S předmluvou Jeffreyho Tuckera

Bitcoin

a jiné krypto peníze budoucnosti

Historie, ekonomie a technologie kryptoměn,
stručná příručka pro úplné začátečníky

Dominik Stroukal
Jan Skalický

GRADA®

GRADA®

Bitcoin

a jiné krypto peníze budoucnosti

Grada Publishing

Bitcoin

a jiné kryptopeníze budoucnosti

Historie, ekonomie a technologie kryptoměn,
stručná příručka pro úplné začátečníky

Dominik Stroukal
Jan Skalický

Praha 2018

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. Druhé, rozšířené vydání 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 ... 13

Předmluva k druhému vydání: Bitcoin už mění svět k lepšímu ... 14

Předmluva k prvnímu vydání: Bitcoin není peněžní systém ... 15

Úvod ... 19

Peníze budoucnosti ... 20
- Vynález, který změní svět k lepšímu ... 20
- Léčba šokem ... 21
- Budoucnost je krásná ... 22

Bitcoin: Příběh ... 23

2009: Genesis ... 24
- Kdo je Satoshi Nakamoto? ... 24
- Padající hvězdy ... 28
- Digitální terorista ... 29
- Poučné příběhy ... 31
- Dobré peníze ... 32
- Nekryté, ale vzácné ... 34
- Peníze bez tiskárny ... 34

2010: Nejdražší pizza dějin ... 38
- Ďobající programátor ... 38
- Chyby ze zlata ... 40

2011: Nahoru, nahoru a dolů ... 43
- Nahoru ... 43
- Dolů ... 44
- Kryptozloději ... 46

2012–2013: Raketou do budoucnosti ... 48
- Kostky jsou vrženy ... 48
- Žít Bitcoin ... 49
- Sjet si hedvábnou stezku ... 52
- Bitcoin a média ... 54

2014–2015: Dolů ke hvězdám ... 57
- Pád z hory Gox ... 57
- Regulace v Evropě ... 59
- Rok stimulujícího klidu ... 60

2016–2017: Hodl to the moon! ... 63
- Sklízení úrody ... 63
- Daň z úspěchu ... 64

Příručka uživatele kryptoměn ... 67
Pořízení peněženky ... 68
První kroky ... 68
Úsporný software ... 69
Mince na webu ... 71
Mobilní Bitcoin ... 73
Kde bitcoiny koupit ... 75
První mince ... 75
Směnárny a burzy ... 78
Další možnosti ... 81
Jak bitcoiny vytěžit ... 82
Krumpáče do rukou ... 82
Horníci v bazénu ... 85
Jak bitcoiny ochránit ... 88
Bitcoin není jiný ... 88
TREZOR ... 88
Jde to i na papíře ... 91
Jak a kde ho používat ... 94
První nákup ... 94
Příjem bitcoinů ... 95
Jak na něm vydělat ... 99
Experiment za všechny prachy ... 99
Algoritmus na štěstí ... 101
Nic jiného než poptávka ... 103
Chceš haš? ... 104
Daně :(... 105
Jak být anonymní ... 108
Nevidět nic ... 108
Vidět všechno ... 109

Ekonomie a technologie kryptoměn ... 111
Ekonomické základy Bitcoinu ... 112
Rakouské kořeny Satoshiho Nakamota ... 112
Svobodné bankovnictví ... 113
Bitcoin jako peníze ... 115
Hlasy z druhých břehů ... 117
Svět bez hospodářských krizí ... 119
Škálování Bitcoinu ... 122
Jak zlepšovat Bitcoin ... 122
Cože? Vidličky a nože ... 124
Fork a změna pravidel ... 125
Vidličky z korundu ... 126
Forkování Bitcoinu ... 128
Bitcoin XT, Unlimited, Classic, Segwit ... 129
UASF, Segwit2x ... 131
UAHF, Bitcoin Cash ... 133

Škálování, neškálování a kolosální poplatky ... 135
Lightning Network ... 137
Blesky v síti ... 139
Alternativní kryptoměny ... 142
Co je to „altkojnt" ... 142
Zoologie altcoinů ... 142
Kdo drží, má za tři ... 144
Čeříme s Ripple ... 146
Klasické deriváty – Namecoin, Litecoin, Peercoin ... 147
Je libo anonymitu? ... 150
CryptoNote není vidět ... 151
CryptoNote je vidět, když chce ... 153
CryptoNote v praxi – Bytecoin, Monero ... 154
Kouzla s anonymitou ... 156
Od Zerocoin k Zerocash ... 157
A co Dash? ... 159
Virtuální mašina jménem Ethereum ... 160
Další kryptoplatformy ... 162
Metacoins ... 163
Sidechains ... 164
ICO, letní láska roku 17 ... 165
Dobrý, zlý a ošklivý altcoin ... 166

Budoucnost Bitcoinu ... 169
Možné problémy ... 170
Je bitcoinů málo? ... 170
Není málo adres? ... 171
Většina útočí ... 172
Pálení elektřiny ... 173
Regulace ... 175
Úřad pro zničení Bitcoinu ... 175
Dějiny úřadu ... 176
První vlaštovky ... 177
EU pro, Čína proti ... 178
Poštátnění Bitcoinu ... 180
Nové trhy ... 183
Víra v Bitcoin ... 183
Apoštolové blockchainu ... 183
Byznys jménem Bitcoin ... 185
Soukromé blockchainy ... 186
Válka o Bitcoin ... 188
První bitvy ... 188
Vítězná linie ... 189

Doslov ... 193
Tečka za tečkou, blok za blokem ... 194

Rejstřík technických pojmů ... 197

Předmluvy

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, nenavrhnul 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.

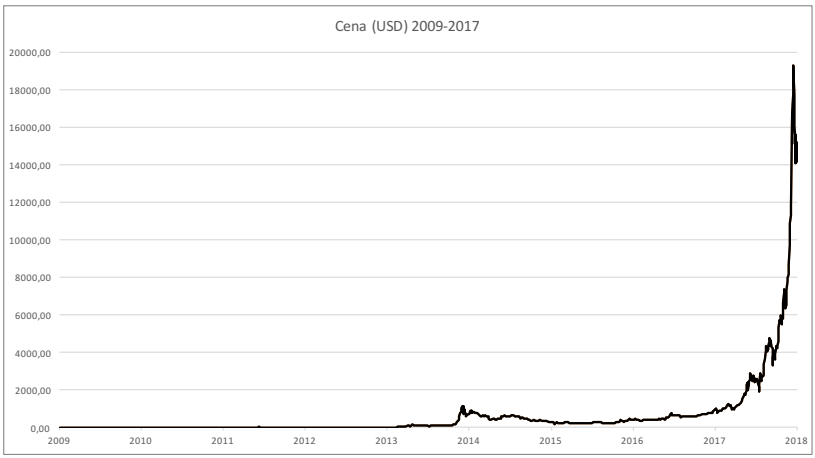
Nakonec to netrvalo dlouho a z Jeffreyho Tuckera se stal jeden z nejviditelnějších stoupenců Bitcoinu na světě. Ve svých přednáškách po celém světě vyvrací přesně to, co si sám kdysi myslel. Přijímá bitcoiny, platí bitcoiny, miluje Bitcoin. Dokonce je mu vyčítáno, že to s láskou k němu přehání.

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.

To je nesmírně důležitá a zásadní inovace. Už od začátků rozšiřování internetu existovaly tendence k vytvoření digitálních peněz. Kryptografové, ekonomové a podnikatelé se snažili přijít s životaschopným konceptem, ale jen minimum pokusů bylo alespoň trochu úspěšných. Hlavním problémem digitálních měn totiž byla možnost **„dvojité útraty"** („double spend"). Pokud víme, že virtuální peníze jsou pouze digitální informací, potom by se mohlo stát, že by někdo duplikoval svůj peníz a zaplatil jím dvakrát.

Dvojitá útrata (Double Spend)

typ útoku na bitcoinovou síť, kdy se útočník snaží použít stejné bitcoiny (přesněji týž výstup nějaké existující **transakce**) vícekrát (přesněji na vstupech více než jedné nové **transakce**). Tento útok se realizuje mnohem snadněji, pokud příjemce platby nepožaduje **potvrzení** příslušné **transakce** – stačí každému příjemci anoncovat (rozeslat) pouze jemu určenou **transakci**. Čím větší počet **potvrzení** příjemce platby požaduje, než ji uzná za provedenou, tím hůře se útok realizuje. Útočník je nucen rychle vytěžit alternativní **bloky** a tím obětovat svůj výpočetní výkon k útoku, jehož nejistota úspěchu roste s počtem **potvrzení**, která musí svojí alternativní větví **blockchainu** „obejít".

Nebezpečí dvojité útraty byl zásadní problém, který se standardně řešil prostřednictvím centrální autority, které uživatelé mohli věřit. Avšak existence centrální autority je problém sám o sobě. Centrum se dá zničit úspěšným útokem škodolibého hackera. Anebo pokud se měna znelíbí vládě, je snadné zavřít centrální server, zatknout jeho provozovatele a měnu zakázat. A že se některým vládám nebude konkurence příliš líbit, se dá pochopitelně očekávat.

Nakamotovi se podařilo tento problém odstranit vytvořením tzv. **blockchainu**, jakési „účetní knihy", která je veřejná a sdílená všemi uživateli Bitcoinu. Ti potvrzují transakce stejně, jako je tomu u centrální autority, avšak v případě Bitcoinu decentralizovaně. Všichni uživatelé mohou vidět záznamy o všech transakcích v celé historii. Pokud někdo nakopíruje bankovku a příjemce kopii nepozná, může zaplatit novou i původní bankovkou. Avšak kdyby byly všechny záznamy o platbách tradičními bankovkami uložené veřejně a u mnoha uživatelů, snadno bychom si všimli, že se podvodník snaží zaplatit něčím, co nemá. Navíc k takové kontrole není zapotřebí budovat centrální autoritu.

Řetěz bloků (Blockchain)

spojový seznam (seznam s odkazy na předky) **bloků**. Spojení je dosaženo obsažením **hashe** předchozího **bloku** v datech **bloku** následujícího. Každý **blok** má tedy jednoznačně určeného předka (s výjimkou úplně prvního bloku, tzv. **genesis blok**, kde místo **hashe** předka je 0). Jelikož předek **bloku** je jeden, graf vztahů mezi **bloky** je strom (neobsahuje cykly – „spojení dokola"). K větvení však dochází velmi zřídka (viz **Fork**) a strom **bloků** tak vypadá spíš jako jedna dlouhá větev místy s krátkými výhonky délky 1–2. Ze všech větví, včetně výhonků, se ale v každém okamžiku pracuje pouze s nejdelší z nich (přesněji s tou, jejíž **bloky** bylo nejpracnější spočítat) a té se říká **blockchain**, protože už nejde o strom, ale o jeden lineární řetěz. **Bloky**, které zůstaly v nepokračujících větvích, se ignorují. Relevantní jsou naopak **bloky** v **blockchainu** a **transakce** v nich zahrnuté jsou považovány za potvrzené.

Tato koncepce umožňuje ukládat historii tak, že je nepřepsatelná, neboť modifikace **bloku** zprostřed řetězu by vyžadovala přepočítání všech následníků (obsahují **hash** předka, který se při modifikaci dat změní), což mj. znamená, že by se při přepočítávání nepracovalo s nejdelší větví – nejdelší zůstává původní řetěz, který navíc je (resp. může být) obsažen na všech ostatních uzlech sítě (síť je decentralizovaná).

Padající hvězdy

Historie digitálních měn není dlouhá, ale obsahuje již řadu důkazů o tom, jak významnou inovací blockchain je. O tom, že řešení problému dvojité útraty pomocí centralizace není životaschopné.

Zprvu se digitálním měnám říkalo spíše digitální peníze a jejich čas přišel až s masivním rozšířením internetu v devadesátých letech. Šlo o první náznaky skutečného řešení problémů tradičního bankovnictví.

S první velkou digitální měnou historie přišla společnost Digicash, později provozující měnu ecash. Digicash vytvořil kryptograf David Chaum, kterému je někdy přezdíváno otec digitálních měn nebo otec anonymní komunikace. Někteří lidé dokonce spekulují, že Chaum je Satoshi Nakamoto. A mohl by být. Během osmdesátých a devadesátých let přišel Chaum s mnoha inovacemi na poli digitální komunikace. V roce 1982 představil kryptografický systém pro anonymní transakce a v roce 1990 ho uvedl v život pod názvem ecash. Naneštěstí o několik let

později vyhlásil bankrot. Mnozí pozorovatelé se domnívají, že Chaum požadoval příliš anonymity pro své uživatele, a nebyl tak schopen do své měny vtáhnout státní peníze. Jeho systém nebyl určený pro nahrazení celého peněžního systému. Chtěl pouze přijít s alternativou k současným peněžním mikrotransakcím, k drobným peněžním převodům, které považoval za příliš složité a málo anonymní, zejména pak pomocí platebních karet či šeků. Chaum byl a stále je dle všeho v silné opozici proti vládnímu establishmentu, podařilo se mu přijít s první digitální měnou a je autorem myšlenky anonymní decentralizované komunikace typu Tor (virtuální „internet v internetu", který přepojuje vaši komunikaci přes různé počítače kolem celého světa, aby nebyla vaše činnost vystopovatelná k vašemu poskytovateli připojení).

Ecash byl výjimečným vynálezem, ale nepředstavoval dostatečnou revoluci. Stejně jako po letech PayPal, který skutečně zjednodušil mikroplatby na internetu, ale stále jde o dolary, o koruny, o tradiční měnu, akorát kódovanou v elektronické podobě. Bitcoinu se taková služba nepodobá. Přitom, z dnešního pohledu zpět do historie, příliš nechybělo.

Brzy však vznikly i další měny, některé velmi podobné Bitcoinu. Objevil se CyberCoin, milicent, Visa Cash, Mondex, ePassport, Liberty Reserve, Liberty Dollar, E-gold a další. Některé byly slepými uličkami, jiné ukázaly cestu, kudy nejít, a naznačily směr, kterým se dostaneme ke kýžené digitální měně. Některé příklady také jasně ukazují, proč se patrně nikdy nedozvíme, kdo je ve skutečnosti Satoshi Nakamoto.

Digitální terorista

Především se totiž ukázalo, že nelze vytvořit konkurenci státním penězům, aniž byste dříve nebo později neskončili u soudu. Dobře to ilustruje příklad měny E-gold. E-gold byla digitální měna krytá skutečným zlatem, které společnost tvůrců nakupovala a skladovala. Vláda se do E-goldu mohla snadno opřít, jelikož znala její tvůrce a sídlo společnosti. Ti skončili u soudu a E-gold skončil.

S pádem E-goldu spadla i měna s názvem 1mdc, která byla založena v roce 2001. Vzájemnou souvislostí totiž bylo, že 1mdc byla kryta E-goldem a sama žádné zlato neuchovávala. To mělo jistě

zásadní výhodu v nákladech (a 1mdc údajně užívala většina majitelů největších účtů na E-goldu), ale nevýhodu ve skutečnosti, že byla měna závislá na existenci jiné měny, která přestala fungovat.

Podobný příběh čekal na tvůrce populárního Liberty Dollaru. V roce 2011 byl jeho vynálezce, Bernard von NotHaus (na rozdíl od Satoshiho Nakamota nejde o pseudonym, jak by se mohlo na první pohled zdát), odsouzen za padělání peněz a terorismus. Bernard von NotHaus si pouze všiml, že americké dolary již desítky let nejsou ničím kryté (a nemají ani žádný pevně stanovený limit zásoby), a mohou tak podléhat zkáze skrze libovůli státu a centrálních bankéřů. Vytvořil tedy alternativní peníze, které byly kryté drahým kovem. Bohužel i to je dnes možné považovat za terorismus. Prokurátorka Anne Tompkins dokonce u soudu prohlásila, že šlo o „jedinečný případ terorismu". Dále tvrdila, že se von NotHaus snažil zničit měnu své vlastní země. Někdo by řekl, že se ji snažil zachránit. Úhel pohledu je mocná zbraň.

Obdobně byl zatčen a odsouzen autor digitální měny Liberty Reserve, kterou používalo přes jeden milion lidí. Americká vláda obvinila Arthura Budovskyho z praní špinavých peněz a společnost mu zabavila. V roce 2013, kdy Budovskyho ve Španělsku dopadli a zatkli, šlo o nejstarší existující digitální měnu, jelikož vznikla již v roce 2001. Společnost jednoduše převáděla tradiční peníze na Liberty Reserve dolary nebo Liberty Reserve eura a poté z každého transferu účtovala jednoprocentní poplatek. Pointou bylo opět ukládání peněz do zlata, avšak Liberty Reserve nabízel i možnost ukládání do dolaru či eura.

Úřadům se tento postup však nezdál. Jeden z šéfů americké kriminální policie dokonce prohlásil, že „pokud by žil Al Capone, tady by skrýval své peníze". Dnes je stránka libertyreserve.com prázdná, respektive na ní návštěvníky čeká pouze známý obrázek konfiskace domény americkými úřady.

Poučné příběhy

Mnohem tragičtější příběh připravil e-Bullion, zlatem krytá digitální měna manželů Jima a Pamely Fayedových. Ti získali mezi lety 2001 a 2008 přes milion uživatelů a nashromáždili přes 50 tisíc uncí zlata. V roce 2008 se však Jim nechtěl rozvést s Pamelou a nechal ji zavraždit, za což byl nakonec odsouzen k trestu smrti. E-Bullion skončil v rukách vlády, přestože byla obvinění proti společnosti samotné stažena. Stačilo se odvolat na americký „protiteroristický" zákon Patriot Act. Nikdo z uživatelů nedostal ani dolar nazpět.

Důležitým mezníkem v dějinách digitálních měn byl CyberCoin, měna společnosti CyberCash, která vznikla na konci devadesátých let. Bohužel se stala obětí problému roku 2000 (Y2K problem). Některé počítače totiž na přelomu tisíciletí nedokázaly nastavit datum na 1. ledna 2000, protože jejich číselný rozsah pro rok dosáhl maximální hodnoty a místo toho se vrátili na jeho začátek – do roku 1900. Autoři CyberCoinu si museli říkat, jak je možné, že počítačoví vývojáři v devadesátých letech byli tak krátkozrací. Nicméně byli a CyberCoin zaznamenal řadu dvojitých transakcí, což ho srazilo na kolena. O rok později vyhlásil bankrot.

Digitální měny ale nikdy nepřestaly být populární, ba naopak. O své místo na slunci se praly i velké firmy jako Visa nebo MasterCard. Visa přišla se svým konceptem Visa Cash a MasterCard zakoupil od National Westminster Bank elektronický peněžní systém Mondex. Tyto platební systémy se neukázaly životaschopné a brzy skončily. Obě společnosti se nadále věnovaly tradičnímu bankovnictví.

Příběhy těchto měn jsou poučné i pro Bitcoin. Pokud má přežít, nesmí být centralizovaný jako Liberty Dollar nebo E-gold. Nesmí být pouze jiným zápisem tradičních měn, jako byl Mondex. Ale protože především nesmí docházet ke dvojité útratě, je obtížné vytvořit alternativu bez centra. Blockchain to dokázal. Je snadné si odpovědět, jestli se těmito příběhy Satoshi při návrhu Bitcoinu řídil, nebo nikoliv.

Dobré peníze

Kvalitní měna však potřebuje víc než jen decentralizovanou správu. Podíváme-li se do jakékoliv učebnice ekonomie, dozvíme se poměrně intuitivní definici kvalitních peněz, která se přepisuje s menšími úpravami už od dob Aristotela. Lze Bitcoin označit za kvalitní peníze?

Dobré peníze by měly být dobře dělitelné. Bitcoin je digitální měna a není u ní tedy problém dělitelnost zajistit vhodným kódováním čísel. Jelikož je cena jednoho bitcoinu (s malým „b“, pokud mluvíme o měně v systému Bitcoin, označované zkratkou **BTC**) již hodně vysoká, začaly se používat menší jednotky. Můžete se tak setkat s centibitcoinem (1 cBTC je 0,01 BTC), častěji milibitcoinem (1 mBTC je 0,001 BTC) či dokonce mikrobitcoinem (1 μBTC je 0,000001 BTC). Už jen fakt, že se takto malé jednotky používají, poukazuje na vysokou hodnotu a popularitu této měny.

BTC

je třísymbolová zkratka jednotky bitcoinové měny (podobně jako USD pro americký dolar). Jelikož konečné množství **BTC** v systému je 21 milionů (viz **Generující transakce**) a očekává se, že hodnota jednoho **BTC** bude příliš vysoká pro běžné platby, existují odvozené jednotky mBTC (milibitcoin; 1 mBTC = 0,001 BTC), μBTC (mikrobitcoin; 1 μBTC = 0,001 mBTC) a satoshi (1 satoshi = 0,01 μBTC = 10^{-8} BTC). Jednotka satoshi zároveň představuje nejmenší dělitelnost bitcoinu (v současné implementaci protokolu) a je pojmenována na počest autora/zakladatele **Bitcoinu**, Satoshiho Nakamota.

Jednosymbolová zkratka pro jednotku bitcoinové měny je dvojitě přeškrtnuté písmeno ‚B‘ (podobně jako ‚$‘ pro USD).

Mikrobitcoin však není zdaleka nejmenší jednotkou. V současnosti je nejmenší jednotka jeden satoshi, který reprezentuje 1/100 000 000 bitcoinu. Bitcoin je tak velmi jednoduše a jemně dělitelný. Dokonce více než kterákoliv jiná známá tradiční měna. Zlato nebo stříbro se dělily mnohem obtížněji, uvážíte-li nutnou technologii, zručnost, případně vyhledání specializovaných mincoven, nutnost převážení apod. Současné papírové peníze jsou velmi snadno dělitelné v rámci elektronických plateb, avšak v hotovostním styku je dělitelnost odkázaná na centrální autoritu. Pokud centrální banka rozhodne o zrušení padesátníků, máme smůlu (a můžeme s nimi leda hrát mariáš, alespoň prozatím).

Další vlastnosti jsou nasnadě. Dobré peníze by mělo být možné snadno skladovat a přenášet. Tradiční peníze ve formě drahých kovů se s touto vlastností potýkaly dlouhou dobu, každopádně dnes je možné si peníze schovat do trezoru doma či v bance, uložit na účet a relativně snadno přeposlat na druhý konec světa. Bitcoin je pouze digitální informace a jako takový ho lze uložit na pevný disk, flashdisk, vytisknout na papír, nahrát do telefonu nebo na specializované servery třetích stran. Přenos z jedné strany světa na druhou je nejsnazší možný, stačí pouze několikrát kliknout.

Dobré peníze by také měly být zaměnitelné. Pokud někomu půjčíte automobil a vrátí vám jiný, patrně nebudete příliš nadšeni. Pokud však někomu půjčíte sto korun a vrátí vám jinou bankovku, ani se nad tím nepozastavíte. To je zaměnitelnost a Bitcoin tuto vlastnost v podstatě má (podrobněji se k tomu ještě dostaneme). Pokud bych někomu půjčil sto bitcoinů a vrátil mi sto jiných, zlobit se nebudu.

Největší kontroverze vyvolává poslední a možná nejdůležitější z vlastností kvalitních peněz. Aristotelovská definice mluví o nutnosti „vnitřní hodnoty" peněz. Kritici státních peněz vytvořených „ze vzduchu" často obraceli svůj zrak zpět směrem ke zlatému krytí a chtěli by navrátit „kryté" peníze, peníze s „vnitřní hodnotou". A má to svou logiku. Například Voltaire moudře prohlásil, že „hodnota papírových peněz nakonec spadne na svou vnitřní hodnotu – na nulu".

Argumentace je následující – pokud by zlaté peníze přestaly být penězi, potom jsou stále užitečné alespoň jako surovina pro výrobu šperků apod. Hodnota zlata i bez peněžní hodnoty bude vždy nenulová. Zatímco však hodnota papírových peněz se může dostat prakticky na nulu, na hodnotu papíru, na kterém jsou peníze vytištěny. To se ostatně stalo v dějinách již několikrát, připomeňme snad jen meziválečné Německo, kde se z papírových peněz lepili dětem draci a stavěly hrady, ženy s nimi vytápěly domácnosti a miliardy poletující ve větru ulicemi nestály za zvednutí stejně tak, jako když proti vám dnes ulicí letí kus novin. Jak je na tom Bitcoin? Čím je krytý, a pokud ničím, jak může fungovat, aniž by jeho hodnota spadla na nulu?

Nekryté, ale vzácné

Nejprve je nezbytně nutné vyvrátit ekonomický mýtus šířící se internetem i mimo něj, že jsou bitcoiny „kryty" elektřinou nebo energií nutnou k jejich vytěžení, prací těžařů či dokonce prací samotného Satoshiho, že jsou „kryty" kryptografií nebo snad matematikou. Fakt, že jsou peníze kryté, znamená, že pokud bychom s danými penězi nemohli učinit žádnou peněžní transakci, stále jim zůstává hodnota komodity, kterou jsou kryté. Pokud nemohu za zlatou minci získat pečivo, stále ji mohu přetavit do podoby náhrdelníku, kterého si někdo cení. Peníze bývaly kryty i kakaovými boby, látkami a dalšími komoditami, které měly i jinou než peněžní hodnotu. Avšak představa toho, že bez peněžní hodnoty Bitcoinu nám zůstane alespoň elektřina, díky které byl vytěžen, je absurdní. Stejně tak nám nezůstane žádná práce nebo snad matematika. „Krytí prací" je nesmyslný koncept sám o sobě.

Čím jsou tedy bitcoiny kryté? Ničím. To ale přináší otázku, která není na první pohled příliš přívětivá. Pokud nejsou ničím kryté, platí zde Voltairova slova, že cena Bitcoinu nakonec spadne na svou „vnitřní hodnotu", tedy na nulu?

Naštěstí neplatí. Peníze žádnou „vnitřní hodnotu" nepotřebují. Aristoteles jednoduše neměl pravdu, i to se takovým velikánům stává. S ním se mýlily i řady autorů, kteří jeho definici dobrých peněz s „vnitřní hodnotou" přepisovali do učebnic až do současnosti. Jako u čehokoliv, co je předmětem směny, je i u peněz hodnota dána užitkem, který mu lidé připisují. Stejně jako hodnota zlatem krytých peněz neměla tendenci vracet se na cenu samotné komodity bez peněžní funkce, tak tuto tendenci nemá ani Bitcoin. Záleží totiž na něčem úplně jiném, a to na vzácnosti. Má-li být hodnota čehokoliv vyšší než nula, musí to být vzácné. Cena obrazů Salvadora Dalího se může měnit v závislosti na poptávce a okolních cenách, ale neexistuje žádná tendence k tomu, aby se jejich cena snižovala na cenu plátna a použité barvy. Jeho obrazy jsou totiž vzácné.

Peníze bez tiskárny

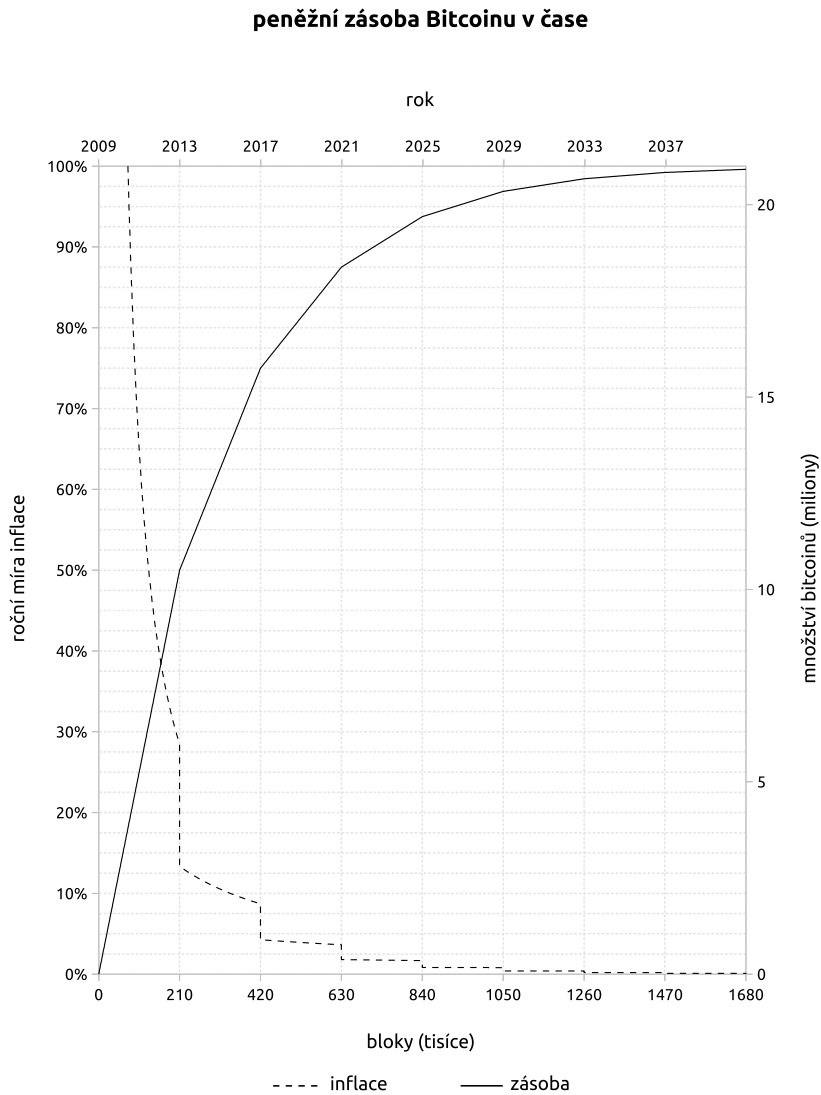
To však neplatilo a do jisté míry stále neplatí u současných papírových i digitálních peněz v systému centrálního bankovnictví.

Pokud je možné „natisknout" biliony nových dolarů, potom jejich vzácnost klesá a s ní i hodnota, respektive jejich cena. Když klesá cena peněz, lze si za stejné množství dané měny koupit méně zboží a služeb. Tomu se obvykle říká (cenová) inflace, tedy růst cen. Pokud rostou ceny zboží a služeb vyjádřené v penězích, potom z definice klesá cena peněz vyjádřená ve zboží a službách. Nové biliony dolarů v oběhu tak nutně tlačí na všeobecný růst cen.

Toho, že ceny rostou v důsledku zvyšování peněžní zásoby (inflace peněz) si všiml jako první již před pěti sty lety Mikuláš Koperník. Není tedy žádným novým zjištěním, že vládci a vlády mají tendenci znehodnocovat měnu, dříve v podobě zlehčování obsahu drahých kovů a dnes skrze tisknutí nových papírových bankovek a navyšování virtuálních čísel na bankovních účtech.

Přestože je dnes v západním světě moc centrálních bank v tomto směru značně omezená, z mnoha jejich sídel vycházejí čím dál silnější hlasy, že je třeba přikročit i k nestandardním metodám, aby bylo v ekonomice více peněz, a byl tak splněn arbitrárně stanovený inflační cíl. Například ve Švédsku a Japonsku se nahlas hovoří o zrušení hotovosti. Živě se diskutuje o možnosti snížení úroků za ukládání i v komerčních bankách do záporných hodnot. Oživil se návrh Silvia Gesella z roku 1906 na hotovost postupně ztrácející hodnotu, diskutuje se zavedení dvojí, taktéž úmyslně hodnotu ztrácející měny dle návrhu Roberta Eislera z roku 1932 (mimochodem dva roky před ním stejný návrh u nás v senátu představil – a odsoudil – senátor František Modráček). Student významného amerického ekonoma Grega Mankiwa přišel s návrhem loterií, kdy by se losovalo, která sériová čísla bankovek přestávají platit. Richmondská pobočka Fedu představila projekt zdanění hotovosti. Ve světle těchto návrhů je zcela legitimní mít obavy. Mít obavy a poohlížet se po decentralizovaných alternativách. Například po Bitcoinu.

Bitcoin tedy nemá žádnou „vnitřní hodnotu" v podobě jiného užití, jako je tomu u zlata, a dokonce lze předpokládat, že ji má i nižší než současné papírové peníze, které mají alespoň onen papír na podpal do kamen. Má ale něco jiného, co mu přináší hodnotu a co zabraňuje výše uvedeným návrhům a jakémukoliv zlehčování měny obecně.


peněžní zásoba Bitcoinu v čase
rok
2009
2013
2017
2021
2025
2029
2033
2037
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
roční míra inflace
20
15
10
5
0
množství bitcoinů (miliony)
0
210
420
630
840
1050
1260
1470
1680
bloky (tisíce)
inflace
zásoba

Satoshi Nakamoto se patrně inspiroval u zlata a zafixoval zásobu své virtuální měny na 21 milionů bitcoinů (úplně přesně 20 999 999,9769 BTC). Číslo je sice stanoveno naprosto arbitrárně, ale vůbec na něm nezáleží. Důležité je, že je bitcoinů omezené množství, což zajišťuje jejich vzácnost. Neexistuje žádný způsob, jak „natisknout" nové bitcoiny. V takovém systému nelze kvantitativně uvolňovat („tisknout"), ani jinak vytvářet peníze z ničeho. Voltairův citát je úzce spjat s možností tisknout nové peníze, což u bitcoinů nelze. Dnes lze sice nové bitcoiny těžit, ale těžba je čím dál náročnější, a až dosáhne čísla 21 milionů, tak se zastaví. To se stane přesně v roce 2140. Nicméně naprostá většina bitcoinů bude vytěžena již v roce 2033. To je vzácnost, se kterou může každý uživatel počítat a nebude narušena. I princip těžby je nápadně podobný těžbě zlata. Bitcoin tedy má všechny vlastnosti dobrých peněz, a může se tak penězi stát.

Blok (Block)

nejvýznamnější datová struktura bitcoinového protokolu. Kóduje množinu **transakcí**, které svým zahrnutím potvrzuje. Právě jedna z **transakcí** v **bloku** je „generující" (viz **Generující transakce**) a pouze jejím prostřednictvím vznikají nové bitcoiny. Validní **blok** musí mít určitou kryptografickou vlastnost, jejíž splnění je náročné na výpočetní výkon. Tato náročnost je navíc proměnná v čase, což umožňuje zpětnovazebnou regulaci k dosažení stability průměrné rychlosti generování nových **bloků** (viz **Těžba**), a tím i deterministické inflace měny. Nalezení (validního) **bloku** je důkazem o vynaloženém úsilí – tento koncept označujeme jako „proof-of-work" (některé alternativní kryptoměny používají odlišný koncept „proof-of-stake").

Na rozdíl od zlata se ale s těžbou bitcoinů začalo teprve nedávno. První bitcoiny byly vytěženy 3. ledna 2009 v 18:15 a pět sekund a vytěžil je sám Satoshi. Prvním „kopnutím" pro sebe získal odměnu 50 bitcoinů. Tomuto **bloku** bitcoinů s názvem 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f (tzv. **hash** bloku) se v komunitě uživatelů začalo dle knihy zrození přezdívat „**genesis blok**". První člověk vlastnil první bitcoiny.

Genesis blok (Genesis Block)

viz **Řetěz bloků**

Revoluce mohla začít.

2010: Nejdražší pizza dějin

Ďobající programátor

Když Satoshi vytěžil první bitcoiny, neměl samozřejmě v úmyslu si je ponechat. Jeho cíle byly mnohem, mnohem větší. Bitcoin se má stát měnou budoucnosti. Je potřeba, aby ho těžili další lidé, aby si je mezi sebou posílali za zboží a služby.

Adresa (Address)

jednoznačná identifikace příjemce platby (analogicky k číslu bankovního účtu v konvenčních platebních systémech). Její fyzickou reprezentací je dlouhé číslo zakódované do řetězce alfanumerických znaků, který má následující vlastnosti:

- jeho délka je 27–34 znaků (14–74 pro nový formát Bech32 dle **BIP** 174)
- rozlišují se velká a malá písmena (neplatí pro Bech32)
- začíná označením verze – číslicí ‚1', ‚3' (P2SH, např. **multisig**) nebo „bc1" (Bech32 pro nativní **segwit**)
- neobsahuje typograficky zaměnitelné znaky ‚0'—‚O', ‚I'—‚l'
- poslední znaky obsahují kontrolní součet (zabezpečení proti špatnému opsání/vykopírování)

příklady:

- 1KZ7MCXC5UJKiNYtvG8c9qEc9WdCz87LBf
- bc1q6rggkagqa8arkyvwj5zzqyjd2945xyjfyl30ul

Bitcoinovou **adresu** lze vygenerovat offline (bez spolupráce sítě), neboť je pouze **hashem veřejného klíče** (stačí mít pár klíčů pro **asymetrickou kryptografii** a následně se aplikuje posloupnost funkcí Base58(version + RIPEMD-160(SHA-256(pubkey)) + SHA-256²(version + RIPEMD-160(SHA-256(pubkey)))[0..3])*. Jelikož vygenerování **adresy** je levná operace, je možné generovat novou **adresu** pro každou nesouvisející **transakci**, což znesnadňuje jejich stopování. **Adresy** uživatele (a k nim příslušející klíče) jsou typicky spravovány bitcoinovou **peněženkou**. Uživatel může prokázat vlastnictví konkrétní **adresy** tím, že podepíše určitou zprávu **soukromým klíčem** příslušejícím k dané **adrese**.

* operátor ‚+' zde značí zřetězení; třetí operand je zabezpečení (první 4 bajty **hashe** klíče)

První transakci tak učinil sám Satoshi a ještě v lednu téhož roku poslal první bitcoiny vývojáři jménem Hal Finney. Stalo se to už ve 170. bloku, který se spolu s genesis blokem stal nejznámějším blokem dějin Bitcoinu. Na **adrese**, ze které Satoshi bitcoin posílal, stále zůstalo osmnáct bitcoinů a je možné, že už je nikdy nikdo nepoužije.

Každopádně Finney se stal prvním příjemcem bitcoinu v historii a jedním z nejdůležitějších lidí v jeho vývoji. Posílat si mezi sebou bitcoiny však ještě není žádný zázrak. Čekalo se na okamžik, kdy bude někdo ochotný za bitcoiny nabídnout své zboží nebo službu.

A čekalo se dlouho, téměř rok a půl. Mezitím si uživatelé bitcoiny posílali, vznikly první ceny vyjádřené v dolarech (přestože New Liberty Standard spočítal, že náklady na vytěžení jednoho bitcoinu jsou 0,0008 dolarů, na začátku roku 2010 se obchodoval 1 BTC jen za 0,000003 dolarů) a Bitcoin začalo sledovat řádově více lidí. Dokonce vznikl Bitcoin Market, první BTC burza.

Avšak skutečný zlom přišel až 21. května 2010, kdy se na fóru bitcointalk.org objevila nabídka: „Zaplatím 10 000 bitcoinů za pár pizz (…) za dvě velké, aby mi něco zbylo na další den. Rád si nechám kus pizzy na pozdější ďobání (…) Pokud máte zájem, dejte vědět, nějak se domluvíme. Díky, Laszlo." Floridský programátor Laszlo Hanyecz už o čtyři dny později poslal jednomu dobrovolníkovi z Anglie 10 tisíc bitcoinů, za které mu domů přišly dvě pizzy objednané od Papa John's za 25 dolarů. 10 tisíc BTC se dalo v květnu 2010 na burze prodat za zhruba dvojnásobek. Takže celkově dobrá cena, i když už ne tak moc dobrá doručovací doba. Hanyecz poté pizzy několikrát vyfotil, jako důkaz, že transakce proběhla úspěšně. Na jedné z fotografií se po pizze s rajčaty a olivami natahuje nejspíš Hanyeczův syn.

Tento příběh obletěl svět dvakrát. Hned po úspěšné transakci a potom v druhé polovině roku 2013, kdy cena za jeden bitcoin přesáhla tisíc americký dolarů. To by znamenalo, že obě pizzy stály dohromady v cenách konce roku 2013 neuvěřitelných deset milionů dolarů. Na konci roku 2017 by každá pizza vyšla dokonce na sto milionů dolarů, tedy více než dvě miliardy korun. Poněkud dražší „ďobání".

Chyby ze zlata

Dnes se na první pohled zdá, že udělal Hanyecz chybu. „Kdyby si ty bitcoiny nechal, dnes mohl být milionář," říká nespočet komentářů pod články o milionové pizze. Možná to ale není tak jednoduché.

V té době o Bitcoinu moc lidí nevědělo. Pouze hrstka nadšenců jej těžila a zkoumala a čas od času se o své zkušenosti podělila na internetových fórech, jako je právě bitcointalk.org. Hanyecz se rozhodl posunout Bitcoin dál, blíže směrem ke všeobecně přijímané měně. A to se mu podařilo. Zpráva o transakci v bitcoinech se šířila internetem i mimo něj neuvěřitelnou rychlostí. Byl to i okamžik, kdy se s Bitcoinem seznámila velká část současných inovátorů, autorů konkurenčních digitálních měn a mnohých startupů, kterými je dnes Bitcoin obklopen.

Je tak dost dobře možné, že by bez něj měl Bitcoin i dnes tehdejší hodnotu, nebo možná už ani neexistoval. Je možné, že to byl právě slavný Laszlo, kdo nastartoval růst jeho hodnoty. Ekonomicky to dává smysl. S růstem poptávky roste cena a příběh o pizze byl prakticky jen reklamou, která přinesla nové potenciální uživatele, a tím i zvýšila poptávku. Ostatně data ukazují, že tomu tak být mohlo. Během následujících čtyř měsíců se cena jednoho bitcoinu zdesetinásobila a o nové digitální měně začaly psát méně i více významné internetové zpravodaje, jako je slashdot.com a další. Byla dokonce objevena chyba v implementaci a uměle vytvořeno 184 miliard bitcoinů. Chyba se však rychle napravila a vše se vrátilo zpět, a přestože jde o nepochybně nevítanou událost, i takový útok ukazuje, jak moc se stal Bitcoin populárním. Bitcoin i Laszlo.

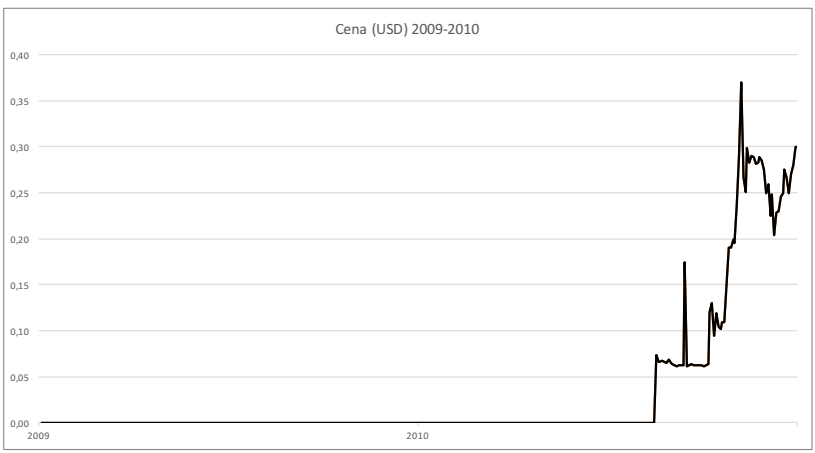
Jeden člen fóra kvůli Hanyeczovi dokonce založil server ounce.me, kde sledoval a dodnes sleduje vývoj ceny tehdy zakoupené pizzy. Vedle zlata, stříbra, dolaru nebo ropy se tak Laszlova pizza stala indexem cen. Dolarový svět má svůj BigMac index, svět digitálních měn zná Bitcoin pizza index.

Šlo o obrovský skok směrem kupředu. Koneckonců, dnes si za bitcoiny může koupit pizzu každý, například na pizzaforcoins.com nebo v České republice na damejidlo.cz. Koupě první pizzy byla zlomová. Laszlo mohl čekat, až tento krok provede někdo jiný, ale nikde není jistota, že by se to muselo stát. Dnes je z něj hrdina, i když možná s lehce nahořklým příběhem.

Rok 2010 přinesl ještě mnoho dalších zlomů. Byla založena později největší burza obchodující bitcoiny Mt.Gox, odehrála se první veřejně známá půjčka, první transakce mezi telefony, státy poprvé varovaly před decentralizovanou měnou, kterou je dle jejich zprávy možné efektivně využívat k financování terorismu – tak sladké záminky k levné diskreditaci všeho, co je státům trnem v oku. Proběhla první krátkodobá půjčka, objevila se první bitcoinová opce, a především v druhé polovině roku vznikl první těžební **pool**, který založil Čech Marek Palatinus, na internetu známý jako Slush. Bitcoin rostl.

Pool

místo k distribuované **těžbě** bitcoinů fungující na principu pojištění zisku za vložený výpočetní výkon. Správce **poolu** organizuje participujícím uzlům práci – rozdává jim data k hashování (viz **Hash**) a sleduje jejich **hashovací rychlost**. Celková **hashovací rychlost poolu** je součtem **hashovací rychlosti** všech uzlů a s vyšší rychlostí roste i pravděpodobnost vytěžení **bloku**. Odměnu za nalezený **blok** (viz **Generující transakce**) pak správce **poolu** rozdělí participantům podle výpočetního výkonu, který dodali (či jiné strategie, kterými si správci **poolů** vzájemně konkurují v přilákání participantů). Není možné, aby si uzel, který těžený **blok** nalezne, ponechal odměnu pro sebe, neboť adresát odměny je vlastností **bloku**, který **pool** těží, a výpočetní výkon dodávaný uzlem se určuje podle počtu **hashů** spočítaných nad tímto **blokem**. Pokud by uzel chtěl podvádět, musel by těžit jiný **blok**, ale potom by nemohl prokázat, že dodává svůj výpočetní výkon do **poolu** (prokazuje se počtem nalezených **hashů** s benevolentnějším cílem, než obtížnost sítě aktuálně požaduje).



Svůj nákup pizzy ve světle následujícího vývoje glosoval sám Hanyecz slovy: „Nemám z toho špatný pocit. Ta pizza byla skutečně dobrá.“ Nedá se mu nevěřit.

2011: Nahoru, nahoru a dolů

Nahoru

Bitcoinu se dařilo. Jeho tržní kapitalizace byla na začátku roku 2011 přes jeden milion amerických dolarů a v únoru dosáhl parity s dolarem. To znamená, že se jeden bitcoin obchodoval za jeden dolar. Můžeme si o „magických hranicích" myslet cokoliv, ale tato zpráva se začala šířit takovou rychlostí, že byl server bitcoin.org kvůli ohromné návštěvnosti dočasně nedostupný. Objevovaly se další obchody denominované v bitcoinech. Jistý Australan nabídl svou Toyotu Supra z roku 1984 za 3 tisíce bitcoinů. Neprodala se, ale další nabídky následovaly. Bitcoiny začaly přijímat první e-shopy a internetové servery začaly nabízet možnost darů v bitcoinech.

Skutečným milníkem byla možnost posílat v bitcoinech dary serveru WikiLeaks, který v roce 2006 spoluzakládal jeho současný šéf Julian Assange. WikiLeaks využívají různých možností internetu k zachování anonymity svých zdrojů, avšak peněžní toky byly jednoduše zablokovatelné, což se také poté, co byly stránky označeny Pentagonem za hrozbu národní bezpečnosti Spojených států, skutečně stalo. Na základě toho daly online platební systém PayPal, největší internetový obchod Amazon, správce domény Dynadot a ostatní společnosti, které zajišťovaly chod WikiLeaks, ještě v roce 2010 od tohoto serveru ruce pryč.

Peněženka (Wallet)

software ke správě **soukromých klíčů** příslušejících k bitcoinovým **adresám** uživatele. Kromě „vedení účtu" (výpočet zůstatků na **adresách** uživatele) bitcoinová **peněženka** typicky umožňuje odesílání plateb (anoncování **transakcí**), vedení historie **transakcí** nebo evidenci známých **adres**. Starší verze první **peněženky** Bitcoin-Qt obsahovala i možnost těžit nové **bloky** a jednalo se tak o plnohodnotného klienta sítě. Implementace **peněženky** může mít kromě konvenční aplikace (vedle **Bitcoin Core** např. MultiBit, Armory, Electrum) i podobu online služby (např. Blockchain.info, BitGo, Coin.Space) nebo hardwarovou (TREZOR, Ledger).

Internet je ale mocný nástroj. Bitcoin umožnil WikiLeaks přijímat dary a zároveň si tak sám sobě udělal velkou reklamu. Server, který zveřejnil mimo jiné také tajné dokumenty o mučení během války v Iráku či dokumenty o americké špionážní síti složené z jejich vlastních velvyslanectví, na své stránky jednoduše nahrál krátkou adresu své **peněženky** a mohl začít přijímat příspěvky. Dnes je již opět možné mu přispívat i jinými metodami. Obecně se však ukázalo, že díky Bitcoinu mohou WikiLeaks a podobné servery fungovat, a ať se nám to líbí či ne, v konečném důsledku začíná Bitcoin reálně měnit i diplomacii, mezinárodní vztahy a politiku obecně.

