAŤ	209
PRINCÍP KOLATERALIZOVANEJ PÔŽIČKY	210
PRÍKLAD PÔŽIČKY CEZ MAKERDAO (OASIS BORROW)	215
PLATFORMA AAVE	218
EFEKTÍVNEJŠIE OTVORENIE POZÍCIE VZHLADOM NA POPLATKY	223
BITCOINOVÉ FUTURES.....	224
KEDY PÔŽIČKU SPLATIŤ?	227
RIZIKÁ A AKO SA S NIMI VYSPORIADAŤ	228
ZÁVER.....	233
DOLÁROVÉ STRATÉGIE V KRYPTOMENÁCH	235
DOLÁRE V KRYPTOMENÁCH.....	236
ÚROČENIE V MONEY MARKETECH	237

POSKYTOVANIE LIKVIDITY NA OBCHODOVANIE	238
DECENTRALIZOVANÝ DOLÁROVÝ ÚČET POMOCOU FUTURES	240
ZÁVER.....	241
NEREGULUJTE KRYPTOMENY!	243
ŽIADNE REGULÁCIE?	246
ZÁVER.....	247
DEREGULÁCIA AKO NÁSTROJ BOJA PROTI KRÍZE	249
NOVÁ KRYPTOEKONOMIKA	252
POVOLENIA NA POBYT A INVESTÍCIE	257
ZVRÁTENIE ODLIVU MOZGOV	259
KRYPTOEKONOMIKA A ŠTÁTNY ROZPOČET	260
MIESTNE VÝHODY POSILNENÉ KRYPTOEKONOMIKOU.....	262
PREČO DEREGULÁCIA.....	263
TRANSFERY RIZIKA A BLOCKCHAINOVÍ KONZULTANTI	267
KRYPTOMENY SÚ REVOLÚCIA	269
PREČO NEMÁM RÁD "BLOCKCHAIN"?	270
SKIN IN THE GAME (ÍSŤ S KOŽOU NA TRH)	272
PREČO SOM SA ROZHODOL VENOVAŤ ČAS KRYPTO-SVETU	275
ZÁKAZOM K INOVÁCIÁM – ZAKÁŽME HOTOVOŠŤ, ABY SME MALI MODERNEJŠIE PLATOBNÉ SYSTÉMY	279
BANKOVÉ PREVODY.....	282
BANKY	283
PREČO NEZAKÁZAŤ HOTOVOŠŤ?	284
CESTA K INOVÁCIÁM	284
KRYPTO NIE, BLOCKCHAIN ÁNO?	287

AKO VZNIKOL BLOCKCHAIN?	288
NA ČO JE DOBRÝ BLOCKCHAIN?	288
VLNY TECHNOLOGICKÝCH "INOVÁCIÍ"	289
KRYPTOMENY, NIE BLOCKCHAIN.....	290
ZÁVER.....	291
CERTIFIKÁCIA ORIGINALITY, NFT, AUKCIE A PRENOS VLASTNÍCTVA	293
ČO JE TO UMENIE ALEBO "MÁM SCREENSHOT TVOJEJ OPIČKY!"	296
FYZICKÉ DIELA A NFT	298
ZNUDENÉ OPIČKY	300
NEHNUTEL'NOSTI.....	301
ZÁVER.....	303
AKO VYTVORIŤ LOKÁLNE PLATOBNÉ SYSTÉMYNA BÁZE BITCOINU	305
BITCOIN, ALE LOKÁLNE	306
LIGHTNING JE VIAC PEER TO PEER	307
PROBLÉMY	309
PREČO LIGHTNING?	309
OKLAMANÍ VYCHYTÁVKAMI - PREČO VÁŠ OBLÚBENÝ KRYPTOPROJEKT PRAVDEPODOBNE NEUSPEJE, AJ KEĎ JE LEPŠÍ	311
LEPŠÍ BITCOIN	313
KOPÍROVANIE VS SIEŤOVÝ EFEKT	316
TECHNOLÓGIE SA VYVÍJAJÚ	316
CHCÚ ĽUDIA VAŠU INOVÁCIU? NAOZAJ?	317
MÁTE NAOZAJ DÔLEŽITÚ FUNKCIONALITU - VIETE ALE VYRIEŠIŤ AJ VŠETKY OSTATNÉ?	318
PODPORA VÝVOJÁROV	318

ČO JE V SKUTOČNOSTI PRODUKT?	320
BITCOIN NEMÁ AUTOMATICKY VYHRATÉ	320
AKO NENALETIEŤ NA KRYPTOMENOVÝ PODVOD.....	323
LEPŠIA KRYPTOMENA	324
GURU FALLACY – AJ VÁŠ OBLÚBENÝ KRYPTO GURU SA MÔŽE ZBLÁZNIŤ	326
KDE JE VAŠA NEFÉROVÁ VÝHODA (EDGE)?	327
TRADING SIGNÁLY – PUMP AND DUMP	328
HEURISTIKA NA DOBRÉ PROJEKTY	328
HEURISTIKY NA OBCHODNÍKOV / TRADEROV	329
STAKING, LIQUIDITY MINING, FARMING, MINING	330
AKO SI DÁVAŤ POZOR NA KRÁDEŽE A SCAMY	332
ČO MÔŽEM ROBIŤ AK SOM SA STAL OBEŤOU PODVODU?	333
SÚ UŽ VŠETKY PRÍLEŽITOSTI NA ZBOHATNUTIE PREČ?	334
NIE JE BITCOIN AKO BITCOIN - AKO BITCOINU VRÁTIŤ PEER TO PEER CHARAKTER A VYUŽÍVAŤ HO NAPLNO.....	335
SUVERENITA	337
NECENZÚROVATEĽNOSŤ	341
NAFUKOVANIE PEŇAŽNEJ ZÁSOBY – MENOVÁ INFLÁCIA.....	342
POŽIČIAVANIE	343
NGU TECHNOLOGIA	343
ZÁBEZPEKA NA PÔŽIČKY	344
PRENOSITEĽNOSŤ CEZ HRANICE.....	344
JEDNODUCHOSŤ NÁKUPU, LIKVIDITA A POUŽÍVATEĽSKÉ ROZHRAŇOVANIE.....	345
DEDIČSTVO	348
SÚ BANK COIN FIRMY ZLÉ?	349

