S předmluvou Jeffreyho Tuckera

Bitcoin

PENÍZE BUDOUCNOSTI

HISTORIE A EKONOMIE KRYPTOMĚN,
STRUČNÁ PŘÍRUČKA PRO ÚPLNÉ ZAČÁTEČNÍKY

DOMINIK STROUKAL
JAN SKALICKY

BITCOIN
PENÍZE BUDOUCNOSTI

Historie a ekonomie kryptoměn,
stručná příručka pro úplné začátečníky

Dominik Stroukal
Jan Skalický

Praha, 2015

Vlastník: Institute for Direct Democracy in Europe

Vydal: Ludwig von Mises Institut CZ&SK

Sazba a obálka: [ds]

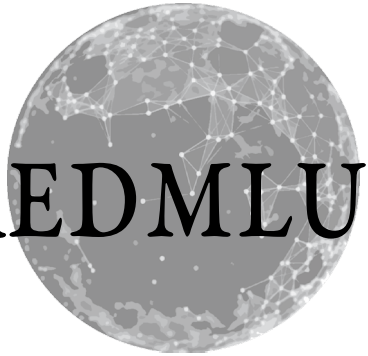
Překlad předmluvy: Jakub Žofčák

Předmluva vyšla v článku Elisabeth Ploshay 4. 1. 2014 na

https://bitcoinmagazine.com/articles/word-jeffrey-tucker-bitcoin-monetary-system-1388799989

ISBN: 978-80-87733-26-4

OBSAH



Předmluva

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 mld. 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, kryptografie a vývoje process-oriented softwaru – 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. Ne-

stačilo pouze to, že tiskla peníze, že dozírala na celý systém a že určovala, co je podstatou peněz. Nikoli – 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 stále 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 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 měrách 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: svo-

bodného 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, s jejich vlastním majetkem, v rámci spojení jejich vlastních výtvorů a jejich 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 jakéhokoli 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

Úvod

ALTERNATIVA EURA A NÁRODNÍCH MĚN? 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 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 nezbyde 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 bitcoin, platí bitcoinem, miluje bitcoin. Dokonce je mu vyčítáno, že to s láskou k němu přehání.

Nedivím se mu.

Když jsem slyšel v roce 2011 o bitcoinu poprvé, považoval jsem ho také za nesmyslnou hru. Peníze přeci 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 na to už jsem stál před přeplněnou přednáškovou aulou na Vysoké škole ekonomické na přednášce European 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 nejvyšším bodě obrázku ukazujícího 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 byla na obzoru alternativa. 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 kniho 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

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) je 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.

Kryptoměna bitcoin byla vytvořena v roce 2009 anonymním vývojářem pod pseudonymem Satoshi Nakamoto na základě průvodního článku, který publikoval v říjnu roku 2008. Sám na internetovém fóru 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 Gavinovi Andersonovi. Následně se úplně odmlčel a dodnes se neví, kdo se za tímto zvučným japonským jménem skrývá. 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 chtělskrýt 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 je 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 2 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, potom je to zcela pochopitelné.

Spekulace se začaly šířit. Za autory byli označeni i následní vývojáři bitcoinu Hal Finney, Gavin Andresen a 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 a 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."

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 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 iniciálech 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**". 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 je 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 pouze jemu určenou transakci. Čím větší počet potvrzení (viz **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, které musí svoji 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.

Blockchain je 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 block", 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 (typicky pouze pokud je aktuální blok vytěžen nezávisle v podobném čase) 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 chainu 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 dvojitého utrácení 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 mikro-platby 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 všimnul, 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. Žalobkyně 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 jí 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 Athura 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 milión 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 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 problém). 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 Dollars nebo E-gold. Nesmí být pouze jiným zápisem tradičních měn, jako Mondex. Ale protože především nesmí docházet k dvojitým transakcím, 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 (označovaného 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 velká pro běžné drobné obchody, existují odvozené jednotky mBTC (milibitcoin; 1 mBTC = 0.001 BTC), uBTC (mikrobitcoin; 1 uBTC = 0.001 mBTC) a satoshi (1 satoshi = 0.01 uBT = 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 přešktnuté 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 zjevně má. 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 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 nemá 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 Salvatora Dalího se může měnit v závislosti na poptávce a okolních cenách, ale neexistuje žádná ten-

dence k tomu, aby se jejich cena snižovala na cenu plátna a použité barvy. Jeho obrazy jsou totiž vzácné.