Dolů

Ne všechno však šlo hladce. Rok po Laszlově pizze byla tržní kapitalizace Bitcoinu na úrovni 200 milionů dolarů. S tím pochopitelně přišly i první problémy. Jedním z nich byla i první a procentuálně největší bublina. Za čtyři dny mezi osmým a dvanáctým červnem roku 2011 spadla cena bitcoinu z 31,91 amerických dolarů na pouhých 10. To je propad o téměř 70 procent! Přestože šlo o propad o „pouhých" dvacet dolarů, což se později stane ještě mnohokrát a propadne se i mnohem více, v relativním měřítku šlo o největší pád, který Bitcoin dodnes zažil.

Tomuto období se začalo říkat Velká bublina roku 2011. A že byla tato bublina skutečně velká, ilustruje nejlépe fakt, že se zpátky na 31,91 dolarů bitcoin nevrátil dříve než 28. února 2013, tedy za více než rok a půl.

Bubliny jsou jistě věcí nemilou, ale stále jsou rizikem, se kterým se musí počítat. Přišly však i první krádeže. Na fóru na bitcoin.org napsal 13. června 2011 uživatel s přezdívkou allinvain, že mu bylo z jeho peněženky odcizeno 25 tisíc bitcoinů. O šest dní později byla napadena burza Mt.Gox a byly ukradeny informace o desítkách tisíc uživatelských jmen, e-mailových adres a hesel. Přestože byla hesla zašifrovaná, některá byla natolik jednoduchá, že bylo možné je snadno rozklíčovat a účty vykrást.

Pravděpodobně stejný člověk či skupina pak pomocí hesla k účtu administrátora dokázala zadat příkazy na prodej stovek tisíc

bitcoinů. Mt.Gox touto umělou nabídkou donutil snížit cenu za BTC z téměř 18 dolarů skoro na nulu a na sedm dní byl uzavřen. Přestože byly tyto umělé **transakce** zpětně vráceny, Bitcoin utrpěl silnou ránu. Někteří uživatelé měli stejná hesla i uživatelská jména jako na Mt.Gox i na webové peněžence MyBitcoin. Okolo šesti set účtů bylo vykradeno. Jeden konkrétní uživatel přišel o 2 tisíce bitcoinů. Po neustálém růstu přišel pád. Důvěryhodnost měny byla podlomena.

Transakce (Transaction)

informace o převodu bitcoinů z určité **adresy** na **adresu** jinou. Interně je **transakce** datová struktura obsahující dvojici množin tzv. vstupů a výstupů, kde vstup referencuje výstup v nějaké již existující **transakci**. Vlastností výstupu je množství bitcoinů, které z něho lze uvolnit, a celkový objem **transakce** je roven součtu hodnot všech jejích vstupů – součtu hodnot všech již existujících výstupů, které jsou vstupy nové **transakce** referencovány. Celkový objem lze mezi výstupy nové **transakce** rozdělit libovolně, pokud součet jejich hodnot není větší. Pokud je menší, rozdíl je chápán jako **poplatek za transakci**. Speciálním typem **transakce** obsahujícím pouze výstupy je **generující transakce**.

Při použití výstupu (jeho referencování vstupem nové **transakce**) dochází k jeho konzumaci v celé výši – výstup není dělitelný (a je použitelný pouze jednou). Pokud převáděná hodnota má být menší než hodnota výstupu(-ů), nová **transakce** bude obsahovat i výstup(-y) pro „rozměnění", kterými si majitel vrátí rozdíl na svoji **adresu** (může být stejná jako **adresa** rozměňovaného výstupu). K uvolnění výstupu (jeho použití na vstupu nové transakce) je třeba podepsat data **transakce soukromým klíčem** patřícím k jeho **adrese**, což dává disponentní právo k výstupu pouze jejímu majiteli. Ve skutečnosti je systém nárokování výstupu obecnější a umožňuje vytvářet složité podmínky, které musí být pro jeho použití splněny (např. uvolnění výstupu více **podpisy**, heslem, postdatování atd.). Složitějším a kombinovaným podmínkám říkáme **kontrakty** a programují se ve skriptovacím jazyce, jehož triviální větou je i běžná podmínka na výše zmíněný **podpis** klíčem patřícím k **adrese**.

Bitcoin ale neměl upadnout v zapomnění. V druhé polovině roku 2011 se odehrála v New Yorku první mezinárodní konference o Bitcoinu a o pár měsíců později i první evropská konference, kterou hostila Praha. V Praze si o Bitcoinu povídali nejen významní vývojáři, investoři a ekonomové, ale i novináři. O kryptoměně se mluvilo stále více a na konci roku 2011 začala cena opět pomalu růst.

Kryptozloději

Přesto anebo právě proto se objevovaly další krádeže. A co hůř, i větší. V březnu 2012 bylo v jedné jediné krádeži odcizeno téměř 50 tisíc bitcoinů, v tehdejších cenách téměř 5 milionů korun. Hackerům se podařilo prolomit ochranu internetového hostingu a bitcoiny jednoduše převedli do svých vlastních peněženek. Jedním z okradených byl i Marek Palatinus, který přišel o více než 3 tisíce bitcoinů. O pět bitcoinů přišel i Gavin Andresen.

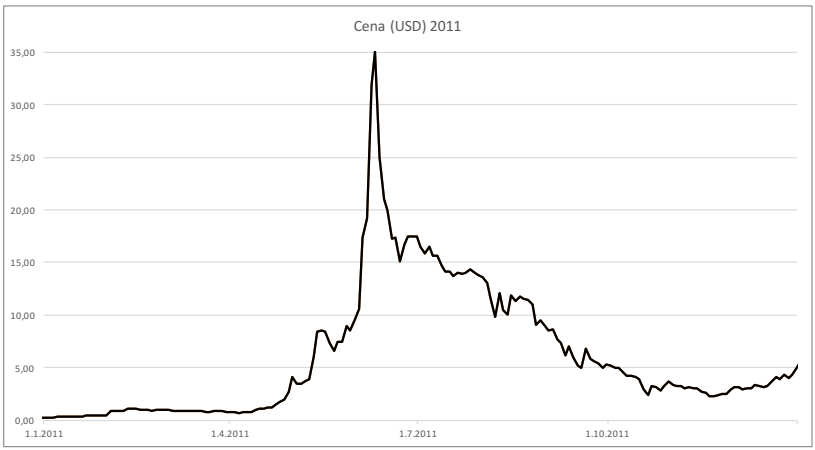
A nejen krádeže. Majitel v té době třetí největší burzy Bitomat v červenci roku 2011 oznámil, že ztratil přístup k souboru, ve kterém byly uloženy bitcoiny uživatelů. Ti tak přišli celkem o 17 tisíc bitcoinů, tedy zhruba 10 milionů korun (ale spíše řádově méně, jelikož tehdejší cena 30 dolarů za bitcoin byla vrcholem, z nějž cena postupně spadla až na 2 dolary).

O měsíc později byla vykradena přední webová peněženka MyBitcoin. Zmizela polovina uložených bitcoinů, okolo 78 tisíc, v přepočtu 16 milionů českých korun.

Rizika Bitcoinu začala být vidět více a více. Do toho všeho přišla „Hedvábná stezka", anonymní a v očích státu ilegální server Silk Road, na kterém se prodávaly všechny myslitelné drogy a další kontroverzní zboží. Na Silk Road se dalo chodit pouze anonymizovaně a prodejní systém fungoval na bázi doporučení a referencí. Ilegální obchod na tomto serveru rostl, roční obrat se odhadoval v řádech desítek milionů dolarů a prodávaly na něm stovky anonymních obchodníků. Pro Silk Road byl Bitcoin jako stvořený – anonymní, těžko zdanitelný, rychlý a nový. Avšak ilegální tržiště dělalo Bitcoinu špatnou reklamu.

S ní přišlo i první velké politické vyjádření. Ve Spojených státech začal o boji proti Bitcoinu uvažovat demokratický senátor Chuck Schumer. Schumer a jeho kolega Joe Manchin v dopise ministru spravedlnosti a protidrogovým autoritám prohlásili: „Jedinou metodou, jak za toto nelegální zboží platit, je nevystopovatelná peer-to-peer měna známá jako Bitcoin. Po zakoupení bitcoinů na burze si může uživatel založit na Silk Road účet a začít nakupovat od jednotlivců z celého světa ilegální drogy a nechávat si je v řádech dnů doručit až domů."

Je však dobře známo, že negativní reklama je také reklama. Bitcoin neoslabil, naopak, stal se vyhledávanějším a s tím rostla i jeho cena.



2012–2013: Raketou do budoucnosti

Kostky jsou vrženy

Cena však dále rostla velmi pomalu. Rok 2012 se stal symbolem napravování předešlých chyb a postupné přeměny Bitcoinu z podivné zábavy pro IT fanoušky v opravdové peníze, se kterými se dá nakupovat běžné zboží.

Jak již bylo řečeno, za bitcoiny se již dříve dalo koupit auto nebo přispět na chod WikiLeaks a dalších serverů. Avšak šlo pouze o individuální případy a dlouho se čekalo na okamžik, kdy začnou bitcoiny přijímat tradiční instituce – restaurace, trafika, lékař nebo taxi.

Jedním z nejdůležitějších partnerů Bitcoinu se stala publikační platforma WordPress. WordPress je nejpoužívanější redakční systém na světě – můžete si ho zdarma stáhnout a spustit na svých stránkách, jednoduše modifikovat a poté publikovat, nebo můžete svůj blog či stránky spustit přímo na webu wordpress.com. Vývojář systému Andy Skelton 15. listopadu 2012 oznámil, že placené funkce systému je možné kupovat za bitcoiny. Spustila se lavina zpráv a nových registrací na BTC burzy.

A přidávali se další. Objevily se první restaurace, kde bylo možné útratu platit v bitcoinech, první lékař, právník, první taxislužby, vznikly větší obchody s různým fyzickým zbožím apod. Vedle toho rostly pochopitelně i možnosti získat za bitcoiny ryze elektronické zboží, zejména software, online předplatné či přístup do placených částí webových stránek.

A nakonec hazard. V dubnu 2012 byl spuštěn server satoshidice.com a později i satoshicircle.com nebo satoshiroulette.com. Netrvalo tedy dlouho, než si někdo uvědomil potenciál Bitcoinu v této oblasti. A zájem byl skutečně velký. Především ze dvou důvodů, kvůli regulaci a rychlosti. Tradiční online či fyzický hazard je masivně regulován a silně daněn. Z toho důvodu je i poměrně vysoké „zvýhodnění podniku“ (house edge), tedy průměrné procento zisku kasina v dlouhém období. Například se dá snadno spočítat, že standardní ruleta má zvýhodnění 5,26 %.

U jiných sázek, jako je například Keno, které v českém prostředí provozuje Sazka, je zvýhodnění až 25 % a hry Šťastných deset nebo Sportka mají zvýhodnění dokonce 50 %. Průměrně se vám tedy z každé vsazené stokoruny vrátí jen padesát korun. Takto vysoké zvýhodnění je produktem vysokého zdanění zisků, které reálné zvýhodnění zásadně snižuje. Také regulace zvýhodnění zvyšuje, protože eliminuje konkurenci. Ta by, jako na každém trhu, tlačila na snížení marží.

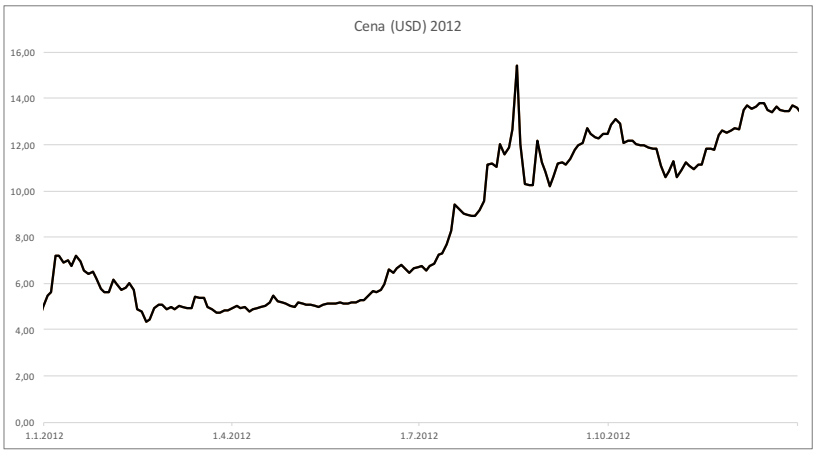
U SatoshiDice je situace jiná. Konkurence může kdykoliv vzniknout a zisky nejsou nijak daněny. Zvýhodnění rok a půl po založení tak je pouze 1,9 %. To znamená, že v průměru z každého vsazeného bitcoinu ztratíte pouhých 0,019 BTC. To už pochopitelně naláká mnoho lidí, aby zkusili své štěstí. Navíc, pokud ho mít budou, potom je jim výhra vyplacena prakticky okamžitě, jak už je tomu ve světě Bitcoinu ostatně téměř vždy.

Nakonec i SatoshiDice bude muset snížit své zvýhodnění, protože se, jak tomu už na trzích s volným vstupem konkurence bývá, objevily služby ještě výhodnější. Například peerbet.org nabízí hry se zvýhodněním 0 %. Ekonomové mohou do učebnic přidat zajímavý příklad tzv. dokonalé konkurence, kde je cena tlačena až na úplné minimum.

Nezůstalo ale jen u hazardu internetového. Na začátku roku 2014 začalo přijímat bitcoiny i nejstarší kasino v Las Vegas – The Golden Gate. Brzy ho následovalo další a lze očekávat, že zbylá kasina nebudou chtít zůstat pozadu. Hazard je Bitcoinem přitahován.

Žít Bitcoin

Taxi, restaurace, hazard. To vše posouvá naši digitální měnu dál. Ale většina poptávky po kryptoměnách byla stále pouze spekulativní. Bitcoin vyměňující se za tradiční měny není ničím jiným než možnou investicí. Digitální měny však mají podstatně vyšší cíl, a to stát se skutečnými penězi, všeobecně přijímaným platidlem. K tomu je možnost nákupu online a zejména v kamenných obchodech nutností přímo z definice peněz jako všeobecně přijímaného prostředku směny.



Pokud ale nejste příliš zruční v IT a při pohledu na pohyby kurzu mezi BTC a například USD se vám dělá nevolno, nebo pokud vůbec nechcete bitcoiny vlastnit, protože sami nevíte, co s nimi, potom proč byste ho přijímali? Stejnou otázku si položili zakladatelé společnosti bitpay.com a už v roce 2011 přišli na odpověď, která právě během roku 2012 stála u začátku konsolidace po relativně neúspěšném roce předchozím. BitPay udělá vše za vás. Na vaše stránky vám vygeneruje jednoduché prostředí, ve kterém je možné zaplatit v bitcoinech dle kurzu v daný okamžik. Bitcoiny jsou pak převedeny do peněženky serveru BitPay, který vám obratem zašle na váš účet dolary. Poplatky jsou minimální, menší než jedno procento. Jednoduché řešení, kterému vděčíme za rozvoj množství zboží a služeb, které je možné za bitcoiny získat. Tak jednoduché, že na konci roku 2013 registroval 15 tisíc obchodů, přičemž o rok dříve to byl pouze jeden tisíc. To je obrovský nárůst, se kterým se musí počítat i do budoucnosti.

O Bitcoinu začaly vysílat televize, psát noviny, a dokonce se začaly vyučovat kurzy na vysokých školách. Z měny, za kterou šlo jen velmi stěží koupit pizzu, se stal prostředek, s kterým šlo při troše snahy vyrazit na nákup každodenních věcí. Našli se lidé, kteří se rozhodli přijímat výplatu pouze v bitcoinech. Přestože šlo pouze o individuální případy a spíše kuriozity, konečně to bylo možné. Když si uvědomíme, že v roce 2012 Bitcoin existoval pouze tři roky a uplynuly pouhé dva roky od Laszlovy pizzy, jde

o neuvěřitelně rychlý vývoj. Tak rychlý, že téměř všechny šokoval. Na konci roku byla cena bitcoinu již 15 dolarů a nikdo nepochyboval, že ještě poroste.

Tohoto vývoje si všimli i politici a úřady v Evropě. Evropská centrální banka vydala v říjnu 2012 zprávu nazvanou „Schémata virtuálních měn", ve které v relativně rozsáhlé části o Bitcoinu tuto měnu velmi poučeně popisuje. Je překvapením, že na svého konkurenta příliš neútočí, ba ho dokonce naopak vychvaluje a představuje v dobrém světle. Studie uzavírá, že kryptoměny jsou rizikem pro centrální bankovnictví, protože by kvůli nim mohly centrální banky získat špatnou reputaci.

Tržní kapitalizace Bitcoinu brzy překročila jednu miliardu, poté 10 miliard a na přelomu let 2013 a 2014 dokonce dosáhla na více než 14 miliard dolarů. To je zhruba cena jedné velké jaderné elektrárny.

Rychlý růst v jednu chvíli začal povědomě připomínat Velkou bublinu roku 2011. V dubnu 2013, kdy bitcoin poprvé dosáhl ceny 100 dolarů, se začalo střílet šampaňským, ale to ještě nebyl konec a do konce dubna Bitcoin vyrostl až na tehdejší vrchol na 266 dolarech. Za rok tak přidal přes neuvěřitelných 2000 %. Brzy však bublina splaskla, ale pouze na 150 dolarů a rychle se začala dofukovat.

Bitcoin začaly přijímat další a další organizace. Například jeden z předních internetových prodejců Overstock, americký basketbalový tým Sacramento Kings, newyorská realitní kancelář BOND, Čínský megaserver Baidu, Shopify, Univerzita v Nikósii a další se každý den přidávaly. Stále častější se stalo i fyzické obchodování v bitcoinech. Mladí lidé se na sociálních sítích fotí s bagetami ze Subwaye nebo kávou pořízenými za kryptoměnu. Je to nové a přitažlivé. Jednoduché. Stačí si pouze zdarma stáhnout jednu aplikaci. Například aplikaci Bitcoin Wallet, určenou právě i pro fyzické obchodování pomocí bitcoinů, si na přelomu roku 2013 a 2014 stahovalo pět tisíc uživatelů denně.

Za bitcoiny se dá již koupit prakticky cokoliv. Objevili se lidé, kteří to chtějí dokázat a začali žít výhradně za bitcoiny. Týden bez tradičních peněz a pouze s bitcoiny žila například reportérka časopisu Forbes Kasmihr Hill, která o svých zážitcích

posléze napsala knihu. Cestovala, spala v hostelu a stravovala se výhradně pomocí kryptoměny, přičemž sama konstatovala, že snadné to není. Ostatně netvrdila, že zkouší za bitcoiny žít, ale pokusí se přežít. Podařilo se jí však dokázat, že žít se za bitcoiny dá. Dokázat to chtěli i novomanželé Austin a Beccy Craigovi. Ti se rozhodli oslovit profesionální dokumentaristy a nechat se po sto dní natáčet, jak cestují po světě, a přitom platí pouze bitcoiny. Podařilo se jim to a světu tak efektní cestou ukázali, že bitcoiny jsou peníze.

Sjet si hedvábnou stezku

V pozadí toho všeho také stále rostl i Silk Road. Ilegální server, který nabízel na deset tisíc různých produktů (z nichž tři čtvrtiny byly drogy) a který stál a padal na možnosti obchodu v bitcoinech. Není proto překvapením, že když byl v druhé polovině roku 2013 dopaden a zatčen jeho údajný provozovatel Ross Ulbricht, na internetu známý jako Dread Pirate Roberts, cena bitcoinu výrazně spadla. Mnoho lidí se začalo zbavovat svých bitcoinů, protože začali cítit, že se může Bitcoin svézt spolu se Silk Road. Prodeje však trvaly jen jeden den a hned následující ráno se cena opět začala rychle vracet zpět.

Silk Road byl obrovský, celkové tržby za dva roky existence přesáhly miliardu dolarů a provedlo se přes 1,2 milionů transakcí. Onu miliardu dolarů vypočítala americká FBI z tržní ceny bitcoinů, které tržištěm protekly – šlo o neuvěřitelných 9,5 milionů bitcoinů. To je ohromné číslo, pokud si uvědomíme, že 9,5 milionů bitcoinů bylo vytěženo teprve v roce 2012. Silk Road měl tedy tržby srovnatelné s peněžní zásobou. Pro srovnání – v České republice by taková firma musela mít tržby ve výši tří bilionů korun nebo jako tisíc dvě stě firem ŠKODA AUTO, a to ještě za předpokladu, že má všechny tržby v korunách.

Silk Road tak dokázal s Bitcoinem slušně zahýbat. Samozřejmě to neznamená, že všichni uživatelé Bitcoinu používali Silk Road, naopak jich bylo minimum, dle FBI necelých patnáct tisíc. Dokonce sám Ulbricht byl zadržen s „pouhými" 26 tisíci BTC. Později však mluvčí FBI uvedl, že bitcoinů bylo 144 tisíc. Úřady 2. října 2013 stránky Silk Road zavřely a FBI řešila, co udělat se zadrženými bitcoiny.

Následující rok bylo v aukci prodáno téměř 30 tisíc bitcoinů zapsaných v deseti blocích americkému investorovi Timu Draperovi, jenž je věnoval bitcoinovému startupu Vaurum, pracujícímu na podpoře rozvojových zemí. Nakonec tak tyto zprávy Bitcoin paradoxně posílily, protože státní aukce dodaly Bitcoinu punc legality.

Mediální vliv na hodnotu Bitcoinu je zásadní. Po uzavření Silk Road cena bitcoinů okamžitě spadla ze 139 na 109 dolarů. Média ale Bitcoinu i pomáhají. Například v roce 2013 vznikla ubytovna pro bezdomovce Sean's Outpost, která je plně financována pomocí bitcoinů. Zakladatel Jason King se pro Bitcoin nadchnul natolik, že se rozhodl na Floridě vybudovat 40 km^2 velký azyl pro bezdomovce nazvaný Satoshiho les. Bitcoin se hned jeví nejen jako nástroj pro anonymní obstarání heroinu, ale jako nástroj pro pomoc lidem v nouzi.

Ross Ulbricht byl na začátku roku 2015 shledán vinným v sedmi bodech včetně prodeje drog, praní špinavých peněz a napadání cizích počítačů a odsouzen na doživotí.

Po Silk Road přišly téměř okamžitě nové ilegální servery nabízející podobné služby. Byly tak založeny Black Market Reloaded, Atlantis, Farmer's Market nebo Sheep Marketplace, ale ani jedna z jmenovaných dlouho nepřežila a skončily podvodem na svých uživatelích. Ti své bitcoiny ani v jednom případě nedostali zpět. Například autor Sheep Marketplace utekl s 96 tisíci BTC, v tehdejších cenách šlo o více než jeden a půl miliardy korun. Okradení začali autora okamžitě hledat a zjistili, že stopy zloděje vedou do České republiky, a dokonce ke konkrétnímu jménu. V březnu 2015 policie tohoto mladého Čecha zatkla, když si zkoušel koupit podezřele drahou vilu a nedokázal vysvětlit původ peněz. V roce 2017 byl odsouzen na 9 let vězení.

Dodnes však vznikají nové pokusy oživit tehdejší slávu Silk Road a založit důstojného pokračovatele. Na konci roku 2015 už existovaly desítky velmi podobných anonymních tržišť a zavření Silk Road tak nepřekvapivě způsobilo pravý opak toho, co americká vláda zamýšlela. Silk Road brzy nahradil a velikostí zásadně předčil Alphabay, ale i jeho tvůrce byl nakonec dopaden. V roce 2017 byl nalezen v Thajsku, kde se oženil a vlastnil luxusní nemovitosti. Oběsil se ve vazbě a jeho projekt nadobro skončil. Další ale neustále vznikají a s každým pokusem silnější a lépe zabezpečené. Tato bitva jen tak neskončí.

Bitcoin a média

Rok 2013 byl pro Bitcoin minimálně stejně zásadní jako rok předchozí, pravděpodobně ale ještě mnohem více, protože ukázal, že Bitcoin není jen hračkou pro IT nadšence, ale něčím, co funguje v reálném světě, za co si lze něco koupit.

O Bitcoinu psal každý. Vznikly první knihy, časopisy, webové magazíny, audio pořady, ale také se téměř nutně objevil článek o Bitcoinu snad v každém myslitelném periodiku. Přišly kritiky, stejně jako chvála. Skoro každý chtěl v roce 2013 k Bitcoinu něco říct. Takový zájem byl překonán až v druhé polovině roku 2017.

Všechna velká média začala psát o Jamesi Howellsovi, který omylem vyhodil svůj harddisk se 7500 bitcoiny, v té době v ceně téměř 10 milionů dolarů. Články o davech nadšenců přehrabujících se v odpadcích na anglických skládkách se dobře prodávaly. Mimochodem hrabou dodnes. Objevily se reportáže ve státních i soukromých médiích, vyprofilovali se první profesionálové, kteří dávali v médiích k problematice Bitcoinu více i méně poučené komentáře a nutně také přišly i velké mediální přešlapy.

Klasickým příkladem je šíření poplašných zpráv, které většinou stojí na uvěřitelném a leckdy pravdivém základě, ale přidají k němu navíc zásadní nepravdy, které původní fakta vrhnou do úplně jiného světla.

Například v červenci 2013 se objevila zpráva, že thajská centrální banka zakázala Bitcoin. Stručně znějící zpráva obsahovala detailní popis toho, co vše se od daného okamžiku nesmí s Bitcoinem provádět, tedy prakticky nic. Vydala ji thajská firma, která se dle svých vlastních slov chtěla věnovat obchodování s Bitcoinem, ale centrální banka jí to neumožnila. Informace se začala šířit a převzala ji i velká média jako Huffington Post.

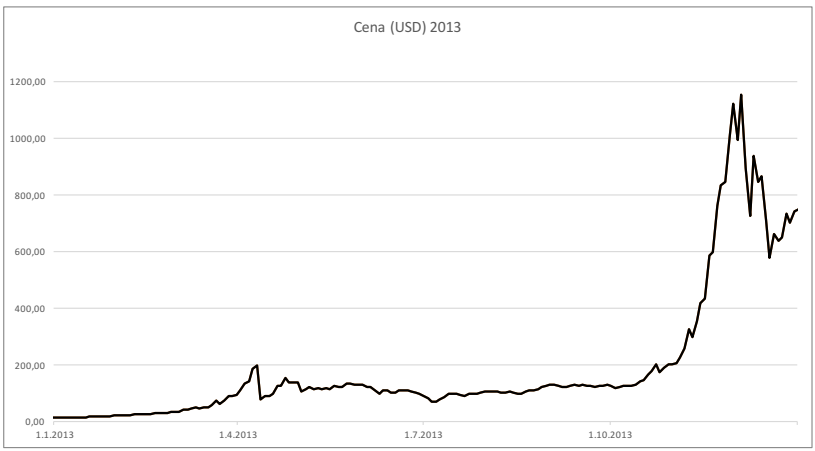
Nicméně „zakázat Bitcoin" není tak jednoduché. I kdyby to thajská centrální banka udělala, tak neexistuje rozumný způsob, jak přiřadit Bitcoin k hranicím Thajska nebo jak vystopovat, zda jej užívá člověk určité národnosti. Nadto se velmi brzy objevily pochybnosti i o samotném zákazu, jelikož thajská centrální banka ani nemá takové pravomoci a nikde z oficiálních zdrojů nelze nic o údajném zákazu zjistit. Nakonec tak spíše šlo pouze o licenci,

kterou thajská firma nedostala, aby mohla vůbec provádět peněžní operace. Poslat do Thajska příteli bitcoiny je stále možné, i bez této organizace. A obchod s bitcoiny je i v Thajsku čím dál významnější a větší.

Podobných zpráv o různých zákazech či omezení Bitcoinu se objevilo ještě mnoho a vždy byly víceméně vyvráceny nebo revokovány ze strany samotných zakazujících. Asi nejvděčnějším příkladem těchto oscilací je i dosud Čína, která se tak postarala o řadu fluktuací v ceně BTC na burze.

Je pochopitelné, že čím více je Bitcoin vidět, tím více lidí o něm chce vědět a následně se o něm i více píše. U něčeho tak nového, jako jsou kryptoměny, je ale snadné podlehnout poplašné zprávě. Všichni se učí Bitcoin chápat, a přestože není pro běžného uživatele složitý, rozumět jeho pozadí a kontextu není triviální. Až bude Bitcoin všeobecně přijímaný a mnohem rozšířenější, budeme se snad s podobnými zprávami setkávat čím dál méně často.

Avšak to je budoucnost a nikdo neví, co budoucnost přinese. Vedle letů do vesmíru možná i širší užívání Bitcoinu. A možná oboje dohromady.



Rakety jménem Bitcoin si všiml i známý miliardář Richard Branson a v listopadu 2013 v televizi oznámil, že jeho společnost Virgin Galactic plánující soukromé lety do vesmíru přijímá bitcoiny. V době oznámení se dal jeden let koupit za zhruba 250 bitcoinů

a během několika týdnů této možnosti využili první zájemci. Ve stejném čase se objevila i nabídka na první luxusní vozy, které je možné koupit za bitcoiny. Nové nablýskané sportovní Lamborghini vás vyšlo na více než 300 bitcoinů a za pouhých 24 bitcoinů bylo možné si koupit legendární DeLorean z roku 1981, známý z filmu Návrat do budoucnosti. Za bitcoiny se podíváte do vesmíru a možná i do budoucnosti. A jen za pár set mincí. Je neuvěřitelné, jak krátký čas uběhl od doby, kdy si Laszlo Hanyecz koupil za 10 tisíc bitcoinů dvě pizzy.

2014–2015: Dolů ke hvězdám

Pád z hory Gox

Začátek následujícího roku byl jízdou na horské dráze. Po rekordní ceně z konce předchozího roku ve výši 1163 dolarů cena začala padat. V lednu opět zájem o Bitcoin vyrostl a s ním i cena až na 1000 dolarů a následně se kurz ustálil mezi 800 a 900 dolary.

S únorem ale přišla jedna z největších událostí v historii Bitcoinu. Burza Mt.Gox přestala vyplácet peníze a zbankrotovala. Mt.Gox měla řadu problémů už v předchozích letech. Burza, která ovládala téměř tři čtvrtiny všech obchodů s bitcoiny, se však stala synonymem k Bitcoinu. Lidé přes ni bitcoiny získali, obchodovali s nimi na stránkách burzy a následně je tam i prodávali. A to i přes problémy, se kterými se průběžně potýkala.

Už v květnu roku 2013 podala společnost CoinLab žalobu na 75 milionů dolarů za porušení smlouvy, která měla umožňovat společnosti CoinLab přijímat uživatele Mt.Gox, avšak ta jim v tom údajně bránila. Ve stejné době americká vláda zabavila Mt.Goxu více než 5 milionů dolarů.

V červnu burza přestala vyplácet uživatelům dolary. Po dvou týdnech sice oznámila, že je vše opět v pořádku, avšak nebylo. Trvalo to týdny a měsíce, než uživatelům přišly peníze, a nakonec v únoru 2014 burza zastavila i vyplácení bitcoinů. Burza tvrdila, že šlo o problém spojený s **maleabilitou transakce**, avšak to se nikdy plně nepotvrdilo.

Lidé však na burze stále mohli směňovat a převádět prostředky již vložené, a tak se vytvářela tržní cena. Ta byla o více než pětinu nižší než na jiných burzách, což svědčí o tom, jakou uživatelé přisuzovali pravděpodobnost tomu, že své peníze ještě uvidí. Decentralizované prostředí kolem Bitcoinu dokonce dalo velice rychle vzniknout projektu bitcoinbuilder.com, který realizoval směnárnu mezi BTC uvnitř Mt.Goxu, tzv. Goxcoinu, a normálnímu vnějšímu BTC. Kurz Goxcoinu se před úplným krachem Mt.Goxu dostal až na cca desetinu neuvězněného BTC. Nakonec 24. února 2014 Mt.Gox zavřela své stránky a o čtyři dny později zkrachovala oficiálně.

Maleabilita transakce (Transaction Malleability)

možnost pozměnění anoncované (a dosud nepotvrzené) **transakce** tak, že význam jejích dat se nezmění, ale vzhledem k rozdílu v binární podobě (konkrétně ve formátu **podpisu** vstupu) se změní její **hash** (TXID). Pokud se do **blockchainu** dostane místo původní **transakce** její pozměněná verze (obě potvrzeny být nemohou, protože uvolňují stejné vstupy), může si nevhodně navržený software (takový, který potvrzenou **transakci** identifikuje na základě jejího **hashe** a nikoliv obsahu) myslet, že k **transakci** vůbec nedošlo. Software se následně může pokusit (buď sám nebo na základě fiktivní stížnosti adresáta platby) **transakci** zopakovat uvolněním jiných bitcoinů, kterými disponuje (jiných výstupů na jím spravovaných **adresách**), čímž předmětnou platbu provede vícekrát. Navíc si může myslet, že výstupy použité v pozměněné **transakci** má stále k dispozici, což způsobí problém při pokusu o jejich opětovné uvolnění v rámci jiné **transakce** v budoucnu.

Ačkoliv je tento problém znám od roku 2011, v plné síle se projevil počátkem roku 2014 v souvislosti s krizí nejznámější a nejstarší bitcoinové burzy Mt.Gox, která jím zdůvodnila dočasné pozastavení výběru bitcoinů, což mělo za následek pokles jejího kurzu a zhoršení důvěryhodnosti. Popisovaný problém byl sice odstraněn ve verzi 0.8 referenčního klienta, leč některé burzy a jiné velké služby používají svůj kustomizovaný software.

Lidé začali na krach reagovat různě. Ostatní burzy se od ní distancovaly a začaly pracovat na tom, aby se jim nestalo to samé. Lidé začali směňovat závazky k bitcoinům na Mt.Gox za normální bitcoiny v ještě větších poměrech, jako například 20 : 1. Jistota jednoho bitcoinu nyní byla ceněna šancí na dvacet bitcoinů na zavřené burze. Začaly se šířit bitcoinové automaty, které umožňují lidem získat bitcoiny bez nutnosti vstupu na burzu.

Údajně uniklý dokument z Mt.Gox tvrdí, že burza přišla o 744 408 bitcoinů při krádeži, které si během dlouhých let nevšimla. Šéf Mt.Gox Mark Karpeles se stal symbolem tohoto podvodu, ačkoliv je možné, že v tomto případě šlo spíše o diskrepanci mezi kompetencí dostupnou a vyžadovanou pro správu tak obrovského majetku, který byl na Mt.Goxu uložen. A cena Bitcoinu padala strmě dolů až ke 340 dolarům.

Regulace v Evropě

Rok 2014 však přinesl i dobré zprávy. V únoru prohlásil britský úřad pro výběr daní a cel bitcoiny za soukromé aktivum, ze kterého tedy není nutné platit daň z přidané hodnoty. Evropská unie se postavila na druhou stranu a vydala skrze European Banking Authority dokument, ve kterém vyjasňuje svůj postoj ke kryptoměnám. Navrhovala, aby byly burzy kryptoměn povinnými osobami a musely tak hlásit vyšší objemy, které přes ně protékají. Tím by se dle zprávy lépe bránilo praní špinavých peněz a narušilo financování teroristických organizací. To byl důležitý signál, který umožnil bankám začít o Bitcoinu uvažovat a Bitcoinu naopak vstoupit mezi tradiční finanční aktiva.

V Evropě se Bitcoinu nebývale dařilo. Ministr financí Velké Británie si dokonce v srpnu 2014 koupil bitcoiny za 20 liber, aby prokázal svůj pozitivní vztah ke kryptoměnám. Mezitím však na druhé straně oceánu přišly v New Yorku první návrhy skutečné regulace virtuálních měn.

I v České republice se Bitcoinu vedlo dobře. Zejména dvě věci se zapsaly do historie Bitcoinu. První bylo spuštění první hardwarové peněženky TREZOR, která zásadním způsobem změnila přístup k ochraně bitcoinů před odcizením. Druhým bylo otevření institutu kryptoanarchie Paralelní Polis v pražských

Holešovicích uměleckou skupinou Ztohoven. Budova pojmenovaná podle konceptu chartisty Václava Bendy nabízí vedle prostoru pro pravidelné přednášky nejen o Bitcoinu i sdílený coworkingový prostor, 3D tiskárny, bitcoinový bankomat a především kavárnu, ve které lze platit pouze bitcoiny. Budova se okamžitě stala hlavním centrem veškerého bitcoinového dění v České republice.

Rok 2014 byl důležitý. A že propad ceny nutně neznamená propad zájmu, dokázal i Microsoft, který se na konci roku rozhodl přijímat bitcoiny.

Rok stimulujícího klidu

Nastal klid. Klid, který pomohl Bitcoinu se stabilizovat a zejména vybudovat kolem sebe důležitou infrastrukturu. Díky předchozím rokům měli uživatelé k dispozici celou škálu důležitých inovací a zkušeností.

Už se vědělo, že může spadnout Mt.Gox. Poznali jsme spíše hypotetickou hrozbu těžebního poolu, který dosahoval na téměř 50 % výpočetní kapacity sítě. Existoval TREZOR, rozšířily se bitcoinové bankomaty, o Bitcoinu byly napsány knihy, natočena videa a filmy, první pár se oddal zápisem této informace do blockchainu a všeobecně byla atmosféra nakloněna novým pokusům. Důležité podhoubí bylo připraveno.

V lednu 2015 otevřel jeden z předních expertů na kryptoměny, ekonom Jakub Jedlinský, na Vysoké škole ekonomické v Praze kurz Kryptoměny a další alternativní měnová řešení ve světové praxi. Navázal tak na původní projekt „Nxt pro studenty“, kdy na stejné škole rozdal studentům tuto alternativní kryptoměnu a představil jim tak základní práci s kryptoměnami.

Během roku se stala řada drobných důležitých událostí, zejména spojených s novými místy, kde lze Bitcoin používat. Dell, T-Mobile v Polsku, web pro streamování počítačových her twitch.tv, čerpací stanice Lukoil v Pobaltí, Movietickets v USA, BitBrno umožnilo v Brně nakoupit si za bitcoiny jízdenky do MHD, bitcoiny přijímal polský letecký dopravce LOT, a především stovky a tisíce malých podniků po celém světě.

Vznikla řada nových pokusů o využití kryptoměn, například v erotickém a porno průmyslu. BitPervy nabízí bitcoiny za sdílení porna, backpage.com umožňuje podávat inzeráty výhradně za kryptoměny a Xotica vytvořila model, kdy uživatelé platí dívkám na webkamerách přímo bitcoiny bez nutnosti prostředníka.

I v Česku se postupně rozvíjela komunita a infrastruktura. Česká hardwarová peněženka TREZOR získala nové funkce, Karel Fillner spustil českou verzi jednoho z nejčtenějších webů o kryptoměnách cointelegraph.cz, v Paralelní Polis se odehrál mezinárodní Hackers Congress, od konce roku 2014 po celé roky 2015, 2016 i 2017 byl každý týden v úterý pravidelný Bitcoin meetup, kde se diskutovalo nad širokým spektrem otázek nejen kolem Bitcoinu, ale o kryptoměnách a jejich pozadí obecně, včetně ekonomických témat.

Do toho všeho vletěl jako tornádo Vít Jedlička s Liberlandem. Aktivní Čech na území nikoho mezi Chorvatskem a Srbskem v dubnu 2015 založil nový mikrostát Liberland. Zpráva o tom oblétla doslova celý svět a o občanství začaly žádat statisíce lidí. Jedlička se netajil tím, že by měnou Liberlandu měl být Bitcoin nebo jiná kryptoměna, čímž po delší době opět vzbudil zájem celosvětových médií o peníze budoucnosti. Na konci roku se trochu i díky tomu cena za bitcoin vyšplhala z 200 dolarů až k 500 dolarům a začala se konsolidovat v pásmu 300–400 dolarů. Zásadními důvody pro růst ceny byly však vedle rozšířeného přijímání kryptoměn i dvě zprávy ze září a října 2015.

V září spustila Čína, kterou lze považovat v absolutních číslech za bitcoinovou velmoc, rozsáhlé kapitálové kontroly. Z Číny začali utíkat investoři a s nimi peníze v řádech desítek miliard dolarů, a tak se nejlidnatější země světa rozhodla pomoci své ekonomice kontrolou přeshraničního toku financí. Světová média spekulovala, jak se toto opatření projeví na ceně bitcoinu a brzy bylo jasné, že měli pravdu ti, kteří sázeli na růst.

Nebyla to jediná dobrá zpráva pro Bitcoin. I na druhé straně euroasijského kontinentu se slavilo, a to když v říjnu Evropský soudní dvůr rozhodl, že se na směnu bitcoinů nevztahuje DPH. Soud byl výsledkem sporů ve Švédsku, které se snažilo Bitcoin považovat za zboží. Z prodeje zboží by poté musely firmy odvádět DPH, což by Bitcoinu pochopitelně zásadně uškodilo. Evropský soudní dvůr však

rozhodl, že se na bitcoiny vztahuje ustanovení o transakcích pomocí oběživa, bankovek a mincí v podobě zákonného platidla, a jsou tedy od DPH osvobozeny.

V prosinci 2015 vyšla i tato kniha. Historie Bitcoinu pokračovala.

2016–2017: Hodl to the moon!

Sklízení úrody

Co se v předchozím klidném roce zaselo, během roku 2016 pomalu rostlo a připravovalo se na sklizeň. Alespoň pro ty, kdo takzvaně hodlovali, tedy své bitcoiny drželi a neprodali. Hodl byl překlep z anglického „hold“, tedy držet, jenž se v komunitě zažil jako jednoslovné vyjádření pro držení bitcoinů navzdory výkyvům cen. Jste také hodleři?

Již v březnu roku 2016 označila japonská vláda Bitcoin a jemu podobné měny za aktivum podobné penězům. V roce 2017 ho potom plně zlegalizovala. Největší norská online banka nabídla svým klientům bitcoinové účty. O spolupráci s kryptoměnami začala mluvit i ruská vláda.

Stále více obchodů začalo bitcoiny přijímat, mezi nimi například švýcarské dráhy, herní portál Steam a největší jihoafrický e-shop Bidorbuy. V roce 2017 se k nim přidal i největší český e-shop Alza. Počet bitcoinových bankomatů ve světě se zdvojnásobil a dosáhl téměř osmi set. BitPay oznámil, že jen za rok 2016 se ztrojnásobil počet obchodů, které přijímají Bitcoin a využívají jeho služeb.

Vedle řady publikací, jako je tato kniha, vznikaly i odborné články. Google Scholar jich za rok 2016 zaznamenal přes tři a půl tisíce. Vznikl i Ledger, první odborný časopis, který se zabývá výhradně kryptoměnami.

Bitcoin zachránil patrně i několik životů, respektive minimálně je zachránil před hrozným životem. Venezuela, která v roce 2017 stála na pokraji zhroucení, zažila několik dobře zdokumentovaných příběhů lidí, kteří pomocí Bitcoinu utekli ze země. Spořit na letenku v době hyperinflace není dost dobře možné, protože vaše úspory se každý měsíc vypaří. Když si ale naspořili v kryptoměnách, měli nakonec více. I kdyby ale měli méně, jako ochrana před masivním znehodnocováním se Bitcoin osvědčil.

To vše se odrazilo v ceně. V první půlce roku 2016 se cena jednoho bitcoinu pohybovala kolem 400 dolarů. V druhé polovině začala růst

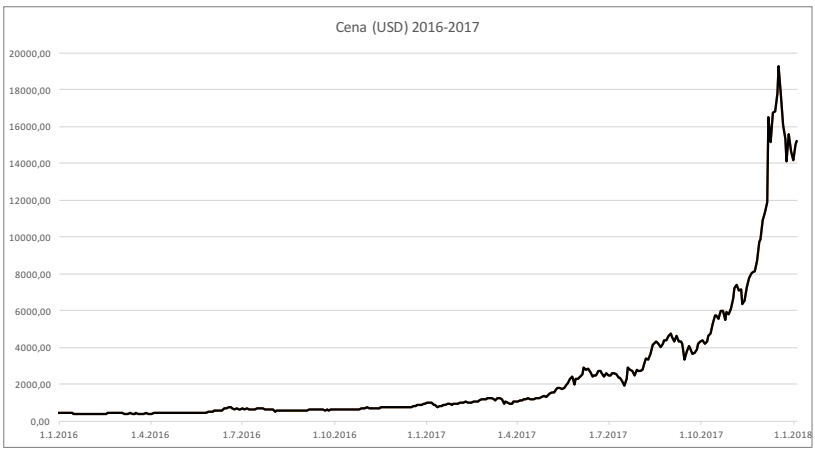
a do konce roku se více než zdvojnásobila. Rok 2017 byl pak jízdou, kterou nikdo nemohl ignorovat. Z 1000 dolarů se cena dostala až téměř na 20 000. Během tohoto růstu zažil Bitcoin několik korekcí, ale trend byl po celý rok 2017 jednoznačně na sever. Lidé se začali opět hlasitě ptát, zda nevidíme jen nafukování bubliny. Na jednu stranu to nelze nikdy vyloučit, na stranu druhou jde v procentech o růst, který jsme v historii této měny zažili už několikrát, a dokonce mnohem vyšší, ačkoliv ne tak nepřerušeně dlouhý. Dvacetinásobek za rok 2017 je ničím v porovnání s rokem 2013, kdy se hodnota znásobila až stokrát, nebo dokonce s rokem 2011, kdy vyrostla 172×.

Daň z úspěchu

Ani nyní se ale Bitcoinu nevyhnuly problémy. V srpnu 2016 přišla jedna z historicky největších burz Bitfinex o 120 tisíc bitcoinů. Ve srovnání s pádem Mt.Gox taková událost již ale nebyla problémem. Zaprvé, protože burza zareagovala a slíbila ztráty nahradit. To pak úspěšně plnila, čímž si získala silnější pozici a důvěru. Zadruhé, což je mnohem důležitější, burza již nebyla jen jedna velká a uživatelé ji k používání Bitcoinu nepotřebovali. Ve světě plném bitcoinových směnáren a bankomatů se burzy staly jen nástrojem spekulantů a obchodníků s velkými objemy. Ztráta se tak nedotkla naprosté většiny uživatelů, na rozdíl od pádu Mt.Gox.

Během posledních let však začal pomalu na povrch vybublávat mnohem palčivější problém. Počet transakcí za jednotku času byl v počátcích bitcoinové sítě naschvál omezen, aby ji nebylo možné úmyslně zahltit. Toto umělé omezení nepředstavovalo v předchozích letech problém, ale s nárůstem počtu uživatelů přestala síť stíhat. Komunita se začala hádat, jak s problémem naložit. Většina chtěla omezení zachovat. Motivy pro zachování i odstranění limitu byly různé – pro zachování hovořila např. zpětná kompatibilita a silnější decentralizace; naopak zase větší propustnost sítě, a tudíž i levnější transakce. Kritériem bylo i vymyslet takové řešení, které bude mít trvanlivější charakter a problém jen neodsune na další rok. Přesto komunita nalezla jakousi shodu na změně, která zajistí mírně vyšší propustnost a zároveň otevírá prostor pro systémovější řešení (tzv. segwit, viz dále). Proti té se však ze záhadných důvodů postavila silná komunita čínských těžařů kolem společnosti Bitmain,

výrobce těžebního hardwaru. Záhadou to přestalo být ve chvíli, kdy se zjistilo, že navrhovaná změna zabraňuje způsobu těžby, který tito těžaři používali. A to jim vadilo! Tzv. AsicBoost (algoritmická optimalizace výpočetní smyčky těžby) jim umožňoval zvýšit těžbu až o 20 procent. Toho se pochopitelně nechtěli vzdát, a tak do celého sporu hodili příslovečné vidle a založili si prvního srpna svůj vlastní Bitcoin – Bitcoin Cash. O tři měsíce později se spustila taková panika, že tato nová kryptoměna vyskočila až na polovinu ceny bitcoinu. Bitcoin Cash začaly podporovat známé osobnosti, dokonce autor předmluvy k této knize. Spor o řešení problému kolem malého počtu transakcí se rozhořel naplno. Ještě si o něm podrobněji povíme v kapitole o škálování Bitcoinu. Uživatelé se však svých bitcoinů nezbavili a kurz nové měny nakonec spadl zpět na šestinu ceny BTC. Debata o budoucnosti ale není zdaleka uzavřená. Ta nejdivočejší léta nás teprve čekají.