ZÁVER.....	350
PREDIKČNÉ TRHY - CROWDSOURCING INFORMÁCIÍ NA DOBRÉ ROZHODNUTIA	351
AKO VYZERÁ PREDIKČNÝ TRH.....	352
ARBITRÁŽ.....	355
INSIDERI – NIE KAŽDÉHO NÁZOR JE ZAUJÍMAVÝ	357
POUŽITIE VO FIRME	358
VÝBER CEO – PODMIENENÉ TRHY	360
ANONYMITA A ETIKA INSIDER TRADINGU	361
FUTARCHY	362
AKO SI TO VYSKÚŠAŤ	362
CHUDOBNÍ EXPERTI	363
KOBRÍ EFEKT A AKO MENIŤ POMOCOU PREDIKČNÝCH TRHOV SVET	364
AKÉ PREDIKČNÉ TRHY EXISTUJÚ?	366
ZÁVER.....	367
FINANCOVANIE TVORCOV OBSAHU A PODCASTING 2.0	369
REKLAMA – OTRAVA, DÁ SA JEJ VYHNÚŤ?	371
AKO ODMEŇOVAŤ TVORCOV PRIAMO?	372
PODCASTING 2.0.....	374
AKÁ JE TEDA BUDÚCNOSŤ OBSAHU?	376
PARALELNÁ EKONOMIKA - ČAS VEKSLÁKOV JE SPÄŤ	377
OPTIMALIZÁCIA VS. ROBUSTNOSŤ	380
ETICKÍ VEKSLÁCI NASTUPUJÚ NA SCÉNU	381
PROXY OBCHODNÍCI.....	383
ZÁVER.....	384

**AKO NÁJSŤ NIEKOHO OD KOHO KÚPIME KRYPTOMENY
A AKO SI VYTVORIŤ VLASTNÚ VEKSLOVACIU SKUPINU.....389**

VIEŠ MI ODPORUČIŤ NEJAKÉHO VEKSLÁKA ALEBO VEKSLOVACIU SKUPINU?	390
ALE JA NIKOHO NEPOZNÁM!.....	390
ZALOŽTE VLASTNÚ VEKSLOVACIU SKUPINU!	391
PRAVIDLÁ PRE VEKSLOVACIE SKUPINY	391
PREČO NEPOUŽÍVAŤ CENTRÁLNE REGISTRE VEKSLÁKOV?	394

**PARALELNÁ POLIS,PARALELNÉ SPOLOČNOSTI,
INDIVIDUALITA A JEDINCI ZACHOVÁVAJÚCI SI SUVERENITU
- POTREBUJEME INVESTOROV V KRAVATÁCH A KOŠELIACH?395**

PREČO PARALELNÉ SPOLOČNOSTI FUNGUJÚ	400
VNÚTORNÉ PRAVIDLÁ	401
ZNIŽOVANIE VNÚTORNÝCH TRANSAKČNÝCH NÁKLADOV	402
UZAVRETOSŤ A OSTRAKIZÁCIA	403
PARALELNÁ POLIS AKO GENERÁTOR SLOBODY	404
SÚVERÉNNY JEDINEC	406
PEER TO PEER SIETĚ VZŤAHOV	409
JE TO PRE KAŽDÉHO?	410

**ŠIFROVANÉ MESSENGERY
- AKO KOMUNIKOVAŤ SO ZACHOVANÍM SÚKROMIA?413**

PREČO SÚKROMIE?	414
ČO SA SNAŽÍME NAHRADIŤ?	418
TECHNOLÓGIE SÚKROMIA	420
PREHĽAD JEDNOTLIVÝCH MESSENGEROV	421
ZÁVER.....	433

LUNARPUNK - BUDÚCNOSŤ KRYPTOMIEN V REGULAČNOM PEKLE.....435

SOLARPUNK A LUNARPUNK	437
KREATÍVNA DEŠTRUKCIA -PREČO JE DECENTRALIZÁCIA ANTIFRAGILE?	439
PEER TO PEER EKONOMIKA A VEKSLÁCI SPRÍSTUPŇUJÚ KRYPTO	442
PREČO KRYPTOANARCHIA FUNGUJE – OODA LOOP	443
KTO VYHRÁ?	446

ZÁVER.....449

KURZY, KNIHY A ĎALŠIE ODKAZY.....451

ZOZNAM POUŽITÝCH FOTOGRAFIÍ.....	453
----------------------------------	-----

Kryptomeny totiž neašpirujú len na to, aby sa stali novými peniazmi. Jednou z funkcií peňazí je platenie - a na platenie používame všeličo, nie len peniaze. Darčekové certifikáty, čiastočne zľavové kupóny, vernostné body. Prenos hodnoty z bodu A do bodu B, napríklad od zákazníka obchodníkovi, je dôležitá funkcia peňazí.

Rôzne platobné siete majú rôzne vlastnosti. Rýchlosť, veľkosť siete (teda koľko užívateľov medzi sebou dokáže posilať peniaze), cena, odolnosť voči cenzúre, podmienky na vstup do siete, anonymita, možnosť alebo nemožnosť "vrátenia" podvodnej transakcie, bezpečnosť a podobne. Tieto siete si konkurujú a to aj v prípade, že podkladová mena je rovnaká.

TVRDÉ PENIAZE

Bitcoin sú tvrdé peniaze a argument Bitcoin maximalistov o tom, že bitcoinov je 21 miliónov a nikdy ich viac nebude, je dobrým argumentom za "tvrdú menu". Je naozaj tvrdšia ako zlato, o ktorom nevieme, aké množstvo zlata existuje a v prípade monetárneho použitia je možné ho ťažiť z extraterestriálnych objektov - asteroidov alebo iných planét. Ťažba zlata na iných planétach môže v skutočnosti vytvoriť novú zlatú horúčku, akurát namiesto "divokého západu", kam sa ľudia vybrali pešo a na koňoch, bude zahŕňať vesmírne lode.