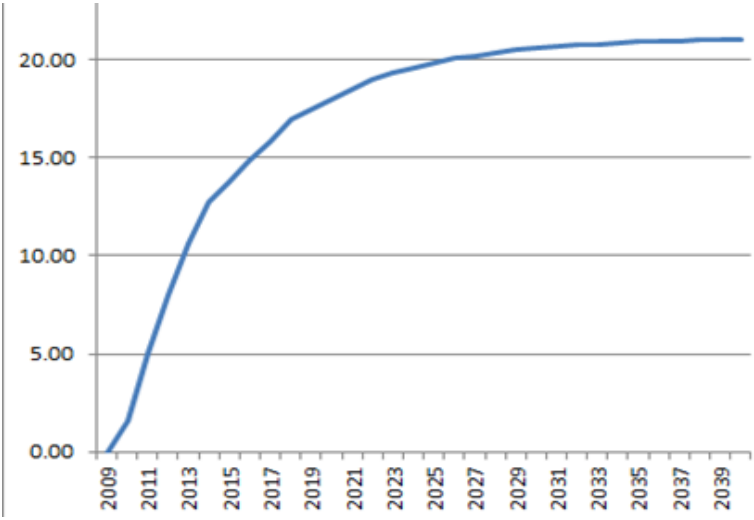
Peníze bez tiskárny

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 všimnul 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 jeho 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.

Satoshi Nakamoto se patrně inspiroval u zlata a zafixoval zásobu své virtuální měny na 21 milionů bitcoinů (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 bitconů 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.

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

Revoluce mohla začít.

Blok je 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 odlišné koncepty, jako je „proof of stake“ a další).

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.

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 blokem Genesis 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.

Bitcoinová adresa je jednoznačnou identifikací 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
- rozlišují se velká a malá písmena
- začíná označením verze – číslicí '1' nebo '3' (novější)
- neobsahuje typograficky zaměnitelné znaky '0', 'O'; 'I', 'l'
- poslední znaky obsahují kontrolní součet (zabezpečení proti špatnému opsání/vykopírování)

příklady:

- 1CttXfQpZ3w2oG3zmcBqwwoceVzsH4DPNC
- 14DRZCpgUvt9bSv682DHfB9CLooPC9hkVq

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! Pět milionů dolarů, tedy zhruba sto milionů českých korun za jednu pizzu. 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 miliónové 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 start-upů, 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 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 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

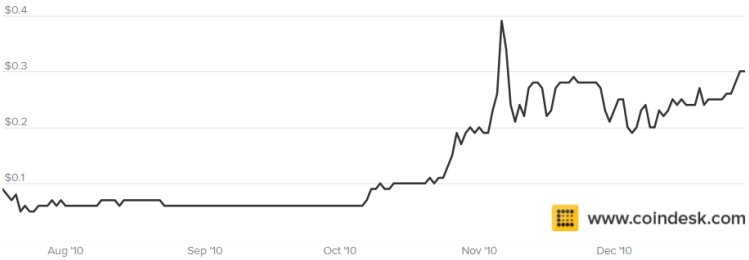
indexem cen. Dolarový svět má svůj BigMac index, svět digitálních měn zná Bitcoin pizza index.

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 bitcoin 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 vzniknul první těžební **pool**, který založil Čech Marek Palatinus, na internetu známý jako slush. Bitcoin rost.

Pool je 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 navzájem 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; pokud uzel nalezne hash s „pravým" cílem, bude tento s jistotou mezi nimi).

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 nabídnul 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.

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 můžou 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.

Peněženka je 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.

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 hodnota 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 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

Transakce je 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 obsahující 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 svojí adresu (může být stejná jako adresa rozměňovaného výstupu). K uvolnění výstupu (jeho použití na vstupu nové transkace) 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 „smlouvy" („contracts") a programují se ve skriptovacím jazyce, jehož triviální větou je i běžná podmínka na výše zmíněný podpis klíčem patřícím k adrese.

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.

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 bitcoinu 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 Andersen.

A nejen krádeže. Majitel v té době třetí největší burzy Bitomat v červenci roku 2011 oznámil, že ztratil přístup k souboru, v kterém byly uloženy bitcoiny uživatelů. Ti tak přišli celkem o 17 tisíc bitcoinů, tedy zhruba 10 miliónů 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, zbraně 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 miliónů 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 vrchnímu zástupci 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 bitcoin se již dříve dalo koupit auto nebo příspěvek na chod WikiLeaks a dalších serverů. Avšak šlo pouze o individuální případy a dlouho se čekalo na okamžik, kdy začnou bitcoin 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. WordPress byl díky své velikosti a rozšíření skutečně důležitým partnerem bitcoinu.

A přidávali se další. Objevily se první restaurace, kde bylo možné útratu platit v bitcoinech, první lékař, právník, první taxi služby, vznikly větší obchody s různým fyzickým zbožím apod. Vedle toho rostly pochopitelně i možnosti získat za bitcoin ryze elektronické

zboží, zejména software, online předplatné či přístup do placených částí webových stránek.