Příručka uživatele kryptoměn

Stručné doporučení, pokud chcete jen nakoupit a držet:

Množství peněz	10 000 korun	100 000 korun	1 000 000 korun
Kde koupit	Simplecoin	Simplecoin	Bitstamp
Kde držet	Coinomi / Jaxx	TREZOR	TREZOR

Pořízení peněženky

První kroky

Příběh Bitcoinu je téměř neuvěřitelný. Přesto a právě proto chce být čím dál více lidí jeho součástí. Lidé začínají bitcoiny nakupovat, směňovat, těžit anebo přijímat ve svých obchodech. Pokud se chcete přidat, není nic snazšího.

Podobně jako u tradičních peněz je nejprve nutné pořídit si peněženku, aby mohly být peníze někde uložené. Možností je několik. Stejně jako u papírových korun můžete důvěřovat sobě nebo druhým. Prozatím si představme, že Bitcoin je unikátní kód, který musí být někde uložen. Můžete si ho uložit na počítači, na externím disku či paměťové kartě nebo ho můžete poslat do zašifrovaného úložiště v internetu. Můžete si ho i vytisknout na papír, chcete-li. Nebo si pořídit speciální bezpečnostní hardware.

Prvním, ale ne příliš uživatelsky přívětivým způsobem, jak si pořídit peněženku, je stáhnout si software oficiálního bitcoinového klienta z webu bitcoin.org. Ten se vyznačuje tím, že v sobě ukládá celý blockchain, tedy veškeré informace o všech dosud proběhlých transakcích.

To může být zajímavé pro toho, kdo se rád podívá celému systému pod pokličku, ale pro běžného uživatele je tento klient asi zbytečně plnohodnotný, zejména pro svou velikost. S rostoucím množstvím transakcí roste i velikost databáze, kterou musíte mít uloženou na počítači. Na konci roku 2017 dosáhla velikosti 150 GB, což je srovnatelné s velikostí pěti moderních počítačových her. Blockchainy jiných kryptoměn, jako je Litecoin či Ethereum, mají zatím řádově menší velikost, zejména protože nejsou tak používané.

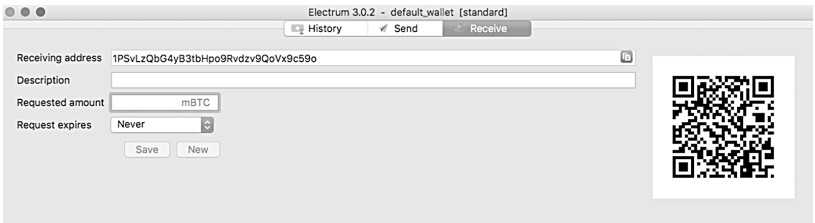
Nejde o zanedbatelné množství dat, a přestože se zatím na většinu současných počítačů vejdou, existují úspornější alternativy. O možnost podívat se do blockchainu a stopovat jednotlivé bitcoiny a transakce nepřijdete. Například na stránkách Blockchain.info můžete do této obří účetní knihy nahlédnout přímo z okna svého prohlížeče, aniž byste cokoliv instalovali a dalších několik dní stahovali data blockchainu. Jiné kryptoměny mají své prohlížeče také, stačí na internetu vyhledat danou měnu a přidat slovo „explorer".

Úsporný software

Rozsahem tisíckrát úspornější volbou může být softwarová peněženka. Jednu z nejpopulárnějších softwarových peněženek představuje program Electrum, který je možné získat na webové stránce electrum.org a následně nainstalovat do počítače. Vedle velikosti obsluhovaných dat je jeho výhodou, že existuje ve verzi pro většinu známých operačních systémů. Po spuštění je hned první možností v programu vygenerování vaší nové peněženky. Program se zeptá, kam se má uložit soubor, ve kterém budou bitcoiny (přesněji klíče pro přístup k nim) uchovány. Takový soubor má standardně příponu .wallet a můžete si ho libovolným způsobem zálohovat.

Při jeho zálohování si představte, že ukládáte složité heslo k vašemu účtu u tradiční banky, bez nějž se už nikdy ke svým penězům nedostanete. A navíc má k účtu přístup kdokoliv, kdo toto heslo zná. Můžete si ho uložit doma na pevný disk v počítači připojeném k internetu, ale riskujete tím, že může být přečten nepovolanou osobou nebo že se poškodí spolu s hardwarem. Flashdisk můžete uschovat ve fyzickém trezoru, ale pokud budete chtít odesílat bitcoiny, bude vám trvat delší dobu, než se vždy k datům dostanete. V prostředí internetu nemusí být v bezpečí nic, pokud si nejste zcela jisti tím, co děláte (o tom, jak bitcoiny zabezpečit, bude pojednáno dále). Každopádně, i když zvolíte peněženku softwarovou, lze určitě důrazně doporučit si svůj soubor s peněženkou zašifrovat přidáním hesla. Electrum vám to nabídne přímo při instalaci. To hlavní je ale 12 slov, které vám program automaticky vygeneruje. Ty si opište nejlépe na papír nebo několik papírů a pečlivě uschovejte. Kdybyste přišli o počítač, můžete pomocí těchto slov znovu získat přístup ke svým penězům.

Celé prostředí programu je intuitivní a vytvořené pro co nejširší okruh uživatelů. Pokud máte vytvořenou peněženku, můžete se podívat na její adresu.



Tato adresa, která se vám zobrazuje v panelu „receive“, je vším, co potřebujete, pokud chcete přijímat bitcoiny. Tlačítkem vedle adresy si ji zkopírujete do schránky a poté ji pomocí známé kombinace kláves Ctrl+V můžete vložit do zprávy komukoliv, kdo by vám chtěl poslat peníze, nebo vystavit na internet.

Pokud už nějaké bitcoiny v peněžence máte, můžete je někomu poslat z vedlejšího panelu „send“. Stačí jen znát adresu toho, komu chcete bitcoiny poslat, a částku, na které jste se domluvili.

Důležité je, že posílání není zcela zadarmo a platí se částka, **poplatek za transakci** (např. 0,0001 BTC). Některé peněženky vypočítávají poplatky automaticky, obvykle ale máte možnost výši poplatku změnit a ovlivnit tak rychlost zahrnutí vaší transakce do blockchainu.

Poplatek za transakci (Transaction Fee)

rozdíl mezi hodnotou výstupů a vstupů **transakce**. Tento rozdíl stanovuje sestavitel **transakce** – odesílatel platby. Bitcoiny v této hodnotě připadnou v rámci **generující transakce** tomu, kdo vytěží **blok transakci** potvrzující. **Poplatek** za **transakci** je motivací k jejímu zahrnutí do těženého **bloku** a po vytěžení všech nových bitcoinů bude přetrvávající motivací k pokračování v **těžbě**.

Softwarových peněženek je pochopitelně mnoho. Mezi další oblíbené a fungující na všech operačních systémech patří Bitcoin Knots nebo Armory. Za povšimnutí stojí, že se vývojáři přizpůsobují poptávce uživatelů a snaží se zesílit ochranu. Tuto svou snahu tak často vsunou přímo do názvu svého produktu. Přesto pořádná ochrana vyžaduje ještě alespoň jeden krok navíc, a to

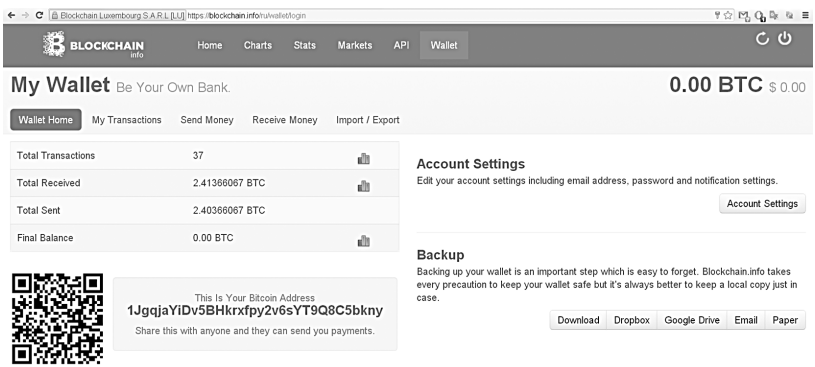
pořídit si hardwarovou peněženku. Více se dozvíte v kapitole Jak bitcoiny ochránit.

Počítačové peněženky mají samozřejmě i další kryptoměny. Litecoin má vedle svého referenčního klienta podporu také v upravené verzi Electrum (electrum-ltc.org), Ethereum má Mist apod.

Mince na webu

Dalším způsobem, jak si pořídit peněženku, je vytvořit si ji online. Mezi nejpopulárnější webové peněženky patří coinbase.com nebo peněženka serveru blockchain.info. Jelikož svěřujete své bitcoiny třetí straně, nikdy nad nimi nemáte úplnou kontrolu. V krátké historii Bitcoinu již bylo vykradeno mnoho webových peněženek a tyto ztráty jsou nenávratné. Někteří uživatelé však více věří třetí straně než sami sobě a svému pevnému disku. To je pochopitelné u menších částek, i když i tam je lepší mít je například v mobilním telefonu. U vyšších sum je uchovávání kryptoměn na webu neomluvitelnou chybou.

Dokud nemáte kryptoměny u sebe, nevlastníte je. Nedůvěřujte třetím stranám. Nikdy.



Je důležité si uvědomit, že pokud nemáte prostředky u sebe, nepatří vám. Technicky patří právě provozovateli webové peněženky. Naučte se jejich služby využívat, ale nedůvěřujte jim.

Založení webové peněženky není příliš odlišné od té softwarové. Například na coinbase.com nebo blockchain.info stačí vyplnit e-mail a heslo. Po potvrzení e-mailové adresy se přihlásíte do webového rozhraní, které je velmi podobné rozhraní Electra.

Nyní máte vytvořenou adresu, na kterou si můžete stejně jako v případě Electra nechat poslat bitcoiny. Pokud již nějaké bitcoiny na adrese jsou, je možné je odeslat. K tomu slouží záložka „Send Money", kde je opět nutné pouze zadat množství bitcoinů a cílovou adresu. Pokud je zůstatek dostatečný, po kliknutí na „Send Payment" jsou bitcoiny odečteny z vaší adresy a přičteny na adresu příjemce.

Ve většině peněženek si můžete všimnout, že lze do kolonky adresáta vložit místo bitcoinové adresy e-mail, případně telefonní číslo. V takovém případě nepřijdou bitcoiny do peněženky, ale služba (například Coinbase) pošle na e-mail či SMS zprávou adresátovi upozornění, že na něj čekají bitcoiny, pokud se zaregistruje pod přiloženým odkazem. Je až neuvěřitelné, kolik lidí považovalo podobný e-mail za dobrý dárek k Vánocům!

I zde je zjevné, že je prostředí navrženo tak, aby bylo uživatelsky co nejpřívětivější a intuitivní. Avšak stejně jako u internetového bankovnictví tradičních bank je i u bitcoinových služeb vedle těchto několika základních možností přítomna i řada doplňkových služeb. Některé po ověření uživatele umožňují dokonce nakupovat bitcoiny za dolary. Konkurence je u Bitcoinu obvykle vysoká, a i v oblasti online peněženek existuje řada jiných poskytovatelů. Některé webové peněženky ukládají bitcoiny na svých počítačích online, ti profesionálnější nahrávají jejich větší část na externí disky, které nejsou připojené k internetu (tzv. cold storage). Ke krádeži těchto bitcoinů by se tedy zloděj musel úložiště fyzicky zmocnit. Samozřejmě je ideální taková data nejen šifrovat, ale i duplikovat do více fyzických úložišť pro dosažení ještě většího zabezpečení proti poruše hardwaru. Pro jedince s obzvláštní mírou paranoie vůči spolehlivosti či trvanlivosti elektronických dat, existují služby, které umí digitální peníze vytisknout i na papír. Ani to není bezpečné, pokud byste tiskli ze zavirovaného počítače. Naštěstí bezpečná řešení existují.

Mobilní Bitcoin

Bitcoin má i své mobilní aplikace pro chytré telefony. To je v současné době asi uživatelsky nejpřívětivější způsob, jak si bitcoiny pořídit a držet je. V závislosti na operačním systému si můžete zvolit z řady podobných aplikací, které fungují obdobně jako Electrum, avšak své bitcoiny můžete nosit u sebe.

Pro Android patří mezi nejlepší a nejoblíbenější aplikace Mycelium či Coinomi. Na iOS potom lze doporučit Jaxx, Breadwallet nebo Bither. Uživatelům Windows Mobile musí stačit Coin.space a vlastníkům BlackBerry Bitcoin Wallet.

Při samotné instalaci vás peněženka vyzve k opsání několika slov. Ta si opište tužkou na papír a pečlivě uschovejte, klidně na více místech. Neopisujte si je do telefonu nebo do počítače. Kdyby se k nim někdo dostal, všechny vaše kryptoměny získá. Na druhou stranu vy víte, že i kdyby vám někdo ukradl telefon nebo se vám rozbil, dokážete své peníze jednoduše obnovit zadáním právě těchto slov do nového telefonu. Těmto slovům se říká seed a je pro vás tím jediným a nejdůležitějším, co musíte ochránit.

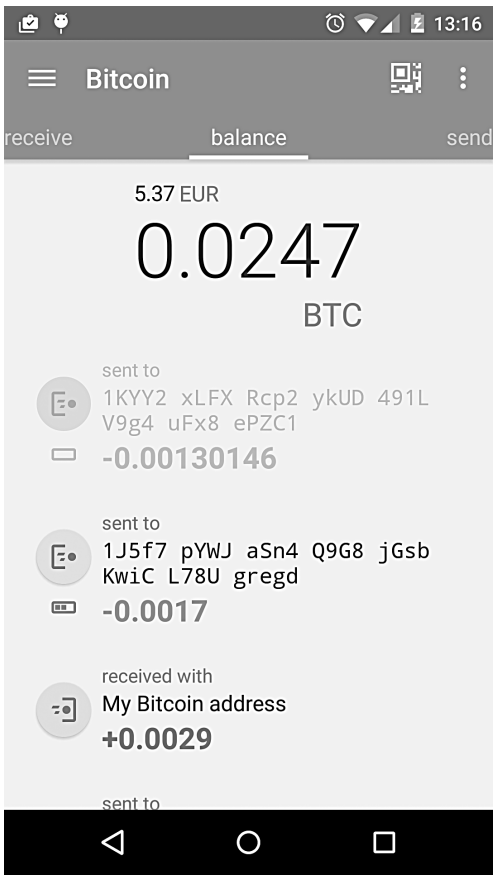
Práce s mobilní peněženkou je intuitivní a mnohem jednodušší než práce s mobilními aplikacemi tradičních bank. Na obrázku je vidět peněženka Coinomi, na které je uloženo 0,0247 BTC. Přestože v nastavení v levém horním rohu je k dispozici řada dalších možností, k práci s bitcoiny stačí pouze hlavní tři záložky. V záložce „Send" je možné vyplnit adresu a množství bitcoinů a odeslat. Lepší variantou je použít v pravém horním rohu ikonu **QR kódu**, čímž se aktivuje čtečka a po přečtení obrázku se předvyplní adresa a množství. Poté stačí pouze potvrdit odeslání.

QR kód (Quick Response Code)

2dimenzionální čárový (tedy spíš „čtverečkový") kód pro optické strojové zpracování. Je tvořen černými čtverečky v matici o velikosti 21×21–177×177 polí na bílém pozadí. Tři charakteristické kontrastní rohy slouží k normalizaci velikosti, orientace a úhlu obrazu. Kód s největší maticí může nést až 2953 bajtů, běžně používané velikosti nesou desítky až stovky alfanumerických znaků (např. bitcoinovou **adresu**). Kód obsahuje 4úrovňové zabezpečení Reed-Solomon, díky čemuž je odolný vůči chybám (znečištění části plochy, ustřižený roh apod.).

Záložka „Balance“ ukazuje zůstatek a po kliknutí na adresu i transakční historii. „Receive“ ukáže QR kód pro příjem bitcoinů. Standardně tedy na jednom telefonu zmáčknete receive, vyplníte, kolik bitcoinů chcete přijmout, což vygeneruje příslušný QR kód, a druhý uživatel kód jednoduše vyfotí a potvrdí. Sestavení celé transakce tak trvá několik sekund.

Výhoda Coinomi je i integrovaná P2P směnárna ShapeShift, kde lze vyměnit bitcoiny na jiné kryptoměny. Funguje to tak, že pokud chcete směnit jednu měnu za druhou, směnárna najde dostatek lidí s opačným požadavkem a přímo vás propojí, aniž by prostředky někde držela. Tím se eliminuje riziko, že by vám peníze někdo ukradl.



Kde bitcoiny koupit

První mince

Peněženku tedy máte a rádi byste ji naplnili výměnou za tradiční peníze. Ještě než to uděláte, můžete si položit dvě otázky. První otázkou je, zda je taková činnost vůbec legální ve smyslu platných zákonů. A odpověď není jednoduchá. Ani finanční regulátoři se zatím nedokázali v Bitcoinu zorientovat a dát jasnou odpověď. Z vyjádření České národní banky a Ministerstva financí vyplývá, že Bitcoin za legální považují. Nikdo zatím nebyl stíhán. Nemusí to tak být navždy, ale pro dnešek jde o legální činnost. Na druhou stranu při nákupu bitcoinů za české koruny musíte manipulovat i s měnou, ke které se již regulace váže. Ministerstvo financí ČR v metodickém pokynu MF-86584/2013/24 k Bitcoinu pouze konstatuje, že je třeba považovat transakce nad 1000 euro za rizikové a transakce nad 15 000 euro ohlašovat. Držme se zde tedy transakcí pod 1000 euro.

Druhá otázka je taktéž nasnadě – proč si bitcoiny kupovat, když se dají těžit? Odpověď není příliš odlišná od odpovědi na otázku, proč si kupovat zlato, když se dá vytěžit. Bývaly časy, kdy se zlato dalo najít pouhou rukou v řece, ale dnes musíte mít sofistikované stroje, vrty, infrastrukturu, obrovský kapitál a štěstí. A stejně tak je tomu i u Bitcoinu, který se zlatem zjevně inspiroval, a tedy by to nemělo být příliš překvapivé. V roce 2010 se daly bitcoiny těžit pomocí osobního počítače a později pomocí stále výpočetně silnějších grafických karet. Dnes je těžba pomocí standardní výpočetní techniky prakticky nemožná, a pokud někdo tvrdí opak, tak jde s nejvyšší pravděpodobností o podvodníka, který se snaží prodat své starší stroje. K těžbě se dnes používají speciální těžební stroje, které jsou optimalizované přímo pro těžbu bitcoinů. Pokud ovšem máte dostatečný kapitál a chcete si takové zařízení pořídit a začít těžit, možné to je. K těžbě se vrátíme v jedné z následujících kapitol.

Nejpohodlnější cestou k prvním bitcoinům či litecoinům jsou bitcoinové bankomaty. Stačí mít nainstalovanou mobilní peněženku nebo vytisknutý QR kód své peněženky v počítači a ten

přiložit ke čtečce na bankomatu. Bankomat tak pozná, kam má bitcoiny poslat. Do bankomatu pak už jen vložíte bankovky, ten je v daném kurzu s marží přepočítá na bitcoiny a požádá vás o potvrzení. Pokud souhlasíte, bitcoiny se vám takřka obratem přičtou do peněženky. V době vysokých poplatků se však bankomaty příliš nevyplácí pro malé částky. Na konci roku 2017 zbylo z nakoupených bitcoinů za 2000 korun jen 1500. Některé české bankomaty nabízí vedle bitcoinů i litecoiny.

Tyto bankomaty fungují často obousměrně, kde stačí zadat, kolik chcete vybrat, automat vygeneruje QR kód, ten vyfotíte telefonem a transakci potvrdíte. Bankomat vám poté vydá papírové peníze. Je to stejné, jako kdybyste si ty papírové peníze kupovali.

Takových bankomatů je v Česku několik, v Praze jsou umístěny například v Paralelní Polis, v Alze, na Arkádách Pankrác, v Centru Nový Smíchov, ve Slovanském domě nebo na Arbesově náměstí. V Brně je bankomat v OC Omega a jeden bankomat je umístěn i v Ostravě a v Karlových Varech. Hezký přehled nabízí aplikace pro mobilní telefon Bitperia či stránky coinmap.org.

Dalším snadným způsobem, jak získat svůj první bitcoin, je koupit ho od někoho z okolí, ať již za koruny, nebo výměnou za zboží či službu. O aktuálním kurzu se můžete informovat na internetu, dnes ho zveřejňují prakticky všechny stránky, kde se dají najít aktuální kurzy mezi tradičními měnami.

Prodejce můžete nalézt buď náhodně, na internetových fórech, sociálních sítích, inzertních a aukčních serverech, např. eBay, nebo se lze vydat institucionalizovanou cestou. Nejrychlejší, ale méně bezpečnou cestou je nákup přes tzv. local (face-to-face, OTC, over the counter). Roztříštěnosti individuálních prodejců a kupujících si totiž velice rychle někdo všiml a založil server localbitcoins.com, na kterém zadáte preferované město (Praha, Brno nebo Bratislava jsou velmi frekventovaná místa) a vyskočí na vás desítky nabídek, seřazených podle ceny. U prodejců jsou vidět banky, jejichž účty disponují, a reference z již proběhlých obchodů. Pokud se vám zdají reference přesvědčivé, cena za bitcoin nízká, prodejci napíšete a domluvíte si platbu. Po zaplacení vám prodejce zašle na vámi uvedenou adresu peněženky vaše nové bitcoiny. Je vhodné podívat se na banky prodejce, jelikož při shodě bank může dojít k převodu peněz a bitcoinů téměř okamžitě. Velká část profesionálních prodejců tak

disponuje účty u nejvýznamnějších tuzemských bank, aby nakupujícím tuto možnost zajistili. Po úspěšném nákupu nezapomeňte přidat referenci, abyste i dalším zájemcům usnadnili jejich nákup.

Local Bitcoins jsou i dobrou cestou k prodeji bitcoinů zpět za koruny. Pokud vám majitel bytu neumožňuje platit nájem v bitcoinech (i takoví domácí jsou!), potom se může stát, že chcete nakoupit koruny. Prodej přes local je velmi rychlý a činí Bitcoin z hlediska tradičních peněz velmi likvidní, tedy své koruny můžete mít téměř okamžitě k dispozici. Pokud nevyžadujete příliš vysokou cenu, potom se zájemci ozývají prakticky ihned. A pokud máte štěstí na zájemce s účtem u stejné banky, převod je okamžitý. Na druhou stranu je oproti burze obchod tváří v tvář o jednotky až desítky procent dražší. Připlácíte si za soukromí a pohodlí.

Je důležité však znát zákony a neobchodovat na ulici velké množství peněz. Dle zákona 254/2004 Sb. o omezení plateb v hotovosti bylo před rokem 2011 nutné provést platbu převyšující 15 tisíc eur bezhotovostně. Nový zákon 261/2014 Sb. zrušil tento eurový limit a zavedl limit 270 tisíc korun.

I pokud si ale předáte několikrát nižší částku, ani tak není jednoduché ji vložit na účet. Dle zákona 253/2008 Sb. je obchodem podezřelým z praní špinavých peněz takový obchod, kdy převádíte majetek bez zjevně ekonomického důvodu, provádíte výběry nebo převody na různé účty bezprostředně po hotovostních vkladech, uskutečníte nápadně více operací, než je pro vás obvyklé apod. Banky tak mohou být ze zákona povinny vyžadovat identifikaci a případně informovat příslušné státní orgány.

Že není radno tyto zákony podceňovat, poznali dva uživatelé Local Bitcoins ze Spojených států. Michaelhack a proy33 si v americkém státě Florida vyměňovali bitcoiny za 30 tisíc dolarů, přičemž byli zadrženi policisty v utajení. Je dobré znát zákony, ale pokud nechcete obchodovat bitcoiny za stovky tisíc, potom nemusíte mít žádné obavy a směně na Local Bitcoins můžete plně důvěřovat.

Směnárny a burzy

V českém prostředí jsou dobrým a velmi rychlým způsobem, jak získat bitcoiny, specializované směnárny. Například na simplecoin.cz lze jednoduše zadat množství požadovaných bitcoinů, e-mail a adresu peněženky. Pokud máte účet u jedné z bank preferovaných směnárnou, přijdou vám objednané bitcoiny prakticky okamžitě po zadání bankovního převodu na obdržené číslo účtu a variabilní symbol. Obdobně lze bitcoiny i prodat a získat za ně koruny. Směnárna nevyžaduje žádnou registraci a na e-mail přijde pouze instrukce k odeslání peněz. Směna je okamžitá. Nevýhoda se však skrývá ve vyšším kurzu, pokud bitcoiny kupujete, a nižším, když je prodáváte (obchodník na burze by řekl, že je zde větší „spread"). Směnárna pak na tomto rozdílu mezi nákupní a prodejní cenou vydělává. Jde o rozumné spojení jednoduchosti, rychlosti a dobré ceny. Vedle bitcoinů si na simplecoin.cz koupíte i litecoiny a další kryptoměny.

Jinou formou nákupu bitcoinů je obchodování na specializovaných burzách. Po krachu Mt.Gox, která byla svého času největší burzou bitcoinů na světě, a vzniku jednoduché konkurence v podobě bitcoinových bankomatů jde spíše o nástroj pro nákup velkých a pravidelných objemů. Pro vyzkoušení bitcoinů není vhodné si účet na burze zakládat, na druhou stranu jsou bitcoinové burzy skvělým nástrojem pro ty, kteří si chtějí vyzkoušet trading, a samozřejmě pro zkušené tradery.

V současnosti patří mezi největší bitcoinové burzy na světě bitstamp.net, bitfinex.com, kraken.com, poloniex.com, gdax.com a další. Burz je několik desítek a ne všechny jsou bezpečné, proto je lepší, pokud chcete investovat vysoké částky, poradit se s odborníky nebo si najmout služby konzultantů.

Burza nabízí některé možnosti, které vám Local Bitcoins nebo bankomaty nabídnout nedokážou, ale také má své nedostatky. K tomu, abyste si založili účet na burze, potřebujete v současnosti (postupem času se toto prostředí stále více institucionalizuje) jejich provozovatelům zaslat své osobní údaje. A ne jen tak ledajaké, burzy po vás většinou chtějí dva dokumenty – osobní identifikaci a doklad o bydlišti. Osobní identifikací je ve vysokém rozlišení naskenovaný řidičský průkaz, pas nebo průkaz totožnosti. S dokladem o bydlišti je to těžší, jelikož je nutné zaslat úřední dokument, který obsahuje vaše jméno a adresu. Nelze však zaslat cokoliv a výpis možných dokumentů není pro každého dost široký. Některé burzy vyžadují tento dokument s ověřeným překladem do angličtiny, jiné cizí jazyk zvládnou přečíst, ale ověření jim trvá déle. Pokud je však seženete a jsou po jednom až dvou týdnech ověřeny, obdržíte e-mail s touto informací a můžete se přihlásit.

Nyní potřebujete na burzu poslat peníze. Korunová burza bitcoinů zatím neexistuje (přestože v době čtení už možná funguje česká burza NakamotoX), a tak je nutné zaslat na burzu eura nebo americké dolary. To jde udělat standardně pomocí SEPA nebo IBAN převodu, který však není většinou zadarmo a trvá několik dní. Rychlejší cestou je poslat dolary například z online platebního systému OKPay, na jehož založení a umístění vkladu však musíte projít cestou ne nepodobnou výše popsanému. Některé

burzy nabízí další možnosti vkladů, například přes jiné kryptoměny, a samozřejmě přímý vklad bitcoinů, pokud již nějaké máte.

Pokud už máte na burze dolary či jinou obchodovanou měnu, můžete se dát do nakupování (a případně i prodeje). Výhodou obchodování na burze je velké množství nakupujících a prodávajících (což znamená i menší spread) a především vstupujete na globální trh. Nyní je jedno, zda jste oba z České republiky a kde máte vedené účty. Jediné, na čem záleží, jsou dolary, bitcoiny a jejich relativní cena.

Stačí v záložce, většinou nazvané „trade" nebo „buy/sell", kliknout na „buy" pro nákup a „sell" pro prodej. Příkazy se dají omezit maximální/minimální cenou nebo nechat vypořádat za okamžitou tržní cenu burzy.

Problémem burz je však horší likvidita vašich bitcoinů. Pokud prodáte bitcoiny za dolary prostřednictvím burzy, jsou dolary vedené stále na jejich účtu. Přístup k nim je tedy omezený a může se stát, že o své peníze přijdete, jak se tomu stalo v případě Mt.Gox. Také bitcoiny nejsou vaše, dokud si je nepošlete do své vlastní peněženky.

Všem burzám nelze věřit, a o to více po zkušenostech s Mt.Gox. Slušná burza by se neměla stydět ukazovat vlastníka, nebo dokonce zemi, ve které fyzicky sídlí. Rozhodně neposílejte peníze do země, do které byste nikdy ani nejeli.

Bitcoinové burzy a koneckonců celý svět Bitcoinu zatím není skoro vůbec regulován. To na jednu stranu dramaticky zvyšuje konkurenci, a tím snižuje cenu za jakoukoliv službu, na stranu druhou ale nesete plné riziko jakéhokoliv špatného kroku. Pokud si uložíte peníze do peněženky, která bude vykradena, nikdo vám vaše bitcoiny nevrátí. Pokud spadne burza, na které máte bitcoiny, byť za miliony dolarů, už je s nejvyšší pravděpodobností neuvidíte.

Další možnosti

Na malé částky není špatnou volbou směnárna Coinbase. Ta má vlastní aplikaci do telefonu a webové rozhraní. Výhodou Coinbase je snadný nákup s minimem ověřování, a to dokonce přes kreditní kartu. Problém je, že Coinbase je služba třetí strany a stejně jako u burz nebo webových peněženek nedržíte své soukromé klíče. Jakmile si tedy bitcoiny přes Coinbase koupíte, okamžitě je přepošlete do vlastní peněženky na adresu, ke které soukromé klíče máte.

Posledním a nejpříjemnějším způsobem, jak získat bitcoiny, je najít si přátele, kteří nějaké mají. V České republice, na Slovensku a stejně tak po celém světě se schází početné skupiny uživatelů a zájemců, kteří spolu vedou živou debatu, informují se o novinkách a v neposlední řadě také čas od času jeden druhému nějaké bitcoiny za koruny nebo za něco jiného pošle. V Praze rádi zajdou na pivo, kávu nebo přednášku do Paralelní Polis (facebook.com/vejdiven, Dělnická 43, Praha 7), v Brně se pořádají pravidelné meetupy na různých místech a v Bratislavě je pořádá Blockchain Slovakia (facebook.com/blockchainslovakia).

Existovala i doba, kdy se daly bitcoiny koupit pomocí služby PayPal. Dnes již prakticky nikdo bitcoiny za peníze z PayPalu nenabídne, jelikož je možné tyto transakce vrátit zpět. V případě PayPalu se stávalo, že si někdo koupil bitcoiny, zaplatil ze svého PayPal účtu, (patrně) obdržel bitcoiny a následně si u služby vyžádal vrácení transakce, protože mu „nic“ nepřišlo (respektive mu přišla – relativně hodnotná – změť znaků). PayPal případné stížnosti na neobdržení bitcoinů neřešil, protože směnu bitcoinů nemá jak ověřit. Prodejci bitcoinů dnes již nechtějí platby přes PayPal riskovat, ale je možné se na platbě přes PayPal dohodnout například na Local Bitcoins. I tam je to ale extrémně riskantní a na internetových fórech se množí špatné zkušenosti. Šéf PayPalu se na začátku roku 2014 veřejně vyjádřil, že Bitcoin podporuje, ale nemá jak ověřit, že k obchodu došlo. Prodejci, kteří nabídnou možnost platby přes PayPal, se mohou velmi rychle stát obětí podvodníka.

Jak bitcoiny vytěžit

Krumpáče do rukou

Proč si bitcoiny kupovat, když jdou vytěžit? Dává to vůbec smysl? Těžaři ho snadno získají pomocí počítače a pro ostatní je za vysokou cenu v dolarech? Smysl to dává, je to velmi podobné čemukoliv jinému, co je vzácné.

Těžba (Mining)

proces, při kterém se pomocí strojově náročného výpočtu hledá další **blok** pro napojení do **blockchainu**. Validní **blok** je nalezen, pokud splňuje podmínku, že jeho **hash** (přesněji **hash** vypočtený nad serializací jeho dat) je nižší než určitý cíl (parametr target – číslo začínající na mnoho nul v numerickém zápisu **hashe**). Tento cíl se odvozuje z momentální obtížnosti (parametr difficulty), která se mění každých 2016 **bloků** v závislosti na rychlosti jejich nalezení tak, aby průměrná rychlost generování nových **bloků** činila 1 **blok** za 10 min. Pokud **blok** nesplňuje podmínku na nízký **hash**, je nutné jeho serializaci pozměnit (obsahuje k tomu určené pole nonce, které může nabývat libovolné hodnoty) a zkusit **hash** přepočítat. **Těžba** je vlastně částečná inverze hashovací funkce (vychází z konceptu tzv. hashcash z roku 1997).

V počátcích **Bitcoinu** se **těžba** prováděla na procesorech samostatných osobních počítačů, ale jak její obtížnost stoupala (zapojovalo se více počítačů při konstantní rychlosti generování **bloků**), přesouvala se od CPU (2009–2010) k paralelním výpočetním architekturám – od GPU (grafické karty, zejm. ATI/VLIW) (2010–2011), přes FPGA (programovatelná hradlová pole) (2011–2012), až k ASIC (zákaznické hardwarové obvody, navržené speciálně k počítání jednoho typu výpočtu). Od roku 2011 se **těžba** navíc distribuuje do tzv. **poolů**.

Stejně jako můžete těžit zlato a vyhnout se tak „placení" za něj, tak můžete těžit i bitcoiny. Někomu se taková činnost vyplatí, ale jinému nemusí. Pokud nemáte nutkání jít těžit zlato, ale raději si ho koupíte na trhu, potom je pravděpodobné, že si myslíte, že se vám to nevyplatí. Trvalo by věčnost, než byste se naučili, jak se zlato těží, museli byste založit důl někde v rozvojovém světě, nastudovat si místní legislativu, zaplatit dělníky a opustit současné zaměstnání, a to vše s rizikem toho, že se vám investované peníze nevrátí, například pokud cena zlata klesne nebo se ukáže, že byl odhad jeho množství nadhodnocený. A tak je tomu i u bitcoinů – existují lidé,

kteří do tohoto rizika jít nechtějí a je pro ně snazší získat bitcoiny směnou.

Těžbu bitcoinů si lze představit jako řešení náročné matematické úlohy. Avšak čím více je bitcoinů v oběhu, tím menší odměnu dostanete, a čím více lidí se snaží úlohu vyřešit, tím je náročnější. Když se snažil sám Satoshi Nakamoto vyřešit „nultý" příklad, stačilo mu prakticky pouze zapnout počítač. Byl sám, bitcoinů bylo vytěženo přesně nula, a tak byla vysoká odměna a extrémně nízká náročnost úlohy. Postupně se náročnost zvyšovala natolik, že bylo velmi obtížné vytěžit bitcoiny pomocí vlastního počítače. Ve srovnání se specializovanými těžebními stroji vypadal i slušně vybavený stolní počítač jako kalkulačka. Úlohu sice vyřeší, ale za velmi dlouhou dobu. Dnes je obtížnost tak vysoká, že výkon celé bitcoinové sítě je 20 000× vyšší než výkon 500 nejvýkonnějších počítačů světa dohromady.

K těžbě teoreticky stačí mít nainstalovaný specializovaný software, například těžební aplikaci z guiminer.org. Ta je již o poznání složitější než doposud představené bitcoinové aplikace. Po spuštění vás software vyzve k registraci v poolu. Po vytvoření účtu můžete zadat své uživatelské jméno a heslo do programu a kliknutím začít těžit. Zní to moc jednoduše na to, aby to fungovalo? Bohužel ano. V počátcích Bitcoinu stačilo k těžbě pouze spustit počítač a software typu GUIminer začal těžit. K **potvrzování transakcí** stačila pouze výpočetní kapacita běžného procesoru (CPU).

Potvrzení (Confirmation)

stav **transakce. Transakce** se považuje za potvrzenou, pokud je obsažena v **blockchainu**. Čím hlouběji je obsažena/„pohřbena", tím bezpečnější je pokládat ji za nezvratitelnou. Hloubka je počet **bloků** mezi **blokem** zahrnujícím **transakci** ve svých datech a **blokem** aktuálně těženým a nazývá se počet **potvrzení**. Jelikož s počtem **potvrzení** se riziko zvratitelnosti **transakce** snižuje exponenciálně, je i nízký počet dostačující pro považování **transakce** za nezvratitelnou. U **transakcí** větších objemů se v praxi často požaduje počet **potvrzení** ≥ 6.

Ačkoliv považujeme obecně počítače za velmi výkonná zařízení, samotný procesor dnes na vyřešení úlohy nestačí a trvalo by mu věčnost, než by něco vytěžil. Do té doby byste za elektřinu potřebnou k řešení zaplatili o mnoho řádů vyšší cenu, než je tržní cena vytěžených mincí. Nebo v rámci poolu byste k vyřešení přispěli

tak malým dílem, že by vaše odměna ani nestála za řeč. Některé programy vás k těžbě pomocí procesoru dokonce ani nepustí.

Hash

zobrazení množiny dat obecné délky do množiny dat omezené délky (např. soubor libovolné délky zobrazí do množiny 256bitových čísel). Obecným požadavkem na hashovací funkci je uniformní pokrytí obrazů (aby jednotlivé obrazy příslušely podobnému počtu vzorů). Požadavkem na kryptografickou hashovací funkci je navíc vysoká nelinearita (aby libovolně malá změna vzoru způsobila libovolně velkou změnu obrazu) a především asymetrická výpočetní složitost (spočítat přímé zobrazení vzoru na obraz je snadné, spočítat obecně nejednoznačné inverzní zobrazení obrazu na vzor je extrémně obtížné). Příkladem hashovacích funkcí jsou různé kontrolní součty (XOR, rotace, tabulky) a CRC (tělesa nad dělením polynomů). Mezi kryptografické **hashe** patří např. funkce BLAKE, MD2-6, RIPEMD, SHA. Bitcoinový protokol používá poslední dvě jmenované (zejm. SHA-256 při **těžbě bloků**).

Velice brzy se zjistilo, že je výhodné těžit bitcoiny pomocí paralelních procesorů grafických karet (GPU). Ty mají až stokrát vyšší výkon a k řešení úlohy jsou výhodnější. Pokud byla karta zvolena rozumně v poměru cena/výkon, přičemž cenou není pouze cena pořizovací, ale také spotřeba elektřiny, potom se dalo na těžbě získat i slušné množství bitcoinů. Grafická karta za 10 tisíc korun dokázala na konci roku 2010 vytěžit každý den bitcoiny v ceně okolo 1000 korun. S přístupem k levné elektřině se tak investice do grafické karty mohla vrátit v řádech týdnů.

Žádný zisk ale na svobodném trhu není věčný. Snadného zisku si všimli další lidé a začali skupovat grafické karty ve velkém a těžit. Několikrát došlo na různých místech světa k nedostatku grafických karet, dle pamětníků dokonce i v České republice. To zvyšovalo obtížnost těžby a snižovalo výnosy. Na konci roku 2011 se denní výnos dostal až k 30–40 korunám. Vzhledem k ceně elektřiny byl výnos tak nízký, že donutil mnohé těžaře s těžbou přestat. Jelikož je obtížnost těžby zpětnovazebně ovlivněna výpočetním výkonem celé bitcoinové sítě, odchod těžařů obtížnost opět snížil a výnos tak zvýšil. Tento způsob zvyšování a snižování obtížnosti vytváří rovnováhu, při které se zisky z těžby snižují až k nule a kladných zisků dosahují jen ti, kteří jsou schopni těžit s nejnižšími náklady, tzn. nejefektivněji.

A tak i grafické karty pomalu přestávaly vynášet. K těžbě se začaly používat konfigurovatelné integrované obvody – hradlová pole (FPGA), která lze na úrovni hardwaru naprogramovat pro řešení konkrétní úlohy. FPGA je levnější a výkonnější, díky čemuž dokáže výnos bitcoinů oproti GPU až zdesetinásobit.

Skutečnou změnu ale přinesly až kolem roku 2013 zcela specializované obvody dle zákaznického návrhu (ASIC). ASIC čip je podstatně dražší než grafické karty a FPGA, ale dosahuje nesrovnatelného výkonu při nízké spotřebě. **Hashovací rychlost** ASIC čipů dosahuje až několika milionů Mh/s, takže srovnání s průměrnou grafickou kartou o výkonu několika stovek Mh/s neukazuje ani tak řádový nárůst, jako neuvěřitelnou cestu, kterou za pár let Bitcoin urazil.

Hashovací rychlost (Hash Rate)

veličina udávající míru výpočetního výkonu uzlu nebo celé bitcoinové sítě. Její jednotkou je h/s – počet spočtených **hashů** za sekundu. Odvozené jednotky jsou kh/s (kilohash; 1 kh/s = 1000 h/s), Mh/s (megahash; 1 Mh/s = 1000 kh/s), Gh/s (gigahash; 1 Gh/s = 1000 Mh/s), Th/s (terahash; 1 Th/s = 1000 Gh/s), Ph/s (petahash; 1 Ph/s = 1000 Th/s), Eh/s (exahash; 1 Eh/s = 1000 Ph/s)… Výkon celé sítě se mezi lety 2009–2018 zvýšil z 1 Mh/s na 10 Eh/s (tj. rozdíl o 13 dekadických řádů).

Zajímavou alternativu začaly nabízet další kryptoměny, které se stále těží na grafických kartách. Těžaři tak začali skupovat grafické karty a těžit například Monero, Ethereum či Zcash. Vstupní náklady jsou nižší, což umožňuje teoreticky vyšší míru decentralizace, ale výnosnost se zpravidla srovnává napříč všemi měnami.

Horníci v bazénu

V dnešním světě tak těží z většiny pouze úzce specializovaní těžaři, kteří zainvestovali statisíce či miliony korun do extrémně výkonných strojů. Sdruženi jsou v několika velkých skupinách – v poolech. Mezi největší pooly patří BTC.com, ViaBTC, AntPool, BTC.TOP, český Slushův pool, F2Pool, 58Coin nebo BTCC pool. Když jsme v roce 2015 jmenovali 8 největších poolů, ze zde zmíněných v seznamu figurovaly pouhé tři.

Těžaři tak těží společně a **generující transakce** včetně poplatků plynou poolu, který je rozděluje. Pooly mají různé vlastnosti, na

některých se platí poplatky a na jiných ne, některé si dělí transakční poplatky, jiné si je ponechávají apod. Konkurence mezi pooly je ale vysoká a některé například nemají žádné poplatky. Jednotliví těžaři si vybírají pool, ve kterém budou participovat, podle toho, jak se jim ta která politika líbí, což je právě zdrojem oné konkurence mezi pooly.

Dá se pochopitelně těžit i mimo pool, především s vysokým výkonem, avšak taková těžba je riziková. Pro zjednodušení si můžeme představit, že těžař disponuje těžebním výkonem, který má šanci vyřešit úlohu a vytěžit následující blok (což bylo zhruba do roku 2013 50 bitcoinů, mezi lety 2013–2016 25, dnes 12,5 bitcoinů atd.) s pravděpodobností 0,1 procenta.

Padesát bitcoinů je slušný výdělek, ale šance na něj je i přes obrovský výkon velmi malá. Pokud by se však přidal do poolu, který má 20 % výpočetní kapacity sítě, získá 20% šanci, že pool blok vytěží a z vytěžených bitcoinů získá svou poměrnou část (0,1 % celého výkonu v poolu sdružujícím 20 % kapacity je 0,5 % výkonu v rámci poolu), tedy 0,125 BTC.

Protože má pool 20 % kapacity, v průměru bude úspěšný jednou z pěti bloků, kdy každý se vytěží v průměru jednou za deset minut. Tedy tento těžař by v průměru každých padesát minut získal 0,125 BTC. Pokud by těžil sám, byl by úspěšný jednou z tisíce pokusů, tedy jednou za týden, s odměnou 50 BTC.

Díky poolu tak získává menší výdělek, ale v pravidelných intervalech. Jde vlastně o formu pojištění. Pooly tak reflektují dobře známou ekonomickou skutečnost, že lidé preferují peníze dnes před stejným množstvím zítra a že většina lidí raději zvolí jistou částku před padesátiprocentní šancí na zisk dvojnásobku nebo ztrátu všeho. Lidé mají jistotu rádi a pojištění je dobrým způsobem, jak jí dosáhnout.

Je tedy pravdou, že bitcoiny může těžit úplně kdokoliv, respektive kdokoliv s počítačem a přístupem k elektřině a internetu (nebo alespoň s tužkou a papírem rychlostí ani ne 1 hash za den). Dále lze tvrdit, že samotná těžba není z uživatelského hlediska složitá. I nejdražší a nejvýkonnější těžební stroje stačí připojit k počítači (skrze USB, síť atd.), spustit jednoduchý software jako je GUIminer, přihlásit se k jednomu z mnoha poolů, kliknout na „start“ a následně jen čekat na odměnu.

Generující transakce (Generation)

speciální typ **transakce**. Kromě „normálních" **transakcí**, pro které platí podmínka nulového součtu hodnot vstupů a výstupů (a **poplatku za transakci**) existuje v každém **bloku** právě jedna **generující transakce**, prostřednictvím které (a pouze tak) vznikají nové bitcoiny. **Generující transakce** nemá žádné reálné vstupy (na jejich místě vystupuje parametr coinbase nesoucí libovolná data) a její objem je roven součtu nově vygenerovaných **bitcoinů** a poplatků za ostatní **transakce** v **bloku** obsažené. Množství nově vygenerovaných bitcoinů je 50 BTC pro **blok** 0 a každých 210 tis. **bloků** (≅ 4 roky) se snižuje na polovinu (v době psaní druhého vydání knihy bylo 12,5 BTC). Toto exponenciální snižování odměny za nově vytěžený **blok** má za následek omezené množství bitcoinů ve kterémkoliv okamžiku. Maximální množství bitcoinů je 21 milionů (součet geometrické posloupnosti) a vzhledem k parametrům systému (rychlosti generování a zaokrouhlovací chybě pro odměnu < 1 satoshi, viz **BTC**) bude dosaženo v roce 2140. Poté budou motivací k těžbě pouze **poplatky za transakci**. Podmínky disponování s výstupy **generující transakce** určuje ten, kdo vytěží **blok**, ve kterém je zahrnuta (v praxi putují tyto bitcoiny na **adresu** těžaře). **Generující transakce** může být jediná **transakce** zahrnutá v **bloku** a u prvních desítek tisíc **bloků** tomu tak bylo – v tomto období vznikaly bitcoiny pro budoucí normální **transakce**.

Na druhou stranu, aby se těžba vyplatila, je dnes zapotřebí investovat do těžby obrovské sumy, mít přístup k levné elektřině a chlazení a být připraven na to, že se stroj za stovky tisíc za pár let nebude dost možná hodit ani na součástky a že budete muset následně opět investovat velké peníze do stroje nového. K tomu všemu rozhodně nepočítejte s tím, že by vám na těžbu bitcoinů poskytla banka úvěr.

Jak bitcoiny ochránit

Bitcoin není jiný

Prolomit bezpečnostní prvky celé bitcoinové sítě je prakticky nemožné. Avšak získat konkrétní bitcoiny z nezabezpečeného počítače již možné je. A je to relativně snadné. Útočník například nejprve do počítače oběti nainstaluje škodlivý software, který není vidět, ale umožňuje mu vzdáleně počítač ovládat. Bitcoiny oběti si pak standardní cestou převede do své peněženky. Ke spuštění škodlivého kódu může dojít spolu s jiným nedůvěryhodným programem nebo může přijít například elektronickou poštou. Možnosti útoku tedy odpovídají klasickým virům a jiným malwarům. Oproti devadesátým letům dvacátého století jsou dnes i standardně zabezpečené počítače mnohonásobně bezpečnější, ale stejně tak metody útoku jsou nyní mnohem důmyslnější, takže o stoprocentním bezpečí se nikdy mluvit nedá.

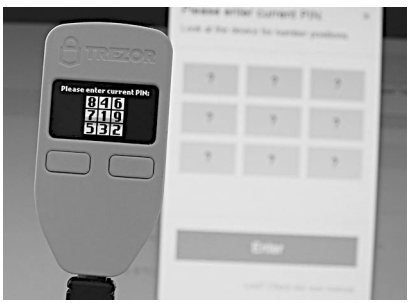
Většina pokročilých uživatelů doporučuje kombinovat různé druhy ochrany a úschovy bitcoinů. Malá část peněz může být v peněžence na chytrém telefonu či v klientu typu Electrum a zbývající větší část uložená na dvou různých zařízeních pod fyzickým zámkem. Ostatně stále jde jen o peníze a obdobně se chovají obezřetní lidé i dnes. V peněžence je rozumné nosit pouze malý obnos na běžné platby a zbytek peněz mít uschovaný ve vlastním trezoru či v bance. Bitcoin není jiný.