Aj počas toho ako ľudstvo používalo tvrdú menu - zlato - však používalo aj striebro. Demonetizácia striebra je jednou z najlepšie zdokumentovaných skutočných konšpirácií. Aj zlato však malo rôzne platobné siete - či už poukážky (v podobe bankoviek), prevod vlastníckeho práva v rámci banky a podobne.

Bitcoin maximalisti však tvrdia niečo, čo podľa mňa nie je pravda: "Ne-tvrdých peňazí máme na svete už dosť a nepotrebujeme ďalšie". To je základná premisa Bitcoin maximalizmu ako ho prezentujú niektorí hardcore maximalisti. Iné peniaze (aj fiat) totiž môžu mať lepšiu platobnú sieť - z jedného z pohľadov, ktoré som menoval vyššie. Neexistuje totiž najlepšia platobná sieť. Niektorí preferuje anonymitu, niektorí bezpečnosť, niekoho zaujíma, či môže zaplatiť v obchode, v ktorom nakupuje potraviny, niektorí potrebujú, aby platba prebehla rýchlo, bez kurzových rozdielov a podobne.

FIAT A NETWORK EFFECT

Vyhadzujem smerovku na skútri, ktorá je prakticky neviditeľná, spomalím a zabáčam. Ostatní účastníci premávky zaregistrovali, že sa niečo deje a všetci spomalili. Niektorí pochopili, že idem zastať a obiehamú ma sprava. Premávka na Bali je pekným príkladom spontánneho poriadku - dopravné predpisy prakticky neplatia, dokonca nie všetci jazdia po ľavej strane ako hovoria predpisy. Miestni náčelníci v niektorých okrskoch zakázali Uber, tak tu jazdia Uberisti z okolitých okrskov. A to všetko aj napriek silnému lobbingu tzv. taxi kartelu, ktorý chcel pýtať premrštené ceny. Niektorí by povedali "chcem podporiť lokálnych taxikárov", ale ja hovorím, že rád podporím lokálnych Uberistov. Taxi mafia väčšinou stojí na rohu s nápisom taxi a keď raz-dvakrát za deň nájde nejakého turistu, tak ho odvezie za premrštenú cenu. Okrem toho terorizujú Uberistov - ak vidia turistu s Uber appkou, začnú na neho kričať, "Uber illegal!". Taxi mafia sú jediní nepríjemní ľudia na celom Bali.

Zosadám zo skútra a vchádzam do bankomatovej búdky. Vyberám dva a pol milióna miestnych fiat šitkojnov, zvaných indonézske rupie. Nasadáme na skúter a prichádzame do Alchemy, jednej z mnohých raw vegan reštaurácií. Našťastie nie natoľko raw, že by nám nespravili flat white s kokosovým mliekom.



Indonézske rupie sú prototyp "shitcoinu". Aj napriek tomu, že indonézske banky vám radi otvoria účet aj bez množstva zbytočných otázok, asi nikto by nebol natoľko šialený, že by v danom shitcoine sporil. Keďže aj indonézska centrálna banka si s radosťou vytlačí ďalšie rupie, ak potrebuje niečo odfinancovať, spĺňa táto mena definíciu toho, čo by mnohí krypto fanúšikovia nazvali scam. A to nie len teoreticky a filozoficky, ale aj prakticky - graf ročného rastu cien v rupiách bežne skáče do dvojčíferných čísel.

Z pohľadu Bitcoin maximalistu by som nikdy nemal urobiť to, čo som urobil - ísť do bankomatu a vymeniť moju tvrdšiu menu za superinflačný altcoin.

Ale podobne ako premávka a zákaz Uberu, na Bali jednoducho život plyní inak. Mohol by som zaplatiť aj americkými dolármi - pri nevýhodnom kurze (moja Revolut karta mi dala určite lepší kurz). Niekde dokážem zaplatiť priamo kartou, s 1-2% poplatkom. Na rozdiel od iných krajín na Bali poplatok za platbu kartou platí zákazník, nie obchodník.

Prečo som teda miestnu menu použil? Odpoveď je jasná - sieťový efekt. Miestna mena na rozdiel od tvrdej meny, v ktorej sporím, funguje v potravinách, dá sa za ňu prenajať skúter, hipsterské vegánske flat white, či miestny superimunitný nápoj džamu. Dokonca aj prenájom domu, v ktorom som býval, sme platili - prevodom na účet cez TransferWise (sieť bankových prevodov má tiež network effect).



BITCOIN AKO PLATIDLO

Ako fanúšik Bitcoinu som samozrejme chcel navštíviť miesta, kde sa dá platiť Bitcoinom. Našťastie medzi ne patrila aj druhá vychytená raw vegan reštaurácia Seeds of life (nie som ani vegán, ani superfanúšik raw stravy, ale Bali je miesto, kde je tento druh stravovania vychytený až na formu umenia - miestna krajina, miestne stravovacie náboženstvo - genius loci).

Po fantastickej večeri som teda išiel slávnostne zaplatiť Bitcoinom. Ešte sme posedeli, dopili vodu, dojedli. Keď odchádzame, čašníčka, ktorá síce vie po anglicky, ale na úrovni čašníčky, nie na úrovni Bitcoin maximalistu a krypto fanúšika, ma volá a ukazuje na peňaženke "Unconfirmed". A je jasné, že kým miner transakciu nevyminuje, považuje ma za dlžníka. Namiesto sofistikovanej diskusie o dôležitosti fee marketu som jej vysvetlil, že tu ešte dlho budem, dal jej adresu, kde bývam, mobil, meno a prisahal som, že to miner vyminuje. Moja peňaženka nevedela replace by fee a vysvetľovať pani čašníčke, ako sa robí child pays for parent som nemienil.

Pri ďalších návštevách som platil pekne rupiami, aj so sprejitým.

HIPSTERSKÁ KÁVIČKA ZA ALTCOINY

Toto je pekný príklad toho, že **funkcia platobnej siete a jej sieťového efektu a funkcia sporenia (uloženia hodnoty - store of value)** sú dve odlišné využitia peňazí. Nejakým spôsobom sú síce previazané, ale platiť môžem aj pomocou sietí a mien, ktoré nepoužívam na sporenie. A nielenže môžem, ale aj to prakticky robím - ja aj každý, kto cestuje alebo si sporí v niečom inom ako bežná mena.