A nakonec hazard. 24. dubna 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 by 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 kasína 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 a zvyšuje ho i regulace, která 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 můžou 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 bitcoin 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.

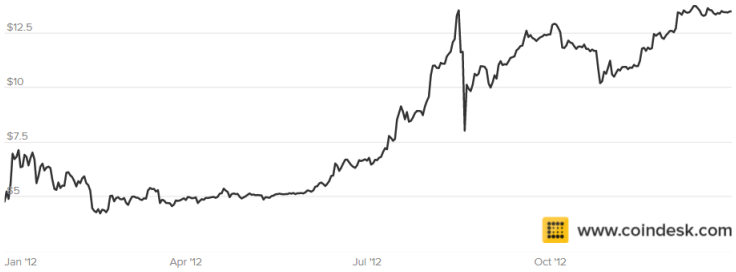
Žít bitcoin

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 bitcoin vlastnit, protože sami nevíte, co s ním, 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 rok od Laszlovy pizzy, jde o neuvěřitelně rychlý vývoj. Tak rychlý, že téměř všechny šokoval. Na konci roku byla dolarová 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 virtuální měny 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 maxima na více než 14 miliardách 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 krytpoměnu. 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 bitcoinem 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.

Na hedvábné stezce

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 před 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 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 ale 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 Ulbircht 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 start-upu 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 plánuje 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.

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.

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. Každý chtěl v roce 2013 k bitcoinu něco říct.

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 nadšeců přehrabujících se v odpadcích na anglických skládkách se dobře prodávaly. 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 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 je 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.

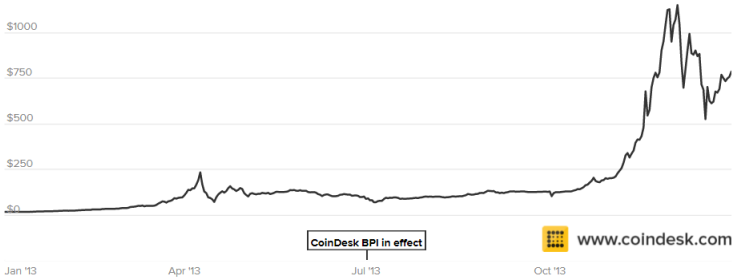
Podobných zpráv o různých zákazech či omezení bitcoinu se objevilo ještě mnoho a vždy byly víceméně vyvráceny nebo revokovány ze strany samotných zakazujících. Asi nejvděčnějším příkladem těchto oscilací je i dosud Čína, která se tak postarala o řadu fluktuací v ceně BTC na burze.

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, chápat jeho pozadí a kontext 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 všimnul 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

vyjde na více než 300 bitcoinů a za pouhých 24 bitcoinů je 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 uběhnul od doby, kdy si Laszlo Hanyecz koupil za 10 tisíc bitcoinů dvě pizzy.



2014–2015: DOLŮ KE HVĚZDÁM

Krach Mt.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 ní 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.

Maleabilita transakce je možnost pozměnění anoncované (dosud nepotvrzené) **transakce** tak, že význam jejích dat se nezmění, ale vzhledem k rozdílu v binární podobě (konkr. 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 transkaci 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.

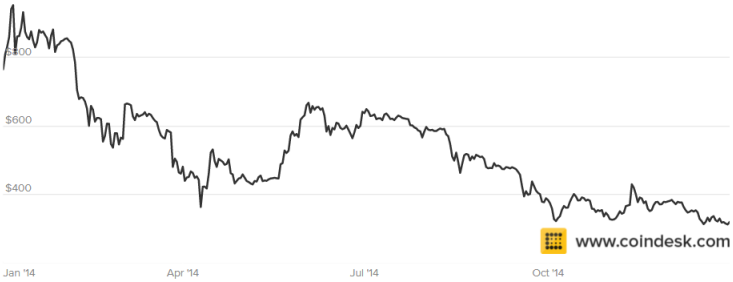
Ačkoliv je tento problém znám od roku 2011, v plné síle se projevil počátkem roku 2014 v souvislosti s krizí nejznámější a nejstarší bitcoinové burzy Mt.Gox, která jím zdůvodnila dočasné pozastavení výběru bitcoinů, což mělo za následek pokles jejího kurzu a zhoršení důvěryhodnosti. Popisovaný problém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

Lidé 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 zavřel asvé stránky a o čtyři dny později zkrachoval oficiálně.

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 bitcoin za soukromé aktivum, z 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. Navrhovali, 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 bit-

coinu 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 dařilo. 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, v 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 hypotetcikou 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 atomsféra 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.