Důvěřovat třetí straně není jednoduché a bitcoiny fyzicky zamykat zase příliš uživatelsky přívětivé. Vznikly tak brzy další metody, jak bitcoiny chránit, a mnoho vývojářů se snaží právě v této oblasti prosadit tím, že naleznou lepší řešení.

TREZOR

O zásadní posun se zasadil český startup SatoshiLabs, který vyvinul hardwarovou peněženku zvanou TREZOR One. Jde o malé USB zařízení, o něco menší než klíč k autu, ve kterém se skrývá malý, jednoúčelový počítač. Od ledna 2018 společnost také nabízí novou generaci hardwarové peněženky, zvanou Model T. Navenek se liší ve

způsobu používání, zatímco TREZOR One (dolní obrázek) spoléhá na dvě tlačítka a monochromatický displej, Model T (horní obrázek) vlastní barevný dotykový displej, schopný zobrazovat mnohem více informací. Pro Model T se také budou vyvíjet nové aplikace a funkce. Nicméně bezpečnost kryptoměn vám zaručí oba přístroje.



TREZORy fungují na dvou jednoduchých, přesto velmi bezpečných principech – izolaci klíčů a nutnosti fyzické přítomnosti jeho uživatele. Při jakémkoliv pokusu o odeslání bitcoinů nebo jiných kryptoměn z TREZORu se musí vždy fyzicky zmáčknout potvrzovací tlačítko na samotném zařízení. Pokud chcete odeslat bitcoiny, jednoduše na TREZORu transakci potvrdíte. To v praxi znamená, že **soukromé klíče** k vašim kryptoměnám jsou uložené jen v TREZORu a nikdy se neodešlou do počítače nebo mobilního přístroje. Což kontrastuje se softwarovými peněženkami, které jsou potenciálně zranitelné vůči škodlivému softwaru. Tento „malware" může zachytit vaše soukromé klíče, a tudíž získat přístup k vašim penězům. Avšak pokud jsou tyto soukromé klíče uložené mimo počítač v TREZORu, potenciální útočník není schopen nic zachytit.

Soukromý klíč (Private Key)

jeden z páru klíčů pro **asymetrickou kryptografii** se nazývá soukromý (též privátní), musí zůstat tajný a majitel ho používá k dešifrování jemu určené zprávy nebo podepisování jím ověřované zprávy. Digitální **podpis** se v bitcoinové síti používá, šifrování nikoliv. Pomocí **soukromého klíče** se podepisuje zpráva s informací, kdo bude novým disponentem bitcoinů (přesněji výstupu existující **transakce**) patřících majiteli klíče. Ke každé bitcoinové **adrese** přísluší jeden **soukromý klíč**, který je uložen v bitcoinové **peněžence**. Jeden **soukromý klíč** může příslušet více **adresám** při užití techniky „HD Wallets".

Pokud vlastníte větší množství bitcoinů či jiných kryptoměn, je jistě vhodné si hardwarovou peněženku pořídit. TREZOR One nebo Model T si lze objednat na internetové stránce u výrobce trezor.io a koupit se dá i na alza.cz, a to dokonce i za bitcoiny.

Po prvním připojení přístroje, One nebo Model T, se automaticky stáhne plugin do prohlížeče, který umožňuje snadnou komunikaci s peněženkou TREZOR Wallet. Jedná se o standardní webovou peněženku, ne nepodobnou klasickému internetovému bankovnictví, v níž se zadávají transakční detaily, jako je adresát, částka nebo i výběr měny. Jen proces podepisování bitcoinové transakce probíhá mimo webovou peněženku, a to právě na fyzickém zařízení TREZOR.

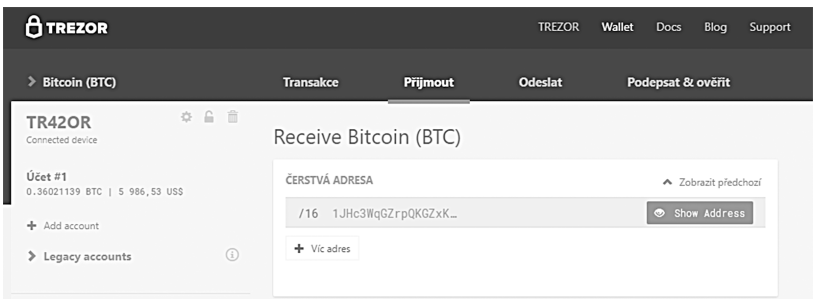
Po připojení a instalaci bude TREZOR vyžadovat PIN, bez kterého vás program nepustí k účtům. Pokud byste měli už nyní zavirovaný počítač, mohl by keylogger číst, jaký PIN zadáváte, proto se PIN zobrazuje na numerické klávesnici na displeji TREZOR One a v počítači se zobrazují pouze čtverečky s otazníky. V případě Modelu T se PIN zadává přímo na obrazovce TREZORu a přístroj také s počítačem nekomunikuje, dokud není odemknutý. Pořadí čísel na displeji se náhodně mění, a tak není možné, aby případný útočník zjistil, jaký PIN jste si zvolili.

Další úrovní ochrany je vytvoření recovery seedu, respektive náhodně generovaných dvaceti čtyř anglických slov (dvanáct u Modelu T). Tato slova si opíšete na papír a bezpečně uschováte, protože z nich je možné zpětně obnovit vaše peněženky s uloženými kryptoměnami, včetně transakční historie. To je dobrá zpráva ve chvíli, kdy svůj TREZOR omylem ztratíte nebo vám ho někdo ukradne. Pokud byste chtěli své bitcoiny ještě více ochránit,

lze recovery seed zabezpečit dalším heslem, pro případ, že by někdo například našel onen papír, na který jste si recovery seed zaznamenali.

TREZOR je ideální formou pro uchování větších částek. Ostatně, funguje stejně jako skutečné trezory. Ve své peněžence lidé nosí obvykle malé sumy na běžné transakce a velké sumy mají uchovány pod zámkem. Podobným způsobem je vhodné uvažovat o Bitcoinu a držet velké sumy v TREZORu a mobilní aplikace využít například jen pro nákup kávy. Nicméně i TREZOR dokáže sloužit jako mobilní peněženka, s aplikacemi od různých vývojářů. Stačí k tomu mít telefon s Androidem z posledních let.

TREZOR umí pracovat s těmi nejdůležitějšími kryptoměnami. Vedle Bitcoinu si na něj tak uložíte Litecoin, Ethereum, Zcash či Dash. Více o těchto měnách budeme psát dále.



Jde to i na papíře

Populární, ale zatím ne příliš uživatelsky příjemnou cestou k ochraně bitcoinů jsou tzv. papírové peněženky. Tyto peněženky jsou pro někoho lákavé, protože zdánlivě připomínají staré dobré papírové peníze, které umíme leckdy ochránit lépe než dokument s důležitým textem. Výhodou papírových peněženek je zejména to, že je po úspěšném vytvoření nelze vzdáleně napadnout, že nemůžou zkolabovat a nemusíte se spoléhat na bezpečnost serverů třetí strany. Na druhou stranu ale s sebou nesou stejná rizika jako papírové peníze, tj. mohou vám být fyzicky odcizeny, mohou být ztraceny nebo zničeny např. ohněm. Jak to funguje?

Nejprve je třeba najít poskytovatele papírových peněženek, například web bitaddress.org. Ten po načtení pohybem myši náhodně vygeneruje adresu a zeptá se, co s ní chcete dělat. Jednou z možností je i „paper wallet". Po jejím zvolení se již objeví samotná papírová „bankovka", kterou je možné vytisknout a vypadá zhruba následovně:

K bitcoinové adrese přísluší **veřejný klíč** a soukromý klíč. Papírová peněženka (kterou si můžete ze stránky služby ihned vytisknout) obsahuje oba, což je postačující pro nakládání s penězi, které na adrese leží. Na adresu v levé části „bankovky" lze poslat libovolné množství peněz v různých transakcích. Můžete si adresu nahrát do aplikace, která vám umožní sledovat a přijímat transakce, ale jelikož v ní není uložen soukromý klíč, nebude možné vaše bitcoiny utratit.

Veřejný klíč (Public Key)

jeden z páru klíčů pro **asymetrickou kryptografii** se nazývá veřejný a kdokoliv ho může použít k zašifrování zprávy pro majitele **soukromého klíče** nebo k ověření jeho **podpisu**. V bitcoinové síti má veřejný klíč význam **adresy** příjemce platby (přesněji, **adresa** se vypočítá z veřejného klíče, viz **Adresa**).

To je důležité, protože Bitcoin je natolik transparentní prostředí, že tuto adresu a pohyby financí z ní a na ní může vidět kdokoliv. K utracení je však potřeba znát soukromý klíč, který jste si vygenerovali pouze pro sebe a je stále skryt na papíře. Ve chvíli, kdy chcete skutečně peníze z peněženky odeslat, musíte v dané aplikaci načíst soukromý klíč naskenováním QR kódu v pravé části „bankovky".

Pochopitelně není úplně rozumné použít výše natisknutou adresu. Kdokoliv, kdo zde vidí její soukromý klíč, může utratit cokoliv, co na adresu přijde. Zkuste na ni něco poslat a uvidíte, jak dlouho bude trvat, než o tyto peníze přijdete. Úschova soukromých klíčů je alfou a omegou ochrany Bitcoinu.

Papír snese všechno a zdá se, že je to velmi bezpečný způsob uložení soukromého klíče. Ale ani zde nelze zaručit, že v počítači není škodlivý software, který soukromý klíč zachytil ještě předtím, než jste ho stačili vytisknout, a odeslal útočníkovi. Lepší ochranu tak získáte, pokud papírovou peněženku generujete s vypnutým přístupem k internetu. Stačí načíst stránku, odpojit se a vygenerovat novou adresu.

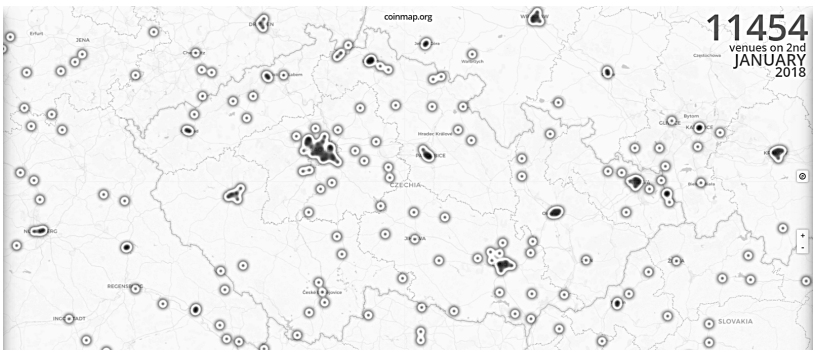
Pro úplnou bezpečnost ale ani to není dostačující a bylo by nutné generovat papírové peněženky z čerstvě instalovaného operačního systému, který by se už nikdy k internetu nepřipojil, a tisk provádět na starých tiskárnách, které není možné napadnout škodlivým programem. Eventuálně soukromý klíč opsat na papír ručně! Přestože tak lze získat bezpečnou adresu a přestože je velmi nepravděpodobné, že by se cokoliv neočekávaného přihodilo, výše popsaný postup zjevně není v souladu s principem Bitcoinu příliš jednoduchý pro uživatele, který si pouze chce koupit zboží. V této oblasti leží ještě velký prostor pro zlepšování a vývojáři jsou si toho dobře vědomi. Nelze pochybovat o tom, že mají dost motivací k tomu, aby nás uživatele těchto nepříjemností zbavili. Papírové peněženky vám tak nyní vytiskne bitcoinový bankomat nebo k tomu určené jednoúčelové zařízení.

Jak a kde ho používat

První nákup

Nyní máme bitcoiny, jsou bezpečně uložené, ale chybí ještě poslední krok. Říká se, že peněz se nenajímě, a u Bitcoinu to platí stejně (nebo spíš víc, pokud uvážíme, že papír se sníst dá). Jak se najíst, ošatit a vůbec přežít, pokud jsme všechny zastaralé koruny vyměnili za kryptoměnu? Jde to vůbec?

Nejjednodušším způsobem, jak zjistit, kde je možné utratit své bitcoiny, je zavítat na agregující server coinmap.org. Stránka shromažďuje a přehledně představuje vybraná místa, kde lze platit pomocí bitcoinů. Pouhých pár let po vytěžení prvního bloku je seznam úctyhodný – nyní je možné bitcoiny platit na tisících míst. Pochopitelně však jde jen o zlomek celkového množství.



Podívejme se tedy například na to, jak si koupit za bitcoiny elektroniku. Jako obchod zvolíme například alza.cz, který nabízí množství zboží, jako jsou počítače nebo digitální fotoaparáty, ale také hardwarová peněženka TREZOR. Standardním způsobem se vloží zvolená položka do košíku, vyplní adresa pro doručení a objednávka odešle. V závěru server vygeneruje QR kód, pomocí kterého je možné transakci zaplatit například z mobilního telefonu. Jde ve skutečnosti o jednoúčelově vytvořenou adresu, na které prodejce očekává pouze a výhradně platbu za toto zboží. Na každou transakci tak generuje jinou adresu, na kterou musíte poslat příslušnou sumu. Na osobním počítači, na kterém máte

nainstalovanou peněženku, stačí kliknout na „Pay with Bitcoin“ a automaticky se otevře softwarová peněženka a vyplní údaje k odeslání. Automaticky se otevírají všechny standardní peněženky jako Electrum a další. Pokud máte bitcoiny v telefonu, stačí QR kód naskenovat a platbu potvrdit.

Nyní stačí pouze kliknout na „odeslat“, a pokud máte dostatek bitcoinů v peněžence, už si stačí jen počkat na objednaný TREZOR.

Důležité je také sledovat čas, který se vám odpočítává, obvykle je to patnáct minut. Pokud příkaz nestihnete odeslat do patnácti minut, musíte si vygenerovat nový.

Pokud potřebujete zaplatit z hardwarové nebo webové peněženky, potom stačí zkopírovat adresu (kliknutím na „View Address“) a vložit ji do příslušného pole na stránce peněženky, zadat částku a stejným způsobem odeslat. Většina odesílacích formulářů jak v softwarových, webových či mobilních aplikacích obsahuje prakticky ta samá pole – adresu, částku v bitcoinech a dolarech a poznámku.

Všimněte si, že objednávka není zásadně odlišná od zaběhlé praxe placení z klasického účtu, dokonce je jednodušší. Pokud si objednáváte počítač jinde, stačí vám adresa příjemce, variabilní symbol a částka. Následně čekáte v případě odlišných bank i několik dní. U platby pomocí Bitcoinu je variabilní symbol a číslo účtu skryto do adresy, kterou systém automaticky vytvořil pro tuto platbu. Obchod tedy očekává, že na tuto adresu dorazí sjednaná suma a nic jiného, přestože by se majitelé soukromého klíče jistě nezlobili.

Příjem bitcoinů

Stále častěji nabízí možnost platby v bitcoinech i lidé na internetových aukcích a bazarech. Obvykle stačí na stránkách bazaru zadat do vyhledávání BTC a zobrazí se seznam věcí, které je možné si za bitcoiny koupit. Jak je možné bitcoiny snadno přijímat?

O Bitcoinu někteří lidé mluví jako o možném pokořiteli a následníkovi Western Union. Zákazníci Western Union zaplatí za přesun 1000 dolarů 2,5 procenta a musejí počkat tři dny nebo mohou peníze odeslat okamžitě a zaplatit přes 8 procent, což není zanedbatelná

částka ani pro ty, kteří Bitcoinu příliš nevěří. A ani okamžitá platba a vysoký poplatek neznamená okamžité předání peněz. Je nutné vyhledat pobočku společnosti a nechat si hotovost vyplatit. Bitcoin nabízí hned dvojí luxus – prakticky okamžitou transakci potvrzenou v řádu desítek minut a minimální poplatek, alespoň u větších částek. Výhodou Western Union a podobných společností je jejich historie. Lidé jsou na jejich existenci zvyklí a důvěřují jim. Nikde však není psáno, že to musí platit navždy.

Obdobný vztah je možné popsat i mezi Bitcoinem a kreditními kartami. Platba 1000 dolarů kreditní kartou Visa se zdá zdánlivě bez poplatků, avšak poplatek existuje. Platí ho mimo zraky spotřebitelů prodejce, který obvykle odvádí finanční společnosti dvě procenta z ceny. Bylo by bláhové si myslet, že tento dodatečný náklad nezvyšuje cenu, ale i kdyby ne, proč by měl prodávající tak vysoký poplatek vůbec platit?

Poplatky za platbu v bitcoinech mohou být i relativně vysoké, v řádech jednotek procent. Záleží na tom, jak velkou preferenci platbě dáváte a jak vysokou částku posíláte (protože poplatek není závislý na výši odesílaných peněz, jak je tomu u výše uvedených institucí). Je tedy pravdou, že například posílání velmi nízkých částek se nemusí vyplatit. Ostatně to ani u Western Union, která minimální částku přímo reguluje.

Podívejme se tedy na Bitcoin i z druhé strany směny, ze strany obchodníka, který ho přijímá. Pokud chcete za staré rádio v aukci bitcoiny, není nic jednoduššího. Stačí pro aukci vytvořit adresu a čekat na zaplacení.

Co ale pokud chcete přijímat platbu na svém e-shopu s kávou? Pokud nechcete programovat vlastní elektronický obchod a máte pouze chuť nabídnout novou službu svým zákazníkům, můžete použít služeb například bitpay.com. Na BitPay se zaregistrujete během několika minut tím, že vyplníte údaje o svém podnikání a zvolíte si měnu, ve které chcete dostávat peníze. Na výběr máte pochopitelně bitcoiny, ale i dolary či eura. Pokud zvolíte tradiční měnu, například dolary, bude BitPay přijímat bitcoiny za vás a posílat vám dolary, které za jejich směnu obdrží. Zvolíte-li příjem v bitcoinech, stačí zadat adresu peněženky, na kterou vám mají chodit. Po přihlášení do systému následně můžete začít přidávat položky do katalogu.

Stačí pouze vložit název a cenu a systém vám automaticky vygeneruje vše potřebné – tedy odkaz, pod nímž se skrývá objednávka. Tento odkaz pak jednoduše vložíte ke svému produktu na stránky. Pokud odkaz sami vyzkoušíte, uvidíte, jak funguje. Stačí vložit požadované informace (které jste si sami zvolili, že chcete o zákaznících sbírat) a kliknout na velké tlačítko s logem Bitcoinu. Po kliknutí na „Pay with Bitcoin" se otevře softwarová peněženka a nákup může být dokončen. Případně zaplatíte z TREZORu nebo z mobilního telefonu. Vy obdržíte bitcoiny a uživatelé více možností a možná i úplně novou zkušenost.

Obchodník má pro příjem bitcoinů i další motivaci – nízké transakční náklady. S tradiční měnou může v zásadě přijímat pouze hotovost nebo platby kreditní/debetní kartou. S příjmem hotovosti klade na své zákazníky jisté břímě v podobě nutnosti mít hotovost u sebe, což je u vyšších částek riskantní a v závislosti na bankovní instituci může být drahý i výběr. Proto zejména vyšší částky kvůli komfortu zákazníků umožňují obchodníci platit bezhotovostně. To však není zdaleka zadarmo. Evropská komise uvádí, že z bezhotovostních plateb si společnosti jako Visa či MasterCard berou v průměru 1,2 % placené částky. Dává tedy smysl, že se již nyní objevují první kamenné obchody, které dávají slevu při platbě bitcoiny. Při slevě 1 % ušetřil obchodník 0,2 % a zákazník právě 1 %. Prodělávají sice karetní společnosti, ale ve svobodném světě je vždy rizikem podnikání, že přijde levnější konkurence.

Speciálním případem je pak platba za službu ze všech služeb nejrozšířenější, za práci. I někteří zaměstnanci začali totiž od svých zaměstnavatelů vyžadovat platbu v bitcoinech a jejich počet přirozeně roste. Organizace Tech in Motion zveřejnila už na začátku roku 2014 výsledky ankety mezi 847 svými členy, z níž vyplývá, že více než polovina lidí měla zcela jistě zájem o možnost nechat si posílat plat v bitcoinech či jiné kryptoměně. Dalších 18 procent lidí označilo možnost „možná" a pouhých 10 procent dotazovaných tuto variantu odmítlo z důvodu, že měna dle jejich názoru nepřežije. Jedno procento respondentů nevědělo, co to Bitcoin je. Výsledky jsou pochopitelně zkreslené oproti běžné populaci tím, že byli dotazovaní většinou mladí muži se zájmem o IT, a také na otázku zcela jistě odpovídali raději spíše ti, kteří jsou z Bitcoinu více nadšení. Nicméně autoři ankety uzavírají, že z výsledků zájem cítit je, což je nepochybné.

A nejde jen o vzdálený sen úzké skupiny lidí. I v České republice vznikla první pracovní místa, na kterých dostanete odměnu v bitcoinech. Jde zatím pochopitelně o pozice ve firmách, které se Bitcoinem zabývají. Příjem těchto firem je totiž z velké části tvořen bitcoiny a dává tak smysl, že v bitcoinech platí i své zaměstnance.

Všude jinde je to o domluvě, ostatně jak jinak. Zkuste se zeptat svých domácích, zda nemůžete platit v bitcoinech nájem.

Jak na něm vydělat

Experiment za všechny prachy

„Už jsem to říkal jednou a řeknu to znovu. Bitcoin je experiment. Chovejte se k němu tak, jak byste se chovali ke slibnému internetovému startupu. Možná změní svět, ale uvědomte si, že investice peněz či času do nového nápadu je vždy riskantní."

Gavin Andresen

Bitcoin je v současnosti nesmírně volatilní. Každý den se jeho cena v dolarech mění o procenta či desítky procent nahoru a dolů. K tomu, aby profesionální obchodníci mohli vydělat velké peníze na výkyvech ceny akcií, dluhopisů nebo třeba komodit, potřebují často masivní půjčky, které vsadí na růst o setiny procent (tzv. obchodování na páku). Volatilita Bitcoinu je lákadlem. Vydělat za noc 10 % je investičním snem a mnozí ho spolu s Bitcoinem prožívají. Na druhou stranu je volatilita oboustranná a není problém přes noc 10 % prodělat. Doporučit Bitcoin jako prostředek ke zbohatnutí nelze, už nyní jde o svět profesionálů, kde ti takzvaní malí střadatelé přicházejí denně o spousty peněz a velcí investoři využívají svých znalostí, zkušeností, a především času k neustálému boji o trochu zisku. Stejně jako u jakéhokoliv jiného investování lze pouze konstatovat zřejmé – pokud se tomu člověk nechce věnovat celé dny a noci, opustit předchozí zaměstnání, zadlužit se, být schopen unést velké ztráty a vzít na sebe obrovské riziko a psychologickou zátěž (a není gambler), potom by měl zůstat raději mimo.

I velkým firmám je jasné, že ne všichni mají odvahu vstoupit do světa velkých peněz. I tak se dá na Bitcoinu vydělat. Stejně jako u jakékoliv jiné komodity se i na investice do Bitcoinu začaly specializovat konkrétní firmy.

Největší investiční společností v této oblasti je dnes Grayscale a jejich Bitcoin Investment Trust. Jde o standardní investiční fond, který vyžaduje minimální vklad 25 tisíc amerických dolarů a ty se

snaží investicí výhradně do Bitcoinu zhodnotit. Bitcoin nabízí i deriváty, podílové fondy a pomalu začínají vznikat první „banky". Zkrátka roste celý standardní finanční sektor.

Investování do Bitcoinu má své neoddiskutovatelné výhody. Na rozdíl od investic do klasických cizích měn, komodit nebo akcií nepotřebujete mít za sebou velkou instituci a množství regulátorů. Stačí si založit účet na burze, poslat dolary a následně jen nakupovat a prodávat ve vhodný čas.

Ale tak snadné to není, když se přou i profesionální investoři. Na jedné straně stojí investoři jako dvojčata Cameron a Tyler Winklevossovi, známí ze sporu o původ Facebooku s jeho veřejně uznávaným zakladatelem Markem Zuckerbergem, nebo Fred Wilson, který v minulosti vsadil na Tumblr, Twitter, Zyngu nebo Kickstarter, přičemž všechny tyto investice se mu bohatě vrátily. Winklevossovi koupili dle dostupných informací zhruba 40 až 50 tisíc bitcoinů za cenu kolem deseti dolarů. Během roku cena vystoupala až k tisíci dolarům za bitcoin a Winklevossovi udělali ze 400 tisíc 40 milionů dolarů. Ve světě, kde se výnosy na spořicích účtech blíží k nule, jde o neuvěřitelné zhodnocení. Kolik jich mají dnes, nevíme, ale určitě na Bitcoinu neprodělali.

Anebo jde o bublinu, řekla by druhá strana. Švýcarský investor Marc Farber, přezdívaný dr. Zkáza, se snaží ukázat, že investoři mají přebytek peněz a zběsile investují, kde se dá, aniž by se nad

svými investicemi více rozmýšleli. Jednou z těchto uměle nafouklých investic je dle něj i Bitcoin. Nositel Nobelovy ceny za ekonomii Robert Shiller mu přitakává. Na Světovém ekonomickém fóru v Davosu na začátku roku 2014 o Bitcoinu prohlásil: „Je to bublina, o tom není pochyb. Je to prostě úžasný příklad bubliny." Ani další nositel stejné ceny Paul Krugman nechodí pro silná slova příliš daleko a na svém blogu při New York Times nazval jeden z příspěvků jednoduše „Bitcoin je zlo". „Myslím, že by měl být zakázán," uzavřel předvídatelně v roce 2017 nositel Nobelovy ceny za ekonomii Joseph Stiglitz.

Algoritmus na štěstí

Investovat tedy, či nikoliv? Otázkou je, zda poroste či neporoste poptávka. Bitcoin lze z pohledu investora vnímat jako klasickou komoditu – má omezené a dobře známé množství, které se mění zcela transparentně a lze jej předvídat. Například zlata je stále teoreticky možné najít velké naleziště a množství významně změnit, u Bitcoinu však nikoliv, množství je jasně omezené a přibývá předem naprogramovanou rychlostí. Jediné, co je třeba sledovat a předvídat, je poptávka. Pokud poptávka vzroste, vznikne dočasně na trhu nedostatek a kupující začnou tlačit cenu nahoru, dokud se trh „nevyčistí", tedy dokud se růst ceny nezastaví. To se na obrovském trhu statisíců a milionů kupujících prakticky nestává a trh v každém okamžiku dynamicky přizpůsobuje cenu jedním či druhým směrem. Krátkodobě lze změny v poptávce odhadovat jen velmi těžko, mnozí ekonomové se dokonce domnívají, že to nelze. Jde z velké části o pohyby v důsledku spekulace, která má podobu tzv. náhodné procházky, tedy nelze ji odhadnout, jelikož se náhodně pohybuje nahoru a dolů nezávisle na předchozím směru pohybu.

Ti, kteří věří, že se na základě předchozího pohybu dá budoucí pohyb odhadnout, se začali věnovat tzv. algoritmickému obchodování. Jde o plně automatizovaný nákup a prodej, který se hojně využívá na akciových a komoditních trzích, kdy se počítačový algoritmus snaží na základě historických dat odhadnout, zda cena vzroste, nebo klesne, a podle toho nakoupit nebo prodat. Algoritmické obchodování má několik hlavních variant, z nichž jsou ve světě Bitcoinu použitelné pouze některé. Například se lze obrátit

k obchodu pomocí algoritmu, který sleduje dlouhodobý, střednědobý a krátkodobý trend. Typů algoritmů, které je možné použít, je nespočet.

Naneštěstí (anebo spíše naštěstí) není možné si z internetu stáhnout již hotový použitelný program. K algoritmickému obchodování tak musíte být vybaveni alespoň základní znalostí programování a nějakého programovacího jazyka anebo mít k ruce programátora, který by formální práci udělal za vás. Přesto si lze práci s programováním alespoň mírně usnadnit. Pro jazyk Java brzy vznikl nástroj zvaný XChange (ke stažení na xeiam.com/xchange), který si lze upravit tak, aby dle zadaných parametrů samostatně obchodoval. Vznikly i další nástroje pro obchodování na bázi arbitráže, tedy nákupu stejného zboží na trhu, kde je levné, a bezprostřední prodej na trhu, kde je cena vyšší, čímž se cenové hladiny vyrovnávají. Pro investory, kteří nechtějí programovat, vznikly speciální služby, které prodávají své vlastní know-how v automatickém obchodování. Služby jako cryptotrader.org nabízí své vlastní algoritmy a slibují vysoké výdělky. Odměnou za ně je měsíční nebo roční poplatek v řádech desítek či stovek dolarů.

Výše uvedené nástroje nejsou v žádném případě bez rizika a lze s nimi přijít stejně tak k zisku, jako ke ztrátě. Příklady ze světa algoritmického obchodování ve světě tradičních komodit jsou více než výmluvné. Na jedné straně stojí miliardáři jako je Karel Janeček, na straně druhé firmy jako Knight Capital, která díky algoritmickému obchodování za několik let vyrostla na tržní kapitalizaci do výše jedné miliardy dolarů, přičemž malou „chybou" v programu, jak sami tvrdí, přišli doslova přes noc o tři čtvrtě této hodnoty. Během několika měsíců byla firma za nízkou cenu koupena a přestala existovat.

Svět Bitcoinu je anonymní a ti největší obchodníci se s veřejností o své úspěchy a neúspěchy příliš nedělí. Když spadnou akcie Knight Capital nebo vzroste zisk Janečkovy RSJ, veřejnost se to snadno dozví. Ztráty a zisky z algoritmického obchodování s bitcoiny nejsou známé a je proto nutné vstup do této oblasti zvážit více než několikrát.

Nic jiného než poptávka

Jiným druhem investice je sázka na delší horizont. Zatímco okamžitý růst či propad lze jen málokdy přisoudit konkrétnímu faktoru v reálném světě (jako je například pokles po zavření Silk Road, Mt.Gox nebo nárůst po oznámení WordPressu, že přijímá bitcoiny), dlouhodobý pohyb ceny takto odhadovat možné je. Pokud investor vsadí na dlouhodobý růst společnosti typu Apple, lze usoudit, že předpokládá růst poptávky po jejích produktech. Stejně je tomu u Bitcoinu. Cena roste s tím, kolik lidí Bitcoin chce. A to, kolik lidí Bitcoin poptává, lze vztáhnout k událostem, které mohou, ale nemusejí nastat.

Investoři jako bratři Winklevossovi věří, že Bitcoin začnou více používat běžní lidé jako alternativu k měnám s nuceným oběhem (státní, tzv. fiat měny). Pokud by tomu tak bylo, poptávka by rostla a s ní i cena. Winklevossovi na základě svých úvah dokonce odhadují cenu jednoho bitcoinu ve výši 400 tisíc dolarů, a to v dohledné budoucnosti. Když jsme psali první vydání v roce 2015, byla na tomto místě předpověď na 40 tisíc dolarů. Jeden z prvních investorů a proponentů Bitcoinu Trace Mayer dokonce věří v mnohem vyšší cenu. Jednoduchým odhadem spočítal, že kdyby se k Bitcoinu odklonilo pouhé jedno procento peněz uložených v daňových rájích, jeho cena by vzrostla na téměř 3 miliony dolarů za bitcoin. Jeho výpočet byl často kritizován, ale na konkrétní částce nezáleží. Důležitá je myšlenka, která ho vede k jednoduchému závěru, že poroste poptávka a s ní cena.

Na druhou stranu existují i reálné faktory, které poptávku snižují a se kterými je třeba počítat. Jsou lidé, kteří předpokládají pokles poptávky na základě státní regulace. Bitcoin je v současnosti prakticky neregulovaný a jeho samotná decentralizovaná podstata jakoukoliv regulaci zásadně komplikuje. Mnoho investorů však nemusí vědět, že je to téměř nemožné, a pouhá informace o regulaci může poptávku a s ní i cenu snížit. Příkladem je již zmíněná zpráva o regulaci ze strany thajské centrální banky. Přestože šlo o nepodloženou a zavádějící zprávu, mnoho lidí tato informace vedla k prodeji bitcoinů a jiné odradila od jejich nákupu. Může dojít ale i na uskutečnitelnou regulaci, kdy se země s větším trhem rozhodne postavit mimo zákon přijímání bitcoinů v kamenných i internetových obchodech. To by silně omezilo praktické využití

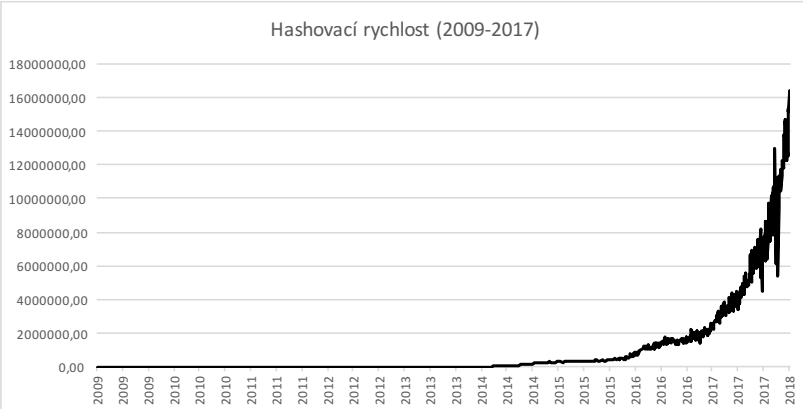
bitcoinů a snížilo skrze nižší poptávku jejich cenu. Dalších omezení lze vymyslet nespočet, ale na vině nemusí být pouze vláda. Pokud se na trhu kryptoměn objeví konkurenceschopná alternativa, je možné, že se začnou peníze přesouvat k ní a Bitcoin začne padat. Lze nalézt mnoho investorů, kteří sází na jiné alternativní digitální měny odvozené od Bitcoinu nebo na jiné digitální peníze postavené na zcela odlišném systému.

Chceš haš?

Do jisté míry střední cestou je možnost investice do vzdálených těžebních strojů. Netrvalo to příliš dlouho a na trhu se objevila služba CEX.io, která nabízí k prodeji výpočetní výkon. Jednoduše si za své bitcoiny koupíte určitý počet Gh/s a začnete vzdáleně těžit. Jde o tzv. cloud mining. Pointou je, že můžete Gh/s i prodávat, pokud jejich cena vzroste, a vydělávat na rozdílu. Stačí se přihlásit a zobrazí se adresa vašeho účtu. Na tu můžete poslat bitcoiny a za ně na interní burze nakoupit výpočetní výkon. Na konci roku 2013 stál jeden Gh/s na měsíc kolem 0,04 BTC. Pokud byste zainvestovali jeden bitcoin, můžete si koupit 25 Gh/s, které během ledna vytěžily zhruba 0,15 BTC hned první měsíc. V lednu 2014 se jeden Gh/s dal prodat za přibližně stejnou částku, tedy 0,04 BTC za Gh/s. Kdo tak učinil, mohl získat během měsíce zhruba 15% zisk. Zdá se to jako slušná návratnost, avšak ani zde není nic zadarmo a bez rizika.

Při virtuálním nákupu výpočetního výkonu pro těžbu BTC sázíte hned na tři čísla, která jsou provázaná, ale nepohybují se nutně společně. Prvně jde o sázku na cenu Gh/s. Technologický pokrok, poptávka a další faktory mohly cenu jednoho Gh/s podstatně snížit a v našem příkladu tak snížit i zisk. Dále jde o sázku na náročnost těžby, která se s vyšší celkovou zapojenou výpočetní silou zvyšuje. Není výjimkou, že obtížnost vzroste během měsíce o desítky procent. Jeden Gh/s s vyšší obtížností vytěží méně BTC, což opět snižuje očekávaný zisk. Třetí veličinou je sázka na cenu Bitcoinu. Pokud během těžby cena Bitcoinu klesne, zisk v dolarovém či korunovém vyjádření klesá. Nákup Gh/s v cloudu se tak vyplatí, pokud očekáváte, že vzroste cena Gh/s, příliš neporoste, nebo se dokonce sníží obtížnost (což by se mohlo stát jen za předpokladu, že by přestalo těžit velké množství lidí a klesl celkový výpočetní výkon sítě), a hlavně očekáváte zvýšení ceny Bitcoinu

na burze. I s menším výnosem se však zbavujete rizika nákupu drahých a rychle zastarávajících těžebních strojů. Obecně ale platí, že nejde o dobrý nápad, pokud dobře nevíte, co děláte. Těžba je specializovaná činnost, která se většině lidí nevyplatí.



Daně :(

Ať už bitcoiny získáte jakkoliv, pokud je budete směňovat za koruny nebo jinou tradiční měnu, musíte počítat s tím, že je dle zákona potřeba zisk zdanit. České zákony příjmy z prodeje bitcoinů klasifikují jako jakýkoliv jiný příjem z prodeje, přičemž ten je nutné zdanit, pokud přesáhne během zdaňovacího období částku 30 tisíc korun. Zákon však rozlišuje jednorázovou, tedy příležitostnou, výdělečnou činnost a činnost opakovanou. Pokud se nákupem a prodejem bitcoinů chcete zabývat soustavně, poté musíte podat daňové přiznání i při nižší vydělané částce.

Pokud jste bitcoiny prodali a vydělali, připravte si pro stát 15 % jako fyzická a 19 % jako právnická osoba. Jednoduše spočítejte, za kolik jste bitcoiny nakoupili a prodali a z rozdílu odveďte státu daň. Problém může způsobit kurz. V jakém kurzu bitcoiny ocenit? Pro účely daní byste měli být schopni kurz při nákupu a prodeji doložit a pracovat s tím, za který jste bitcoiny získali. Pokud jste je získali jako příjem a prodali, kurz stanovte podle jedné z velkých burz a držte se jen jednoho. Lepší praxe zatím neexistuje.

Jestli jste fyzická osoba, a ne firma, potom je vám jedno, když bitcoiny držíte a kurz vyroste. Sice se můžete cítit bohatší, ale dokud bitcoiny neprodáte či neutratíte, může vás nechat finanční úřad klidnými. Nezapomeňte, že i nákup za bitcoiny třeba v e-shopu je nutné následně zdanit, pokud jste předtím bitcoiny koupili levněji. Úplně stejně, jako kdybyste bitcoiny nejdřív prodali za koruny a poté teprve koupili danou věc.

Pokud máte jako firma příjem přímo v bitcoinech a neprodáte je, situace je o poznání složitější. Většina finančních a daňových odborníků se shoduje pouze na tom, že je nutné „nějak" bitcoiny ocenit a zanést do skladu, aby se mohly na konci účetního období přecenit. V jakém kurzu? Účetně existují dvě základní možnosti, které nelze kombinovat. První je nechat celkovou sumu přepočítat kurzem na konci roku. Obdobně to funguje u příjmů v cizí měně, kdy Ministerstvo financí na konci roku tzv. Pokynem D vyhlásí jednotné kurzy platné pro uplynulý rok. Druhou možností je používat kurzy průběžně, obdobně jako u příjmů v cizí měně, kdy se používá kurz vyhlašovaný ČNB.

Firmy mohou bitcoiny i nakupovat, v tom není problém. Nicméně stát na ně pamatuje s větší péčí než na fyzické osoby. Pokud nakupujete kryptoměny na firmu, doporučuje se zřídit si pro ten účel samostatný účet a všechny transakce mít pečlivě zdokumentované.

Je Bitcoin zboží? Musí se platit daň z přidané hodnoty? Jak už bylo psáno výše, Soudní dvůr Evropské komise v rozsudku Skatteverket vs. Hedqvist (C-264/14) z roku 2015 došel k důležitému závěru, že směna bitcoinů za státní peníze je osvobozena od DPH. Bitcoin tedy není zboží. Samozřejmě, pokud nakupujete za bitcoiny jiné zboží, DPH se standardně odvádí.

Tak nebo tak si s Bitcoinem zatím český finanční dohled neví příliš rady. Zatím nejsou známé žádné informace o tom, že by finanční úřady poskytovaly svým úředníkům školení v dohledávání bitcoinových transakcí.

Důležitou změnu přinesla novela zákona o praní špinavých peněz (253/2008 Sb.) s účinností od 1. ledna 2017, která poprvé nadefinovala virtuální měny. Do této definice zjevně Bitcoin spadá. O virtuální měně se v zákoně nově mluví jen jednou, a to v definici

osoby poskytující služby spojené s virtuální měnou jako osoby povinné. To prakticky znamená, že musíte identifikovat protistranu a informace hlásit finančnímu úřadu. Naneštěstí zákon nyní říká, že se povinnou osobou stává kdokoliv, kdo poskytuje služby spojené s virtuální měnou. Co se rozumí službou zatím nevíme. Je i psaní této knihy službou spojenou s virtuální měnou? Její prodej? Prodej reklamy na tuto knihu? Musíme si bohužel počkat na první soudy.

Jak být anonymní

Neviděť nic

Tvrdí se, že Bitcoin je anonymní, což není úplně čistá pravda. Bitcoin teoreticky plně anonymní být může, ale taková anonymizace je riskantní a nákladný proces. Přesto se dá o jisté anonymitě mluvit a Bitcoin je označován jako pseudoanonymní.

S Bitcoinem se pohybujete po internetu a ten jako takový anonymní není (ale může být, pokud chcete a budete se snažit). Za relativně nízkou částku dokáže dnes policie vystopovat vašeho poskytovatele internetu a od něj získat informaci o tom, kdo jste. Někteří uživatelé, kteří nechtějí být jednoduše dohledatelní, používají softwarové anonymizéry jako je Tor, jež velmi dobře skrývají jejich internetovou identitu.

Pokud chcete získat bitcoiny za koruny, také to není snadné učinit v úplné anonymitě. Již skoro všechny burzy požadují prokázání totožnosti, zejména při nakládání s většími částkami, a na Local Bitcoins posíláte peníze z neanonymního bankovního účtu. Vždy je ale možné zakrýt si obličej a vyměnit hotovost za bitcoiny s prodejcem osobně nebo využít bitcoinového bankomatu.

Přesto je ale dále vidět pohyb vašich bitcoinů. Dobře to ilustruje příklad s krádeží velkého množství bitcoinů z elektronické peněženky. Jelikož je blockchain veřejný, lze vidět, na kterou adresu ukradené bitcoiny odešly. Některé se přesunuly jen do jedné, jiné putují přes více adres. Jakmile by však někdo z této peněženky zaplatil v internetovém obchodě, může být vystopován. Ukradené peníze tak velmi často končí bez hnutí na adrese, na kterou se okradení čas od času v blockchainu podívají.

Skutečnou anonymitu poskytují pouze takzvané „mixéry“ nebo „pračky“ bitcoinů. Existují servery, které shromáždí velkou část bitcoinů a následně je redistribuují mezi množství peněženek tak, že je jejich původ zamaskován. Problémem mixérů však je, že poptávku zjevně netvoří uživatelé, kteří si chtějí za bitcoiny koupit kávu, ale spíše ti, kteří jej využívají jako anonymní prostředek k nelegálním cílům. Může se tak snadno stát, že se vám z mixéru místo anonymního bitcoinu vrátí bitcoin obdržený za nákup

narkotik a co chvíli u vás zvoní policie. Vysvětlovat důvody pro použití mixéru nebude jednoduché. Bitcoin je zkrátka v tomto smyslu transparentní účetní kniha.

Teoreticky tedy úplná anonymita možná je, ale když se mluví o anonymitě, nejde obvykle o tento její druh.

Například je velmi snadné vytvořit pro každou transakci novou přijímací adresu. To se hodí, pokud nechcete, aby vaši plátci věděli, kolik bitcoinů a kdy přes vaši peněženku prošlo. Některé peněženky dokonce mají takovou možnost automaticky. Jde přesně o ten druh anonymity, který máme rádi na každodenních hotovostních platbách.

Vedle Bitcoinu ale vznikla řada dalších kryptoměn, které si na anonymitě zakládají. O těch pohovoříme později.

Vidět všechno

Bitcoin má výhodu spíše v opačném stavu – může být absolutně transparentní, jelikož všichni vidí do jedné účetní knihy a mohou stopovat konkrétní bitcoin na jeho cestě mezi různými uzly sítě. Podíváme-li se kolem sebe, transparentnost peněz je stále více poptávaná. Charity, dobročinné spolky a neziskové organizace obecně, politické strany a obecní sbírky, ti všichni se snaží (i když leckdy úmyslně neúspěšně) o co nejvyšší transparentnost. Současné banky tak přicházejí s různými transparentními účty, kde veřejnost může vidět do výpisu přijatých a odeslaných plateb. V Bitcoinu jde o vlastnost přímo zabudovanou v jeho podstatě. Blockchain je veřejný a sdílený a pokud někdo chce vědět, kde přesně končí jeho bitcoiny, není nic snazšího než se do něj podívat.

Pokud by se Bitcoin zásadně rozšířil, může tato jeho vlastnost kompletně změnit politiku a veřejnou správu. Můžeme si představit obec, která má svou transparentní adresu, ze které nemůže jen tak zmizet několik tisíc bitcoinů na neznámé místo. Kdokoliv se může podívat do blockchainu a stopovat každý utracený bitcoin na cestě mezi adresami peněženek.

Přílišný důraz na anonymitu Bitcoinu plyne asi z příběhu, který se kolem něj psal, nikoliv z jeho vlastností. Vždyť klíčovou vlastností, se kterou Bitcoin ovládl svět kryptoměn, je blockchain,

sdílená, veřejná a plně transparentní účetní kniha. Můžete si stáhnout seznam všech transakcí v celé historii. Představte si, jak by vypadala taková účetní kniha od počátku věků. Co vše bychom se dozvěděli?

Anonymita se k Bitcoinu přimkla pravděpodobně kvůli anonymnímu autorovi, tajemnému Nakamotovi, a ilegálním obchodům na Silk Road. Přestože je tedy akcentována spíše možnost anonymity, je to právě transparentnost, která je Bitcoinu vlastní. Že tomu tak je, lze vypozorovat také z faktu, že brzy vznikla jiná kryptoměna podobná Bitcoinu, která tuto transparentní část odstraňuje.

Nejlépe však anonymitu Bitcoinu ilustruje sám Satoshi Nakamoto. Jelikož víme, že vytěžil genesis blok, lze sledovat stopy transakcí dále v čase až do současnosti. Pokud byste to udělali, skončili byste u několika adres, na kterých leží neutracené bitcoiny. A neutracené s nejvyšší pravděpodobností zůstanou navždy, protože jakmile by si za ně Satoshi koupil let do vesmíru nebo i jen bagetu, tisíce zvědavých profesionálních i amatérských detektivů by mu byly v patách.

Ekonomie a technologie kryptoměn

Ekonomické základy Bitcoinu

Rakouské kořeny Satoshiho Nakamota

Přestože jsou ekonomické vzdělání a motivy Satoshiho Nakamota známé jen velmi okrajově, lze určitě nalézt ekonomické kořeny této měny v souboru ekonomických teorií známých pod názvem rakouská ekonomická škola.

Rakouská škola je větev ekonomického myšlení, která vznikla v druhé polovině devatenáctého století pod rukama rakouských ekonomů Eugena von Böhm-Bawerka, Carla Mengera, Friedricha von Wiesera a dalších. Za základní dílo rakouské školy jsou považovány Základy národohospodářské nauky Carla Mengera z roku 1871. Historiky ekonomického myšlení je tato kniha považována za první dílo představující analýzu na základě mezních veličin, což spustilo tzv. marginalistickou revoluci, která přetvořila pohled na ekonomii. Významným autorem první vlny rakouských ekonomů byl Eugen von Böhm-Bawerk, jenž se věnoval analýze kapitálu a široce kritizoval učení Karla Marxe, což je ostatně prvek přetrvávající v rakouské škole dodnes.

Z druhé generace autorů jsou patrně dva nejvýznamnější rakouští ekonomové Ludwig von Mises a Friedrich Hayek. Mises utekl před válkou do Spojených států, kde v roce 1949 vydal své magnum opus Lidské jednání. Hayek se proslavil v Anglii zejména naučně populární knihou Cesta do otroctví a v roce 1974 obdržel Nobelovu cenu za ekonomii. Jejich přínosem bylo zejména ekonomické vyvrácení možnosti racionální kalkulace za socialismu, kdy akcentovali roli cen jako nositele informace o vzácnosti a praktickou nemožnost nashromáždění všech potřebných informací centrálním plánovačem.