S maximalistami súhlasím v tom, že asi nie je úplne dobré spamovať Bitcoinový blockchain hipsterskými vegánskymi flat whiteami. Podľa mňa by to prežil, ale ak chceme zabezpečiť dlhodobú udržateľnosť siete, je to minimálne niečo, nad čím má zmysel uvažovať. V Paralelní Polis v Prahe a neskôr v Bratislave sme problém s vysokými feečkami začali riešiť akceptáciou Litecoinu. Maximalistom sa to nepáčilo (mimočodom, ani mne), ale Bitcoin bol v tom čase na platby jednoducho drahý a nespoľahlivý.

Je značný rozdiel vo Facebook komentároch vysvetľovať svoju maximalistickú životnú filozofiu a to, ako tento problém buď trh vyrieši alebo ako bitcoin treba čisto hodlovať verzus situácia "pani prišla cez pol mesta na kávičku na stretnutie a len poplatky za platbu sú trikrát drahšie ako jej kapučínko".

Druhá možnosť je samozrejme nastaviť supermalý poplatok a veriť, že sa bloky niekedy uvoľnia a miner to raz vyminuje. Niektoré transakcie však nevyminoval - a to je prejav spomínanej nespoľahlivosti. Tá sa prejavovala tak, že ak klient dal príliš malý poplatok, nemusela sa transakcia nikdy potvrdiť, jednoducho vypadla z mempoolu. Klient tieto peniaze časom minul inde.

Nové heslo Bitcoin maximalistov by teda malo znieť: "Neexistuje obed zadarmo, iba ak ho platíte Bitcoinom s nízkym poplatkom". Ale nie je to úplne udržateľný spôsob prevádzkovania akejkoľvek obchodnej prevádzky.

Akceptovanie nového coinu nie je ľahká vec - treba mať na to infraštruktúru, prepojenie s používaným POS systémom, zaškolený personál. Ak platia zákazníci Monerom, barista, ktorý vie urobiť skvelú kávu by mal vedieť aj to, že ak klient zaplatí za flat white a o dve minúty sa rozhodne dať si aj koláčik, výdavok z prvej Monero transakcie môže klient vďaka obmedzeniu siete (nie peňaženky) minúť až cca o 20 minút.

Teda ak si Monero kúpi v ATM, prvú platbu môže urobiť za 20 minút a ďalšiu za ďalších 20 minút. Ak klient platí pomocou stablecoinu DAI (alebo akéhokoľvek iného ERC-20 tokenu), mal by človek za terminálom vedieť, že na to, aby mohol klient transakciu poslať, potrebuje mať aj nejaké Ethereum. A keďže doublespend je triviálny, naozaj je dobré dať vysoké fee a počkať na konfirmáciu.



Platba kryptomenami momentálne vyžaduje vzdelaných klientov aj vzdelaných obchodníkov. V Paralelnej Polis sa snažíme vytvárať vzdelaných klientov. Čo s obchodníkmi?

VISA VS DOLÁR

Vízia Bitcoinu nebola len nahradiť americký dolár, ale aj platobné siete Visa, Mastercard, SWIFT, SEPA. Veriaci v spasiteľa Satoshi Nakamotu môžu filozofovať o tom, či "peer to peer electronic cash" v názve paperu znamenal aj platobnú funkciu. Faktom je, že platobné siete **musíme nahradiť**. Súčasné platobné siete sú drahé, pomalé a najmä sú čoraz viac špiónážnym, nie platobným systémom. Banky a kartové spoločnosti na základe "odporúčaní" neziskovníkov ako Financial Action Task Force (FATF) alebo nadnárodných organizácií ako napríklad OECD bránia dobrovoľnému obchodu medzi ľuďmi. Európska únia dala celú krajinu - Panamu - na "watchlist". Platobné systémy sa stávajú medzinárodným daňovým donucovacím systémom. Ak sa vás banka pýta, čo chcete predávať, predtým ako

vám otvorí účet alebo ak služba na akceptovanie karty chce presný popis toho, čo chcete predávať, niečo nie je v poriadku.

Správna odpoveď by mala byť "chcem ponúkať produkty a služby súkromným osobám a firmám a vy máte len spracovať platbu, a do toho, čo si predávame vás nie je nič".

Môže sa to zdať ako keby vás e-mailový server dva dni po odoslaní e-mailu upozornil, že nerozumie štvrtému odstavcu a potreboval by jeho dovysvetlenie, inak ho nedoručí.

Bitcoin maximalisti túžia nahradiť dolár ako rezervnú menu alebo aspoň vytvoriť tvrdé peniaze, ktoré môžu používať na ochranu proti skrytému inflačnému zdaneniu. A s týmto cieľom súhlasím, podporujem ho a moja odpoveď na otázku "v čom sporím" je už niekoľko rokov "Bitcoin a zlato".

Lenže okrem problému inflačnej dane a sporenia riešime aj iný problém - ako zaplatiť za hipsterský flat white bez toho, aby o tom hneď vedelo niekoľko desiatok firiem, ktoré sa živia prácou s údajmi o súkromných finančných transakciách. Len PayPal uvádza viac ako 600 partnerov, s ktorými zdieľa údaje o vašich finančných transakciách. A je dosť pravdepodobné, že mnohé z tých, ktoré uvádza v kategórii marketingového prieskumu tieto údaje ďalej agregujú a zabalíčkovane predávajú ďalej. Platobné siete sú špiónážne systémy a pre svet je veľmi užitočná dobre fungujúca platobná sieť, ktorá aspoň čiastočne zachováva súkromie (resp. úroveň súkromia má pod kontrolou jej používateľ - či už človek sám alebo obchodník) a nie je cenzúrovateľná (teda napríklad dokážem poslať dobrovoľný príspevok pre WikiLeaks).

Pre platobnú sieť sú dôležité nízke poplatky, ak má byť naozaj masovo používaná. Čím väčší sieťový efekt chceme, tým výhodnejšia sieť musí byť pre obe strany. Necenzúrovateľnosť, súkromie a nízke poplatky sú "killer kombo".

AKO DOSIAHNUŤ SIEŤOVÝ EFEKT

Sieťový efekt hovorí o hodnote siete. V závislosti od štruktúry siete hodnota narastá **lineárne, kvadraticky alebo exponenciálne**.

Lineárny sieťový efekt predstavuje napríklad vysielanie (televízia a rozhlas). Čím viac poslucháčov, tým drahšie môžem predat reklamu, teda hodnota je priamo úmerná počtu účastníkov.

Internet, lokálne siete, ale napríklad aj platobné siete sa riadia tzv. Metcalfovým zákonom, ktorý je pomenovaný po vynálezcovi lokálnej siete Ethernet. Ten si uvedomil, že ak prepojí medzi sebou štyri počítače, hodnota nie je dvakrát vyššia ako keby som prepojal medzi sebou dva počítače, ale je závislá kvadraticky. Prečo to tak je? Ak sú prepojené dva počítače, mám jedno možné komunikačné prepojenie - počítače komunikujú navzájom. Pri troch počítačoch mám tri možné prepojenia, čiže sieť je hodnotnejšia o dve prepojenia navyše. Pri štyroch počítačoch to je šesť prepojení. Vzorec počtu možných spojení je $n*(n-1)/2$ (čo je asymptoticky proporčné n^2). Podobné to je aj pri platobnej sieti - ak sa zapojí do platobnej siete jeden nový užívateľ, môže posilať a prijímať platby s každým používateľom, teda celkové množstvo možných prepojení rastie v závislosti od počtu existujúcich užívateľov kvadraticky.

Sieťové efekty sú pri peniazoch extrémne dôležité a ak máme platobné siete, ktoré navzájom nedokážu priamo komunikovať, ich vzájomné prepojenie alebo naviazanie na sieťový efekt výrazne zvyšuje hodnotu siete.

Vytvorenie sieťového efektu je veľmi zložité, ale napojenie sa na existujúci sieťový efekt môže byť relatívne jednoduché. V časti o vízii sa pozrieme na to, ako prepojiť sieťové efekty viacerých kryptomien a povieme si o tom, ako sieťový efekt vyhackoval Facebook alebo kalendárové pozvánky.

Ako aj pri iných protokoloch Internetu, nemusí sa jednať o jeden protokol. Inak si píšeme instantné správy (Signal, Slack, rôzne "messengeri"), inak vyzerá sieť s obrovským sieťovým efektom (e-mail), zdieľanie súborov (Dropbox, OneDrive, Google Drive, iCloud a množstvo ďalších služieb) a podobne. Aj keď sieťový efekt je dôležitý, dá sa rôznymi spôsobmi "hackovať".

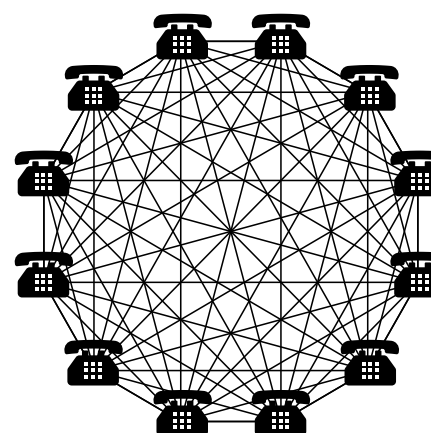
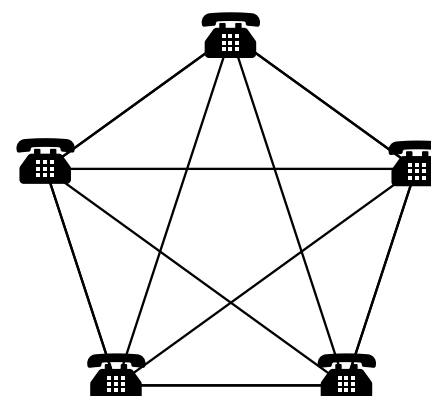
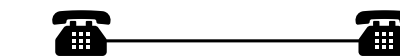


Diagram demonštrujúci sieťový efekt na viacerých jednoduchých telefónnych sieťach. Čiary reprezentujú potenciálne telefónne hovory medzi telefónmi a zvyšujú hodnotu siete.

Môj najobľúbenejší príklad hackovania sieťového efektu je e-mail. Jeho sieťový efekt využili kalendárové pozvánky. Ak niekto nemal kalendárovú aplikáciu podporujúcu štandard iCalendar, dostal obyčajný e-mail s textom "Juraj vás pozval na schôdzku, ktorá sa bude konať v stredu 12:00 v Medickej záhrade v Bratislave". Ak štandard iCalendar pozná, vyskočí táto pozvánka v kalendári a dokážem ju prijať - prijatie tiež príde e-mailom, ktorý dokáže automaticky spracovať kalendárová aplikácia organizátora, ale ak sa to nepodarí, prečíta si to organizátor ako bežnú e-mailovú správu.

Podobný efekt využil aj Facebook, aj keď mnohým ľuďom to tak neprišlo. V čase vzniku Facebooku moja vtedajšia firma spravovala servery jedného z najväčších slovenských poskytovateľov e-mailu zadarmo. Keď Facebook prichádzal na Slovensko, postupne sa počet e-mailov zdvojnásobil až stonásobil. Väčšinou bol odosielateľ práve Facebook. "Niekto komentoval váš príspevok". "Nová žiadosť o priateľstvo". "Jurajovi sa páči váš príspevok". Facebook šikovne využil sieťový efekt e-mailu a e-mailový klient bol vlastne jedným z rozhraní Facebooku, dávno pred appkou s notifikáciami.

E-mail má pritom asi najhorší "fee market". Odoslať aj prijať e-mail nič nestojí. To vytvorilo obrovské požiadavky na decentralizovaný výpočtový aj úložný výkon. Táto forma "Facebook spamu" prišla takmer okamžite a navyše - všetci

tie e-maily chceli, nemohli sme ich jednoducho zahodiť ako spam. Aj napriek tomu sa s tým ľudia vysporiadali, začali vznikať efektívnejšie e-mailové servery, antispam riešenia a podobne.