Vedle toho se věnovali teorii peněz, které považovali za tržní prostředek směny, který vzniká dobrovolně z komodit, a teorii hospodářského cyklu, v níž Mises a později i Hayek zdůrazňovali negativní vliv centrálního bankovnictví a výhody svobodné soutěže i na poli peněz. Vznikla tak rakouská teorie hospodářského cyklu.

V současnosti se rakouští ekonomové sdružují zejména kolem velkých amerických think-tanků, jako je Cato Institute ve

Washingtonu, Mises Institute v Auburnu nebo Foundation for Economic Education v Atlantě nebo sociální síť liberty.me. Mezi nejznámější protagonisty se řadí ekonomové jako Jeffrey Tucker, Israel Kirzner, Tom Woods nebo Walter Block či například americký kongresman a kandidát na prezidenta Ron Paul. V Čechách a na Slovensku jsou centrem rakouské školy zejména think-tanky Liberální institut, Ludwig von Mises Institut CZ & SK a slovenský INESS.

Důraz na laissez-faire, tedy na nikým centrálně neřízené spontánní tržní prostředí, je nápadně podobné Bitcoinu a světu kryptoměn obecně. Dokonce Evropská centrální banka ve své zprávě o virtuálních měnách konstatuje, že teoretické kořeny Bitcoinu lze nalézt v rakouské ekonomické škole.

Svobodné bankovnictví

A skutečně, porovnáme-li desítky let stará díla rakouských ekonomů a Bitcoin, nelze si myslet nic jiného. Hayek nazval svou známou knihu Denacionalizace peněz, což je přesně to, co Bitcoin dělá. Přes sto let staré Misesovo dílo Teorie peněz a úvěru končí slovy:

„Současný neuspokojivý stav peněžních záležitostí je výsledkem socialistické ideologie, jíž jsou naši současníci oddáni, a hospodářských politik, které tato ideologie zplodila. Lidé si stěžují na inflaci, ale zapáleně podporují politiku, která nemůže být prováděna bez inflace. A tak zatímco roní hořké slzy nad nevyhnutelnými dopady inflace, zatvrzele odporují jakémukoliv pokusu snížit vládní výdaje.

Reforma měnového systému a návrat k tvrdým penězům předpokládají radikální změnu v politické filosofii.“ [Mises, Ludwig von, 1912, Teorie peněz a úvěru, překlad Vladimír Krupa]

Avšak i v rámci rakouské ekonomické školy Mises, Hayek a další pochopitelně nepíšou o P2P sítích, **asymetrické kryptografii** nebo digitálních měnách a ani jim to nelze zazlívat, jelikož jde o nový koncept na poli technologie, o kterém nemohli ani snít. Na druhou stranu i mnohem mladší rakouští ekonomové nepřestávají tvrdit, že Bitcoin nepřežije.

Asymetrická kryptografie (Public Key Cryptography)

skupina kryptografických metod, u kterých šifrovací a dešifrovací klíč není stejný (resp. z šifrovacího klíče není možné odvodit klíč dešifrovací). Asymetrie klíčů umožňuje adresátovi šifrované zprávy nesdílet s odesílatelem tajný dešifrovací klíč (viz **Soukromý klíč**) a naopak druhý z páru klíčů zveřejnit (viz **Veřejný klíč**). Jednou z aplikací **asymetrické kryptografie** je digitální **podpis** (někdy též elektronický **podpis**). Při podepisování zprávy (či pouze jejího **hashe**) se **podpis** spočítá pomocí **soukromého klíče**, což může učinit jen jeho vlastník. To, že tak vlastník učinil (že zprávu podepsal), může naopak každý ověřit pomocí jeho **veřejného klíče**. Šifrování i **podpis** je možno kombinovat. Bitcoinový protokol používá algoritmus digitálního **podpisu** ECDSA.

Důvodem je zejména staletí trvající snaha liberálních ekonomů, mezi něž se „rakušáci" jednoznačně řadí, vrátit do peněžního systému a udržet v něm zlato jako základ hodnoty peněz. Proto se velmi často současní ekonomové této tradice ptají, čím je Bitcoin krytý, a ještě častěji ho srovnávají právě se zlatem.

Srovnání se zlatem je nasnadě. Jak Bitcoin, tak zlato má své zastánce v reálném světě a v ekonomické teorii. Na straně zlata stojí především ekonomové, kteří zakládají své argumenty zejména na tom, že je zlato prostředkem směny po tisíce let a možná i více. To je pochopitelná výhoda. I dnes by lidé, dokonce bez zájmu o počítače nebo bez jakéhokoliv přístupu k nim, pravděpodobně zlato přijímali. Bitcoin zatím nikoliv. Výhodou zlata je, že ho lidé znají a rozumí mu.

Na druhou stranu, zlaté systémy mají zásadní nevýhodu v nutné centralizaci. Zatím nikdo nepřišel s decentralizovaným systémem, který by v sobě nesl zlato. Centralizace je napadnutelná, zneužitelná a centrum může být zničeno. Bitcoin je ale volatilní, jeho cena roste a klesá každý den o jednotky procent. Zlato má v čase stálejší cenu. Avšak s růstem uživatelů se i cena Bitcoinu ustaluje. Otázkou je, zda do tohoto kruhu noví uživatelé vstoupí – pokud je cena nestálá, tak je to od vstupu odrazuje, pročež se cena nemůže stabilizovat. Argumenty zastánců zlata i zastánců Bitcoinu dávají smysl. Možná je cestou ven řešení založené na tom nejlepším z obou světů – na propojení zlata a blockchainu.

Otázkou, která stále zůstává otevřená, je současný stav. Jde o peníze? Legálně jde o peníze, jen když se to někomu hodí. Když se před texaským soudem bránil vlastník společnosti Bitcoin Savings

& Trust proti obvinění ze zpronevěry, hájil se tím, že bitcoiny nejsou peníze. Soudce Amos Mazzant ale mluvil jinou řečí: „Bitcoin je měna ve formě peněz a investoři společnosti Bitcoin Savings & Trust tedy poskytli investici ve formě peněz." Černé na bílém.

Ovšem jeden výrok soudce, i když amerického, z Bitcoinu peníze neudělá. Dokonce ani výrok německého federálního ministerstva financí, které v srpnu roku 2013 označilo Bitcoin za formu soukromých peněz a účetní jednotku, čímž explicitně umožnilo užívat bitcoiny ve směně. Ovšem ze zákona také podléhají dani, která se nemusí platit, jsou-li drženy déle než jeden rok. Z právního hlediska lze tedy Bitcoin za peníze označit velmi snadno. Ekonomická otázka, zda jde o peníze, je podstatně složitější.

Bitcoin jako peníze

Častou definicí peněz, a to jak ekonomů hlavního proudu, tak i těch rakouských, je ta, že peníze jsou všeobecně přijímaný prostředek směny. Již bylo ukázáno, že Bitcoin splňuje všechny atributy kvalitních peněz, takže penězi být může, ale dá se za peníze považovat nyní, případně kdy tomu tak bude?

Odpověď je složitá, protože otázka je založena na relativně vágní definici. Co přesně si představit pod „všeobecně přijímaný" je téměř neřešitelné. Odpověď tedy budeme muset hledat analogií k současným penězům, například ke korunám. České koruny lze patrně považovat za peníze, přestože jsou přijímány jen v České republice a jen výjimečně je někdo přijme ve zbytku světa. Peníze tak zjevně je možné ohraničit územím. Jsou bitcoiny bez problémů přijímány na nějakém území? Zatím nikoliv.

Proč ale zůstat u území geografického? Například dolarové bankovky nejvyšší hodnoty jsou jen stěží bez problémů přijímány na celém světě, ale v geograficky neohraničené komunitě mafiánů jde zcela jistě o všeobecně přijímaný prostředek směny. Stodolarové bankovky jsou peníze gangsterů. Lze najít komunitu, kde jsou bitcoiny všeobecně přijímaným prostředkem směny?

Pokud ji nenadefinujeme rovnou a triviálně jako komunitu uživatelů Bitcoinu, tak patrně nikoliv. Dokonce ani v IT komunitě, v komunitě voličů pirátských stran nebo v komunitě rakouských

ekonomů nelze Bitcoin považovat za všeobecně přijímaný, aniž bychom se snažili onu všeobecnost jakkoliv kvantifikovat. Stále jde o zanedbatelné množství lidí.

Kdy tedy bude Bitcoin všeobecně přijímaný? Ti, kteří tíhnou ke statistice, rádi cílí na čísla jako 90 % nebo 99 % a uznali by tedy Bitcoin za peníze, pokud by ho užívalo právě tolik lidí. Respektive užívali jako prostředek směny nebo pro ně byl, jak říká Mises, nejlikvidnějším statkem. To znamená, že je možné ho s co nejmenšími náklady přetvořit ve zboží či službu. Téměř všichni lidé používají mobilní telefon, ale nelze ho považovat za peníze, jelikož je obtížné za něj získat doučování z angličtiny. Možné to je, ale nákladné. Peníze jako nejlikvidnější komodita umožňují získat prodejem telefonu prostředek směny ke koupi vyššího množství doučování, než by tomu bylo v přímé směně, pokud by s ní vůbec druhá strana souhlasila. Prvním definičním znakem toho, že se Bitcoin stal penězi, bude stav, kdy bude podstatným množstvím lidí považován za nejlikvidnější aktivum.

Druhým symbolem zevšeobecnění Bitcoinu jako prostředku směny bude zásadní změna struktury koše zboží a služeb, které se za bitcoiny kupují. Dnešní struktura bitcoinového spotřebitelského koše je úplně jiná než struktura korunového. Podle mezinárodního výzkumu ING Bank utratí 40 procent Čechů nejvíce z měsíčního rozpočtu za bydlení a 35 procent za potraviny. Dalších 20 procent utratí nejvíce za energie. Když se podíváme na podobné statistiky u Bitcoinu, vidíme, že nejvíce bitcoinů je utraceno za hazard a posláno jako dary jednotlivcům nebo neziskovým organizacím. Potraviny, nájem nebo energie netvoří prakticky žádnou část bitcoinové ekonomiky. S nárůstem uživatelů by se měl tento koš přeměňovat do podoby koše tradičních měn. Až uvidíme podobná čísla, Bitcoin budou peníze.

Třetí znamení toho, že se z Bitcoinu staly peníze, je výsostně spojeno právě s rakouskou školou. Ludwig von Mises a další autoři této tradice velmi nahlas a velice často upozorňují, že naše civilizace stojí a padá na racionální kalkulaci v prostředí cen, které se vytváří na svobodném trhu za pomoci peněžního systému. Zjednodušeně řečeno, pokud se rozhodnete, že začnete prodávat kolečkové brusle ze zlata, budete pravděpodobně velmi rychle vyřazeni z trhu, protože budou vaše výnosy nižší než náklady.

Pokud nakupujete, téměř vždy porovnáváte alternativy a k tomu vám pomáhají ceny. Peníze jsou nositelem hodnotných ekonomických informací. Bez peněz není možné racionálně kalkulovat, protože je nutné srovnat cenové poměry mnoha různých statků, kterých je v dnešním světě prakticky nekonečno. Peníze to umí skoro až kouzelně. Kouzlo cenového systému nepřekonatelně popsal Leonard Read ve své eseji Já, tužka. Ukazuje, jak se skrze ceny a dobrovolnou lidskou spolupráci v tržním prostředí vytváří jedna jediná obyčejná dřevěná tužka s gumovým koncem. Na její výrobě spolupracuje téměř celý svět, aniž by kdokoliv z nás věděl, k čemu svým malým dílem přispívá.

Pro Bitcoin z toho plyne závěr, že se stane penězi, až v něm budou lidé provádět ekonomickou kalkulaci. Lze to vidět na příkladu již zmíněných zlatých kolečkových bruslí. Dnes do takového byznysu pravděpodobně nepůjdete, protože si v hlavě rychle spočítáte, že na výrobu takové brusle by bylo zapotřebí zlata za mnoho milionů korun, přičemž poptávka by byla přinejlepším velmi nízká, a to i za relativně nízkou cenu, takže byste prodělali. Ale i u ziskového byznysu, kdy si spočítáte, že vyděláte odhadem tisíc korun měsíčně, usoudíte, že bude lepší do něj nejít, protože si můžete zisk srovnat s obětovanou příležitostí, například být zaměstnán a brát řádově vyšší plat. Ve světě Bitcoinu takovou kalkulaci provádí málokdo, pokud vůbec někdo. Jestliže víte, že si můžete pořídit nové Lamborghini za 9 BTC, neporovnáváte to s alternativou v podobě koupě dvou set tisíc piv za bitcoiny nebo se svou mzdou, kterou pravděpodobně ani v bitcoinech nedostáváte. Jednoduše si přepočítáte bitcoiny na koruny a víte, jestli se to vyplatí, nebo ne. Až budeme ekonomickou kalkulaci automaticky provádět v bitcoinech a korunové ceny naopak zpětně přepočítávat do cen bitcoinových, potom se Bitcoin stal všeobecně přijímaným prostředkem směny.

Hlasy z druhých břehů

Existují však i ekonomičtí odpůrci Bitcoinu. Velmi častý argument proti Bitcoinu je jeho omezené množství. Jde o původní argument proti zlatému standardu – říká se, že zlata je málo (kdyby se dalo dohromady všechno doposud vytěžené zlato z celého světa, vyplnilo by pouze dva olympijské plavecké bazény), avšak

takový argument nedává žádný smysl. Ceny zboží se množství zlata jednoduše přizpůsobí. Je to stejné, jako v případě nafukování peněžní zásoby; pokud je peněz více, ceny jsou vyšší, pokud méně, ceny jsou nižší. Je tak pravděpodobné, že by dnes určité zboží místo unce zlata stálo třeba jen gram zlata. Jelikož se obchodují pouze poukázky na zlato, je hypoteticky možné dělit jejich hodnotu donekonečna. Stejně tak Bitcoin.

Jednou z hlavních teoretických výtek je jeho omezené množství a s ním se pojící deflační prostředí. Ve světě tradičních měn centrální banky spolu s vládami cíleně znehodnocují měny – vytváří více a více peněz, které posílají do oběhu a způsobují tak inflaci. Bitcoin takové chování znemožňuje a pokud by byl všeobecně přijímaným, ceny by se měnily pouze v závislosti na tržních vlivech. Zásoba bitcoinů je stálá nebo dokonce mírně klesající, jelikož některé bitcoiny zůstanou navždy ztracené, pokud zkolabuje počítač bez zálohy nebo majitel zapomene heslo. Pokud tedy poptávka po bitcoinech nebude klesat, což lze předpokládat, jejich cena bude mírně růst. Pokud se peníze zhodnocují, tedy pokud roste jejich cena, potom musí klesat ceny všeho ostatního a dochází k cenové deflaci. Navíc je snižování cen v tržním prostředí přirozené i bez změny ceny peněz, jelikož se vytváří nové produkty, inovuje se technologie a konkurence tlačí ceny směrem dolů.

Někteří ekonomové tak upozorňují na možný vznik tzv. deflační spirály. Jde o modelovou situaci, kdy lidé očekávají růst ceny peněz, a proto je hromadí pro úschovu hodnoty, čímž opět zvyšují cenu peněz, což vede k ještě většímu hromadění atd. Pokud lidé hromadí peníze, tak je neutrácí, takže podniky přicházejí o zakázky a propouští, což opět snižuje koupěschopnou poptávku lidí a nadále prohlubuje krizi.

Tento argument má své opodstatnění. V současném světě tradičních peněz by opravdu umělé zhodnocování peněz mohlo vést k ekonomickým problémům. Peníze jsou vytvořeny skrze komerční banky, kdykoliv někomu dají půjčku. Jednoduše mu připíšou nově vytvořené peníze na účet, čímž se nové peníze dostanou do oběhu. Centrální banka se snaží k vyššímu půjčování, a tedy i zvýšení peněžní zásoby komerční banky motivovat snižováním své úrokové sazby. Proto jsou po vypuknutí poslední krize v celém západním světě úrokové sazby centrálních bank na

minimu, prakticky na nule. Existuje totiž strach, že by si lidé přestali půjčovat, a naopak některé půjčky splatili, čímž by docházelo ke snižování peněžní zásoby a následně ke zhodnocení peněz a deflaci. Lidé by se obávali, že bude v budoucnu dražší splatit půjčku než nyní, a byli by motivováni dříve splácet a nebrat si další půjčky. To by vedlo k ještě hlubší deflaci atd.

Ponechme stranou důležité, ale pro Bitcoin irelevantní argumenty i proti tomuto tradičnímu vysvětlení deflační spirály v prostředí dnešních peněz. Důležitější je skutečnost, že Bitcoin je spontánně vytvořenou de facto komoditou, a nikoliv konstruktem obíhajících dluhů. Zaprvé, jak již bylo řečeno, deflace je přirozený jev tržní ekonomiky. Snižování cen v důsledku konkurence je pozitivní jev, nikoliv negativní. Zadruhé, západní svět naprostou většinu svých dějin prožil v deflačním prostředí komoditního standardu a velkými hospodářskými problémy si procházel zejména kvůli snaze panovníků platit své válečné závazky a drahé dvory skrze znehodnocování peněz. Zatřetí, hromadění bitcoinů v důsledku snižování cen by nemohlo vést k nekonečné spirále, protože do problému vstupují i protichůdné motivace. Pokud by lidé hromadili bitcoiny a nepoužívali je ve směně, zvyšovala by se relativně hodnota jiného prostředku směny, což by snižovalo cenu bitcoinu. Celý systém tak sám sebe přirozeně reguluje. A nakonec, skutečnost, že Bitcoin oproti současným penězům motivuje lidi více spořit, jen reflektuje lidskou přirozenost. Vyšší úspory financují investice a umožňují nám žít rok co rok kvalitnější životy.

Svět bez hospodářských krizí

S výše uvedenými závěry se pojí také důležitá implikace pro teorii hospodářského cyklu. Protože jsou peníze nositelem informací a zdrojem cenového systému, na kterém stojí a padá fungování celé ekonomiky, přikládají jim rakouští ekonomové velkou roli i ve vysvětlení hospodářských cyklů. Proč by jindy soudní lidé investovali do projektů, které se následně hromadně ukážou jako špatné? Proč napříč celou ekonomikou, a dokonce i napříč zeměmi? Vysvětlení na základě stádního chování dává jistě smysl, ale rakouská teorie hospodářského cyklu přidává další velmi silné vysvětlení, pomocí kterého se daří úspěšně vysvětlovat všechny

krize minulých staletí. Jednoduše řečeno, jde o narušení právě zmiňovaného cenového systému. Lidé reagují na informace a ty přenášejí do cen, na základě kterých provádí ekonomickou kalkulaci. Pokud stát nebo centrální banka znehodnocuje peníze, systematicky narušuje ceny a s nimi i informace, které nesou. S přílivem levných peněz (tj. když se tzv. „tisknou peníze") se začnou zdát ziskové i dříve neziskové projekty, především ty časově velmi náročné, jelikož je relativně levnější si půjčit peníze na dlouhou dobu. Příklady takového impulzu k dlouhodobým projektům lze hojně vidět například ve stavebnictví nebo u hypoték. Nicméně uměle nízká cena peněz nesla špatnou informaci, která neodpovídala realitě. Ve chvíli, kdy se investoři ze skutečných výsledovek dozvědí, že udělali chybu, je už obvykle pozdě. Zjistí to jednoduše, například tak, že se do jejich nově vystavěných bytů a kanceláří nikdo nestěhuje. Jelikož je takových projektů řada napříč celou ekonomikou a jsou vzájemně provázány ve všech oblastech podnikání, následný pád je všudypřítomný.

Když někdo uměle pohne s cenou jedné věci, vznikne u ní ekonomický problém – buď přebytek, nebo nedostatek. Pokud se hýbne s cenou na jednom trhu, dojde opět k problémům na něm a na trzích jemu blízkých. Pokud je ale problém se vším, někdo si musel pohrávat s cenou všeho. A jelikož je ve své podstatě vše propojeno penězi, patrně někdo uměle měnil cenu peněz. Anebo ještě lépe, někdo si hrál s cenou času. Pokud by byl úrok napříč ekonomikou uměle vysoký, řekněme v desítkách procent, snadno si představíme, že by lidé příliš spořili. Příliš, protože by to nereflektovalo skutečná, uměle nenarušená přání lidí, kteří by si za vysoké sazby naopak nic nepůjčili. Na druhou stranu uměle nízké sazby způsobují přesný opak – více se utrácí a zároveň se více investuje, zejména do dlouhodobých projektů. Tedy utrácí se více, než je přirozené, čemuž říkáme období boomu, po kterém přichází krize. Skutečně zajímavé je tedy zkoumat, co způsobuje boom, jelikož ten je příčinou krize.

Připomeňme si, že bitcoinů je omezené a všem známé množství. Nelze jich „natisknout" více a tím celý tento proces a hospodářský cyklus vůbec spustit. Lidé by stále mohli podlehnout stádovému efektu nebo udělat hromadně náhodnou chybu. Ale velká část hospodářského cyklu, který je spouštěn umělou expanzí peněžní zásoby, je ve světě Bitcoinu odstraněna. Z představy,

že by invence v podobě Bitcoinu dokázala eliminovat něco, co už začaly učebnice ekonomie pomalu považovat za nezbytný prvek tržních ekonomik, naskakuje husí kůže. Jde samozřejmě o teorii, a to tak obsáhlou, že je velmi těžké ji empiricky ověřit i zpětně, natož extrapolovat do budoucna. Jestli ale má rakouská teorie pravdu, potom byl světu v roce 2009 představen nástroj na eliminaci hospodářského cyklu. Jen si představte, co za nástroj před námi leží.

Škálování Bitcoinu

Jak zlepšovat Bitcoin

Bitcoin se vyvíjí. A k lepšímu. V decentralizovaném světě Bitcoinu může doslova každý navrhnout změnu fungování bitcoinové sítě a protokolu prostřednictvím tzv. **BIP**. Team vývojářů **Bitcoin Core** o návrzích změn diskutuje v komunitě a případně je implementuje v SW. Součástí diskuze je i proces, kterým těžaři mohou o změně hlasovat. Dělají to nastavováním rezervovaných bitů v hlavičce jimi vytěžených bloků (to lze také díky BIP, konkrétně dle BIP 9). Pokud po určitou dobu takto signalizují svoji připravenost pro přijetí změny (v posledních typicky 1000 blocích je vysoká shoda na přijetí změny – typicky 75 % nebo přísnějších 95 %, tzv. „point of no return"), vejde návrh změny v platnost a dojde k jeho tzv. uzamčení. Po určité době od uzamčení pak dojde k aktivaci změny a síť se začne chovat podle nových pravidel. Právník by řekl, že změna vejde v účinnost.

BIP (Bitcoin Improvement Proposal)

dokument obsahující návrh na změnu fungování **Bitcoinu**, případně jinou důležitou informaci související s bitcoinovým ekosystémem. Označuje se zkratkou „BIP" a číselným pořadím **BIPu**. Např. **BIP** 1 popisuje, co je to **BIP**, jak ho tvořit a jak s ním pracovat. **BIP** většinou obsahuje návrh na přidání nové funkcionality, včetně motivace pro její zavedení, přesné specifikace, návrhu řešení a analýzy dopadu na kompatibilitu. V rámci zpracování pak **BIP** prochází různými stavy (koncept, akceptováno, zamítnuto, hotovo…). Osoba v roli **BIP** editora je pověřena jejich správou v SW repozitáři na adrese github.com/bitcoin/bips.

Žijeme ovšem v decentralizovaném světě a nikdo nemá právo nikoho nutit k tomu, aby přešel na změnu, která se mu nelíbí – ani kdyby s ní 99 % ostatních souhlasilo (Bitcoin není demokracie, nýbrž svoboda). Komu se změna nelíbí, nemusí na novou verzi SW přecházet. Riskuje tím ale to, že jím používaný SW nebude dostatečně kompatibilní s chováním SW ostatních, a on tak vytvoří malý ostrůvek odlišně fungujícího „původního" Bitcoinu, na kterém zůstane sám. Málokdo by chtěl zůstat sám, protože smyslem sítě, a to nejen té bitcoinové, je právě interakce s ostatními. Užitná

hodnota sítě narůstá kvadraticky s počtem jejích uživatelů (tzv. „síťový efekt“), čehož jako lidé rádi využíváme ve všech sociálních sítích, i těch reálných nedigitálních. Jednoduše nechceme být sami.

Bitcoin Core

referenční implementace klienta pro síť **Bitcoin**. SW původně vyvíjený Satoshi Nakamotem pod názvem **Bitcoin** (resp. Bitcoin-Qt obsahující grafické rozhraní) byl později přejmenován k odlišení této konkrétní implementace od názvu samotné sítě. Implementace je vyvíjena v jazyce C++ a obsahuje kód k provozu plnohodnotného síťového uzlu (stahuje a validuje celý **blockchain**), ale dá se použít rovněž jako **peněženka**. Starší verze prováděly i **těžbu** na CPU. Po Satoshi Nakamotovi převzal roli hlavního vývojáře Gavin Andresen a po něm v roce 2014 Wladimir van der Laan.

V případě malých změn způsobí uživateli používání staré verze SW třeba jen nějaký diskomfort nebo nedostupnost nových funkcionalit, ale co když se změna týká něčeho fundamentálního v bitcoinovém protokolu, např. formátu transakcí nebo bloků? Taková situace může uživateli používání staré verze SW zcela znemožnit. Jeho verze může např. považovat bloky vytěžené podle nových pravidel za nevalidní, a tím vlastně neuvidí nic, co se v síti od doby účinnosti změny stalo. Jeho stávající peníze sice v ohrožení nejsou (to platí vždy!), protože ty získal ještě v době platnosti pravidel původních (kterým jeho SW rozumí), ale už by třeba nemohl přijímat nové peníze, protože ty by mu lidé posílali v nových blocích (kterým jeho SW nerozumí).

Takové situace, kdy dochází k podstatným změnám pravidel, mohou být nepříjemné pro všechny zúčastněné strany – pro komunitu, která musí změny správně navrhnout; pro vývojáře, kteří musí změny správně implementovat; pro těžaře, kteří se musí na změny připravit; a pro uživatele, kteří musí změny přijmout. Bitcoin je, i z tohoto důvodu, velmi konzervativní systém a změnám se brání tím více, čím většímu počtu subjektů mohou přivodit nějaké nepříjemnosti. Zároveň ale jsou některé změny nezbytné pro vyřešení problémů, které se časem objevují. Abychom pochopili stručnou historii vývoje Bitcoinu zejména v poměrně chaotickém roce 2017, pojďme se podívat na to, jaké situace se změnami mohou nastat.

Cože? Vidličky a nože

Už víme, že data o bitcoinových transakcích se ukládají do bloků a bloky se řetězí/zapojují za sebou do blockchainu. Pokud se nalezne – „vytěží" – nový blok, je zapojen za předchozí a všichni těžaři začínají těžit další, který bude zapojen za tento nový. Pokud se však vytěží dva (či více) bloků v podobný okamžik, potom je více bloků zapojeno za stejný předchozí blok. To už ale není řetěz, kdy všechny bloky jsou uspořádány za sebou. Taková situace čas od času skutečně nastane – dva těžaři vytěží blok a rozešlou ho ostatním dřív, než se o sobě vzájemně dozví. Jejich bloky přitom nejsou úplně stejné – mohou obsahovat trochu odlišnou množinu nových transakcí. Přinejmenším odměnu za těžbu adresují někomu jinému.

Této situaci říkáme **fork** („vidlička" podle tvaru, který dva bloky zapojené za stejný blok připomíná). Jak se ale rozhodne, který z nových bloků platí a který ne, zvlášť když mohou obsahovat např. dvojitou útratu stejných mincí? Bitcoin tuto situaci řeší elegantně. Platný blockchain je vždy ten nejdelší, který máme k dispozici (tzn. obsahující všechny známé bloky). Najednou ovšem máme dva stejně dlouhé (oba nové bloky prodlužují předchozí blockchain o jeden blok). Pak je platný ten, na jehož nalezení bylo vykonáno více práce. A to už je konkrétní číslo, kterým se bloky trochu liší. Lze tedy jednoznačně rozhodnout, který z těchto dvou bloků je „lepší", a ten je použit k pokračování blockchainu.

Fork

situace, kdy více různých **bloků** je zapojeno za stejný předchozí **blok**. K **forku** dochází, pokud v době mezi vytěžením **bloku** a jeho propagací do sítě došlo k vytěžení jiného **bloku**. **Fork** může být také důsledkem změny bitcoinového protokolu (viz **Softfork** a **Hardfork**). **Bloky forku**, které nejsou použity pro další rozvoj **blockchainu**, se označují jako orphan **bloky**.

Pojmem **fork** se označuje i odvětvení SW za účelem jeho nezávislého vývoje, např. Bitcoin XT je vývojovým forkem **Bitcoin Core**. Tento jiný význam je třeba odlišovat od **forku blockchainu**.

Situace s forkem se tedy velmi rychle sama vyřeší tím, že těžaři pokračují v těžbě jen nad jedním z konců vidličky a druhý se v blockchainu nepoužije (stane se z něj tzv. osiřelý – orphan

blok). Samozřejmě že i při forku se může opět stát to, že dva těžaři vytěží bloky nad oběma konci vidličky ještě dřív, než se dozví o samotném forku. Takový fork délky 2 se však vyřeší tím samým mechanismem opět poté, co se celá síť o nových blocích dozví. Opět lze totiž rozhodnout, který ze dvou možných, o dva bloky delších, blockchainů je lepší.

Čím delší fork, tím s menší pravděpodobností nastane, protože vícekrát rychle za sebou nebo v podobný okamžik by se musel blok vytěžit. Pravděpodobnost takové situace tedy klesá exponenciálně, a to je důvod, proč bloky v určité hloubce můžeme považovat za prakticky nezměnitelné. Odtud se bere onen požadavek na to, abychom čekali alespoň na několik potvrzení, tedy na zahrnutí transakce do bloku větší hloubky, např. 6.

Fork a změna pravidel

K forku ovšem nedochází jen vlivem náhody v časování sítě, ale i díky změně pravidel jejího fungování. Představme si změnu protokolu, která přináší nějakou novou funkcionalitu Bitcoinu a k tomu je potřeba pozměnit datový formát bloku, potažmo transakce. Po aktivaci takové změny může síť generovat nové, pozměněné bloky. Pokud všechny uzly sítě – těžaři i obyčejní uživatelé – přejdou na novou verzi SW, síť generuje pozměněné bloky dle poptávky uživatelů po nové funkcionalitě, všichni uživatelé pozměněným blokům rozumí a není žádný problém.

Co se však stane, když někteří uživatelé na novou verzi SW nepřejdou? To záleží na tom, jestli stará verze SW považuje pozměněné bloky za validní či nikoliv. Je zřejmé, že stará verze SW nebude umět pracovat s novou funkcionalitou, kterou změna přináší. To však ještě neznamená, že stará verze nové bloky odmítne zcela. Pokud je změna pravidel navržena jako zpětně kompatibilní, starý SW bude fungovat dál. Pro uživatele je toto optimální stav – na nový SW musí upgradovat, pouze pokud chtějí používat novou funkcionalitu.

Takové zpětně kompatibilní změně pravidel říkáme **softfork**. Na nový SW musí upgradovat pouze těžaři. Je jasné, že bez jejich podpory by novou funkcionalitu nebylo možno využít, protože by nikdo nebyl schopen generovat pozměněné bloky. I proto mají

těžaři možnost o návrzích změn hlasovat – aby se zjistilo, zdali budou vůbec ochotni na nový SW přejít a má-li tedy cenu změnu vůbec implementovat. Zvlášť u podstatných změn v protokolu je požadována vysoká shoda, např. 90 % a více. Předejde se tím i situaci, kdy by někteří těžaři na nový SW nepřešli a jejich bloky, byť validní ve starém SW, by nebyly validní v novém SW ostatních těžařů. Tyto bloky by pak tvořily časté forky a zůstávaly osiřelé. To však těžař nechce, protože tím přichází o odměnu za jejich vytěžení. Raději tedy přejde na nový SW, a přestože se na změně shodlo „pouze" 90 % těžařů (resp. jejich výpočetního výkonu), nakonec ji přijmou všichni.

Softfork

změna bitcoinového protokolu, pro kterou platí, že datové struktury (**bloky**, **transakce**) vytvořené podle nových pravidel jsou vždy validní i podle pravidel starých. Taková změna je zpětně kompatibilní, neboť staré verze klientského SW považují nová data stále za validní. Není tedy třeba provádět jejich upgrade, pokud nechceme využívat funkcionality, které nová pravidla přinášejí.

Softfork pravidla zpřísňuje – množinu validních dat zmenšuje (resp. nezvětšuje) a některým rezervovaným hodnotám v protokolu dává nový význam. Příkladem významných **softforků** je P2SH („pay to script hash") nebo **segwit**.

Nicméně ne každou změnu lze implementovat jako zpětně kompatibilní. Míra, v jaké to lze udělat, závisí na tom, jak flexibilně byl původní protokol navržen. Dopředné kompatibility se dosahuje prozřetelností při jeho návrhu (ponecháním různých rezervovaných hodnot v protokolu) a zpětné kompatibility nového protokolu různými triky. Konkrétní techniky, jak tohoto dosahovat, nejsou předmětem této knihy. Je to ale jedna z oblastí, kde se projeví dobrý programátor, resp. architekt SW. Hoši vývojáři od Bitcoinu dobří jsou a zatím všechny změny protokolu se jim povedlo implementovat jako softforky.

Vidličky z korundu

Až to jednou jako softfork nepůjde, dojde ke změně, která nebude kompatibilní se starým SW. Takové změně pravidel říkáme **hardfork**. Stará verze SW považuje nové bloky po hardforku za

nevalidní. Z jejího pohledu se život na síti jakoby zastavil a uživatelé, kteří nepřejdou na novou verzi SW, nemohou síť dále používat. Upgradovat na nový SW musí tedy všichni – těžaři i uživatelé. V tomto případě se ale na rozdíl od softforku stane něco jiného, pokud někteří těžaři nepřejdou. Těžaři, kteří zůstanou ve staré síti, budou generovat staré bloky nad posledním blokem před hardforkem, a dojde tak k forku, který se nevyřeší výše uvedeným mechanismem! Staří těžaři nebudou své bloky považovat za osiřelé a těžit nad bloky nových těžařů, jako tomu bylo u softforku, protože z pohledu starých jsou nyní bloky nových nevalidní, a tudíž si jich vůbec nevšímají.

Hardfork

změna bitcoinového protokolu, pro kterou platí, že datové struktury (**bloky**, **transakce**) vytvořené podle nových pravidel nejsou obecně validní podle pravidel starých. Taková změna není zpětně kompatibilní, neboť staré verze klientského SW považují nová data obecně za nevalidní. Je tedy třeba provádět jejich upgrade, abychom mohli síť i nadále využívat.

Hardfork pravidla uvolňuje – množinu validních dat zvětšuje. Důsledkem **hardforku** může být tzv. split – rozdělení **blockchainu** trvalým **forkem** (někdy se pojmem **hardfork** nepřesně označuje až tato situace). Příkladem významného **hardforku** je Bitcoin Cash.

Pokud tedy při hardforku všichni nepřejdou na nový SW a alespoň jeden těžař zůstane u staré verze, blockchain se rozdělí trvalým forkem. Taková situace se označuje jako tzv. split blockchainu. Spolu s těžařem zůstanou u staré verze SW i někteří obyčejní uživatelé. Jinak by těžař neměl žádné zákazníky pro měnu, kterou těží, a vynakládal by svůj výpočetní výkon na těžbu zbytečně. A jestli se toto stane (dojde ke splitu), záleží na tom, jestli lidé budou chtít původní pravidla stále používat. Budou-li tací, vzniknou z původně jedné měny měny dvě. O svoji hodnotu u uživatelů budou mezi sebou soupeřit rozdílem svých pravidel, kvalitou dalšího vývoje a silou komunity, která se kolem nich utváří. Je to zkrátka decentralizovaná diverzifikace v praxi.

Ještě by vás mohlo napadnout, jak je to s mincemi, které jsem před hardforkem držel – jaké budu mít po něm – mince měny původní, nebo té se změnou? Je asi zřejmé, že mince měny původní mi zůstanou, protože neexistuje žádný důvod, aby tomu bylo

jinak – původní měna žádnou změnu nevidí, jen občas v síti zaznamená blok, který z jejího pohledu není validní. A druhá měna sice obsahuje nějakou změnu navíc, ale ta se stěží bude týkat zůstatků na účtech v okamžiku hardforku. Takže ani zde není žádný důvod k tomu, abych o své mince přišel. Z pohledu uživatele je tedy opět všechno v pořádku – o nic nepřichází, naopak získá zdarma mince druhé měny. Tedy pokud mince skutečně vlastní on a nedisponuje jimi za něj třeba online peněženka nebo burza. Pak je uživatel vydán na pospas rozhodnutí jejich provozovatelů, jestli mu bude přiznáno vlastnictví i mincí druhé měny. Je ale možné, že hodnota mincí po hardforku klesne a že ani v součtu s těmi novými nebude taková, jaká byla před hardforkem. To záleží na tom, jak trh rozdělení měny vyhodnotí.

Forkování Bitcoinu

S tímto teoretickým úvodem se můžeme konečně podívat na to, co zásadního se kolem vývoje Bitcoinu dělo zejména v průběhu let 2016 a 2017. Povíme si pohádku o (začátku) řešení problému škálování Bitcoinu. Škálováním zde myslíme přizpůsobování sítě stále se zvětšujícímu počtu uživatelů. Bitcoin totiž získával stále větší popularitu a nestíhal.

Již v roce 2013 existovala vážnější diskuze o další budoucnosti Bitcoinu, konkrétně o řešení problému jeho škálování pro stále rostoucí počet transakcí. Velikost jednoho bloku – nositele informací o transakcích – je totiž omezena na 1 MB (přesněji na 1 milion bajtů) a víme, že průměrná doba mezi dvěma vytěženými bloky je zpětnou vazbou držena na cca 10 minutách. Z obvyklé velikosti transakce (resp. z velikosti transakce s obvyklým počtem vstupů 1 a výstupů 2) cca ¼ kB pak snadno dopočítáme maximální počet transakcí za jednotku času. Ten činí cca 7 transakcí za sekundu. A to je žalostně málo! Centralizované platební systémy jako např. Visa umějí zpracovat o několik řádů více. Bylo jasné, že zanedlouho přijde doba, kdy poptávka po transakcích bude větší, než kolik činí tato malá, a navíc konstantní nabídka.

Na první pohled se možná zdá jako nejsnazší řešení odstranit limit na velikost bloku a bylo by po problému. Situace je však složitější. Limit na velikost bloku byl zanesen Satoshim do zdrojových

kódů Bitcoinu v roce 2010 (pro detailisty se jednalo o commity do SVN repozitáře klienta Bitcoin-Qt [r103] z 15. 7. 2010 – limit na sestavování bloku při těžbě; a [r156] z 19. 9. 2010 – limit pro validaci bloku, mimochodem už předtím tam byl limit 32 MB). Satoshi tento limit zavedl údajně jako ochranu před potenciálním spamovým útokem na tenkrát ještě skoro prázdný blockchain, s úmyslem ho časem odstranit. Představte si to tak, že by někdo posílal nesmyslné transakce s cílem síť zahltit. Zamýšlené dočasnosti odpovídala i nulová flexibilita jeho implementace – jednoduché omezení konstantou. Již v říjnu 2010 navrhl reformulaci limitu ve zdrojových kódech na poněkud flexibilnější tvar Jeff Garzik, ale jeho návrh se neaplikoval. S hlasitým návrhem na odstranění limitu přišel později tehdejší hlavní Core vývojář Gavin Andresen, odkazuje na komentář samotného Satoshiho o dočasnosti onoho limitu. Narazil ale na silný odpor ostatních. Tou dobou už totiž s implementací pracovalo mnoho lidí na to, aby se spolu jednoduše dohodli. Bitcoin je prostě konzervativní svět.

Zásadní problém případného odstranění limitu na velikost bloku je totiž fakt, že by se jednalo o hardfork, a takovým změnám se vývojáři snaží vyhnout. Hardfork proto, že nová verze by připouštěla větší bloky, než povoluje verze původní. Pokud bychom limit naopak zpřísňovali, jednalo by se o softfork, ale zvětšování množiny validních bloků je vždy hardfork. Navíc by bylo třeba dohodnout se na nějakém novém limitu nebo obecnějším schématu jeho průběžného zvětšování, případně úplně jiném řešení. A to je mnoho možností, před kterými stojí mnoho lidí, takže bylo zaděláno na klasický politický problém. Ano, i ve světě Bitcoinu je politika.

Bitcoin XT, Unlimited, Classic, Segwit

Od roku 2015 se začaly objevovat první konkrétní návrhy řešení škálování, lišící se mírou konzervativnosti změn. Jednalo se o myšlenky přesunu malých transakcí mimo blockchain – tzv. off-chain mikroplatby. Objevil se nápad na zmenšení transakcí pomocí tagů (Flexible Transactions), který by ovšem vyžadoval také hardfork. A mnoho dalších hardforků podle hesla „když už hardfork, tak ať to stojí za to“.

V roce 2015 navrhl Core vývojář Mike Hearn Bitcoin XT – hardfork s navýšením velikosti bloku dle BIP 101 (skokově na 8 MB s postupným násobením velikosti na dvojnásobky každé dva roky). V lednu 2016 vznikl Bitcoin Unlimited, kde velikost bloku není určena konstantou, nýbrž dynamicky, většinovou shodou signalizujících těžařů. V únoru 2016 se pak objevil konzervativnější Bitcoin Classic – hardfork s navýšením dle BIP 109 (fixně na 2 MB), jehož vývoj byl ukončen až v listopadu 2017 v reakci na nedodržení části dohody New York Agreement, ale k tomu se ještě dostaneme. A řada dalších návrhů… Oponenti navyšování velikosti bloku spatřovali zásadní nevýhodu tohoto přístupu v inklinaci k větší centralizaci. Jejich argumentem bylo, že zpracování větších bloků má i větší požadavky na HW, které uspokojí jen velcí hráči na poli těžařů. Politická diskuze se tříštila a řešení, na kterém by panovala shoda, bylo v nedohlednu.

V prosinci 2015 přišel návrh na tzv. **segwit** dle BIP 141. Spíše než o systémové řešení škálování jde o některá vylepšení a opravy nedostatků, které protokol Bitcoinu dlouhodobě trápily. Nicméně na problém škálování má pozitivní dopad hned ve dvou ohledech. Vlivem implementačního triku se do bloku vejde zhruba o 80 % více transakcí (pokud by všichni používali segwit) a odstranění maleability transakce usnadňuje implementovatelnost tzv. „Lightning Network" (LN) pro realizaci mikroplateb off-chain – mimo hlavní blockchain. LN by šla teoreticky implementovat i bez segwitu, ale takto je možné vyhnout se některým nepříjemnostem (např. v podobě dlouhého čekání v některých chybových stavech). Segwit je v otázce škálování takový konzervativní přístup říkající: „nejprve vyřešme známé systémové problémy a z čistého stavu můžeme dále řešit problém škálování". A nejlepší argument pro segwit je, že byl nalezen způsob, jak ho na rozdíl od řady ostatních návrhů implementovat jako softfork. Segwit byl tedy přidán do kódu a k jeho aktivaci mělo dojít po uzamčení souhlasem, který by signalizovalo 95 % těžařů. Jednalo se však o velkou, a tudíž i kontroverzní změnu a úroveň konsensu se dlouho pohybovala pouze kolem 30 %, takže se nedařilo segwit uzamknout. Politika.

Segwit

návrh na změnu dle **BIP** 141. Název **segwit** je zkrácenina spojení „segregated witness“, což zachycuje hlavní změnu nesenou tímto **BIPem**. Znamená vnitřní reorganizaci dat **bloku** tak, že dojde k oddělení **podpisu** (resp. odemykacího skriptu) **transakcí** od **transakcí**. Lehčí uzly sítě mohou zahazovat ověřené **podpisy** starších **transakcí** a šetřit tak místo (je to vlastně jedna z forem prořezávání databáze bitcoinového **ledgeru**). Důsledkem tohoto oddělení je rovněž odstranění **maleability transakce**, což zjednodušuje škálování na vrstvách nad **Bitcoinem** – vlivem separace **podpisu** lze **transakce** podepisovat antichronologicky, což rozšiřuje prostor pro schémata výměny částečně podepsaných **transakcí** (např. Lightning Network).

UASF, Segwit2x

Uživatelům se samozřejmě nelíbilo, že se na poli řešení škálování dlouho nic neděje a že s tím sami nemohou nic dělat. O přijmutí BIPu pro segwit, který by uživatelé přijmout chtěli, (ne)rozhodovali těžaři svojí signalizací. Přitom jsou to právě uživatelé, kteří svým jednáním dávají bitcoinům hodnotu, a z této hodnoty se platí i existence těžařů. Rozhodli se tedy položit těžařům takříkajíc nůž na krk a navrhli tzv. UASF („User Activated Softfork“ – uživatelsky aktivovaný softfork) dle BIP 148. V něm uživatelé (resp. zástupci velkých firem podnikajících nad Bitcoinem) oznamují, že po 1. 8. 2017 nebudou akceptovat vytěžené bloky nesignalizující pro segwit. Vyvinuli tak neagresivní tlak na těžaře: „nelíbí se mi tvoje chování, a pokud ho nezměníš, začnu tě (tvoje bloky) ignorovat“. Asi těžko bychom našli větší strašák pro těžaře, než když si jejich pracně vytěžených bloků nebude velká část uživatelů všímat – vždyť právě v nich je informace o odměně, kterou si za těžbu zasloužili. Navíc je to nebezpečná varianta řešení v podobě špatně kontrolovatelných důsledků takového stavu. Tato hrozba pro celou síť přiměla zúčastněné strany k vyvinutí většího úsilí o řešení celé situace.

A tak v květnu 2017 vznikla dohoda „New York Agreement“ (NYA). Tato dohoda získala zejména potřebnou podporu těžařů, hlavně z Číny, kteří toho času ovládali cca 80 % hash rate (výpočetního výkonu sítě). Jejím obsahem byly dva body – aktivace segwitu a zvětšení bloku na 2 MB dle BIP 102 tři měsíce po aktivaci segwitu

(přesněji o 90 × 144 bloků později, neboť čas v Bitcoinu se počítá na bloky). Segwit + 2× zvětšení bloku = Segwit2x – označení modifikace SW, které se v souvislosti s touto dohodou používá. Formálně je Segwit2x zachycen v BIP 91, který po aktivaci způsobí, že celá síť bude odmítat bloky nehlasující pro segwit, čímž se předejde výše popsanému UASF. Problém vyřešen! Na uzamčení Segwit2x stačila podpora 80 % těžařů (resp. 269 z 336 posledních bloků signalizujících kladně). Je to vlastně mechanismus pro redukci 95 % souhlasu na 80 %. K aktivaci BIP 91 došlo 21. 7. 2017, tedy posledních pár dní před termínem stanoveným v UASF. Segwit se tedy uzamkl a 24. 8. 2017, po tři čtvrtě roce od možnosti pro něj signalizovat (od bloku 439488), se konečně aktivoval (od bloku 481824).

K plánovanému zvětšení bloku hardforkem, jež bylo součástí dohody NYA, v určeném termínu 16. 11. 2017 nicméně nedošlo. Podpora uživatelů postupně oslabila a byly identifikovány nevyřešené technické problémy koexistence dvou sítí (např. tzv. „**replay protection**"). Celková averze vůči hardforku byla a je charakteristická především pro komunitu kolem vývoje. Vlastně ani pořádně nevznikl SW implementující tuto část Segwit2x, která neměla podporu vývojářů Bitcoin Core. Jeden z nich, Greg Maxwell, prohlásil, že část NYA o zvětšení bloku byla učiněna pod nátlakem. 8. 11. 2017, týden před očekávaným nasazením, byl vývoj Segwit2x větve pozastaven. O měsíc později v prosinci byl Segwit2x oprášen jinou skupinou vývojářů, se spuštěním naplánovaným na 28. 12. 2017. Žádný zázrak se ale nekonal.

Bitcoin Core se tedy v listopadu nehardforknul, softfork segwit byl v srpnu protlačen přes Segwit2x a k UASF nedošlo (resp. BIP 148 neměl žádný efekt, neboť segwit se stihl uzamknout v termínu do 1. 8. 2017). Zdálo by se tedy, že politicky vyhrocená situace v létě 2017 se vyjasnila. Máme tu ale ještě UAHF.