Adam Back, súčasný CEO Blockstream, dokonca vymyslel Proof of Work riešenie na boj proti spamu - Hashcash. Ten ale nemal sieťový efekt a neujal sa. Aj napriek tomu sú inovácie v e-maili stále možné. Jednou z nich sú sofistikované algoritmy rozpoznávajúce spam. Druhým sú "softforky" e-mailového protokolu - SPF, DKIM a DMARC, ktoré umožňujú zlepšiť doručiteľnosť správnych e-mailov a znížiť množstvo spamu. Niektorí e-mail nahradili - používajú ho maximálne ako identifikátor na prihlásenie, ale komunikácia prebieha v inej aplikácii (Slack, Facebook Messenger, Twitter, Signal, Threema, WhatsApp). A dá sa vytvoriť aj inovatívne riešenie, ktoré rieši niektoré z problémov e-mailu nad daným protokolom. Pre súkromie je to napríklad ProtonMail, Tutanota alebo priamo používanie PGP alebo S/MIME. Pre použiteľnosť a zníženie množstva nežiadaných správ to bola napríklad služba Earn.com, kde musel odosielateľ za doručenie správy zaplatiť adresátovi alebo zo stále fungujúcich Hey.com, kde vám môžu písať len ľudia, s ktorými si písať chcete.

Zaujímavým spôsobom hackovania sieťového efektu sú aj platobné systémy. Vráťme sa do hipsterskej raw reštaurácie na Bali. Môžem platiť rupiami, dolármi, bitcoinom alebo kartami. Pri každom spôsobe sa vystavujeme nejakému riziku a nejakým nákladom. Pri rupiách mám riziko inflácie, takže ich nechcem držať veľa a už vôbec nie dlho. Preto som si vybral vždy iba dva a pol milióna rupií (asi 130€). Na výber som využil sieťový efekt bankomatov a kariet - z množstva kariet som vybral tú, ktorá má najnižšie poplatky a najvýhodnejší kurz. Ak mal obchodník dobrý kurz, platil som aj dolármi. A ak som nechcel vyberať a nemali vysoké poplatky za platbu kartou, mohol som zaplatiť kartou - tiež som si vybral poskytovateľa, ktorý mal najlepšiu kurz. Podobne to bolo aj s platobnou sieťou - rozdiel v cene za prevod cez štandardný medzinárodný prevodný príkaz a s použitím TransferWise bol aj v jednotkách percent.

Pri všetkých týchto prípadoch je jedno, v akej mene sporím. Na prístup do platobnej siete viem veľmi efektívne vymeniť jeden druh (digitálnej alebo fyzickej) vzácnosti za iný - či už explicitne (výber z bankomatu, zmenáreň) alebo to za mňa urobí prevádzkovateľ automaticky.



PRÍLEŽITOSTI

(OBCHODNÉ A PRACOVNÉ)

PRE SPRÁVCOV IT SYSTÉMOV

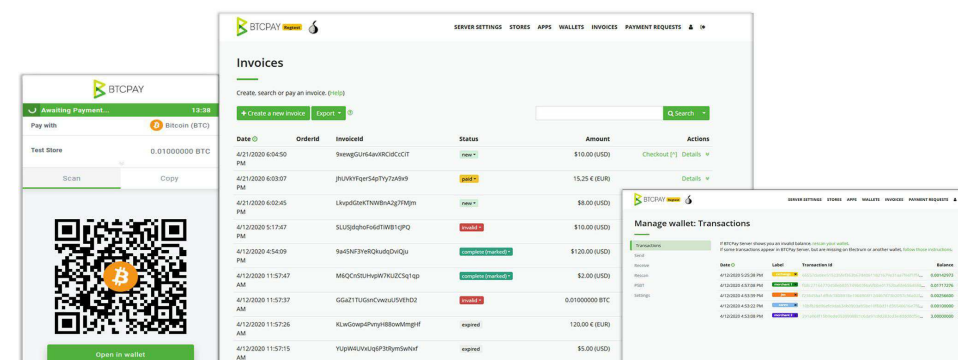
Platobné siete na báze kryptomien prinášajú nové požiadavky aj na vývojárov softvéru a správcov IT systémov. Internet do vynájdenia Bitcoinu nemal protokol na priamy prenos hodnoty (teda vzácnosti). Mali sme protokol na výmenu kopírovateľných správ (napríklad vo forme e-mailov - SMTP, súborov - FTP, HTTPS, či streamovaného videa). Protokol na výmenu niečoho vzácného sa dal síce ovládať pomocou API volaní, ale samotný prenos nešiel cez štandardizovaný protokol cez otvorený internet, ale v rámci privátnych sietí (SWIFT, Visa, MasterCard a pod.).

S príchodom kryptomien máme natívne protokoly, pomocou ktorých dokážeme posilať niečo vzácne (napríklad Bitcoin). Táto sada protokolov sa v prípade Bitcoinu volá LNP/BP - "Bitcoin Protocol / Lightning Network Protocol".

Pre správcov systémov z toho vyplýva niekoľko novinek:

- Spravujú systémy, v ktorých je niečo hodnotné a nevratné. Mnohé burzy, vrátane slovenskej Eterbase to zistili na vlastnej koži - ak ich niekto hackne a ukradne im coins, sú preč. Nie je banka, do ktorej by sa dalo zavolať, aby vrátili transakciu, pretože všetky potvrdené transakcie sú finálne. To vytvára úplne nové požiadavky na bezpečnosť systémov.
- Je potrebné spravovať cold storage a hot wallets riešenia, dokázať medzi nimi rozumne bezpečne posilať peniaze. Správcovia by mali rozumieť multisignature schémam a vedieť bezpečne uložiť coins, s ktorými organizácia nechce hýbať (napr. ich má v rámci pokladne ako finančnú rezervu).
- Správcovia musia rozumieť platobným bránam, pretože platobná brána (napríklad BTCPayServer) nemusí byť iba API, ktoré voláme, ale softvér, ktorý toto API poskytuje je tiež v správe organizácie, pre ktorú pracujeme. Je to ako keby ste okrem komunikácie s PayPalom pomocou platobného pluginu museli bežať aj server PayPalu.

- Treba rozumieť platobnej funkcii kryptomien - kedy je transakcia potvrdená a čo to znamená.
- Treba rozumieť smerovaniu platieb v sieti Lightning network a čo to znamená pre prevádzku. Je to podobné ako ovládať sieťové smerovacie protokoly typu OSPF.



Open-source systém pre obchodníkov na prijímanie kryptomien BTCPayServer.

Tieto nové internetové protokoly však umožňujú aj nové veci. V prvom rade, je to na správcov, aby si vybrali aký softvérový stack budú používať - rovnako ako si vyberajú, či ako webserver použijú nginx alebo Apache, budú si vyberať implementáciu full-node, platobnej brány, lightning daemon a podobne. V tomto je možné inovovať a zlepšovať dostupnosť, bezpečnosť, rýchlosť a užívateľské pohodlie.

Lightning protokol dokonca umožňuje mikropłaty, napríklad za výpočtový výkon alebo API volania. Niektorí cloudoví poskytovatelia to už poskytujú a pomocou kryptomien dokážete zaregistrovať doménu, či si prenajať virtuálny server. Zaujímavá je aj možnosť preúčtovať platby v rámci organizácie - okamžite, pay as you go.

Z pohľadu správcov samozrejme nedôjde k adopcii vo všetkých organizáciách rovnomerne. Správcovia "family offices" bohatých rodín už túto potrebu naplňajú dnes. Väčšie eshopy alebo poskytovatelia platobných služieb (napríklad spomínané platobné brány) postupne nabiehajú.

Zaujímaví sú aj "domáci správcovia", keďže na to, aby ste mohli bežať svoj kryptomenový "family office" nepotrebuje okrem Bitcoinu vlastniť aj tri hrady a štyri jachty. Domáci užívatelia "suverénnych Bitcoin nodes" ako Nodl, MyNode alebo RaspiBlitz bežia platobný systém, nodu, či crowdfunding modul u seba doma a prístupujú k týmto službám cez Tor odkiaľkoľvek na svete z počítača alebo mobilných aplikácií.

PREVÁDZKOVATELIA INFRAŠTRUKTÚRY

Veľká časť kryptomenovej infraštruktúry bude outsourcovaná. Príkladom je firma Infura, ktorá poskytuje pomocou plateného API prístup k Ethereum a IPFS implementáciám. Spravuje ich, stará sa o škálovanie, dostupnosť a podobne. Prevádzkovatelia infraštruktúry budú zamestnávať správcov krypto systémov.

Špeciálnym prípadom infraštruktúry sú poskytovatelia Lightning infraštruktúry (Lightning Service Providers - LSP). Sú to firmy ako ACINQ, Breeze, Bitrefill, ktoré poskytujú peňaženku, likviditu, smerovanie a zabezpečujú platby v platobnej sieti.



Náčrt architektúry Ethereum Dapp bežiacej na infraštruktúre spoločnosti Infura

VÝVOJÁRI INFORMAČNÝCH SYSTÉMOV

Integrácia na platobné brány (či už self-hosted ako BTCPayServer alebo brány tretích strán ako CDPay, BitcoinPay alebo BitPay) sa až tak veľmi nelíši od bežných integrácií na systémy ako Stripe alebo PayPal. Kryptomenové platobné siete však poskytujú mnohé doteraz nevídané možnosti, ktoré vývojári môžu použiť.

Jednou zo základných novinek sú tzv. "Streaming payments" alebo rýchle mikroplatby. Užívatelia môžu platiť napríklad za streamované video alebo nabíjanie elektrického auta v sekundových intervaloch. To znižuje potrebu dôvery v druhú stranu - ak prestane fungovať video/dodávka energie, prestane klient platiť. Ak prestane klient platiť, prestane byť dodávaná služba.

Druhou dôležitou funkciou sú skriptovateľné platby, z ktorých najjednoduchšou sú multisig adresy, teda adresy vyžadujúce m-z-n podpisov. Pomocou 2-z-3 multisig schémy je možné implementovať bankovú službu "dokumentárny akreditív", čo robím aj v mojej firme TEDSig.com. Predstavte si, že predávate nehnuteľnosť. Predávajúci chce, aby kupujúci "zamkol" peniaze (tradične sa to robí u notára alebo v banke) a tie sa uvoľnia po zapísaní zmeny vlastníka nehnuteľnosti. Za normálnych okolností ide všetko v pohode a obe strany sa dohodnú na uvoľnení platby predávajúcemu (pripoja svoje dva podpisy k vopred dohodnutej platbe). V prípade nezhody problém rieši tretia strana (u nás zastrešená advokátskou kanceláriou Blockchain Legal).

Kontrakty na strane Bitcoinovej siete môžu byť oveľa zložitejšie. Môžu mať formát "pošlem ti ekvivalent 100€ o mesiac", čo do veľkej miery rieši volatilitu (technológia sa volá Discreet Log Contracts, pozrite si našu víziu aj s možnosťou implementácie nad sieťou Lightning Network).

Vývojári taktiež môžu vytvárať a nasadzovať tokeny nad rôznymi sieťami - Liquid, Ethereum... Tie môžu reprezentovať vernostné body a podobne.

Vývojársky ekosystém kryptomien je bohatý a už dnes môžete používať knižnice, hotové riešenia, dokonca môžete skripty na "programovateľné peniaze" programovať v rôznych jazykoch - pri Bitcoine sú to napríklad Bitcoin Script, MiniScript, Ivy, alebo minsc, pri Ethereum Solidity a Vyper.

Aj keď vývojári často skočia hneď po riešeníach na sieti Ethereum, kvôli “turing-complete” programovacím jazykom, na ktoré sú zvyknutí, nad Bitcoin scriptom (ktorého modifikácie používa aj Litecoin a Bitcoin Cash) sa toho dá urobiť skutočne veľa, vrátane derivátových obchodov. Je nad ním dokonca priamo postavená sieť Lightning network.

V čase písania tohto textu sú príležitosti pre programátorov takmer neobmedzené. Je toho ešte veľmi veľa, čo treba v ekosystéme kryptomien vyvinúť. Odporúčam začať zapojením sa do vývoja niektorých open-source projektov.