Replay Protection

odolnost sítě po **hardforku** vůči tomu, aby se její **transakce** nedaly zaměnit s **transakcemi** sítě původní a naopak. Neexistuje-li taková odolnost, může útočník zachytit **transakci** původně určenou jen pro jednu síť a rozeslat ji i do druhé, což způsobí nezamýšlený převod mincí na stejnou cílovou **adresu** i ve druhé síti. Tomuto typu útoku se říká „replay attack". Odolnosti vůči němu lze dosáhnout např. pozměněním formátu **transakce** (řešení v Bitcoin Cash).

UAHF, Bitcoin Cash

Připomeňme si, že žijeme v decentralizovaném světě a v takovém si každý může pro sebe neuspokojivou situaci řešit po svém. Skupina uživatelů kolem čínského výrobce těžebního HW a provozovatele těžebních poolů Bitmain vydala v červnu 2017 prohlášení, ve kterém vyjadřuje svoji obavu z hrozby UASF, jehož podpora přetrvávala i po NYA. UASF by sice v případě úspěchu segwit části Segwit2x neměl žádný efekt, ale v Bitmainu byli znepokojeni z jeho pokračující existence. Navíc se čínští těžaři neměli příliš v lásce s vývojáři Bitcoin Core, kteří nechtěli hardfork, a těžaři zase nechtěli segwit bez zvětšení bloku. Zkrátka NYA asi nebyla tak konsensuální, jak by se zdálo, a v rámci manifestace tohoto rozkolu přišel Bitmain s vlastním řešením, příznačně pojmenovaným UAHF („User Activated Hardfork" – uživatelsky aktivovaný hardfork). Jedná se o hardfork s velikostí bloku až 8 MB (resp. plánem postupného navyšování do srpna 2019), aktivovaný 12 hodin po případném UASF.

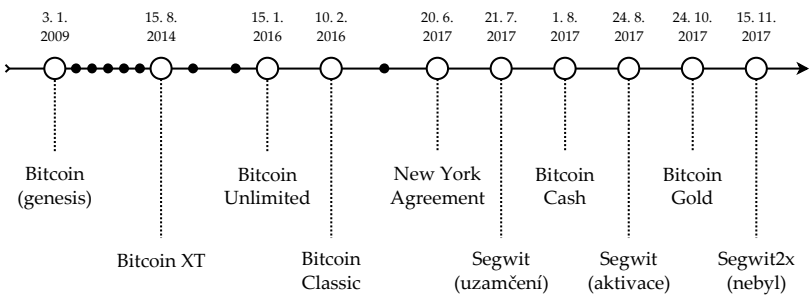
UAHF se zpočátku nebránil adopci segwitu a vyvíjely ho v tichosti tři týmy. Viditelnou se stala implementace s názvem Bitcoin ABC a k ní příslušející síť pojmenovaná Bitcoin Cash. Měna této sítě má zkratku BCH (ev. BCC). Klient Bitcoin ABC vychází z poslední verze Bitcoin Core před forkem a má odstraněný kód pro segwit. Obsahuje i oboustrannou replay protection vůči BTC díky lehce pozměněnému algoritmu na ověřování validity transakce. Rovněž byl upraven algoritmus pro nastavování obtížnosti generování nových bloků (viz Těžba), neboť s obtížností zděděnou z původního blockchainu by těžba prvních BCH bloků mohla trvat velmi dlouho, pokud by dostatečná část těžařů nepřešla na tuto síť. Rychlost generování BCH bloků zpočátku vykazovala velké fluktuace, protože těžaři přecházeli mezi těžbou obou sítí podle toho, co pro ně bylo výhodnější z hlediska momentální ceny měny.

K hardforku došlo 1. 8. 2017 (od bloku 478559) a blockchain Bitcoinu tak zaznamenal svůj první a velmi kontroverzní split (rozdělení blockchainu trvalým forkem). Nikdo moc netušil, co přesně se bude dít. Burzy zaujímaly k situaci různá stanoviska. Některé slibovaly svým uživatelům, že po splitu získají mince obou blockchainů. Jiné varovaly své klienty, že podpora Bitcoin Cash není zaručena, a doporučovaly uživatelům výběr BTC před splitem. Většina z nich nicméně

v několika týdnech po splitu implementovala i podporu BCH jakožto dalšího měnového páru. Čínská burza a těžební pool ViaBTC, interesovaná ve vzniku Bitcoin Cash, nabídla obchodování s jeho měnovými páry dokonce týden před splitem. Mnoho lidí si myslelo, že krátce po splitu klesne cena BCH (nebo dokonce BTC) na nulu a vesmír zkonverguje opět k jedné měně. To se ovšem nestalo a během zbytku roku 2017 se cena BCH pohybovala kolem 20 % ceny BTC. Mezi podporovatele Bitcoin Cash se zařadila velká jména jako Gavin Andresen, Roger Ver, Kim Dotcom nebo Rick Falkvinge. Relativní úspěch BCH hardforku se ještě týž měsíc pokusil zopakovat projekt Bitcoin Gold zaměřený na možnost těžby užitím slabšího HW (podobně jako Litecoin, viz dále), ale jeho cena se pohybovala jen kolem 10 % BCH.

Pro zajímavost dodejme, že úplně první split blockchainu to přece jen nebyl. K historicky prvnímu došlo již v březnu 2013, a sice na 6 hodin vlivem nezamýšlené nekompatibility pravidel pro validitu transakce v nové verzi SW. Byl to vlastně nechtěný hardfork. Nastalá situace se vyřešila downgradem z verze 0.8 zpět na 0.7 a poškozený řetěz bloků ze sítě zmizel. Cena na burze se přitom propadla zhruba o čtvrtinu, leč rychle se zotavila. Také k prvnímu softforku došlo již dávno před segwitem. V říjnu 2010 byla odstraněna kritická chyba spočívající opět ve špatné kontrole validity transakce (integer overflow), která byla zneužita k sestavení transakce generující 184 miliard BTC. Chyba byla opravena a poškozený kus blockchainu přegenerován. To v té době ještě nebyl problém, protože Bitcoin používalo málo lidí a bloky obsahovaly málo transakcí. Jde ovšem o jedinou dosud nalezenou a zneužitou bezpečnostní chybu v Bitcoinu, což je fantastické.

chronologický přehled důležitých událostí týkajících se forkování Bitcoinu



Škálování, neškálování a kolosální poplatky

Tak tedy máme na světě hardfork Bitcoinu a jmenuje se Bitcoin Cash. Přistupuje jinak k otázce škálování než „pravý" Bitcoin. Mimochodem který je pravý a který odvětvený? Zde je situace ještě jednoduchá – odvětvený je Bitcoin Cash, protože jeho pravidla se změnila na zpětně nekompatibilní se starým SW. Konkrétně Bitcoin Cash povolil bloky (větší bloky), které dříve povoleny nebyly. Nehledě k tomu, že to byl Bitcoin Cash, který implementoval replay protection a vypořádával se tak s existencí Bitcoinu, ne naopak – Bitcoin o existenci Bitcoin Cash neví (ve smyslu úprav SW). Co kdyby ale jednou došlo k hardforku v samotném Bitcoin Core? Který pak bude ten pravý Bitcoin? Určitě se totiž najdou dostatečně ortodoxní jedinci, kteří budou pokračovat v provozování původního SW v původní síti. Core vývojáři vědí, proč se hardforku tak brání.

Každopádně dlouho panující neshoda na řešení problému škálování dala vzniknout různým subkomunitám hádajícím se o to, jak vlastně řídit změny v Bitcoinu. Ale dá se decentralizovaný systém v tomto smyslu vůbec „řídit"? Jeden z původních vývojářů Mike Hearn v roce 2016 prohlásil, že Bitcoin je mrtvý. Tou dobou byla síť již zcela naplněna transakcemi a řešení škálování v nedohlednu. V roce 2017 docházelo k výraznému růstu počtu dlouho nepotvrzených transakcí a v důsledku toho i k neúnosnému zvyšování poplatku za transakce v rámci boje uživatelů o jejich rychlé potvrzení.

Koncem roku 2017 byly k vidění neuvěřitelně drahé transakce. Poplatek nezřídka převyšoval 1000 satoshi za bajt velikosti transakce. Za obvyklou transakci činil poplatek v přepočtu při tehdejším kurzu stovky korun, což je nepoužitelná částka i pro platbu středně velkých obnosů. Velké transakce (mající mnoho vstupů a výstupů, např. výběry z burz adresované mnoha uživatelům nebo různé konsolidace mincí) stály v řádech desetin BTC, což odpovídalo desítkám tisíc korun. V bloku 500546 nalezneme transakci o velikosti 73 kB, přesouvající 25 BTC z pěti set adres, s poplatkem jeden celý bitcoin, tehdy 350 tisíc korun! Poplatky za transakce již dávno nebyly zanedbatelné vůči množství vytěžených bitcoinů, naopak se mnohdy přibližovaly toho času platné odměně za blok 12,5 BTC.

Kde je tedy ono škálování, když už máme tolik očekávaný segwit, ale transakce jsou stále dražší nebo pomalejší? V polovině prosince 2017, v tom největším přetlaku nepotvrzených transakcí (zůstávají v tzv. **mempoolu**), jsme udělali vlastní experiment. Ručně jsme vygenerovali transakci s relativně malým poplatkem 30 sat/B a rozeslali do sítě. Do konce roku se nepotvrdila. Můžete se sami přesvědčit, kdy (či jestli vůbec) se potvrdila, vyhledáním adresy 1BringStateAuthoritiesDown15et5WL, na kterou jsme odeslali navždy nedobytných 1984 satoshi.

Mempool

virtuální prostor pro **transakce** čekající na **potvrzení**. Každý uzel má **mempool** vlastní. Na přelomu let 2017 a 2018 se velikost kompletního **mempoolu** pohybovala v řádu stovek MB. Při velikosti **bloku** 1 MB (efektivně o něco více při použití **transakcí** se **segwitem**) to znamenalo průměrné čekání na **potvrzení transakce** v řádu dnů.

Problém škálování zůstal v Bitcoinu ke konci roku 2017 nevyřešen. Segwit není řešení škálování, ačkoliv si to spousta lidí myslí. Jak už jsme říkali, je to spíše podklad pro možná řešení. Všechna možná řešení škálování lze rozdělit v zásadě do dvou skupin – buďto budeme usilovat o zapsání všech transakcí do blockchainu, tzv. on-chain = uvnitř řetězu (bloků), nebo některé transakce přesuneme off-chain = mimo řetěz (bloků). On-chain přístup je cesta, kterou si zvolil Bitcoin Cash, a je jasné, že vede skrzeva zvětšování bloku (s odvoláním na to, že taková byla myšlenka původního Bitcoinu). U této cesty je ovšem otázkou, zda bude k dispozici taková technologie, která umožní v reálném čase zpracovávat bloky dostatečně velké, aby obsáhly „všechny transakce světa". A nejen to, ale aby přitom zůstala síť stále decentralizovaná (což také byla myšlenka původního Bitcoinu) a nikoliv v rukou několika mocných, kteří si mohou takovou technologii dovolit. Uvidíme.

Off-chain přístup naopak v blockchainu nechává jen některé transakce, typicky velké a takové, které nemusí být realizovány rychlostí blesku. Ty ostatní, typicky různé mikroplatby za kávu či pivo, se snaží přesunout jinam. Přesněji někde jinde po nějakou dobu akumulovat, a teprve až bude potřeba udělat jejich vypořádání (jak konečné, tak průběžné), dozví se o nich hlavní blockchain. Je to vlastně hierarchizace platebních systémů nad hlavním

blockchainem, na který můžeme pohlížet jako na vrstvu první úrovně. Vrstvou další úrovně může být např. již zmíněná Lightning Network. Pojďme se na ni bleskově podívat.

Lightning Network

Lightning Network (LN) je jedním z vyvíjených návrhů řešení problému škálování. Je to vrstva druhé úrovně nad Bitcoinem pro rychlou realizaci mikroplateb. Jde tedy o řešení off-chain – do blockchainu se neukládají všechny detaily o mikroplatbách, ale až nějaký agregovaný stav. Jak LN pracuje? Otevírá se tzv. „Lightning kanál", do kterého dvě strany vloží nějaké své peníze. Z hlediska Bitcoinu je kanál **multisig** adresa, se kterou mohou disponovat pouze obě strany současně. Zároveň ale platí, že po nějaké definované době (např. měsíc) si svou část vkladu na tuto adresu mohou strany vzít zpět. Je to vlastně příklad (smart) **kontraktu**, který kombinuje multisig (podmínku více podpisů) a podmínku časovou (timelock). Časová podmínka existuje proto, aby i v případě nekooperující protistrany nikdo nemohl přijít o své peníze. LN je tzv. trustless – nespoléhá na důvěryhodnost kohokoliv, takže její použití je v tomto ohledu stejně bezpečné jako použití samotné bitcoinové sítě.

Multisig

podmínka uvolnění bitcoinů z výstupu **transakce** užitím více **podpisů**. Typický případ vyžaduje současné užití m z n **soukromých klíčů**, kde m < n. Typickou aplikací je řízení přístupu ke kolektivně spravovaným prostředkům. Je to vlastně speciální případ **kontraktu**. **Multisig transakce** je **transakce** uvolňující bitcoiny pomocí **multisig** podmínky. **Bitcoin** má podporu pro **multisig transakce** od svého začátku, ale teprve s implementací **BIP** 16 (P2SH) získal možnost reprezentovat **multisig** výstup jednoduchou **adresou**, kterou lze předat odesílateli. Jinou možností, jak aplikovat více **podpisů** (zkombinovat více **podpisů** do jednoho) nabízí kryptografická metoda Schnorr signatures.

Otevřený kanál mezi uživateli je tedy adresa, na které leží peníze obou, a možnost, jak je dostat zpátky v nějakém poměru vkladů. Po vytvoření kanálu odpovídá tento poměr počátečním vkladům. Při každé mikroplatbě se však zůstatky v kanálu aktualizují ve prospěch příjemce a na vrub plátce. Podobně jako když si na výletu

s přáteli píšete dlužníček, abyste nemuseli všechny vzájemné dluhy ihned vypořádávat. Zároveň je tento systém kryptograficky bezpečný. Aktualizace zůstatků probíhá vygenerováním speciálních transakcí, které si strany vymění, ale nerozesílají do bitcoinové sítě. Držení těchto tzv. commitment transakcí dává stranám jistotu, že nepřijdou o peníze odpovídající poslednímu stavu kanálu, pokud by druhá strana přestala na schématu aktualizace zůstatků kooperovat. V rámci tohoto schématu se různě vyměňují částečně podepsané transakce. Pokud má podkladová síť segwit, mohou být tyto procesy jednodušší. Účelem naší knihy však není jejich detailní popis. Řekneme si však alespoň to, že není možné zneužít jinou než poslední commitment transakci k uzavření kanálu. Pokud by se o to jedna ze stran pokusila, odkryla by tím jistou informaci, kterou by druhá ze stran mohla využít k tomu, aby si přisvojila všechny peníze v kanálu. Této možnosti trestu za případné podvádění se dosahuje opět i pomocí časových zámků v transakci.

Kontrakt
viz **Transakce**

Kanál může být otevřený libovolně dlouho, ale je možné ho uzavřít kdykoliv podle potřeby. Obecně tehdy, pokud je žádoucí zapsat do blockchainu poslední stav, např. po vyčerpání peněz (všechny se „přelily" k jedné straně) nebo pokud jedna ze stran přestala kooperovat. Uzavření kanálu se provede rozesláním commitment transakce odpovídající poslednímu stavu kanálu (resp. tzv. settlement transakce, jež se liší pouze absencí časových zámků, a strany ji společně vygenerují, pokud stále kooperují a dohodly se na uzavření kanálu). Do bitcoinového blockchainu se tedy dostanou pouze dvě transakce – pro otevření a uzavření kanálu. To, co se dělo mezitím, je věcí LN, resp. vyměňování „dlužních úpisů" v podobě transakcí aktualizujících zůstatky v kanálu. Podobně jako na tom výletu, kde vypořádání provedete jednou na konci podle poznámek v dlužníčku. LN je vlastně systém pro zúčtování (clearing) transakcí bez zúčtovacího centra (někoho, kdo by centrálně spravoval peníze vložené do kanálu). Až výsledné vypořádání (settlement) proběhne on-chain po uzavření kanálu. Sečteno podtrženo, v Bitcoinu jsme objevili dávno objevené. Když zajdete na pivo ke kamarádovi, klidně vám to nechá na sekeru. V restauraci platíte vždy při odchodu. A pokud jste na festivalu, platíte si každé pivo zvlášť. Proč by to nemohlo fungovat i u Bitcoinu?

Blesky v síti

Takto jsme si popsali, jak LN pracuje mezi dvěma uživateli, kteří mezi sebou mají otevřený platební kanál. Nedá se ovšem předpokládat, že všichni se všemi si budou otevírat kanály kvůli jednorázovým platbám. To by vlastně počet transakcí v blockchainu naopak zdvojnásobilo – místo jedné obyčejné by byly dvě. Ale LN má být síť propojující uživatele mezi sebou skrze jejich platební kanály. Pokud dva uživatelé nemají platební kanál otevřený spolu, ale v síti mezi nimi vede cesta přes jiné uživatele, může se platba přenést skrze kanály po této cestě (připomíná to platební systém Ripple, o kterém si povíme v dalších kapitolách). Ale je to bezpečné, nechat své peníze přenášet přes ostatní? Je! Obdobně jako nemusíme důvěřovat protistraně u otevřeného kanálu, nemusíme důvěřovat ani uzlům po cestě přes více kanálů. Toto je kryptograficky ošetřeno pomocí tzv. „hash locků", kde pro utracení výstupu transakce musí uživatel přijít s daty odpovídajícími určitému hashi. Aby pro nás byla síť trustless z hlediska protistrany i uzlu po cestě, hash locky a časové zámky se kombinují do tzv. HTLC („Hashed Timelocked Contract"). Když se chce, dokáže být technologie velmi důmyslná.

Aby byla síť trustless pro všechny zúčastněné strany, platba musí proběhnout atomicky, tzn. buď celá (přes všechny uzly po cestě) nebo vůbec (nikdo peníze se nepřesunou jinam). Důsledkem toho je, že každý kanál po cestě od vás k cíli musí umět zaplatit částku o velikosti vaší platby. Toto omezení tak může být problém u větších plateb. Zároveň to vytváří tlak na výběr poplatků za zprostředkování transakce v závislosti na její výši. Na rozdíl od blockchainu, kde záleží na velikosti transakce nikoliv hodnotové, ale datové – v bajtech. To dává smysl, protože do blockchainu se tato data uloží navždy, a u transakce v LN se data pouze přesunou sítí. Také je potřeba si uvědomit, že kanálů na jednom uzlu sítě musí být otevřeno mnoho, aby síť byla hustá a cesty mezi vzdálenými uzly mohly být dostatečně krátké. Čím budou cesty delší, tím závažnější má toto omezení vliv, protože po cestě se přenese jen platba odpovídající velikosti nejmenšího uzlu. Jenže čím více kanálů na uzlu bude, tím méně peněz z celkových peněz uzlu může být vloženo do každého z nich. Existuje dokonce hypotéza, že díky tomuto jevu nebude LN v globálním měřítku

dobře fungovat. Jak už jsme psali u Bitcoin Cashe: uvidíme. Minimálně jeden z autorů této knihy je v tomto spíše skeptičtější a zajímavý potenciál ke škálování spatřuje v tzv. sidechainech, resp. drivechainech.

Anebo by LN síť musela být centralizovanější – s menším množstvím velkých LN uzlů s velkým množstvím kanálů na spoustu uživatelů. Na takových uzlech – hubech – by musely ležet velké peníze, aby mohly peníze ostatních efektivně přeposílat. LN huby za to budou vybírat poplatky, nejspíš procentuální a/nebo paušální, a bude to zkrátka plně komerční služba. To ovšem inklinuje k centralizaci platebního systému, čemuž se Bitcoin snaží vyhnout. Čím budou vstupní náklady na provoz takového hubu vyšší, tím méně nahodilejší jejich provoz bude a centrálním autoritám se budou snáze diktovat jeho pravidla. Včetně stanovování toho, kdo platby provádět smí a koho za to naopak zavřeme do vězení.

Další nevýhodou LN je skutečnost, že příjemce platby musí být online. Klasická on-chain platba se prostě zapíše do blockchainu a na tom příjemce nemusí nijak participovat (pokud není těžař). Naopak nespornou výhodou LN je rychlost realizace plateb, která je omezena pouze rychlostí sítě, takže teoreticky rychlostí světla, jak propagátoři LN rádi uvádějí. Samozřejmě že nějaký čas spolkne i generování a výměna částečně podepsaných transakcí, ale to pro nákup kávy vliv nemá (pro nanosekundové obchodování na burze by mělo). Také jsou transakce v LN daleko anonymnější než on-chain, neboť se nikam navždy neukládají a útočník na vaše soukromí by musel zachytávat toky dat na síti v reálném čase. Oproti tomu analýzu dat uložených v blockchainu může udělat kdykoliv později.

Principy LN nebrání ani realizaci atomických swapů, tedy výměny digitálních tokenů různých typů, např. bitcoinů za litecoiny. Můžeme tedy prostřednictvím trustless sítí propojovat různé kryptoměny a provozovat kryptograficky bezpečné směnárny a platební brány. S LN se tak potenciálně otevírá prostor pro další možnosti a nové příležitosti ve světě kryptoměn. Hlavními vývojáři LN jsou společnosti Blockstream (zaměstnává některé z předních vývojářů Bitcoinu) a Lightning Labs. Koncem roku 2017 je LN dostupná na **testnetu** BTC a LTC. Na hlavním blockchainu se LN testuje. Rok 2018 bude pro LN klíčový.

Testnet

paralelní síť **Bitcoinu** určená k testovacím účelům. Tvoří oddělený **blockchain** s vlastními mincemi tBTC. Má také vlastní **genesis blok**. Některé větší změny mají svůj vlastní **testnet**, např. SegNet pro testování **segwitu**.

Alternativní kryptoměny

Co je to „altkojnt“

Není jen Bitcoin. Je také rodina, přátelé, sport, hezká knížka… Ehm, teď vážně… Víme, že není jen Bitcoin. Jsou i jiné kryptoměny. A je jich mnoho, ke konci roku 2017 více než tisíc. Na webové stránce coinmarketcap.com nalezneme přehled většiny z nich, včetně jejich tržní kapitalizace a vývoje kurzu, jsou-li obchodovány na některé z globálních kryptoburz. Říká se jim altcoiny, jakožto portmanteau od slov alternativní a (Bit)coin. Některé mají vskutku exotické názvy inspirované čímkoliv, co je zrovna (ne)populární, jako např. Trumpcoin nebo PutinCoin. Mnoho z nich nestojí za průzkum, protože jde víceméně o lehce přeparametrizované klony Bitcoinu nebo jiných starších coinů. Některé ale za průzkum stojí a správný kryptofanatik by měl být schopen se v nich orientovat.

První altcoiny se začaly objevovat v letech 2011 a 2012. Masivní popularitu získal svět altcoinů v letech 2013 a 2014, kdy většina z nich byla obchodovatelná proti BTC. Volatilita některých altcoinů byla monumentální i ve srovnání se samotným Bitcoinem. Lidé se bavili veřejným organizováním akcí typu pump & dump (ve velkém nakoupit, vyhnat tak cenu do nebes, a pak prudce prodat – ti, co byli poslední, v tom zůstali s masivní ztrátou, ale zítra je taky den a šlo se na jiný altcoin). Opět se redistribuoval majetek, opět některé burzy zkrachovaly (např. Cryptsy), něco byl podvod, něco úžasná nová technologie. Byla to bláznivá jízda. Ale svobodná, a to na ní máme rádi, nebo ne? To jest na úvod a nyní se podívejme, jaká je „zoologie“ světa altcoinů – podle jakých kritérií je můžeme dělit a jaká rozhodnutí v jejich návrhu jsou příčinou jakých vlastností, kterými se jednotlivé alternativní kryptoměny vyznačují.

Zoologie altcoinů

Základem většiny altcoinů je samotný Bitcoin. A platí to jak pro protokol (resp. specifikaci datových struktur a síťové komunikace), tak pro softwarovou implementaci, kterou altcoiny postavené nad Bitcoinem odvětvují z volně dostupného SW repozitáře

Bitcoinu a dále upravují. Teoreticky by mohly mít vlastní implementaci stejného protokolu, ale proč znovu vynalézat kolo (leda jako nezávislou implementaci pro testování). Ne všechny altcoiny ovšem vycházejí z Bitcoinu. Jiným existujícím protokolem je tzv. CryptoNote, který rozšiřuje anonymizační schopnosti kryptoměny, a budeme mu věnovat samostatnou kapitolu. Některé altcoiny jsou naopak řešeny úplně jinak než Bitcoin a uvedeme si zde i zástupce takových.

Další dělení altcoinů můžeme provést podle toho, jde-li pouze o měnu, nebo o nějakou univerzálnější platformu, která může sloužit jako základ odvozených projektů. Měna by v ideálním případě měla mít tu vlastnost, že její jednotky – mince – jsou zaměnitelné. Pokud mají mince vystopovatelnou transakční historii, toto neplatí a některé mince mohou být méně hodnotné než jiné (např. takové, které zprostředkovaly státem zakázaný, tzv. ilegální obchod). Této vlastnosti se říká zaměnitelnost (fungibility). Bitcoin zaměnitelnost nesplňuje, protože transakce uložené v blockchainu na sebe transparentně navazují a cesta konkrétní mince může být vystopovatelná od jejího vytěžení až po současného majitele, resp. jeho adresu. Z adresy samotné majitele nepoznáme, ale budeme-li ho znát jinak, můžeme do jisté míry stopovat i jeho ostatní transakce. Tomuto stupni anonymity se někdy říká „pseudonymita“. Od čisté měny bychom zaměnitelnost měli jako uživatelé požadovat. Jinak nám při placení v hokynářství hrozí, že zpět dostaneme mince poznamenané ilegálním obchodem, a návštěva policie nás jistě nepotěší. Naopak od platformy, která využívá toho, že mince lze nějak označovat – barvit – a tím jim dávat nový význam, zaměnitelnost požadovat nemůžeme. Takové barevné mince, digitální tokeny, mohou reprezentovat např. nějaké fyzické nebo i digitální vlastnictví, tzv. „smart property“.

Dále nás zajímá, jaká je monetární strategie měny. Ta je většinou deterministická – jednoznačná a známá dopředu. Může být konečně inflační, jako např. u Bitcoinu, kde se ví, kolik mincí kdy existuje a že maximálně jich bude 21 milionů, nikdy víc. Může být i nekonečně inflační se známým tempem uvolňování mincí nových, jako např. u Monera. Důležitá je i prvotní distribuce mincí. Ta může vycházet z klasické těžby od okamžiku nulové peněžní zásoby, jako u Bitcoinu. Nebo těžba nemusí vůbec existovat a při uveřejnění měny je vydáno i určité množství jejích mincí, jako

např. u Ripple. Případně něco mezi, kdy jsou nové mince tvořeny těžbou, ale ještě před uveřejněním měny ji po nějakou dobu těžil jen autorský tým. Této strategii se říká premine (předtěžba) a v kryptokomunitě není příliš populární. Nicméně i taková měna se může v okamžiku uveřejnění nějak redistribuovat uživatelům, jako v případě projektu AuroraCoin, jehož vznik byl motivovaný kolapsem bankovního systému na Islandu. U projektů financovaných modelem typu ICO nakupují investoři mince v předprodeji a jejich vlastnictví se před spuštěním SW zanese do genesis bloku. Nebo je projekt financován tak, že z každého vytěženého bloku jde určitá část nových mincí autorům, jako např. u Zcash. A jistě bychom identifikovali i další možnosti.

Velmi důležitá odlišnost kryptoměn je ve strategii konsensu (shody) na stavu, resp. zápisu do **ledgeru** (konkrétněji blockchainu). Zápisem do ledgeru se potvrzují transakce, takže to má vliv i na jejich rychlost. Je potřeba vědět, kdo a kdy může zapisovat (konkrétněji vytvořit nový blok). O to se může starat opět klasická těžba pomocí proof-of-work, kdy v procesu tvorby dalšího bloku je zvýhodněn ten, kdo vykoná víc práce za jednotku času. V tomto modelu je konkurenční výhodou silnější HW a vyznačuje se velkou spotřebou energie na „zbytečné" výpočty. Ony však zbytečné nejsou, protože jejich účelem je právě docílit konsensu na stavu ledgeru. Některé altcoiny je zároveň využívají i jinak, např. koproduktem při těžbě Primecoinu je hledání vysokých prvočísel. Konsensus pomocí proof-of-work je stochasticky napadnutelný při systematickém vynakládání úsilí odpovídajícího nadpolovičnímu výpočetnímu výkonu sítě (tzv. „51% útok"). Je tomu tak proto, že takový výkon dokáže v konečném čase přepočítat libovolně dlouhou část blockchainu a nahradit ji nějakou vlastní, ještě delší.

Ledger
viz **Bitcoin**

Kdo drží, má za tři

Alternativou k modelu proof-of-work (PoW) je proof-of-stake (PoS). V něm není zvýhodněn majitel silnějšího HW, nýbrž držitel většího množství stávajících mincí. Existuje více variant, které

dále zohledňují dobu jejich držení apod. Držení mincí je jednoznačně dané obsahem ledgeru, takže nepotřebujeme žádnou umělou pomůcku při rozhodování o tvůrci dalšího bloku, jakou je např. práce na „zbytečné" výpočty. Mimochodem to znamená, že mezi bloky nemusí uplynout čas potřebný k vynaložení této práce, takže blockchain může narůstat rychleji, jakožto i potvrzování transakcí. Tvůrci bloku v PoS se neříká těžař, ale razič (forger, minter). První mince mohou vzniknout arbitrární distribucí nebo pomocí PoW a na PoS se přechází až časem. PoW a PoS lze různě modifikovat a kombinovat do hybridních strategií i po celou dobu života měny – prokládat více bloků vytěžených pomocí PoS blokem vytěženým PoWem (případně jinak zajistit větší zabezpečení) atd. Oproti těžařům v PoW mají raziči v PoS větší zájem na ochraně měny, neboť ji vlastní, což bude mít dopad i na kvalitu generovaných bloků a absenci motivace na síť útočit.

Avšak jako obyčejně, když něčeho existuje víc než jedno, i PoS má svoje nevýhody. Především je to obtížnější řešení situace, kdy se blockchain rozvětví (fork). Dokonce i jeden razič může vytvářet nové bloky nad více řetězy, protože mince má v obou. Vlivem malých nákladů na tvorbu bloku nastane taková situace snáze než u PoW. V současnosti se ale zkoumají metody, jak to řešit. Přesněji, jak konsensuálně trestat raziče, který se takto chová. Je k tomu potřeba dívat se nejen na nejdelší řetěz bloků. Konkrétně kryptoměna Ethereum přišla v roce 2014 s návrhem algoritmu Slasher a později Casper, ale to už zacházíme do přílišných technikálií. Kromě Etherea, které s PoS koketuje, ho využívá např. Peercoin, Nxt a částečně Dash. K těmto altcoinům se však ještě dostaneme podrobněji dále.

Máme tedy základní představu o prostoru vlastností, kterými se jednotlivé kryptoměny od sebe liší. A to jsme vůbec nezmiňovali nastavení parametrů konkrétních algoritmů a modelů, jakými je např. doba mezi bloky, velikost bloku, typ hashovací funkce aj. Vidíme tedy, že prostor je poměrně velký a už nás možná tolik nepřekvapuje, kolik altcoinů existuje. Jejich svět je vlastně příkladem decentralizované diverzifikace v praxi. S tímto úvodem se můžeme pustit do podrobnějšího popisu některých vybraných nejznámějších. Pojďme se tedy chvíli zabývat tvrdými fakty o konkrétních altcoinech.

Čeříme s Ripple

Ripple je spíš real-timový platební a zúčtovací systém než příklad klasické kryptoměny. Historie jeho vývoje sahá dokonce hlouběji než u Bitcoinu a i jeho popularita vyjádřená cenou v roce 2017 strmě narostla, takže dává smysl věnovat mu několik odstavců. Systémy podobné Ripplu jsou na národní úrovni typicky provozovány centrální bankou. Ripple byl vyvíjen od roku 2004 pod názvem Ripplepay. Motivací k jeho vývoji bylo vytvořit decentralizovaný systém, ve kterém by si uživatelé mohli vytvářet a vyměňovat vlastní peníze a dluhy (jakoby elektronické směnky). Nyní je Ripple vyvíjen stejnojmennou společností, kterou roku 2011 založil Jed McCaleb (neobyčejně produktivní autor p2p výměnné sítě eDonkey, zakladatel burzy Mt.Gox a pozdější konkurenční platební sítě Stellar s tokeny lumens (XLM)). Roku 2012 byla založena společnost OpenCoin (později Ripple Labs), která vyvíjí protokol Ripplu (RTXP) na základě původního konceptu Ripplepay.

Transakce v Ripplu se nepotvrzují těžbou, ale na základě konsensu důvěryhodných uzlů (tzv. „proof-of-correctness“). Tento proces je rychlejší a nespotřebovává tolik výpočetního výkonu, leč musí spoléhat na důvěryhodnost (uživatelem vybraných) uzlů, takže není trustless jako Bitcoin. Naopak zjevnou výhodou je perioda bloku v řádu jednotek sekund. Síť spravuje sdílený ledger – decentralizovanou databázi Ripple účtů, která kromě vlastní měny obsahuje i nabídky a poptávky jiných aktiv. Jeho součástí je tedy i jakási decentralizovaná burza. Ripple ledgerů může existovat více, obdobně jako může existovat více blockchainů. Obsah ledgeru (jeho poslední stav) je určen shodou alespoň 80 % uzlů. Transakce je návrh na změnu ledgeru, a pokud se uzly neshodnou na všech transakcích, sporné se vyřadí a cyklus konsensu se opakuje do okamžiku, než se na novém obsahu shodne potřebná většina.

Výchozí ledger založený společností Ripple obsahuje od svého vzniku fixní počet 100 miliard jednotek vlastní kryptoměny – tokenů s označením XRP. 20 % z tohoto množství si ponechali zakladatelé, 80 % získalo Ripple Labs. Část zásoby se postupně rozdala různým neziskovým organizacím a jednotlivcům v rámci propagace systému. Dělitelnost měny je na 6 dekadických řádů, nejmenší jednotka se nazývá drop (1 XRP = 1 000 000 drops).

XRP se používá i k placení malých transakčních poplatků, které chrání síť před spamováním (navíc každý Ripple účet musí držet alespoň 20 XRP). Kromě XRP obsahuje Ripple síť tokeny pro různé další druhy aktiv – konvenční měny, kryptoměny, komodity atd. Pro převod XRP na BTC existují tzv. Bitcoin Bridge (jeden z nich provozuje bitcoinová burza Bitstamp). XRP se v rámci sítě převádí kryptograficky bezpečně a reálně. Při převodu ostatních aktiv se do ledgeru ukládá podepsaný „dlužní úpis", takže reálné vypořádání vyžaduje důvěryhodnost stran. Pokud neexistuje přímá důvěra mezi obchodujícími subjekty, hledá se v síti cesta, která důvěryhodnost zprostředkuje. Tento proces se nazývá rippling (čeření) a dal systému jméno. Na konkrétní nalezené cestě pak závisí transakční poplatky, případně i možnost mezipřevodu měn.

Ripple je vlastně decentralizovaná platební síť pro digitální tokeny nejednoho druhu, v tom trochu připomíná Lightning Network, ale Ripple je založený na důvěryhodnosti uzlů mezi sebou. To se řadě lidí líbí, a tak od roku 2013 oslovuje hlavně sektor finančních institucí. Od roku 2014 začaly Ripple protokol využívat první banky (jako úplně první německý Fidor). Ripple je decentralizovaný z hlediska topologie sítě, ale z hlediska vývoje a určování pravidel jde o systém centralizovaný kolem společnosti Ripple. A to je proregulační společnost, která slyší na požadavky centrálních autorit o nutnosti lepší monitorovatelnosti transakcí (záminky všichni známe – zbraně, drogy, dětská pornografie – ale zde postačí i „suspicious or unusual activity", jež vystupuje v odůvodnění funkcionality „Balance Freeze" přidané 1. 8. 2014). V centralizovaném prostředí to ani jinak být nemůže, protože kdyby Ripple nespolupracovala, těžko by s ní banky chtěly mít něco společného a stát by si na Ripple rychle posvítil. Zejména proto není Ripple příliš populární u ortodoxních kryptoanarchistů a jiných cypherpunkerů.

Klasické deriváty – Namecoin, Litecoin, Peercoin

Najděte slovo a přidejte za něj „coin". Tyto tři altcoiny jsou typickými představiteli klasických derivátů Bitcoinu. Namecoin (NMC) je první altcoin vůbec a byl představen již 18. 4. 2011.

Parametricky (počet mincí, perioda bloku, algoritmus hashe) je totožný s Bitcoinem. Adresy jeho peněženek začínají na „N" nebo „M", abychom je snadno odlišili od adres pro BTC. Namecoin je prvním využitím blockchainu bitcoinového typu jakožto platformy pro jinou aplikaci, než je (pouze) měna. Umí totiž do svých bloků ukládat data. Přesněji záznamy dvojic klíč (resp. namespace/name) a hodnota (max. 520 B). Za registraci záznamu se platí 0,01 NMC, které se obarví speciální namecoinovou operací. Není to však poplatek těžaři, na rozdíl od běžného poplatku za transakci, která registraci nese. Tyto mince se poté už nepoužívají k placení, nýbrž k případnému převodu vlastnictví datového záznamu s příslušejícím klíčem. Je to vlastně první implementace smart property nad blockchainem.

K čemu je to dobré? Taková decentralizovaná databáze jmenných záznamů může mít řadu aplikací: registr identit (viz NameID), adresářové služby, časová razítka, posílání zpráv apod. Hlavní aplikace Namecoinu je ovšem decentralizované DNS (překlad alfanumerických názvů počítačů v internetu na číselné IP adresy, např. seznam.cz na 77.75.77.53). Toto DNS spravuje názvy počítačů v top-level doméně .bit a díky své povaze nepodléhá centrální DNS autoritě ICANN. Můžete si tak zaregistrovat např. doménu kinderporno.bit, kde budete provozovat květinářství či obchod se zvířátky (pro překvapené explicitně podotýkáme, že jde o paralelu s českým webem úmyslně šokujícího názvu kinderporno.cz, zaměřeným proti cenzuře internetu). Jakmile takovou namecoinovou doménu vlastníte, nikdo vám ji z povahy decentralizovaného blockchainu nemůže vzít. Leda byste ji zapomněli prodloužit, což je třeba učinit každých 250 dnů (resp. 36 000 bloků) pomocí jiné speciální operace. Existují dokonce komerční registrátoři domén .bit, kteří interakci s Namecoinem provedou za vás (např. dotbit.me nebo peername.com). Za povšimnutí stojí také to, že Namecoin se dá těžit současně s Bitcoinem jedním výpočtem pomocí techniky zvané „**merged mining**". Přestože dnes Namecoin nepatří mezi nejviditelnější altcoiny, historicky sehrál důležitou roli. Byl první a přišel s první nepeněžní aplikací.

Asi vůbec nejznámějším derivátem Bitcoinu je Litecoin (LTC). Litecoin byl představen 7. 10. 2011 a jeho autorem je Charlie Lee, tehdejší programátor Googlu. Jak název napovídá, jedná se o odlehčený klon Bitcoinu, navržený původně pro mikroplatby. Jeho

odlehčenost spočívá v tom, že generuje 4× rychlejší bloky (perioda cca 2,5 minuty), má 4× víc mincí (84 000 000) a je přizpůsoben k těžbě na slabším HW. Toho bylo docíleno volbou jiného hashovacího algoritmu, konkrétně algoritmu scrypt místo SHA-256 použitém v Bitcoinu. Scrypt se totiž hůř paralelizuje, neboť používá techniku tzv. „key stretching", kdy se výstup hashovací funkce mnohokrát za sebou vrací zpět na vstup. Navíc je paměťově náročnější. V důsledku toho zůstala těžba Litecoinu delší dobu na procesorech a grafických kartách než u Bitcoinu.

Merged Mining

technika umožňující současnou **těžbu** dvou **blockchainů**. Funguje tak, že těžený **blok** primárního **blockchainu** (např. **Bitcoinu**) obsahuje v datech (v coinbase txin skriptu) **hash** těženého **bloku** sekundárního **blockchainu** (např. Namecoinu). Když se **blok** primárního chainu najde, je to dostatečný důkaz vynaloženého úsilí i pro sekundární chain. **Merged mining** vyžaduje podporu jen u sekundárního **blockchainu**. Primární **blockchain** neví, že se této techniky účastní, a proto se od něj žádná speciální podpora nevyžaduje.

Litecoin používá adresy peněženek s prefixem „L" nebo „M", již od května 2017 má aktivní segwit, a je tudíž o něco napřed i v implementaci Lightning Network. V tomto ohledu je Litecoin využíván trochu jako předvoj velkých změn v Bitcoinu. Navíc v době vysokých transakčních poplatků začala řada obchodů jako alternativu k Bitcoinu přijímat právě Litecoin. Často slýcháme přirovnání, že Litecoin se má k Bitcoinu stejně, jako se má stříbro ke zlatu – Litecoin je takové „digitální stříbro".

Klasických derivátů je celá řada, zmiňme ještě alespoň Peercoin (PPCoin, PPC), jenž byl uvolněn v srpnu 2012. Jeho autory jsou Scott Nadal a Sunny King (taktéž autor Primecoinu). Na tomto altcoinu je zajímavé, že jako první používá proof-of-stake, resp. kombinaci proof-of-stake a proof-of-work. Jeho měna PPC je nekonečně inflační s inflací 1 % ročně a zároveň s deflací za fixní transakční poplatky (0,01 PPC/kB), které nezískávají těžaři (v proof-of-stake nejsou), ale ničí se. Peercoin používá adresy začínající na „P". Jeho hlavním nedostatkem je centralizující prvek v podobě autorem podepisovaných značek blockchainu. Dle staršího vyjádření vývojářů se pracuje na decentralizovaném řešení. Uvidíme, jestli se Peercoin ještě vrátí do popředí zájmu, ale v současné konkurenci to bude mít těžké.

Je libo anonymitu?

Říkali jsme si, že Bitcoin nesplňuje vlastnost zaměnitelnosti (fungibility). Mince nejsou zcela zaměnitelné, protože každá má svoji vlastní transakční historii. To je řečeno trochu zjednodušeně. Transakce uložené v blockchainu na sebe sice navazují, ale jejich obsahem nejsou konkrétní „mince", nýbrž konkrétní hodnoty vstupů do a výstupů z transakce. Vstupů i výstupů transakce může být více, ale také nemusí. Představme si, že známý těžař vytěží 50 BTC – objeví se v generující transakci. V další transakci rozešle těchto 50 BTC rovným dílem pěti lidem včetně pana Hladovce. Taková transakce bude mít jeden vstup o 50 BTC a pět výstupů po 10 BTC. Hladovec si u pekaře koupí housku za 1 BTC. Zaplatí transakcí, která na vstupu použije jím ovládaný výstup s 10 BTC, a ten rozdělí mezi dva nové výstupy – 1 BTC na adresu pekaře a 9 pošle zpět na svoji (výstup se konzumuje vždy celý). Pekař teď ovládá výstup s 1 BTC. Když se na něj podívá do blockchainu, zjistí, že je součástí transakce s jedním vstupem o 10 BTC. Pohledem na tento vstup zjistí, že odkazuje na výstup z transakce s jedním vstupem o hodnotě 50 BTC a pěti výstupy po 10 BTC. A postoupí-li ještě o krok zpět, zjistí, že vstup 50 BTC odkazuje na výstup z generující transakce známého těžaře. Pekař tedy mohl vystopovat cestu svého bitcoinu až po jeho vytěžení.

Takové stopování bylo jednoduché, protože po cestě byly jen transakce s jedním vstupem. Stačilo tedy postupovat po nich zpět směrem ke generující transakci. Transakce ale často mívají vstupů vícero. Pokud by si Hladovec nekupoval housku, ale celou pekárnu za 5000 BTC, platil by nejspíš transakcí se spoustou vstupů. Ty by odkazovaly na spoustu výstupů z jiných transakcí, kterými zase jiní platili v minulosti Hladovcovi. To by stopování značně zkomplikovalo, poněvadž bychom nevěděli, po jakém vstupu se vydat, a museli bychom nahlížet do všech. Čím více by byly cesty mincí takto spojovány a opět rozdělovány – čím více by byly v transakcích „promixovány" mezi sebou, tím hůře by se nám stopování provádělo. Ne, že by to nešlo vůbec, protože odkazy mezi vstupy a výstupy by existovaly stále, ale už bychom nemohli říct, že si Hladovec koupil housku nebo pekárnu za mince toho či onoho – koupil si je trochu za mince od toho a trochu od tamtoho. Při určitém stupni promixování bychom mohli říct už jen toliko, že

si to koupil trochu za mince od všech. Na tomto principu fungují již dříve zmíněné mixéry (tumblery) – služba třetí strany, kam pošlete své bitcoiny a ony se promixují s bitcoiny jiných uživatelů. Je to ovšem pouze jednorázové promixování a musíte důvěřovat provozovateli mixéru, že vám peníze vůbec pošle zpátky. Nešlo by to nějak lépe, třeba uvnitř samotné kryptoměny?

CryptoNote není vidět

V roce 2012 vznikl protokol CryptoNote. Není to název kryptoměny; je to popis, jak kryptoměnu implementovat. CryptoNote řeší výše popsaný problém Bitcoinu s vystopovatelností (traceability) transakcí. Integruje totiž bitcoinový mixér přímo do sebe. U klasického mixéru je potřeba kooperace všech, aby poskytli své podepsané výstupy do společné mixovací transakce. CryptoNote na to jde mazaně – v transakci lze použít i cizí výstupy! Jak ale předejít tomu, aby bylo možné se na jejich úkor obohatit? CryptoNote umožňuje vytvořit skupinu výstupů se stejnou hodnotou a každému disponentovi původních výstupů dovolit z této skupiny utratit onu hodnotu právě jednou. Používá se k tomu tzv. „ring signatures" – kryptografická technika, která dovoluje digitálně podepsat kýmkoliv ze skupiny. Z podpisu se ovšem nedá zjistit, kdo to byl. Stačí tedy v blockchainu najít stejně velké výstupy, jako je ten váš, vytvořit z nich tuto skupinu a hodnotu svého výstupu utratit svým podpisem. Detektiv pátrající v blockchainu pak neví, kdo z disponentů těchto výstupů takovou operaci provedl. A ostatní disponenti, kteří vůbec netuší, co se to s jejich výstupy bez jejich vědomí stalo, nemusí panikařit – na každého z nich čeká v této skupině „částečně utracených promixovaných výstupů" právě jedna možnost podepsat a utratit tak i svoji původní hodnotu.

Jenže jak najdu existující výstupy s hodnotou na chlup stejnou, jako má ten můj – co když takové ani neexistují? V CryptoNotu jsou hodnoty transakcí automaticky rozdělovány do menších denominací s logaritmickým odstupňováním, podobně jako u klasických peněz – 5, 10, 20… Kč. Existuje tedy velký výběr cizích mincí, se kterými můžete promíchat ty své. Celé si to lze představit tak, že s náhodně zvolenými skupinami uživatelů dáte na hromadu pětikoruny, desetikoruny, dvacky… a při placení si

z nich vezmete náhodné mince ve výši vašeho vkladu. Je jasné, že transakční historie se rozpadla. Ovšem musí to dělat všichni, jinak vám hrozí, že ačkoliv sami se budete snažit svoje platby anonymizovat, někdo jiný to neudělá a pošle vám peníze zkažené. Proto je vhodné vynucovat nějakou minimální velikost skupiny pro mixování („ring size" nebo „mixin"), což některé implementace dělají (např. Monero přešlo z velikosti 2 na 4).

Ale to není všechno, co CryptoNote nabízí. Výše popsané je vlastně zabudovaný mixér na vstupu transakce, který umožňuje skrývat adresu odesílatele platby. CryptoNote umí skrývat i adresu příjemce. V Bitcoinu má uživatel adresu, kam si nechává posílat platby. V rámci jedné peněženky může mít adres i několik a organizovat si je třeba podle druhu plateb. Dokonce mu nic nebrání vygenerovat si novou adresu pro každou jednotlivou platbu. Pokud bude naopak používat pro všechny platby adresu stejnou, je to sice pohodlnější, ale na úkor anonymity. Dojde-li nějakým způsobem ke spárování takové adresy a identity uživatele, např. jeden obchodní partner to rozhlásí, je zřejmé, že i ostatní platby z/na tuto adresu souvisí s tímto uživatelem. Paranoidní jedinci tedy generují jednorázové adresy pro každou platbu (ono je to i špetku bezpečnější, jelikož nenecháváte peníze na adresách, od kterých jste už v nějaké dřívější transakci odhalili svůj veřejný klíč). V CryptoNotu není potřeba jednorázové adresy generovat ručně, protože se to děje automaticky.

CryptoNote tedy řeší i tento problém s provázáním plateb přes adresu příjemce (linkability). Používá k tomu techniku tzv. „stealth addresses". Jde o to, že k jednomu soukromému klíči (tomu, co umožňuje peníze utrácet = vybírat) může existovat více klíčů veřejných (toho, co umožňuje peníze přijímat = vkládat). A to aniž by byla tato asociace navenek vidět. V CryptoNotu mají oba klíče dvě části – spend a view. Jistými kryptografickými operacemi s nimi se dá docílit toho, že odesílatelům plateb sice stačí znát jeden veřejný klíč příjemce, ale v každé transakci na něj aplikují ještě jiný, náhodný klíč, jehož veřejná část je součástí transakce. Pouze držitel soukromého view klíče (příjemce platby) pak může takové platby identifikovat jako jemu určené. Blockchainový detektiv vidí takové platby jako adresované pokaždé jinam a opět nic nevypátrá. Navíc tím odesílatel získal možnost prokázat, že zaplatil, neboť on jediný zná soukromou část náhodného

klíče, jenž posloužil k vygenerování stealth adresy použité v dané transakci. Líbí se vám CryptoNote? Vše výše popsané ani nemusíte jako uživatel znát. Prostě jen platíte a přijímáte platby, podobně jako jste zvyklí u Bitcoinu.

CryptoNote je vidět, když chce

Kryptoměna implementovaná podle CryptoNotu je tedy opravdu hodně anonymní a splňuje vlastnost zaměnitelnosti. Ale není té anonymity příliš? Co kdybych přece jen chtěl s někým svoje transakce sdílet, např. založit transparentní účet? Není problém, odhalíte svůj soukromý view key. Ten sice umožní ostatním příchozí platby vidět, ale k utrácení peněz z účtu je třeba soukromý spend key a ten si ponecháte v utajení. A kdyby nestačilo vidět příchozí platby a bylo nutné odhalit všechny pohyby na účtu, i odchozí, a mít tak možnost dopočítávat zůstatky, např. pro účely auditu? I na to existuje řešení, ačkoliv vlivem možnosti mixovat výstupy na vstupech je to výpočetně složitější. Pomocí soukromého spend key je potřeba vypočítat tzv. „key images" pro každou transakci nad zmixovaným výstupem a ty dát k dispozici auditorovi. Ten potom vidí i dovnitř částečně utracených výstupů a dokáže tak rozlišit, jestli byl daný výstup adresovaný účtu již účtem utracen, či nikoliv. Toto „jemnější nastavení práv" – vkládat, vybírat; vidět příjmy, vidět výdaje – je důsledkem rozdělení klíčů na dvě části (spend a view). V Bitcoinu máme 2 klíče a dvě operace – vkládat (znám veřejný klíč, potažmo adresu) a vybírat (znám soukromý klíč). Příjmy i výdaje vidí každý. V CryptoNotu máme 2 × 2 klíče a čtyři operace. Co z toho komu umožníme dělat, je jen na nás. Můžeme využít vysokou míru anonymity, kterou nám CryptoNote nabízí, ale můžeme být i transparentní, auditovatelní a řádnými plátci daní, když na to přijde.

Ještě dodejme, že obě myšlenky na posílení anonymity – ring signatures i stealth addresses – zmiňuje už Satoshi v srpnu 2010 na webovém fóru bitcointalk.org. Přesněji místo ring signatures Satoshi navrhuje použít group signatures, což je podobný koncept, který se liší v detailech, jimiž vás už nebudeme unavovat. Místo stealth addresses pracuje Satoshi s pojmem „blinded key", ale princip je opět stejný. Ať je to kdokoliv, je to zkrátka hlava pomazaná, ten Satoshi.

Takhle vypadá CryptoNote epesně, takže co nevýhody? Přece jen jsou, ačkoliv se dají unést. Předně připomeňme, že mince s rozpadlou transakční historií už nelze barvit. Ale to jsme přece chtěli, jinak bychom neměli zaměnitelnost. Takže tohle je spíš vlastnost než nevýhoda. Za největší skutečnou nevýhodu můžeme považovat to, že pokud by někdy v libovolně vzdálené budoucnosti došlo ke kryptografickému prolomení ring signatures (např. pomocí kvantových počítačů), znamenalo by to deanonymizaci kompletně celé historie transakcí. S vědomím tohoto rizika je potřeba ke CryptoNotu přistupovat. Další menší nevýhoda spočívá v tom, že transakce nelze generovat offline (v Bitcoinu toto lze). Potřebujeme totiž vědět, jak se s našimi výstupy nakládalo do současnosti – zdali je někdo nepoužil při mixování svých mincí, což může udělat kdokoliv a kdykoliv. V neposlední řadě je potřeba zmínit i to, že kryptoměna implementující CryptoNote je výpočetně náročnější než Bitcoin a datová reprezentace transakcí je díky mixování větší.

CryptoNote v praxi – Bytecoin, Monero

První kryptoměna založená na protokolu CryptoNote je Bytecoin (BCN). Bytecoin tedy není derivátem, resp. vývojovou větví Bitcoinu, je to zbrusu nová implementace. Byl spuštěn v červenci 2012, lépe řečeno měl být. V kryptokomunitě totiž panují dohady o tom, jestli spuštění Bytecoinu nebylo antedatováno, aby tím jeho autoři získali výhodu v podobě neviditelného preminu (předtěžby), jenž měl dosáhnout 82 % celkové emise. A jak už jsme psali, na preminy je komunita citlivá. Navíc byl jeho raný vývoj možná příliš anonymní i na poměry kryptoměn. Hypotéza spiknutí jde tak daleko, že operuje i se zakrytím preminu autory CryptoNotu, a sice antedatací jejich white paperu. A s white paperem CryptoNotu skutečně není něco v pořádku, neboť verze 1 z roku 2012 obsahuje v citacích odkaz na diskuzní vlákno založené až v květnu 2013. Jenže to samo o sobě ještě nedokazuje premine Bytecoinu. Situace by vyžadovala důkladnější rozbor.

Osobně si vybavujeme, že altcoin s tímto názvem a logem jsme zaregistrovali poměrně brzy, kdy ještě moc altcoinů neexistovalo; mohlo to být někdy kolem přelomu let 2012 a 2013. Každopádně Bytecoin obestřela dezinformační exploze a asi i to ho drželo delší dobu v pozadí. Což je škoda. V druhé polovině roku 2017 jeho

tržní kapitalizace výrazně vzrostla a toho času se pohyboval na žebříčku kryptoměn kolem 30. místa. Bytecoin je konečně inflační se stropem 184,470,000,000 BCN, má periodu bloku 2 minuty a používá proof-of-work s hashovacím algoritmem CryptoNight. Ten je paměťově náročný, čímž úmyslně zhoršuje možnost paralelizace výpočtu a upřednostňuje těžbu na procesorech a grafických kartách. Bytecoin byl původně implementován v jazyce Java, ale v roce 2013 byl přepsán do C++. Jeho zdrojové kódy jsou základem pro mnoho dalších měn implementujících CryptoNote, např. DarkNote, Dashcoin (neplést s Dash) nebo asi nejznámější současný představitel CryptoNote měn, Monero.

Monero (XMR) vzniklo 18. 4. 2014 pod původním názvem BitMonero, který byl krátce po představení zkrácen do současné podoby. Je odvětveno z Bytecoinu a vyznačuje se velmi aktivním vývojem s častými hardforky. Na rozdíl od Bytecoinu je nekonečně inflační, s inflací klesající k nule ve dvou fázích. Do roku 2022 bude uvolněno 18,4 milionů XMR a poté nastane fáze postupně klesající inflace menší než 1 % ročně. XMR je dělitelné na 12 dekadických řádů (Bitcoin na 8), pro označení menších a větších jednotek se používají předpony SI, takže nejmenší jednotkou je piconero, největší meganero. Poplatek za transakci se snižuje v závislosti na počtu transakcí za jednotku času (ačkoliv za všechny v součtu se zvyšuje). Velikost bloku není fixní, nýbrž adaptivní – z posledních 100 bloků se počítá medián velikosti a další bloky pak mohou být o něco větší.

Monero dále ještě rozšiřuje anonymizační schopnosti CryptoNotu. V něm sice není vidět odesílatel ani příjemce platby, stále ale je vidět placená částka, resp. hodnoty jednotlivých vstupů a výstupů transakce. Na první pohled by se mohlo zdát, že toto vidět musíme, aby byla kontrola, že nikdo nepadělá nové mince. Nám by ale stačilo vědět, že součet hodnot vstupů do transakce je roven součtu hodnot výstupů z ní (ev. plus poplatek za transakci). A skutečně existuje možnost, jak dokázat pouze platnost této rovnice, aniž bychom přitom museli odhalovat její členy. Příslušná technika se jmenuje „Confidential Transactions" a přišel s ní Core vývojář Greg Maxwell. Podepisuje se přitom tzv. „Pedersen Commitment". Podepisování transakcí u Monera funguje jinak než u Bitcoinu, kvůli mixování vstupů. Výzkumníci Monera ale objevili způsob, jak se jimi používané ring signatures dají zkombinovat s Confidential Transactions a výsledné schéma, tzv. ringCT („Ring Confidential

Transactions“), do své měny začátkem roku 2017 implementovali. V Moneru tedy není vidět vůbec nic – kdo, komu, ani kolik se platilo!

Kouzla s anonymitou

CryptoNote a jeho deriváty nám ukazují, jak anonymizovat kryptoměnu. Přístup se zabudováním mixéru do samotných transakcí však není jediná možnost, jak zaměnitelnosti mincí docílit. Trochu jiným způsobem k tomu přistupuje protokol s názvem Zerocoin, jehož vznik se datuje do začátku roku 2013. Připomeňme si, že v Bitcoinu se oprávnění disponovat mincemi na výstupu nějaké transakce prokazuje digitálním **podpisem**, který umí vygenerovat pouze jejich držitel. Ten pak na základě toho může rozhodnout, co se s nimi dál stane. U Bitcoinu s těmito konkrétními, u CryptoNotu s mincemi odebranými z větší hromady, kterou zformovalo víc uživatelů. Čím víc uživatelů a větší hromada, tím větší anonymita a zaměnitelnost. Proč tedy neudělat jednu velkou hromadu pro všechny uživatele? A přesně to dělá Zerocoin.

Podpis (Signature)
viz **Asymetrická kryptografie**

Zerocoin je postaven na tzv. „zero-knowledge proofs“ (ZKP). Je to kryptografická technika, jak dokázat pravdivost nějakého tvrzení, aniž by přitom byla odhalena jakákoliv další informace. Možná se budete divit, ale toto lze. Vlastně to každý známe třeba z kouzelnického vystoupení. Pokud před vašimi zraky vytáhne kouzelník z balíčku karet desetkrát za sebou tu správnou, aniž by viděl jejich líc, je to vlastně zero-knowledge důkaz o tom, že se ve svých kartách vyzná i jinak než podle jejich lícové strany. Jak to dělá, si ale nechává pro sebe – neodhaluje žádnou další informaci kromě té, že to umí. A co kdybychom obdobně uměli dokazovat, že jsme oprávněni disponovat nějakými penězi, aniž by bylo odhaleno, které konkrétní to mají být? Tak pracuje Zerocoin! Můžete si to představit tak, že ty konkrétní peníze zničíte, ale umíte dokázat, že jste to udělali. Až je budete potřebovat, ostatní vás nechají vyrobit si nové ve stejné výši. Nové peníze ale budou mít čistou transakční historii, a o to nám jde.

Protokol Zerocoinu je navržen jako rozšíření Bitcoinu. Obsahuje tzv. akumulátor, kde se hromadí „zničené“ mince. Jde vlastně o bitcoiny, které chceme anonymizovat. V akumulátoru z nich vznikají nově vytěžené zerocoiny, které teprve čekají na své použití někým, kdo se v tomto procesu svých bitcoinů zbavil. Na rozdíl od CryptoNotu, kde dochází k promíchání mincí „pouze“ několika uživatelů, v akumulátoru se vlastně míchají mince všech. Stejně jako u CryptoNotu, i zde je nutné dělit hodnoty transakcí do menších denominací, aby anonymizace mohla fungovat. Zde to však může být slabina, pokud v akumulátoru současně existuje pouze malé množství stejných denominací. Anonymizace Zerocoinem totiž není povinná; je to možnost, které uživatelé mohou, ale nemusí využít. Do Bitcoinu se toto rozšíření (zatím) nedostalo, a tak vznikly samostatné blockchainy na bázi Bitcoinu, které protokol Zerocoinu implementují. První a nejznámější z nich je Zcoin (XZC). Mezi další měny s tímto rozšířením patří např. Anoncoin (ANC), SmartCash (SMART) nebo PIVX.

Kromě slabiny s rozdělením zerocoinů do menších denominací, což omezuje míchací potenciál akumulátoru, je nepříjemnou vlastností Zerocoinu velikost transakcí. Vlivem toho, že při utrácení mincí se pomocí ZKP pracuje s celým akumulátorem (terminologií CryptoNotu jakoby maximální možný mixin), i výsledná transakce je patřičně velká. Obyčejná transakce může mít třeba 30 kB, což je cca 100× víc než u Bitcoinu. To je nepříjemné pro její ověřování i pro velikost blockchainu. I z hlediska výpočetní náročnosti je Zerocoin několikrát žádostivější než Bitcoin. Chtělo by to ještě nějaké kouzlo.

Od Zerocoin k Zerocash

Některé nevýhody Zerocoinu odstraňuje jeho nástupce Zerocash, představený na konci roku 2013. Tento protokol není koncipován jako rozšíření Bitcoinu, ale jako samostatný blockchain. Nepotřebuje tedy převádět základní minci na anonymizovanou a naopak. Také už není nutné používat v implementaci fixní množinu denominací. Zerocash umožňuje, podobně jako Monero, navíc skrývat i výši transakce (resp. hodnoty vstupů a výstupů). Jeho transakce zabírají mnohem méně místa než transakce v Zerocoinu – velikost obyčejné transakce je řádově 1 kB. Zároveň se dají rychleji ověřovat. Obojí je výborná zpráva pro

blockchain a těžaře. Horší to však mají uživatelé, protože transakce v Zerocashi jsou extrémně náročné na tvorbu, ještě víc než v Zerocoinu. Jsou k tomu třeba řádově gigabajty paměti a minuty procesorového času současných běžných počítačů. Implementace peněženek pro telefony a slabší zařízení je tedy problematická. Obecně je však lepší mít možnost transakce rychleji ověřovat i za cenu jejich pomalejší tvorby, neboť ověřování se dělá mnohokrát (každý, kdo kontroluje blockchain), kdežto tvorba pouze jednou.

Redukci bolestivé velikosti transakce umožnilo použití speciálního typu ZKP, který se nazývá zk-SNARKs. Tato kryptografie je však velmi složitá, což přináší i několik nevýhod. Předně má dopad na již zmíněnou výpočetní a paměťovou náročnost. Dále existuje jen málo lidí, kteří pořádně rozumí použité teorii. To znamená, že případné chyby nejen v implementaci nemusí být včas podchyceny. I kvůli skrývání výše transakce by se tak na nějaký sofistikovaný útok generující nové mince vůbec nemuselo přijít! To souvisí i s další nevýhodou Zerocashe.

Před samotným začátkem používání takové kryptoměny je nutné vygenerovat jisté parametry, z nich něco vypočítat, a poté je zaručeně zlikvidovat. Říká se tomu „trusted setup" a parametry k likvidaci se nazývají malebně „toxic waste" – toxický odpad. Pokud toxický odpad zůstane, je s jeho pomocí opět možno generovat neomezené množství nových mincí. V praxi se proto před spuštěním měny pořádá ceremoniál, kterého se účastní např. šest stran, a jeho účelem je minimalizovat pravděpodobnost setrvání toxického odpadu na světě. Jenže i seberituálnější spuštění tuto pravděpodobnost nesníží až na nulu. Ostatní kryptoměny takovou podmínkou netrpí. I Zerocoin lze implementovat bez trusted setupu.

První implementací Zerocashe je Zcash (ZEC), který byl spuštěn začátkem roku 2016. Ve výchozím stavu je u něj vypnuta anonymizační schopnost (použití tzv. „shielded pool"), zřejmě kvůli výpočetní náročnosti. Uživatel si ji může kdykoliv zapnout, ale jak už jsme říkali u Monera, dosažitelná úroveň anonymity závisí na tom, kolik lidí toto dělá. V akumulátoru se totiž mixují jen mince, jejichž uživatelé mají anonymizaci zapnutou. Čím méně jich bude, tím lépe se bude provádět např. časová analýza vstupů do a výstupů z akumulátoru, potažmo analýza plateb. Dobrá zpráva ale je, že pokud to

sami chcete (např. pro účely auditu), Zcash umí být transparentní (tzv. „transparent pool“). Jinou implementací Zerocashe je např. Komodo (KMD).

A co Dash?

Povídání o anonymních kryptoměnách ukončíme představením posledního vybraného zástupce, kterým je Dash (DASH). Ten totiž používá ještě trochu jiný způsob anonymizace. Dash vychází z Litecoinu a z hlediska vývoje a komunity kolem je jedním z vůbec nejaktivnějších altcoinů. Jeho historie sahá do ledna 2014, kdy byl spuštěn pod názvem XCoin (XCO). Po měsíci existence byl přejmenován na Darkcoin (DRK) – název, který lépe vystihoval jeho anonymizační sklony. Po dalším roce byl přejmenován na současný název Dash, jakožto portmanteau od slov digital a cash. Jeho autor Evan Duffield si je zřejmě vědom marketingové síly dobrého názvu a nebylo mu líto za účelem přejmenování „skoupit“ konkurenční anonymní kryptoměnu Dashcoin, postavenou na CryptoNotu. V decentralizovaném světě se ale skupuje obtížně, takže Duffield ve skutečnosti koupil jen přístup k webu a SW repozitáři projektu Dashcoin (DSH); jeho mince ale žije dále s vývojem kolem nového webu (dashcoin.info).

Dash přichází hned s několika inovacemi, které z něj dělají jakýsi decentralizovaný autonomní systém. Kromě toho, že používá hashovací algoritmus X11, nasazuje částečně i proof-of-stake. V síti Dashe existují kromě uživatelů a těžařů ještě tzv. master uzly (masternodes). K jejich založení je sice nutné pozastavit 1000 DASH jako základní ochranu před kompromitací uzlu, ale provozovatelé takových uzlů jsou na oplátku zvýhodněni za to, že zajišťují běh velkých uzlů infrastruktury. V rámci proof-of-stake jde totiž 45 % nových mincí právě jim. Dalších 45 % mincí jde v rámci klasického proof-of-work obyčejným těžařům. Zbylých 10 % mincí je určeno k financování vylepšení ekosystému. Končí v tzv. pokladnici (treasury), o jejímž využití rozhodují opět master uzly. Formou hlasování mohou prostředky z pokladnice přidělovat různým návrhům na vylepšení, které dodává komunita. Takový model je zdrojem kladné zpětné vazby pro růst užitné hodnoty kryptoměny.

Master uzly nabízejí něco navíc přímo i samotným uživatelům. Mohou pro ně realizovat rychlé platby, pokud se uživatel

rozhodne master uzlům důvěřovat. Transakce se pak považují za potvrzené již na základě konsensu master uzlů, a jen pokud ho nelze dosáhnout, čeká se na obvyklé potvrzení těžbou. Tato funkcionalita se nazývá InstantSend (instantní odeslání). A konečně – jak Dash anonymizuje? Pomocí druhé speciální funkcionality master uzlů s názvem PrivateSend (důvěrné odeslání), která je založená na technice zvané CoinJoin.

CoinJoin je opět variací na mixování mincí více uživatelů, podobně jako u CryptoNotu i Zerocoinu. CoinJoin však pracuje s aktuální nabídkou transakcí v síti a spojuje je do větších v reálném čase. Pokud v jedné transakci platí pan A panu B a současně ve druhé pan C panu D, po spojení těchto dvou transakcí do jedné se už nedá rozlišit, kdo přesně platí komu, pouze, že pánové A a C platí pánům B a D. Účastníků takto spojené transakce může být samozřejmě i více a k dosažení ještě lepší anonymity se opět pracuje jen s určitými denominacemi mincí. Výhodou tohoto přístupu je kromě jeho jednoduchosti to, že informace o tom, jaké transakce se spojují, není navždy zapsána do blockchainu, jak je tomu u CryptoNotu. Nevýhodou je naopak požadavek současné existence transakcí ostatních. Ke kompromitaci platícího může dojít i při vyjednávání o transakcích ke spojení, neboť zde je to síťová operace, jíž se účastní nejen počítač platícího uživatele. U Dashe jsou to právě master uzly, které toto zajišťují.

Vidíme tedy, že anonymizačních možností kryptoměn a jejich konkrétních implementací je mnoho. Každá má své výhody i nevýhody a žádná dosud známá není ve všem lepší než ostatní. Na uživateli, jeho potřebách a preferencích záleží, jakou kryptoměnu si oblíbí a jaké se naopak raději vyhne. Jsme teprve na začátku toho, co svět kryptoměn nabízí, ale už nyní můžeme pozorovat jeho velkou rozmanitost. Ta však zdaleka nesouvisí jen s možnostmi anonymizovat platby, čehož je i Dash dobrým příkladem. Jsou i další aspekty, které altcoiny rozvíjejí, a v dalších kapitolách se zaměříme právě na ně.

Virtuální mašina jménem Ethereum

Ačkoliv nejde primárně o kryptoměnu, nemůžeme si mezi vybranými zástupci altcoinů dovolit nezmínit projekt Ethereum s jeho druhým až třetím místem v pořadí tržní kapitalizace,

o které ke konci roku 2017 soupeří s platebním systémem Ripple. S nápadem na projekt Ethereum přišel koncem roku 2013 tehdy 19letý ruský programátor Vitalik Buterin. Yellow paper (technickou specifikaci) projektu sepsal spoluzakladatel a technický ředitel Gavin Wood (v lednu 2016 z projektu odešel). Tito lidé si všimli, že paradigma decentralizovaného blockchainu spolu s kryptograficky zabezpečenými transakcemi má obecnější využití, než je pouze kryptoměna. Koneckonců už v té době existovaly jiné aplikace nad Bitcoinem nebo vlastním blockchainem (z již zmíněných např. Namecoin). Zároveň je v dnešní době na vzestupu trend cloudových služeb, který přenáší výpočty mimo fyzický prostor uživatele. Ethereum postavilo svůj model na myšlence přesunu výpočtů do blockchainu. Začátkem roku 2014 byl projekt ohlášen a v červenci 2015 byla uvolněna první verze SW.

Ethereum je vlastně virtuální stroj (EVM – „Ethereum Virtual Machine"), globální decentralizovaný virtuální počítač pro obecné výpočty, tedy nejen pro převod digitálních tokenů – jednotek kryptoměny mezi účty, resp. adresami uživatelů. Výchozí programovací jazyk tohoto počítače se jmenuje Solidity a je tzv. turingovsky ekvivalentní. To znamená, že je stejně silný z hlediska možností, co v něm lze naprogramovat, jako kterýkoliv jiný běžně používaný jazyk (např. C nebo Java). Aplikace napsané pro EVM běží nad blockchainem, který jim slouží jako paměť pro data i kód programu. Z povahy toho, k jakým datům mají aplikace přístup, jsou jejich programem vlastně smart kontrakty. Mohou však být komplexnější než podmínky na výstupech transakcí u Bitcoinu. Vznikla virtuální mašina a teď jen vymyslet, co má pohánět.

Ethereum má i vlastní měnu ether se zkratkou ETH. Za povšimnutí stojí pojmenování menších jednotek, kterými autoři uctili velká jména kryptosvěta a cypherpunku: attoether = wei (Wei Dai), microether = szabo (Nick Szabo), miliether = finney (Hal Finney). Prostřednictvím ETH platí uživatelé těžařům za běh aplikací. Těžaři vlastně realizují výpočty EVM a jejich (mezi)výsledky zapisují do blockchainu. V tomto ohledu je práce systému a rozdělení rolí jeho účastníků podobná jako u Bitcoinu. Měna je nekonečně inflační s aktuální rychlostí 5 ETH za 15 sec. Těžba funguje na bázi PoW, ale Ethereum hodlá přejít na kombinovaný proof-of-work a proof-of-stake pomocí algoritmu Casper. Ani Ethereum však není bez mínusů. Nevýhodou tohoto přístupu

k decentralizovanému výpočtu je, že není distribuovaný. Všechny těžební/výpočetní uzly počítají totéž, takže rychlost výpočtu je v porovnání s distribuovanými počítači velmi nízká. Je to daň za vysoké zabezpečení výpočtu.

Ethereum je tedy platforma pro decentralizované aplikace. Existujícími příklady mohou být třeba počítačová hra Etherplay.io nebo Golem, jenž nabízí pronájem nevyužitého výkonu počítače. Typickou aplikací Etherea je ICO, o kterém ještě budeme mluvit. Na druhou stranu nepříliš úspěšným projektem bylo The DAO, pokus o decentralizovanou autonomní organizaci, který však skončil zneužitím chyby v kódu aplikace, čímž útočník získal třetinu ze 150 milionů dolarů vybraných na financování projektu. Po diskuzi v komunitě se vývojáři Etherea rozhodli, že ukradené peníze „zachrání" jednoúčelovým hardforkem. Tento přístup typu „účel světí prostředky" se pochopitelně ne všem líbil, takže někteří těžaři hardfork neakceptovali a blockchain se začátkem roku 2017 rozdělil na „oficiální" Ethereum a Ethereum Classic (ETC) s původními pravidly.

Další kryptoplatformy

Jak můžeme vidět na příkladu Etherea, možnosti altcoinů se neomezují zdaleka jen na kryptoměnu. Je vůbec otázka, jestli zde můžeme výraz altcoin ještě použít. Každopádně univerzálnějších platforem je v kryptosvětě vícero a některé starší než Ethereum. V této podkapitole si uděláme stručný přehled a klasifikaci těch ostatních a seznámíme se s pojmy, které se v tomto kontextu používají.

Přibližně od roku 2013 se objevuje termín „Bitcoin 2.0", který přišel s altcoinem MasterCoin (MSC). Myslí se jím právě platformy pro výměnu obecnějších digitálních tokenů (nejen peněz), s obecnějším skriptovacím jazykem (než má Bitcoin). To první umožňuje realizovat smart property, to druhé smart kontrakty (víc smart než v Bitcoinu). Obojí dohromady je potom smart ještě víc (nemáte také pocit, že je toto adjektivum poněkud nadužíváno?). Nicméně potenciálních aplikací takových platforem nalezneme mnoho: registry vlastnictví („digital assets"), decentralizované burzy (DEX), decentralizovaná úložiště dat (např. StorJ, Filecoin),

„proof-of-existence“ – ukládání hashů dokumentů do blockchainu, což je důkazem jejich minimálního stáří (např. poex.io), atd. Fantazii se zde rozhodně meze nekladou.

Podívejme se nyní na způsoby architektonického řešení takových platforem.

Nejjednodušší řešení je vlastní nezávislý blockchain. Příkladem takové architektury je již zmíněné Ethereum z roku 2014 – decentralizovaný počítač. Ještě o něco starší je Nxt (NXT) z konce roku 2013, což je rovněž jakási komplexní smart kontraktová infrastruktura. Implementuje digitální aktiva (digital assets) a jejich směnu (obarvuje vlastní mince), nabízí úložiště dat (i aliasů jako Namecoin), obsahuje kryptograficky silný systém hlasování, umožňuje tvorbu odvozených kryptoměn atd. O něco novější je další populární smart kontraktová kryptoplatforma Bitshares (BTS) z roku 2014. Na ní je zajímavé, že používá tzv. „delegated proof-of-stake“ (DPoS). Ten zajišťuje konsensus na základě omezeného množství delegátů volených držiteli měny. Důsledkem DPOS je velmi rychlé potvrzování transakcí v řádu sekundy.

Metacoins

Jinou architektonickou možností kryptoplatforem jsou tzv. metacoiny. Ty staví na tom, že si svoje transakční data ukládají do cizího (typicky bitcoinového) blockchainu. To obecně lze v nějaké omezené míře (u Bitcoinu např. do parametru „nicnedělající“ skriptové operace OP_RETURN), které si musí být metacoin vědom. Naopak podkladový coin o ničem neví, tomu se data ukládaná do jeho blockchainu metacoinem jeví jako nezajímavé transakce.

Metacoiny tedy vyžívají podkladový coin jako blockchainovou databázi, za jejíž používání platí transakčními poplatky. Do této skupiny patří i různé barviče mincí, např. Coinprism z roku 2014 – implementace Open Assets protokolu (nemá své mince, ale využívá toho, že bitcoiny nejsou záměnné, a obarvuje je – „colored coins“). Dále sem patří Counterparty z roku 2014 s měnou XCP, která vznikla zničením určitého množství BTC (odesláním na nedobytnou adresu, tzv. „proof-of-burn“). Patří sem i již zmíněný MasterCoin ohlášený roku 2012, implementovaný roku 2013 a roku 2015 přejmenovaný na Omni.

Omni je podkladovou vrstvou k několika dalším existujícím projektům, např. Tether nebo MaidSafeCoin. Tether (USDT) sice později přešel nad Litecoin, ale jeho zvláštnost spočívá v tom, že mince reprezentují americký dolar v poměru 1 : 1. Reálné dolary na krytí mají být uloženy u emitenta kryptoměny a motivací projektu je docílit komfortnějších plateb s fixním kurzem na dolar. MaidSafeCoin (MAID) je pak poukázkou budoucí měny SafeCoin – až bude existovat, tak se za ni MAID smění. Nyní slouží k financování teamu MaidSafe, který vyvíjí projekt SAFE („Secure Access For Everyone"). To je ambiciózní myšlenka plné decentralizace veškerých internetových služeb, včetně globálního decentralizovaného úložiště dat a šifrované komunikace.

Sidechains

Další z možných architektur kryptoplatforem jsou tzv. sidechainy. Tato architektura na rozdíl od metacoinů obsahuje vlastní blockchain. Ten je ale nějakým způsobem pevně navázán na cizí (opět typicky bitcoinový) blockchain, tzv. mainchain (od toho pak název sidechain – postranní řetěz). Pokud metacoiny využívají podkladový coin jako databázi, u sidechainů můžeme říct, že ho využívají naopak jako měnu (vzpomeňme na druhé dělení altcoinů, které jsme si uváděli v kapitole o jejich zoologii).

Hlavní myšlenka sidechainů vypadá tak, že mince z mainchainu se na nějakou dobu přesunou do sidechainu, tam se s nimi stane něco nového/zajímavého a později se vrátí zpět do mainchainu. Tento trik nám umožnuje implementovat nové funkcionality a pravidla, která by na mainchainu vyžadovala hardfork, jako softfork! Sidechain je tedy takový „plugin" do mainchainu. Mince sidechainu je možné vytvořit zablokováním mincí mainchainu, např. jejich odesláním na speciální adresu – adresu sidechainu. Tento směr přenosu nevyžaduje od mainchainu žádnou podporu, ani softfork. Sidechain zkrátka monitoruje transakce v mainchainu a umí rozpoznat ty, které znamenají přesun mincí do něj.

Někdy se pojmem sidechain označuje i pouze jednosměrná („one-way") varianta, kdy se mince zničí (podobně jako vznikly tokeny u Counterparty), leč obvykle se tím myslí varianta obousměrná („two-way") s možností vrátit mince ze sidechainu

zpět do mainchainu. Oba směry přenosu mají kryptograficky zaručenou bezpečnost (pomocí tzv. SPV – „Simple Payment Verification"). To je zásadní rozdíl oproti konverzi mincí užitím nějaké centralizované služby (např. přes burzu). Ta může den ze dne zmizet, a ne že by se to čas od času nestalo.

Sidechain může být těžen spolu s mainchainem pomocí merged miningu, takže jeho existence nepřináší novou výpočetní náročnost. Zároveň však zůstává izolováno zabezpečení na obou chainech, což znamená, že při zkompromitování sidechainu nedojde ke zkompromitování mainchainu a naopak. To je velká výhoda pro zkoušení nových funkcionalit. Hlavní výhodou sidechainů však je, že mohou nové funkcionality pro minci mainchainu přidávat, byť zprostředkovaně, pomocí zpětně kompatibilních změn pravidel. I proto se jedná o jedno z možných řešení problému škálování. V komunitě však ještě ke konci roku 2017 převažuje preference pro Lightning Network. Pozor, LN není sidechain – jak někteří mylně uvádějí – netvoří paralelní blockchain, pouze si vyměňuje (nerozeslané) transakce mezi uzly své sítě. Naopak třeba Bitcoin XT by se dal implementovat jako sidechain k Bitcoinu. Případně volitelná anonymizace bitcoinových plateb by se dala dodělat jako sidechain implementující Zerocoin či Zerocash akumulátor. Dalším příkladem sidechainu je Truthcoin (toho času ve vývoji) realizující decentralizovaný trh s předpověďmi (Prediction Market).

ICO, letní láska roku 17

Svět akcií zná své IPO, tedy prvotní úpis akcií. Kryptoměny nechtěly zůstat pozadu a přišly s ICO, initial coin offering. Prvotní úpis mincí! Už v roce 2013 altcoin MasterCoin vybral okolo 5000 BTC, za které investorům poslal své nově vzniklé mince. Doufal, že ty se zhodnotí a pro všechny zúčastněné to bude výhodný obchod. Podobně o rok později vzniklo i Ethereum. To vybralo během prvního dne miliony dolarů v bitcoinech a investorům za ně poslalo první ethery. Skutečný boom ale přišel až v roce 2017. V létě začal jeden projekt za druhým vybírat peníze za své nové mince, digitální tokeny. Vznikly stovky projektů, z nichž ty nejviditelnější dokázaly vybrat dokonce miliardy korun. Investoři pak doufali, že nakoupené tokeny budou mít v budoucnu vyšší hodnotu.

U některých projektů to dávalo smysl. Měly nápad, slušný tým vývojářů a sílu dílo dokončit. Vybrané sumy se ale vymykaly jakýmkoliv mezím. Nápad na nový webový prohlížeč Brave vybral za půl minuty po započetí ICO v přepočtu téměř tři čtvrtě miliardy korun. Chatovací aplikace Kik si přišla pro více než dvě miliardy korun. Celkem lidé nakoupili tokeny za desítky miliard korun. Rekordmany jsou decentralizovaná úložiště souborů Filecoin a projekt sebe-vylepšujícího se blockchainu Tezos. Každý z nich vybral přes pět miliard korun.

Vidina velkých zisků hnala do ICO stále více firem. V létě roku 2017 byly ICO všude. A jedno vedle druhého byly jako přes kopírák. Hezké webové stránky, přípona .io, nejlépe řecký či latinský název, problematická oblast a řešení pomocí „blockchainu". Vrcholnými představiteli nesmyslnosti, která se s ICO spustila, byly projekty jako například Dentacoin, tedy „zubaři na blockchainu". Zubaři jsou důležití, tak proč je nedat na blockchain? Že to nedává žádný smysl? Nevadí, i tak dosáhla tržní kapitalizace na několik miliard korun.

Naštěstí si problémy ICO uvědomuje veřejnost čím dál více a požaduje jiný přístup. Vznikají tak alternativy, z nichž zajímavé je IPCO (kombinace IPO a ICO). To slibuje vytvořit jakési „kryptodružstvo", kde nákupem mincí získáte nejen mince samotné, které nemusí mít hodnotu, ale i reálný podíl na zisku společnosti. To už smysl dává.

Dobrý, zlý a ošklivý altcoin

Mincí všeho druhu bylo najednou tolik, že se v nich začali ztrácet i odborníci. Jak ale poznat dobrou kryptoměnu?

Těch dobrých je málo. Takové kryptoměny musí prvně řešit reálný problém. Poptávka po bitcoinech je samozřejmě hodně spekulativní, ale pod tím vším je hodnota v symbolické snaze nahradit dnešní dysfunkční peníze. Litecoin má podobný cíl. Ethereum chce být decentralizovaným počítačem světa. Monero, Zcash nebo Dash chtějí nahradit anonymní hotovost.

Dobrá kryptoměna by měla mít rozumnou distribuci. Bitcoin se podle předem známého plánu distribuuje těžařům. Peercoin

nové mince dodává jako úrok držitelům. Čím dál více měn ale sází na úplné vytěžení hned na začátku (premine) a z původní distribuce jde rovnou vše tvůrci. Ten potom mince nabízí, ale pochopitelně si obvykle velkou část nechává a je tak schopen výrazně měnu ovlivňovat. Předtěžené altcoiny mají výhodu v nižších poplatcích a rychlosti, ale daní za to je velká centralizace, a tedy i zranitelnost.

Nakonec, dobrá kryptoměna by měla mít živý ekosystém. Řada měn jsou jen rychlá schémata na jednoduché zbohatnutí. Představte si, že vytvoříte miliardu altcoinů a pošlete mi jednu jednotku za dolar. Pak ji ode mě koupíte za dva dolary. Proběhly dvě transakce v celkovém objemu tři dolary, ale tržní kapitalizace měny je rázem dva krát miliarda mincí, tedy dvě miliardy dolarů. Navíc během jednoho dne vyrostla o sto procent z jedné na dvě miliardy. Toho si všimnou spekulanti a začnou nakupovat. Zkušený spekulant se sveze na jakékoliv vlně, ale většina prodělá.

Dobré kryptoměny by tedy měly mít hlubší smysl, být decentralizované a použitelné. Takových moc není, ale jen v prvních pár desítkách největších je Bitcoin, Ethereum, Litecoin, Dash, Monero, Zcash nebo Bytecoin. A koneckonců i Dogecoin, recesistická měna, která vznikla na základě internetového memu, ale překvapivě patří mezi ty nejúspěšnější kryptoměny, které kdy vznikly.

„Ošklivé" altcoiny jsou ty, které výše uvedené nesplňují. Jsou pouhou spekulací, hezky nazvaným projektem, nebo jsou centralizované. Z principu ale nedělají nic špatně. Nikoho neokrádají, nabízí skutečný produkt.

Naneštěstí jsou vedle dobrých a ošklivých i zlí. Ti okrádají. Přestože není těžké je rozeznat, řada lidí se nechá napálit. Tyto projekty obvykle nemají ani žádnou skutečnou kryptoměnu, jen vás tvůrci donutí jim poslat peníze. Jde o tradiční pyramidové hry, kde vydělají ti na špičce, dokud se přidává dostatek lidí. Typickým představitelem populárním v České republice je společnost OneCoin. Ta vznikla v Bulharsku a je typickou pyramidovou hrou. Měna se nikde neobchoduje, a přitom slibuje výdělky. Cena není určená nabídkou a poptávkou, ale sama společnost si ji vymýšlí. Není tak divu, že roste. Členové OneCoinu vás nalákají na vstupní balíčky, které vám přidají onecoiny. Samozřejmě si ve skutečnosti kupujete úplně něco jiného, v případě OneCoinu

si kupujete online vzdělávací kurzy. Když se tedy se společností budete soudit, že vyhodila vaše desítky tisíc korun za tokeny, se kterými nejde nic dělat, prohrajete. Koupili jste si jen předražené vzdělávání. Jakmile někde vidíte nakupování „balíčků", dejte od toho ruce pryč. Samozřejmostí je navíc nutnost vydělávat na hledání dalších lidí, kteří se zařadí do pyramidy pod vás. Žádná slušná kryptoměna po vás nic takového chtít nebude.

Vedle OneCoinu vznikly i další pyramidové podvody, zejména Nanocoin, Octacoin, Crypto888, Futurocoin a Dascoin. Poslední jmenovaný je zatím nejsofistikovanější. Zatímco OneCoin neměl ani blockchain, takže reálně neexistoval, Dascoin ho má. Ale nedává žádný smysl. Zatímco bitcoinové bloky jsou desetiminutové, dascoiny se těží každé tři sekundy. Pokud chcete poslat informaci o transakcích za poslední tři sekundy skrze internet do celého světa, nemáte žádnou šanci to stihnout. Technicky je tedy jasné, že je měna centralizovaná. A také se nikde neobchoduje. Vypadá na oko ale lépe. Opět by vás ale mělo upozornit, že ho prodávají kravaťáci na podivných seminářích, kde vám dopředu ani neřeknou, o kterou kryptoměnu jde. Chtějí vás obrat, dávejte si pozor.

Budoucnost Bitcoinu

Možné problémy

Je bitcoinů málo?

Přestože se zdá, že je Bitcoin na své cestě nezastavitelný, existují i problémy, se kterými se potýká. Některé z nich jsou zanedbatelné, jiné minimálně teoreticky destruktivní. Na druhou stranu většina široce známých problémů jsou pouze mýty.

Například je mýtem, že bitcoinů je málo. Jde o obdobný argument jako se zlatem. Stejně jako zlata, i bitcoinů je omezené množství. A stejně jako zlato, i bitcoiny lze dělit prakticky do nekonečna, pokud by to bylo pro směnu vhodné. Je zjevné, že dnes si za minci zlata nelze koupit sklenku vína, aniž byste nenechali velmi štědré spropitné. Stejně tak je dnes nepraktické obchodovat s bitcoiny na úrovni celých jednotek. A tak stejně jako u zlata, i u bitcoinů existuje dělení.

U kryptoměn je dělení dokonce možné teoreticky až do nekonečna, u zlata existují fyzická omezení, i když patrně pouze teoretická. Stěží by se na požádání vyplácely tři atomy zlata, zatímco tři biliardtiny z biliardtiny bitcoinu jsou vyplatitelné stejně dobře, jako celé tři bitcoiny. Pouze by se pro zjednodušení směny upravila prostředí softwarových peněženek apod., aby uživatelé nemuseli vypisovat všechny nuly, a menší jednotce by se začalo říkat nějakým hezkým slovem. To vše spontánně fungovalo napříč dějinami celého světa a není důvod se domnívat, že by tomu muselo být u Bitcoinu jinak. Bitcoinů není málo. Ano, dnes je dělitelný pouze na nejmenší satoshi, ale i těch je dostatečné množství i pro vzdálenou budoucnost.

Není jich tedy málo, ale jsou vzácné. V takovou chvíli nutně začíná hrát svou roli cenový systém. Říká se, že pokud by byly všechny bitcoiny vytěženy a nikdo je nechtěl dát do oběhu, protože by spekuloval na zvýšení ceny, nebylo by čím platit.

Elementární základy ekonomie však ukazují, že je taková situace nepravděpodobná, a především snadno řešitelná, i pokud by nastala. Stejně jako u jakéhokoliv jiného zboží či služby vyrovnává přebytečnou poptávku zvýšení ceny. Pokud by byli lidé, kteří by bitcoiny poptávali a nikdo jim je nechtěl poskytnout,

museli by zvýšit cenu. Na postupně rostoucí cenu by zareagovali první vlastníci, kteří si držení bitcoinů cení nejméně, a prodali by je. Pokud by stále panoval na trhu nedostatek, cena by obdobně rostla až do okamžiku, než by byli poptávající i nabízející spokojení. Na takovém postupu není nic zázračného, jakkoliv kouzelný se zdá. Jde pouze o tržní síly v praxi. Tak, jak je vidíme neustále všude kolem sebe.

Není málo adres?

Velice častou otázkou je, zda se „neplýtvá adresami" a ty někdy nedojdou. Zaprvé z fundamentálních důvodů, protože se negenerují nové adresy, ale de facto se obsazují adresy existující, i proto je možné vygenerovat si adresu offline. Zadruhé, i zde jste byli několikrát vyzváni, ať si zkusíte založit peněženku a generovat nové a nové adresy, a na většinu z nich pravděpodobně nikdy nepřijde žádný bitcoin.

Může se ale například stát, že si dva lidé vygenerují stejnou adresu? Může, ale pokud se toho obáváte, nechme promluvit teorii pravděpodobnosti. Jde o situaci s tak nízkou pravděpodobností, že pro účely praxe a s přihlédnutím k velikosti a stáří vesmíru, je jistota, že nenastane. Nebo by si někdo vsadil, že během ledna padne ve Sportce pokaždé ta samá kombinace? Adres je obrovské množství a jejich masové generování by nedávalo žádný smysl. Pro ilustraci může sloužit výpočet, který koluje po internetu jako jednoduchý důkaz. Výpočet je ve skutečnosti sofistikovanější, ale zjednodušeně říká: pokud bychom dokázali generovat bilion klíčů za sekundu (což je vysoce nadhodnocené číslo, ale i kdyby) a mohli použít každý jediný atom planety Země jako pevný disk k uložení jednoho bajtu dat (což je snad ještě více nepředstavitelné, ale i kdyby) a mohli k uskladnění používat přímo energii Slunce (i kdyby), tak bychom potřebovali k výpočtu 37 kvadriliard Zemí, 237 miliard Sluncí a 3,7 noniliard let, tedy 270000000000000000000000000000000000000000000× více, než je předpokládané stáří vesmíru. A to vše při výše popsaných předpokladech. Pokud se to zdá neuvěřitelné, možná pomůže k představě stará dobrá informace, že možných variant šachové hry je více, než atomů ve vesmíru. Dokonce jich je odhadem tolik, jako kdyby každý atom vesmíru obsahoval půl vesmíru a sečetly se všechny takto vnořené atomy.

A nakonec, i kdyby se to stalo, při dodržení elementárních zásad opatrnosti by vlastník přišel o malou částku. Tedy, pokud už by někdo chtěl páchat zlo, nebylo by pro něj snazší praštit náhodného kolemjdoucího po hlavě a vybrat mu kapsy?

Obdobných otázek s kryptografií je mnoho. Mohla by být kryptografie za Bitcoinem prolomena? Je to velmi nepravděpodobné, ale pokud by se začaly objevovat silné počítače, které by naznačovaly, že je v blízké budoucnosti možné kód prolomit, není dle vývojářů problém přejít na silnější algoritmus. Nyní to však není nutné a Bitcoin je z tohoto hlediska velmi bezpečný. Tvrdí se dokonce, že Satoshi Nakamoto musel trpět stihomamem. Extrémní strach z prolomení Bitcoinu ho vedl k takovému zabezpečení, které nepřestává fascinovat kryptografy po celém světě.

Většina útočí

Problémem, který je považován za největší slabinu Bitcoinu, je takzvaný 51% útok. Pokud by získal útočník více než polovinu výpočetní síly celé bitcoinové sítě, potom by získal několik výhod, které by potenciálně dokázaly celou síť paralyzovat. Přestože by stále nemohl vytvářet nové bitcoiny nebo měnit parametry sítě, mohl by provést se svými bitcoiny dvojitou útratu nebo bránit ostatním v těžbě dalších bloků.

A nejde jen o teorii – těžební pool GHash.IO se začal na začátku roku 2014 blížit polovině výpočetní kapacity sítě, v jeden okamžik měl až 42% podíl. Strach jsme mít mohli, ale útok by byl stále velmi obtížný, protože ona hranice 50 % v sobě neskrývá žádný ostrý přechod, jehož překročením se stane něco ošklivého. Jedná se stále o pravděpodobnostní jev, stejně jako bezpečnost potvrzené transakce není nikdy zcela absolutní, ani pokud se dostane do libovolné hloubky blockchainu. A především by byl takový útok ekonomicky neracionální. Jaká by byla motivace poolu, aby Bitcoin zničil? V Bitcoinu je přirozeně zabudován zajímavý samoregulační prvek, kdy sami těžaři mají motivaci Bitcoin chránit, protože jim generuje příjem. GHash.IO toho byl příkladem. Těžaři sami začali dobrovolně měnit své působení v poolech a podíl GHash.IO se začal zmenšovat. K tomu samotný pool vydal oficiální stanovisko, ve kterém konstatoval, že provedl a provede preventivní kroky, které povedou

ke snížení výpočetní kapacity, aniž by však musel zavádět poplatky. Například dočasně pozastavil přijímání nových členů a u své sesterské služby CEX.IO, kde je možné nakupovat výpočetní výkon a těžit vzdáleně bitcoiny, změnil pravidla tak, aby bylo možné nakoupený výkon používat i na jiných poolech než na GHash.IO. Je tedy teoreticky možné podniknout takový útok? Ano. Ale zaprvé, proč by to kdo dělal, a zadruhé, z jakého důvodu by včas nezareagovali samotní těžaři?

Pálení elektřiny

Je pravda, že Bitcoin ke konci roku 2017 spotřebovával energie zhruba jako celé Slovensko, tedy 0,15 % světové spotřeby. Jedna bitcoinová transakce stála stejně, jako elektřina na den pro devět amerických domácností. Neměli bychom se toho ale bát.