ANALÝZA VEREJNÝCH PLATOBNÝCH SIETÍ

Analyzovanie verejných platobných sietí alebo “blockchainová analýza” je tvorená ľuďmi a firmami, ktorí poskytujú službu analýzy blockchainu pre štáty, daňové úrady, banky a podobne. Osobne ich vnímam negatívne, pretože sú opačnou stranou súkromia, snažia sa ho narúšať. Je to ekvivalent organizácie alebo analytika, ktorý sa rýpe v cudzom súkromí a nahlasuje podozrivé transakcie.

Túto rolu uvádzam preto, lebo je to pracovná príležitosť vytvorená na poli kryptomien a mali by sme vedieť, že tieto služby využívané bankami a daňovými úradmi existujú. Zároveň niektoré typy firiem, ktoré pracujú s kryptomenami, musia využívať ich služby, aby preukázali, že bojujú proti praniu špinavých peňazí - ide najmä o burzy.

Hodnotovo stojím na druhej strane a dúfam, že technické vylepšenia kryptomien budú prácu tzv. “chain analytikom” sťažovať ako to bude len možné.

Nie je však dobré bojovať proti praniu špinavých peňazí, ktoré boli ukradnuté alebo získané nekalým spôsobom? Samozrejme, zarábanie nekalým spôsobom neschvaľujem. Mali by sme sa však sústrediť na to, aby sme zločinom zabráňovali. Ak banka preperie peniaze napríklad z vydierania alebo krádeže z verejného rozpočtu, znamená to, že predtým došlo ku krádeži alebo k vydieraniu a to je práve to, čomu by sme mali zabrániť, vyšetriť a prípadne obete odškodniť. Toky peňazí nás často dovedú k zločinom, ale tam bohužiaľ vyšetrovanie končí. Vydierač alebo zlodej nie je potrestaný, iba finančná inštitúcia, ktorá mu pomohla zlegalizovať príjmy z tejto činnosti dostane pokutu alebo stratí licenciu. A to je málo.

Peniaze ako také sú pritom “zameniteľné” (fungible). Ak platím 10€ bankovkou na pokladni v potravinách, nečakám, že pokladnička bude robiť aj rolu “forenzného analytika” a skúmať, či som náhodou tých 10€ nezískal nekalým spôsobom. Ale presne k tomuto “blockchain analýza” smeruje. A je to lukratívny biznis.

Viac o narušeníach súkromia v kapitole o KYC.

BEZPEČNOSŤ KRYPTOMIEN

V tejto kategórii máme niekoľko rolí. Jednak ochranu samotných kryptomien, teda vytvorenie bezpečnostného úložiska na kryptomeny - tzv. “cold wallet” alebo “cold storage” ukladanie kryptomien na offline počítačoch, správa peňaženiek alebo multisignature schém (tieto schémy vyžadujú viac podpisov na poslanie kryptomien).

Ďalšou dôležitou súčasťou je fyzická bezpečnosť - čo sa stane ak do kancelárie napríklad burzy príde človek s nabitou zbraňou - odíde s podpísanou transakciou alebo nie? Dá sa zabrániť tomu, aby do tej kancelárie vôbec vstúpil?

Samozrejme, netreba zabezpečiť iba peňaženku, téma je to komplexná. Všetko čo vyvíjajú vývojári a spravujú správcovia IT systémov treba zauditovať. Smart kontrakty resp. skripty, API platobných brán, systémy, na ktorých toto všetko beží.

Verím, že bezpečnostní analytici a firmy sa budú špecializovať na bezpečnosť kryptomien, pretože sa trochu odlišuje od bežnej bezpečnosti. Psychológ Nathaniel Branden mal vo svojej kancelárii plagát s nápisom: “Nikto vás nepríde zachrániť”. Počas skupinovej terapie sa ho klientka pred ostatnými účastníkmi opýtala: “Ale Nathaniel, ty si prišiel”. “Áno, ale iba preto, aby som vám povedal, že vás nikto nepríde zachrániť.” Pri kryptomenách je to podobné. Ak burzu (ako napríklad slovenskú Eterbase) niekto hackne a prevedie kryptomeny na inú adresu, nepomôže im polícia ani centrálna banka. Kryptomeny sú fuč a nikto vás nepríde zachrániť.

Z tohto pohľadu sú kryptomeny citlivejšie na bezpečnosť ako napríklad banky. Ak niekto napadne banku alebo centrálnu banku, je možné peniaze ľahšie vystopovať a prípadne vrátiť transakciu. Podobne je to aj s platobnými kartami -

O bitcoine alebo kryptomenách počul azda každý. V médiách sa objavujú vo chvíľach, kedy už navždy umreli (cena trochu padla) alebo keď sa všetci zbláznili a nakupujú (cena trochu stúpla). Málokto sa však zaoberá tým **ako kryptomeny používať vo svojom živote**.

Ako používať niečo, čoho cena šialene skáče? A ak nás cena nezaujíma, dajú sa kryptomeny použiť inak? Napríklad na financovanie tvorcov, či crowdfunding. Môžete si pomocou kryptomien zobrať pôžičku? Ako ich využiť v medzinárodnom obchode, či na propagáciu svojich produktov? Ako vybudovať lokálnu krypto ekonomiku vo svojej sociálnej bubline? Dá sa bitcoin využiť na rozšírenie osobných a sociálnych kontaktov? Bitcoin môžeme použiť dokonca aj ako formu "poistenia" proti zlyhaniu tradičného finančného systému.



Juraj Bednár je sériový podnikateľ a hacker. Založil niekoľko firiem v oblasti informačných technológií. Je spoluzakladateľom neziskového projektu **Paralelná Polis** (Praha, Bratislava), vďaka ktorému objavil potenciál kryptomien v živote aj v podnikaní a autorom kníh **Hackni sa!** a **Veľký reštart**, ktoré sú svojou štruktúrou podobné a ich cieľom je pootvoriť mysle a ukázať možnosti, ktoré svet prináša, ak máme odvahu experimentovať.

ISBN 978-80-570-4272-3



9 788057 042723