Vypadá to, že je Bitcoin drahý, protože srovnáváme nesrovnatelné. U Bitcoinu vychází samotná platba na několik dolarů, platba kartou obvykle stojí dvě procenta. V tom se tedy příliš neliší, naopak je Bitcoin velmi levný u velkých částek.

Pokud ale vezmeme celkové náklady a vydělíme je počtem transakcí, vychází cena celého systému na transakci relativně draze. To ale i současný finanční systém. Jeho objem je odhadován na 350 bilionů korun. I kdyby banky byly polovinou finančního systému, obslouží za 175 bilionů korun celkem 450 miliard transakcí. Každá transakce tak stojí téměř 400 korun, což je překvapivě přibližně elektřina na den pro stejných devět amerických domácností. Bitcoin je stejně drahý, jako naše současné peníze.

Samozřejmě jde o velmi hrubý výpočet. Navíc ověřování bitcoinových transakcí a provoz současných peněz nelze jednoduše srovnávat. Pálení elektřiny a nakupování drahých budov v centrech měst slouží úplně jinému účelu. Hlavně ale přestaňme porovnávat úplně odlišné veličiny.

Je naivní si myslet, že ty nejlepší věci jsou zadarmo. Dobré věci prostě něco stojí. I kdyby byl Bitcoin dražší, což do budoucna nelze vyloučit, potom buďme rádi, že si můžeme připlatit za lepší peníze. Za takové, které nemůže nikdo ovládat a systematicky znehodnocovat.

Jeden problém ale zůstává. Hrozba, které se vyhnout teoreticky dá, ale prakticky se to moc často nestává, je lidská hloupost. Stejně jako kdekoliv jinde, i v prostředí Bitcoinu může někdo na něco zapomenout nebo jednoduše udělat něco špatně.

Příkladem je začátek roku 2014, který přinesl obrovský propad ceny bitcoinů až na pětinu hodnoty z konce roku předchozího. Chybou bylo chování burzy Mt.Gox a uživatelů, kteří jí důvěřovali a nechávali si u ní své bitcoiny, jako by to byla online peněženka. O své bitcoiny pak při krachu burzy přišli. Posměšně se říká, že Mt. Gox doplatil na to, že byl původně založen k úplně jinému účelu – k obchodování karet stolní hry Magic: The Gathering. Odtud také její název, MtG Online eXchange.

Regulace

Úřad pro zničení Bitcoinu

Existuje i možná hrozba, které se Bitcoin patrně nevyhne – státní regulace. Všechny výhody Bitcoinu totiž vidí i jeho nejmocnější konkurence, státní fiat peníze (tedy peníze s nuceným oběhem, vytvořené z ničeho, vzniklé úvěrováním), k jejichž množství má klíč centrální banka a potažmo stát. Tomu se pochopitelně nelíbí, že vzniká konkurence, natož v takové podobě, která není příliš ideální k výběru daní, kontrole peněžních toků a centralizovanému ovládání. Jak říká část slavného rčení: vlády nesnáší konkurenci.

Bitcoinu se vlády kolem světa příliš nebrání. Není se čemu divit, prozatím jde o marginální měnu, kterou užívá zanedbatelné množství lidí. Na přelomu let 2013 a 2014 bylo na světě kolem dvou milionů uživatelů této měny a provedli denně kolem 50 tisíc transakcí, z nichž většina byla registrována na internetových kasinech. Pro srovnání bylo jen v České republice registrováno denně přes jeden a půl milionu karetních transakcí. Bitcoin je pro regulátory zatím prakticky ničím.

Ale – Bitcoin roste. Coinbase se na konci roku 2017 stala nejstahovanější aplikací na iPhone. Počet uživatelů se zvýšil minimálně na desítky milionů. A tak se i čím dál více setkáváme a budeme setkávat se snahami všemožných vlád Bitcoin tzv. zaimplementovat do legislativy, jinými slovy regulovat a měnit k obrazu svému. Jenže ono to moc nejde.

Uveďme příklad, který krásně ilustruje snahy o regulaci decentralizované měny. Jistý americký regulátor zjistil, že Bitcoin je považován za měnu, což je v rozporu s platnou legislativou, která jasně říká, že jediné peníze jsou státní dolary. I jal se regulátor regulovat a sepsal dopis se žádostí o ukončení činnosti. V opačném případě prý sáhne k trestu. Když však chtěl žádost dokončit, uvědomil si, že neví, komu ji má adresovat. Poslal tak dopis na neziskovou organizaci, která má slovo Bitcoin v názvu. Tam si papír přečetli a tím celý příběh slavně skončil.

Představa zmateného státního úředníka je jistě zábavná, ale skrývá se v ní vše, co s sebou Bitcoin nese. Skutečnou decentralizaci, absolutní opak současných státních peněz. A tak je i složité Bitcoin regulovat. Stejně jako se snaží vlády již od jeho vzniku regulovat internet, a nebyly příliš úspěšné, tak se pravděpodobně stane cílem neúspěšných regulačních útoků i Bitcoin.

Na druhou stranu jasně vidíme rozdíl mezi internetem a Bitcoinem. Bitcoin má motivaci stát se globální měnou, světovou účetní jednotkou, penězi. To zcela podkopává jakoukoliv činnost vlády, na rozdíl od „pouhého" internetu. Motivace zastavit Bitcoin je řádově vyšší. Internet sice dokázal, že je mocnou opozicí všech vlád, lží, privilegovaných monopolů, daní a podvodů, ale dodnes si nekladl žádné vyšší cíle. Bitcoin má v sobě vyšší cíl přímo zabudovaný. A s ním i problém v podobě neutuchající snahy ho ovládnout či zničit. Podíváme-li se však opět na příběh s úředníkem a dopisem – jak to udělají?

Dějiny úřadu

Jistou nápovědu nám dá historie, a to dokonce historie nedávná. Podívejme se znovu na E-gold zmíněný na začátku této knihy. E-gold vznikl v roce 1996 a šlo o první světově úspěšnou virtuální měnu. Od Bitcoinu se lišila zásadně, zejména v tom, že nebyla decentralizovaná. E-gold byla měna založena na fyzickém zlatě. Delší dobu nikomu nevadila a byla ignorována, přičemž její význam rostl. Nicméně přišlo jedenácté září a s ním i Patriot Act, zákon zaměřený na boj s terorismem. V rámci tohoto boje se zaměřil i na tzv. „peněžní služby bez povolení". Bez povolení, to bylo u E-goldu jasné. Ale peněžní služba? To by přeci znamenalo, že lze E-gold, potažmo zlato, označit za peníze. A to by musely americké úřady přiznat, což se jim pochopitelně nelíbilo. A nelíbí! Označit zlato za peníze by popíralo veškerou vládní snahu tento fakt popřít. Když nemohla hora, šlo se k hoře. Vláda tak postupně mezi lety 2006–2008 přestala bojovat proti peněžním službám bez povolení, ale nově proti „systémům, které umožňují jakoukoliv směnu hodnoty". Horší definici by člověk pohledal. E-gold byl nakonec zničen, musel zaplatit téměř 4 miliony dolarů, zakladatelé byli odsouzeni a vláda jejich zlato znárodnila.

Pokud vám chce vláda zavřít podnik, nemůžete udělat vůbec nic. Nicméně Bitcoin má proti E-goldu výhodu v tom, že žádným podnikem není. Nemá žádné centrum, které se dá zavřít, žádný server, který se dá zabavit a žádného šéfa, kterému můžete vyhrožovat nebo ho poslat za mříže.

Můžete ale podniknout jiné kroky. U Bitcoinu existuje neodstranitelná možnost regulace substitutu, tedy státních peněz. Centrální banky mají zákonnou možnost nakupovat cizí měnu a ovlivňovat tím směnný kurz mezi státní měnou a Bitcoinem. Tím by však Bitcoin posílil, a nadto byl svým způsobem legitimizován, k čemuž není politická vůle. Můžete ale regulovat reálné příjemce bitcoinů. Přijímáte bitcoiny? Potom nám vyplníte tento formulář a vzhledem k problémům, které jsou s Bitcoinem spojeny, vám bude polovina vydělaných bitcoinů zabavena. Očekávejte daňové kontroly, neočekávejte soucit. Dále může stát regulovat vývojáře, dát slovo Bitcoin na blacklist a všemožně jinak se snažit odstranit to, co se nám na Bitcoinu líbí. Pokud budou mít prodejci dodatečné náklady s přijímáním bitcoinů (bude zakázané je přijímat, tedy to nebudou smět nikam napsat a případně by byli tajně kontrolováni), tak budou mít pochopitelně nižší motivaci bitcoiny přijímat, což vede k nižší motivaci bitcoiny držet i u uživatelů, a jejich hodnota a s ní i cena letí dolů.

První vlaštovky

A vlády to udělají. Už přilétly první vlaštovky. Newyorský hlavní finanční kontrolor Ben Lawsky prohlásil: „Je v dlouhodobém zájmu virtuálních měn podřídit se přiměřeným ochranným opatřením, která ochrání spotřebitele, odstraní ilegální aktivitu a ochrání naši národní bezpečnost.“ Rozumějme tomu správně; je to v dlouhodobém zájmu, jde tedy o něco, co my krátkozrací vidět nemůžeme, a naopak pokud to nevidíte, pak jste krátkozrací; přiměřeným opatřením, tedy přesně takovým, jaká jsou potřeba; ochranným opatřením, protože nás chrání, a to je dobře; která ochrání spotřebitele, jelikož chudák spotřebitel musí být ochráněn, jinak by mohl například používat měnu, která neztrácí na hodnotě několik procent každý rok; odstraní ilegální aktivitu, protože za bitcoiny se kupují zbraně, drogy a zejména dětská pornografie, Bitcoin JE dětská pornografie, o tom není pochyb; a ochrání naši národní

bezpečnost, protože Lawsky je Američan a pokud chcete něčemu dát skutečný punc důležitosti, musíte větu zakončit právě takto.

A Lawsky není sám. Demokratický senátor Chuck Schumer prohlásil: „Je to praní špinavých peněz!" Ostatně, přesně to byla i linie argumentace proti E-goldu. Nositel Nobelovy ceny za ekonomii Paul Krugman o Bitcoinu napsal: „Je to plýtvání elektřinou!" Pochopitelně pokud jste zastáncem ekonomické školy, která stojí a padá na tom, že má centrální banka plnou kontrolu nad peněžním systémem, který nastavuje dle potřeb (a výsledků důmyslných makroekonomických modelů), potom musíte v Bitcoinu vidět pouze plýtvání elektřinou.

Vlády se snaží a budou snažit ještě více. Budou argumentovat, že podporou Bitcoinu schvalujete zločiny, které se pomocí této měny financují. Soudná argumentace však nemůže zavrhnout prostředek jednání, ale pouze jednání samotné. Účel nesvětí prostředky, stejně jako je nešpiní. Bitcoin qua Bitcoin je pouze prostředkem směny, který může být využit k dobrým i špatným cílům. Ostatně jako dolary nebo diamanty. Bitcoin není dětská pornografie. Trestejme zločin, ne peníze.

Ostatně odpovězme si na otázku, jakými penězi je financováno 99 % současného zločinu a 100 % státem posvěcených válek. Stejně riziková pro možnou trestnou činnost je přece i hotovost tradičních peněz. Je plně anonymní a hojně využívaná k daňovým únikům, praní špinavých peněz nebo financování terorismu. Zakázat kvůli tomu hotovost se zatím nikomu (vyjma několika akademiků zejména ve Švédsku a Japonsku) nechce.

EU pro, Čína proti

Nejdále došlo zatím Německo, které připravilo kapitálovou daň z držení bitcoinů. Bitcoin by jako účetní jednotka měl být zanášen do účetnictví a v případě zisků by měla být část odváděna státu. Obdobně se zachovalo Finsko, které považuje bitcoiny za komoditu, a výnos z jejího prodeje či těžby podléhá dani z kapitálu. V ČR zatím jen Ministerstvo financí doporučuje dávat si na Bitcoin pozor a nařizuje oznamovat jakékoliv transakce nad 15 tisíc eur. Eur! Česká národní banka se v únoru 2014 vyjádřila k Bitcoinu obsáhleji a na dvou stranách textu komentuje vztah Bitcoinu k českému

právnímu řádu. V textu není nic zásadního, jde pouze o ujasnění toho, že není k obchodu s Bitcoiny potřebné povolení ČNB a ani nepodléhá jejímu dohledu. Pokud chcete s Bitcoiny podnikat, musíte mít podnikatelské oprávnění a k obchodu s investičními nástroji založenými na Bitcoinu musíte získat povolení obchodníka s cennými papíry. Nic, co by nebylo zřejmé, ale je přinejmenším zajímavé vidět, že je Bitcoin v hledáčku regulátorů.

K první skutečně velké regulaci Bitcoinu přistoupila Čína. Čínská centrální banka (PBOC) zakázala v prosinci 2013 všem čínským finančním institucím provádět jakékoliv obchody s bitcoiny či s bitcoinovými burzami. Nařízení PBOC snížilo cenu bitcoinů a začátek roku 2014 nebyl pro měnu příliš veselý. Nicméně samotná regulace byla vyhlášena velmi vágně a velké čínské burzy nezastavila. BTC China a další nepřestaly obchodovat, a dokonce navyšovaly své objemy.

Evropská unie má nakonec Bitcoin ráda. Evropský soudní dvůr na konci října 2015 v rozsudku ve věci platby daně z přidané hodnoty z bitcoinů prohlásil, že „je nesporné, že virtuální měna ‚Bitcoin' nemá jiný účel než účel platidla a že je za tímto účelem akceptována určitými hospodářskými subjekty". „Je přitom nesporné, že virtuální měna ‚Bitcoin' nepředstavuje ani cenný papír přiznávající vlastnické právo v právnických osobách, ani cenný papír srovnatelné povahy," dodává. V důležité definici píše, že

„virtuální měnu lze definovat jako druh neregulovaných digitálních peněz, které jsou emitovány a kontrolovány svými tvůrci a přijímány členy určitého virtuálního společenství. Virtuální měna ‚Bitcoin' patří mezi virtuální měny s tzv. ‚obousměrným tokem', které mohou uživatelé nakupovat a prodávat na bázi směnného kurzu. Takovéto virtuální měny jsou, pokud jde o jejich používání v reálném světě, analogické s ostatními směnitelnými měnami. Umožňují nákup jak skutečného, tak i virtuálního zboží a služeb. Virtuální měny se liší od elektronických peněz, (…) v tom, že na rozdíl od těchto peněz se v případě virtuálních měn kapitál nevyjadřuje v tradičních účetních jednotkách, například v eurech, nýbrž ve virtuální účetní jednotce jako je ‚bitcoin'."

Francouzský ministr financí Bruno Le Maire vyzval v prosinci roku 2017 své kolegy ze skupiny mocných států G-20 k diskuzi o možné společné regulaci Bitcoinu. Domnívá se, že Bitcoin může

sloužit k praní špinavých peněz a samozřejmě k financování terorismu. Přestože to nedává žádný smysl (a také se nic takového nikdy nepotvrdilo), jako mediální zpráva je to dobré. Úsměvné na tom je, že to přichází z Francie, kde se Bitcoin používá z celého vyspělého světa snad úplně nejméně. Schválně si zkuste na coinmap.org prohlédnout mapu Evropy a kde se na ní dá platit bitcoiny. Francie bude uprostřed svítit úplně nedotčená.

Postátnění Bitcoinu

Bitcoin se zásadní regulaci patrně nevyhne. Dnešní svět je na vládních zásazích natolik závislý, že k tomu nakonec dojde i konsensuálně, ačkoliv jistě ne jednohlasně, většina uživatelů souhlasit bude. Pokud se digitální měna má stát všeobecně uznávaným platidlem, bude muset s vládou začít spolupracovat. Jakkoliv se to může příčit samotné původní myšlence.

První, k čemu prostředí digitálních měn v dnešní době směřuje, je spolupráce s vládou na identifikaci uživatelů. V dějinách není období státní identifikace občanů ničím příliš vzdáleným, naopak. Ještě před první světovou válkou neměla většina obyvatel západního světa žádný dokument, který by je dokázal identifikovat. A nebyl to zásadní problém, jelikož jen málokdo to potřeboval. Většině lidí stačilo, že je dokázali identifikovat lidé v jejich okolí, a to i bez jakéhokoliv dokumentu. Pro nákup na místním trhu není občanský průkaz koneckonců nutný ani dnes. Ale ve chvíli, kdy z České republiky přeletíte půlku světa a chcete si u Američana v Los Angeles pronajmout na rok pokoj, identifikace vám snižuje cenu. I dnes je patrně možné si pokoj pronajmout i bez identifikace, ale zaplatíte více – prodávající se bude vyšší cenou jistit proti riziku, že byt vykradete či zničíte a utečete pryč. Možná by vás nakonec dohledal, ale detektivní kancelář by ho stála určité peníze a jistotu by neměl. S jasnou identifikací, kterou poskytne autorita, které lze důvěřovat, jistotu také nemá, ale může být klidnější. Na policii může pouze udat vaše jméno a bydliště či rodné číslo.

Obdobně to funguje na jakémkoliv velkém globalizovaném trhu. Pokud bychom se podívali do útrob některé velké světové burzy, setkali bychom se s lidmi, kteří obchodují s miliony a miliardami

dolarů jen pomocí jednoho kliknutí myši. Když se kupující ze Soulu rozhodne koupit akcie americké firmy za stovky milionů dolarů, nemusí do firmy letět a představit se. Může dokonce nakupovat v jednom okamžiku od stovek různých prodejců a nemusí znát ani jednoho jediného z nich. A pro ně je identita kupujícího taktéž nedůležitá, raději věnují čas rodině či něčemu jinému, co je baví. Ani jedna strana identitu znát nepotřebuje. Důležité však je, že pokud by chtěla, tak může. Kdyby kupujícímu akcie nepřišly (což právě díky jasné identifikaci všech zúčastněných institucí a aktérů prakticky ani nelze), potom by mohl chtít náhradu po konkrétním člověku nebo ještě lépe po burze, která si ráda zajistí, aby identifikaci všech účastníků znala. Jde pouze a jen o riziko. Mnoho lidí si rádo připlatí za nákup na velkých aukčních portálech místo anonymních online bazarů. Pokud se cokoliv pokazí, víte, na koho se máte obrátit.

V prostředí digitálních měn je taková identifikace zatím velmi ojedinělá. Velké bitcoinové burzy po svých uživatelích vyžadují doklad o identifikaci. Nicméně je tomu tak ne kvůli snižování rizika obchodů s bitcoiny, ale kvůli obchodům s dolary. Jakmile máte své bitcoiny, pokud chcete, jakákoliv identifikace může být zapomenuta.

Svět současných peněz se s tím potýká taktéž, a to v případě hotovosti. Hotovost také může být absolutně anonymní. Není tedy překvapením, že si mafiáni v amerických filmech (a v celosvětové skutečnosti) nosí kufříky plné bankovek. Pro běžné nákupy je anonymní hotovost vhodná, ale je nepoužitelná pro velké transakce na dálku. Bitcoin a jiné digitální měny jsou dnes v tomto smyslu spíše „hotovostní", tedy jdou z neznámé ruky do jiné neznámé ruky.

Vývojáři jsou si toho samozřejmě vědomi a přemýšlí se, co s tím. Jedním z řešení jsou nadstavby nad Bitcoin. Ty jsou sice zamýšleny spíše pro účely vydávání dluhopisů, akcií a jiných aktiv a jejich následnou snadnou směnu bez nutnosti centrální databáze, ale v budoucnu by mohly sloužit i k lepší identifikaci. Bitcoin by tak mohl, ale samozřejmě nemusel, nést i informaci o identifikaci vlastníka pro účely státu. Konkrétní implementace se zatím zdá být vzdálená, ale ve světě Bitcoinu jako by čas utíkal rychleji, a je tak možné, že se na řešení přijde velmi brzy.

Jiným řešením by mohly být institucionalizované peněženky, jakási obdoba bankovních účtů v současném systému. Stát by

jednoduše věděl, které adresy vám patří. Je otázkou, jestli si lidé zvolí pohodlí zvyku na státem identifikované peněženky a budou stále platit vysoké daně, nebo si zvolí vyhnout se takové možnosti postupem času úplně a tratit bude státní pokladna. To druhé zní pravděpodobněji.

Nové trhy

Víra v Bitcoin

„Když jde o peníze, každý je téhož náboženství," napsal kdysi Voltaire. A platí to plně i o Bitcoinu.

Bitcoin vidí jako příležitost lidé zcela odlišných politických i jiných přesvědčení. Jedni v něm vidí možnost odstranit současný silně monopolizovaný bankovní sektor, jiní vidí jeho příležitosti v globalizovaném obchodu a další se radují, že Bitcoin omezí vlády. Ostatně i populární politik a environmentální aktivista Al Gore o Bitcoinu říká: „Domnívám se, že skutečnost, že ve světě Bitcoinu nahradí tyto funkce [vlády] algoritmus (…) je vlastně docela super." Je to o to vážnější, že to tvrdí někdo, kdo byl od svých dvaceti osmi let postupně kongresmanem, senátorem, viceprezidentem a rovněž dvakrát kandidátem na prezidenta Spojených států.

Kde všude může Bitcoin znamenat revoluci? V půjčkách, na finančních trzích obecně, ale i ve smlouvách nebo ve společenských vědách.

Není žádných pochyb o tom, že Bitcoin přinesl a přinese revoluci v půjčkách. Bill Gates prohlásil:

„Někdo se zájmem o finance by mohl pomáhat s inovacemi v podobě například digitálních měn, které snižují transakční náklady, a chudí si díky nim mohou půjčovat za pět procent ročně místo patnácti."

Apoštolové blockchainu

Obrovským pokrokem pro lidstvo je i „vynález blockchainu". Tato databáze transakcí sdílená všemi uživateli může od základů změnit způsob, jakým používáme online služby. Je nepochybné, že systém P2P konsensu může dát vzniknout inovativním vyhledávačům, sociálním sítím, systémům vlastnických práv k nejen finančním aktivům apod. Meze jsou dány pouze fantazií.

Zdánlivě neomezené množství nových možností s sebou nesou takzvané obarvené mince („colored coins"). Jde o koncept

vystavěný nad infrastrukturou Bitcoinu, který přidává k informaci, kterou s sebou každý bitcoin nese, ještě další údaje, tedy minci „obarvuje“. Blockchain pak standardně zaznamenává pohyb této informace.

Fanoušci obarvených mincí rádi ilustrují jejich potenciál na příkladu pronájmů bytu. Představme si, že máme dům, který chceme pronajmout. K tomuto účelu zašleme na nově vytvořenou adresu jeden bitcoin (nebo libovolně malou část). Tento bitcoin „obarvíme“ informací, která bude říkat, že vlastník soukromého klíče k tomuto bitcoinu má oprávnění ke vstupu do našeho bytu. Nájemci pak jednoduše předáme klíče. Nebo pokud chceme vypadat jako lidé z budoucnosti, přidáme na dveře otevírací mechanismus, který se spustí pouze po načtení našeho obarveného bitcoinu. Nájemník nakonec jednoduše ukončí smlouvu tím, že nám zašle bitcoin zpět. Vlastní realizace barvení probíhá tak, že barvená mince ve své transakční historii projde přes smluvenou bitcoinovou adresu.

Majitel bytu navíc pošle „klíč“ od bytu do společné, přesně nadefinované transakce s kupujícím, který má možnost buď transakci potvrdit zasláním dostatečného množství peněz, nebo z transakce odejít. Není však možné vzít si klíč, protože bez zaslání peněz se klíč nepošle. Pokud peníze pošle, odejdou jak peníze, tak klíč. To samé platí pro druhou stranu.

Co když by nájemník nechtěl byt opustit a neplatil? Stačí jednoduše přidat funkci, která nájemníkovi nechá obarvený bitcoin umožňující vstup do bytu pouze pokud bude na zadanou adresu chodit každý měsíc smluvený nájem. Pokud nájem nedorazí, skript to vyhodnotí a „klíč“ k bytu nám zašle zpět (resp. umožní, abychom s ním mohli disponovat opět my). Stejným způsobem může probíhat například aktivace imobilizéru v automobilech, vstupních karet do veřejné dopravy apod. Internet je již nyní plný nápadů nespočtu lidí, kteří chtějí zahýbat světem.

Skriptování a smart kontrakty mohou usnadnit poskytování záloh, zjednodušit **escrow** tak, že není třeba žádné třetí strany, nebo dokonce vytvořit automatizované směnárny různých digitálních měn. Způsobů, jak využít možnosti Bitcoinu, byla popsána celá řada. Programátoři jako by se předháněli v tom, kdo vymyslí něco nového nebo vylepší cokoliv stávajícího. Stačí jen fantazie.

Escrow

obchodní interakce s účastí nezávislé třetí strany („escrow agent"), u které jsou uschovány směňované statky do doby naplnění podmínek nutných k provedení vlastního vypořádání. Hlavním úkolem escrow agenta je zajištění atomicity transakce – obchod je proveden se ziskem pro obě strany, anebo vůbec (a uschované statky jsou vráceny). Kromě zajištění atomicity transakce může escrow agent poskytovat i doplňkové služby jako např. verifikaci kvality nebo certifikaci pravosti směňovaných statků. Model **escrow** eliminuje riziko při interakci s nedůvěryhodnou protistranou. Nevýhoda **escrow** spočívá v nutnosti existence agenta důvěryhodného pro obě strany interakce (a dodatečných nákladech na jeho zapojení).

Sofistikované modely na bázi kryptografických metod (viz **Kryptografie**) umožňují bezpečnou interakci s nedůvěryhodnou protistranou i bez použití escrow agenta. Např. pomocí bitcoinových **kontraktů** lze sestavit model pro decentralizovanou směnu digitálních kryptoměn.

Byznys jménem Bitcoin

To vše až neuvěřitelným způsobem šetří lidskou práci. Dějiny civilizace jsou snahou o co nejlepší život s co nejmenší námahou. Proto vzhlížíme k automobilům, počítačům anebo Bitcoinu. Stovky milionů lidí již nemusí dělat zbytečnou práci a mohou se věnovat něčemu užitečnějšímu. Bitcoin má moc eliminovat obrovské množství práce ve finančním sektoru. Finanční sektor tvoří v západním světě zhruba 10 % HDP a zaměstnává kolem 5 % pracovní síly. Každý dvacátý člověk by mohl dělat produktivnější a užitečnější činnost (přestože se se ztrátou zaměstnání nutně pojí i některé smutné příběhy). To je neuvěřitelné množství prostředků, které mohou přinést zásadní civilizační růst, stejně jako tomu bylo v případě knihtisku, spalovacího motoru, osobních počítačů, internetu a dalších velkých vynálezů dějin.

A nejenže práci šetří, ale vytváří nové podnikatelské příležitosti. Bitcoinové startupy vyrůstají jeden za druhým, řada lidí se snaží uchytit v novém odvětví hned zkraje a získat tak jistou výhodu před konkurencí, která se bude chtít velmi záhy objevit. Lidé v sobě objevují to, co významný americký ekonom Israel Kirzner nazval „ostražitostí" – sledují svět kolem sebe a nachází v něm realizovatelné ziskové příležitosti. Vznikají tak nové a lepší

služby, které platby pomocí bitcoinů usnadňují, nové a lepší technologie těžby a koneckonců také nové, a v něčem i lepší kryptoměny samotné.

Bitcoin je byznys. Bitcoinová hazardní stránka primedice.com dokázala za první tři měsíce existence vytvořit obrat ve výši 15 milionů dolarů. To přitahuje další a další konkurenty, kteří chtějí část těchto zisků pro sebe. Primedice.com musela zlepšovat své služby, inovovat, nebo by si zisky neudržela. Zákony svobodné mezilidské interakce jsou neúprosné. Pooly, které byly dříve na pokraji 51 procent výkonu sítě, mohou ze dne na den spadnout na praktickou nulu, služby typu BitPay, které za poplatek usnadňují přijímání bitcoinů, dnes vydělávají obrovské peníze, ale konkurence přichází s inovativními postupy – a pochopitelně i s nižšími poplatky. To, co se v roce 2008 mohlo zdát jako sci-fi, je o pár let později realitou. Za bitcoiny se dá letět do vesmíru.

Podobný vývoj jsme již zažili s masovým nástupem internetu. Začaly vznikat první pokusy zpříjemnit jeho užívání i lidem, kteří příliš nerozumí počítačům – objevily se první internetové prohlížeče, vyhledávače a katalogy webových stránek a jednotlivé služby si vzájemně konkurovaly. Některé projekty se staly historií, na jiných jejich zakladatelé vydělali jmění. Zatímco v roce 1990 neexistovala ani jedna webová stránka a v roce 1997 jste si mohli klidně zaregistrovat doménu google.com, již v roce 2012 měl Facebook miliardu uživatelů a Google utržil příjmy přes 50 miliard dolarů.

Bitcoin může být stejný, ponechá-li se mu volnosti, které se dostalo internetu. Kde může být svět kryptoměn za deset let, podíváme-li se na příklad internetu, není ani ve hvězdách, ale kdesi na temném konci vesmíru.

Soukromé blockchainy

Banky všeobecně Bitcoin vnímají skepticky. Není to dáno jenom tím, že ho považují za konkurenci, pokud o něm vůbec přemýšlejí. Bitcoin pro ně má i řadu praktických nevýhod.

První zjevnou nevýhodou je pomalé potvrzovaní transakcí. Transakce se zapíše do blockchainu až po deseti minutách, a to je pro používání u mikrotransakcí nepraktické. I kdyby chtěli

používat blockchain pro velké platby, problémem je transparentnost. V blockchainu je možné sledovat transakce, a toho se mohou bát významní klienti, kteří spíše preferují soukromí. Navíc platby nelze z definice vracet, vlastnictví bitcoinů je totální. Do toho všeho potom přichází regulační nejistota, i kdyby se jim Bitcoin líbil sebevíc. Neví, zda se proti němu nepostaví vlády, a nepoškodí tak jejich reputaci. Posledním problémem je pak samotná těžba, u které nemají banky žádnou možnost kontroly.

Přesto se řada velkých bank rozhodla do Bitcoinu zainvestovat, a to zejména do technologie, na které funguje, do blockchainu. Blockchain je natolik robustní, že by banky jeho implementací mohly ušetřit významné sumy. Není to ale tak jednoduché.

Banky by totiž rády zachovaly jen některé části bitcoinové technologie a jiné změnily. Je to ale vůbec možné? Bitcoin funguje zejména kvůli motivaci těžařů, kteří ověřují transakce s vidinou výdělku. Pokud by banky spustily svůj vlastní omezený blockchain a vydávaly omezené povolenky pouze ověřeným těžařům, přestává mít tento model smysl. Blockchain samotný je pouze jiným způsobem implementace databáze pro ukládání dat o transakcích. Banky by tak pouze nahradily své databáze blockchainem, ale bez jeho největší výhody, decentralizace. Soukromé blockchainy se zdají jako nesmysl.

A nejde jen o soukromé banky. I centrální banky začaly koketovat s myšlenkou, že by si vytvořily vlastní kryptoměny. I pro ně však platí to samé. Pokud by nechaly měnu decentralizovanou, potom by jen vytvořily další altcoin podobný Bitcoinu a nedávalo by příliš smysl ho používat. Kdyby si naopak nechaly centrální banky nad měnou kontrolu, vytvořili by nakonec to samé, co už dávno mají.

Válka o Bitcoin

První bitvy

Překotný vývoj Bitcoinu směrem vzhůru se na první pohled zastavil. Přelom roku 2013 a 2014 začal být zejména z popudu bývalého starosty kanadské Ottawy a fanouška Bitcoinu Larryho O'Briena nazýván začátkem války o Bitcoin. Spíše než o Bitcoin samotný, který se nijak významně nezměnil a stále bez problémů funguje, jde o válku o veřejné mínění. Pokud si široká veřejnost bude myslet, že je Bitcoin složitý, že se s ním financuje terorismus anebo ho jednoduše nebude smět koupit, protože to zakážou nebo jen nedoporučí regulatorní orgány velkých zemí, potom tuto válku Bitcoin prohraje.

Na začátku prosince 2013 nejprve zakázala Čínská centrální banka obchodovat bankám s bitcoinovými burzami a brzy se přidalo Rusko s varováním před kryptoměnami. Přestože byly obě zprávy prakticky neúčinné, změnily veřejné mínění. Informace jsou vzácné a nákladné na získání, takže se nelze divit, že se lidé bez většího zájmu o Bitcoin do jeho nakupování příliš nepohrnou, pokud uslyší podobné zprávy, nehledě na jejich základ. Když pak v roce 2017 Rusko s velkou parádou pozatýkalo ozbrojeným komandem mladé kluky, kteří poskytovali služby spojené s Bitcoinem, nechtělo se nám tomu věřit. Stejně tak, když Čína ve skutečnosti ve stejném roce obchody s Bitcoinem reálně omezila. Padly první výstřely.

Události, které mohou obracet veřejné mínění, mohou nabývat různých podob. V lednu 2014 zatkla americká policie místopředsedu Bitcoin Foundation a zakladatele jedné z prvních BTC burz BitInstant Charlieho Shrema. Shrem byl spolu s obchodníkem Robertem Faiellem, známým jako BTCKing, obžalován z praní špinavých peněz a provozování peněžního zprostředkování bez licence. 24letému Shremovi hrozilo 25 let vězení a Faiellovi o pět let méně. Podle americké policie Shrem prodal svým zákazníkům na burze přes 1 milion dolarů v bitcoinech, které byly následně použity k nákupu drog na nelegálním serveru Silk Road. BTCKing údajně prodával bitcoiny přímo na Silk Road, takže musel vědět, že se za ně bude nakupovat nelegální zboží, a Shrem věděl o tom,

co Faiella dělá, a sám si prý také na Silk Road koupil drogy. Shrem byl nakonec odsouzen na konci roku 2014 ke dvěma a BTCKing ke čtyřem letům vězení. Dnes je první jmenovaný na svobodě a dále propaguje Bitcoin.

Dalším krokem k podlomení důvěryhodnosti Bitcoinu bylo smazání všech BTC aplikací, které lze nainstalovat na tablety a telefony od společnosti Apple. Technologický gigant se tak rozhodl ignorovat své starší motto, že pouze „neposední rebelové, kteří nemají žádný respekt ke statu quo a vidí svět jinak" mohou změnit svět, a své neposedné uživatele odřízl od světa Bitcoinu. Apple se rozhodl jít proti Bitcoinu, čímž nezanedbatelně snížil jeho možnosti a s tím i hodnotu. Na internetu se hned začaly objevovat petice, videa naštvaných zákazníků, kteří různými způsoby ničí své iPhony, ale po dlouhou dobu se nic nezměnilo.

Navíc se Bitcoinu začaly čím dál více věnovat velké komerční banky. Bohužel negativně. Jedna z největších bank na světě, americká JPMorgan, vydala zprávu, ve které kritizuje Bitcoin jako „velmi podřadný oproti fiat měnám". Její šéf se začal opakovaně v roce 2017 vyjadřovat proti Bitcoinu. Nakonec ale vyšlo najevo, že jeho banka sama bitcoiny nakupovala. Australská Commonwealth Bank zmrazila účet zakladatelům bitcoinové peněženky CoinJar. Vedle toho všeho přišly i problémy BTC burz, zejména krach Mt.Gox a pozdější problémy Bitfinexu.

Po teroristických útocích v Paříži v listopadu 2015 informovala agentura Reuters, že členské země EU na příkaz Evropské komise zasáhnou proti anonymním platebním systémům, jako jsou kryptoměny. Vyšetřovatelé se totiž domnívali, že útočníci měli část příjmů v bitcoinech…

A nakonec i příchod silné konkurence a vysoké poplatky.

Zhroutí se nyní Bitcoin a upadne v zapomnění?

Vítězná linie

S téměř absolutní jistotou nikoliv. Obchod s bitcoiny v Číně a v Rusku rostl navzdory zprávám regulátorů. Stejně tak obchod kvete ve zbytku světa, kde mnoho zemí slaví své první směny zboží za BTC. Zatčení Shrema nemá nic společného se samotným

Bitcoinem. Jakkoliv jde o právně otevřený případ, podle zpráv policie Shrem pouze prodával měnu, kterou další lidé užívali k nelegálním činnostem, což samo o sobě nic nelegitimního není, a možná ani nelegálního. Navíc obžaloba často neznamená vinu, přestože se čím dál více zdá, že tyto dva pojmy v médiích splývají v jeden. Nyní je Shrem venku z vězení a pomáhá vyvíjet bitcoinové aplikace.

Apple může zakazovat bitcoinové peněženky, ale tím škodí pouze sám sobě. I po zákazu šlo užívat webové peněženky a vývojáři se snaží uživatelům prostředí co nejvíc zpříjemnit. Vznikaly tak nové projekty, jako je Coinpunk s podtitulem „peněženka, kterou Apple nemůže zakázat". To, co jedni vidí jako konec, vidí druzí jako příležitost. Svobodná práce je kreativní, užitečná a v konečném důsledku pomáhá nám všem. Nakonec i Apple povolil a dnes je možné jeho telefony použít k platbám bitcoiny. Na podzim roku 2015 dokonce vyšel Bitcoin i na obálce časopisu The Economist s titulem „The Trust Machine". V článku se výmluvně píše: „Jednoduše řečeno, [blockchain] je stroj na vytváření důvěry." Jen za posledních pár měsíců psaní této knihy byl její první autor šestkrát v České televizi mluvit o Bitcoinu. Bitcoin se stává hlavním proudem.

A i banky obrátily. Řada z nich se začala Bitcoinu věnovat a snaží se hledat způsob, jak využít blockchain. Banky Goldman Sachs a Santander investovaly do Circle Internet Financial a Ripple, Visa oznámila na konci roku 2015, že pracuje na systému založeném na blockchainu, jenž by usnadnil remitance, a nakonec desítky velkých bank se setkaly v nadějném startupu R3, jenž chce přiblížit technologii za Bitcoinem tradičním bankám a pomoci jim ji využít. Je mezi nimi Bank of America, Morgan Stanley, Goldman Sachs, JPMorgan a Citi, německé Commerzbank a Deutsche Bank, anglické banky Barclays a HSBC, španělská BBVA, australská National Australia Bank, kanadská Royal Bank of Canada, švédské banky Nordea a SEB, francouzská Societe Generale, švýcarské banky UBS a Credit Suisse, skotská Royal Bank of Scotland, japonská Mizuho Bank, italská UniCredit Bank, nizozemská ING a další. Zakladatel R3 David Rutter se během půl roku stal jednou z nejvýznamnějších postav světa kryptoměn. Jakkoliv to vypadá, že jdou cestou úplně mimo blockchain, proč ne? Třeba na něco přijdou. Důležité je zkoušet.

Zhroutí se Bitcoin někdy v budoucnu a upadne v zapomnění?

Dost možná ano. Bitcoin je první, a přestože první má výhodu, neznamená to nutně, že nemůže přijít lepší konkurence. Vyhledávali jsme na Yahoo!, když ještě neexistoval Google. Psali jsme si na ICQ a zdálo se, že žádný jiný messenger nikdy nemůže ani vzniknout, když jsou všichni Češi na ICQ. K čemu zakládat nové sociální sítě, když už jsou stejně všichni na MySpace? Stačí měsíce, maximálně roky a realita se mění. Většina průkopnických sociálních sítí nebo vyhledávačů dnes ani neexistuje. Na volném trhu se hráči mění každý okamžik. Musí přicházet s novými a lepšími produkty, musí se o své zákazníky prát. A to i na trzích s velkým síťovým efektem, jako jsou například sociální sítě. To, že všichni něco používají, nutně neznamená, že to tak budou dělat vždy.

Stejné je to i s penězi, které jsou sociální sítí svého druhu. Nikoho nepřekvapí tvrzení, že Facebook nejspíš nebude navždy jedničkou mezi sociálními sítěmi. Stejně tak mění lidé své peníze, ba i celé peněžní systémy. Jestli Bitcoin jednou nahradí tradiční měny, může být sám později nahrazen jinou, ještě lepší měnou. Patrně však takovou, která by bez něj nemohla nikdy vzniknout.

Předvídat budoucnost neumí nikdo, ale jedno se dá napsat s jistotou: Bitcoin změní svět. K lepšímu.

Doslov

Tečka za tečkou, blok za blokem

Bitcoin není tečkou. Bitcoin je inovace, která otevírá dveře. Knihtisk nebyl sám o sobě revolucí, ale ve spojení s dalšími tisíci a miliony drobných i velkých vynálezů vedl k současnosti, k lepšímu světu. Kdyby zůstal ve své původní podobě a využíval se pouze k tisku biblí, byl by jistě inovací stále zajímavou, ale nekonečně méně významnou. Stejně tak tomu bylo u rádia, počítačů nebo internetu. Internet byl důležitý vynález, ale svůj obrovský význam získal až s nespočtem různých způsobů, jak ho využít k práci, zábavě, uspokojování lidských tužeb a potřeb.

Také Bitcoin je zajímavou inovací. A právě nyní hledá své miliony způsobů využití.

Najde je. Lidská kreativita ve svobodném světě je nekonečná.

Na cestě dějinami jsme zažili neustálý boj o moc lidí nad lidmi. Vedle přímočaré nadvlády jedněch nad druhými ve formě otroctví, válek, daní a monopolních privilegií se vládám po celém světě podařilo plně ovládnout peníze.

Současné státní peníze jsou vítězstvím socialismu. Pátým bodem desatera Komunistického manifestu Karla Marxe a Bedřicha Engelse z roku 1848 byla „Centralizace bankovnictví v rukou státu prostřednictvím centrální banky". Dnes už považujeme centrální banky za standardní symbol svobodných tržních ekonomik, ale nic nemůže být vzdálenější pravdě. Monopolní privilegia vytvářet peníze z ničeho a zavírání lidí do vězení za nabízení alternativ nemají se svobodou společného vůbec nic.

Současné peníze jsou nesvobodné. Bitcoin je osvobodí. Bitcoin není bublina. Bitcoin je špendlík. Špendlík namířený na centrální bankovnictví.

Byli jsme svědky vytvoření nové komodity, nad kterou nelze mít centralizovanou moc a kterou nelze svévolně nafukovat. A lidem se začala líbit. Proč používat peníze, které se systematicky znehodnocují a u kterých musíme každé ráno doufat, že se do jejich správy nedostane zlý nebo hloupý člověk, který by se rozhodl snížit jejich hodnotu o desítky procent, aby pomohl svým vlastním zlým či

hloupým plánům? Proč, když máme možnost držet peníze, které se systematicky zhodnocují, kdykoliv jsme produktivnější, kdykoliv je vyšší konkurence a kdykoliv vymyslíme nové technologie?

Na své zatím krátké cestě dějinami zažil Bitcoin růsty i pády. Zájem o něj však roste. A lidé ho používají čím dál více. A to navzdory tomu, že musí z donucení používat státní alternativu. Také v následujících letech bude prožívat své krize. Východisko z nich se bude hledat v krátkozrakých řešeních. Vy, čtenáři této knihy, máte své místo v této důležité revoluci. Na vás, uživatelích, stojí budoucnost Bitcoinu. Je na vás, abyste odmítli právě ta krátkozraká řešení a hledali řešení pevná, dlouhodobá a zásadová.

Je nesmírně důležité, aby stál Bitcoin na pevných základech. Čím více pak budou v problémech státní peníze, tím lépe na tom bude Bitcoin. Budou státy proti lepším penězům bojovat? Alespoň se ukáže, kvůli komu doopravdy existují. A pokud se státy vzpamatují a vrátí peníze lidem? Potom by Bitcoin nemusel být potřeba. Tak nebo tak Bitcoin svou roli v dějinách peněz splní.

Buďme u toho.

Rejstřík technických pojmů

Adresa (Address) 38
Asymetrická kryptografie (Public Key Cryptography) 114
BIP (Bitcoin Improvement Proposal) 122
Bitcoin 20
Bitcoin Core 123
Blok (Block) 37
BTC 32
Dvojitá útrata (Double Spend) 27
Escrow 185
Fork 124
Generující transakce (Generation) 87
Genesis blok (Genesis Block) 37
Hardfork 127
Hash 84
Hashovací rychlost (Hash Rate) 85
Kontrakt 138
Kryptografie (Cryptography) 25
Ledger 144
Maleabilita transakce (Transaction Malleability) 58
Mempool 136
Merged Mining 149
Multisig 137
P2P 24
Peněženka (Wallet) 43
Pool 41
Poplatek za transakci (Transaction Fee) 70
Podpis (Signature) 156
Potvrzení (Confirmation) 83
QR kód (Quick Response Code) 73
Replay Protection 132
Řetěz bloků (Blockchain) 28
Segwit 131
Softfork 126
Soukromý klíč (Private Key) 90
Testnet 141
Těžba (Mining) 82
Transakce (Transaction) 45
Veřejný klíč (Public Key) 92

Lidí, bez kterých by tato kniha nemohla vzniknout, je dlouhá řada. Zvláštní poděkování si ale zaslouží:

Barča Nedvědová

Martin Pánek

Liberální institut (www.libinst.cz)

Jakub, Didi a Fanda z AltLift s.r.o.

Andrej Cabaj

Aleš Janda

Hynek Jína

Jan Tomášek

Josef Olšák

Robin Pokorný

Pavel Peterka

Iveta Cvrčková a Lukáš Teplý (ať jste brzy doma!)

Ji[rt]ka Černovští a Ida Lozanová (za akceschopnost)

Petr Kuška a Michal Kružík

Pavel Faltýnek

Zuzana Tejnická

Marta Kozlerová

Kryptoměny představují jednu z cest, jak se do jisté míry osvobodit od státní nadvlády a útlaku. Chcete znát i jiné cesty? Nebo dokonce váháte, zda je to vůbec potřeba? Odpovědi a především mnoho dalších zajímavých otázek naleznete na webu www.urza.cz.

Urza

www.penizebudoucnosti.cz

www.stroukal.cz **dominik@stroukal.cz**
www.linkedin.com/in/jan-skalicky **bitcoin@skalda.org**

Edice Finance pro každého

Mgr. Ing. Dominik Stroukal, Ph.D., Ing. Jan Skalický
Bitcoin a jiné kryptopeníze budoucnosti
2., rozšířené vydání

Vydala GRADA Publishing, a.s.
U Průhonu 22, Praha 7
tel.: 234 264 401, fax: 234 264 400
www.grada.cz
jako svou 6821. publikaci

Realizace obálky a sazba Karel Novotný
Počet stran 200
Vytiskla tiskárna Tisk Centrum s.r.o., Moravany
Druhé vydání, Praha 2018
První vydání vyšlo v roce 2015 jako Bitcoin: Peníze budoucnosti

ISBN 978-80-271-0818-3 (ePub)
ISBN 978-80-271-0817-6 (PDF)
ISBN 978-80-271-0742-1 (print)

„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.“

prof. Ing. Josef Šíma, Ph.D. | rektor, VŠ CEVRO Institut

„Jako bankéři nemusíme v Bitcoinu vidět jen spekulativní příležitost, ale také vstupní dveře do digitálního světa finančních inovací. Tato kniha může být klikou ke zmíněným dveřím.“

Ing. Vlastimil Nešetřil, Ph.D. | výkonný ředitel, J&T Banka

„Kromě zájemců o kryptoměny knihu doporučuji i studentům ekonomie.“

Mgr. Vítězslav Línek, Ph.D. | matematik

„Autoři jsou přední čeští odborníci na Bitcoin a kryptoměny obecně.“

Marek „Slush“ Palatinus | tvůrce první hardwarové peněženky TREZOR, SatoshiLabs

Poznejte svět kryptoměn rychle a jednoduše s touto knihou

Mgr. Ing. Dominik Stroukal, Ph.D. vystudoval Národohospodářskou fakultu VŠE v Praze a Fakultu sociálních věd UK, kde se věnoval sociologii médií. V současnosti je ředitelem Liberálního institutu, zakladatelem společnosti Bit Agency a přednáší ekonomické předměty na VŠ CEVRO Institut a několika dalších školách. Profesně se věnuje ekonomii médií, teorii ekonomických systémů a kryptoměnám.

Ing. Jan Skalický vystudoval výpočetní techniku na Elektrotechnické fakultě ČVUT. V současnosti pracuje jako SW architekt a lektor kurzů programování. Kromě pozic specialisty vývoje mikropočítačových systémů pracoval i v jaderné elektrárně Temelín. Je příznivcem rakouské ekonomické školy, klasického liberalismu a decentralizovaných systémů, mezi něž patří i Bitcoin a jiné kryptoměny.

GRADA®

GRADA Publishing, a.s.
U Průhonu 22, Praha 7
obchod@gradapublishing.cz
www.grada.cz

ISBN 978-80-271-0742-1