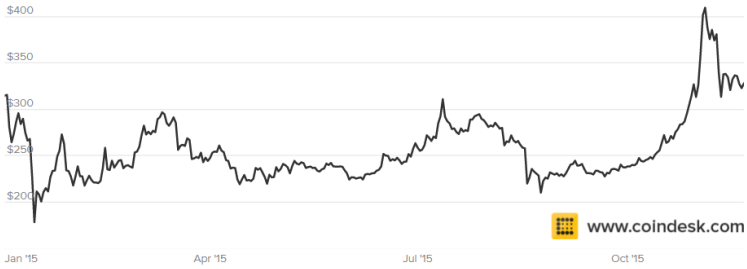
I v Čechách se postupně rozvíjela komunita a infrastruktura. Česká hardwarová peněženka Trezor získala nové funkce, Karel Fillner spustil českou verzi jednoho z nejčtenějších webů o kryptoměnách cointelegraph.cz, v Paralelní Polis se odehrál mezinárodní Hackers Congress, od konce roku 2014 po celý rok 2015 byl každý týden v úterý pravidelný bitcoin meetup, kde se diskutovalo nad širokým spektrem otázek nejen kolem bitcoinu, ale o krytpoměnách 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 rozhodnul, že se na směnu bitcoinů nevztahuje DPH. Soud byl výsledkem soudů 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 rozhodnul, že se na bitcoiny vztahuje ustanovení o transakcích pomocí oběživa, bankovek a mincí v podobě zákonného platidla, a jsou tedy od DPH osvobozeny.



Příručka uživatele Bitcoinu

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. 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.

Prvním, ale ne příliš uživatelsky přívětivým způsobem, jak si pořídit peněženku, je stáhnout si software oficiálního bitcoin klienta (www.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 souboru, který musíte mít uložený na počítači. Na konci roku 2015 dosáhl velikosti téměř 50GB, což je srovnatelné s velikostí dvou až tří moderních počítačových her.

Nejde tedy o zanedbatelné množství dat, a přestože se zatím soubor na většinu současných počítačů vejde, existují úspornější

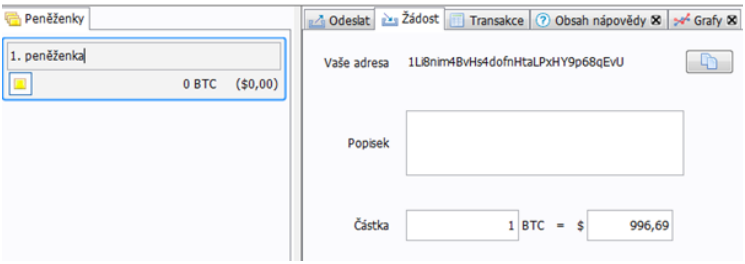
alternativy. O možnost podívat se do blockchainu a stopovat jednotlivé bitcoiny a transakce nepřijdete. Například na stránkách Blockchain.info můžete do této obří účetní knihy nahlédnout přímo z okna vašeho prohlížeče, aniž byste cokoliv instalovali a dalších několik dní stahovali data blockchainu.

Úsporný software

Rozsahem tisíckrát úspornější volbou může být softwarová peněženka. Jednu z nejpopulárnějších softwarových peněženek představuje program MultiBit, který je možno získat na webové stránce www.multibit.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, v kterém budou bitcoiny (přesněji klíče pro přístup k nim) uchovány. Takový soubor má standardně příponu .wallet a můžete si ho libovolným způsobem zálohovat

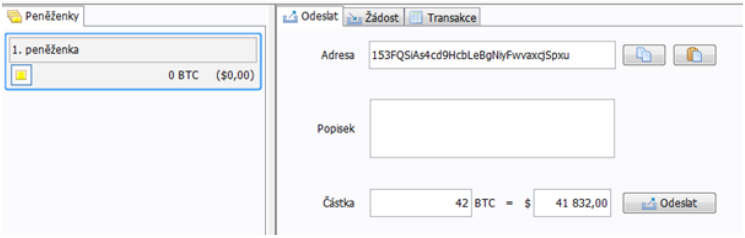
Při jeho zálohování si představte, že ukládáte složité heslo k vašemu účtu u tradiční banky, bez nějž se už nikdy ke svým penězům nedostanete. A navíc má k účtu přístup kdokoliv, kdo toto heslo zná. Můžete si ho uložit doma na pevný disk v počítači připojeném k internetu, ale riskujete tím, že může být 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 kliknutím na „Soubor / Přidat heslo“ si svůj soubor s peněženkou zašifrovat.

Celé prostředí programu je intuitivní a vytvořené pro co nejširší okruh uživatelů. Pokud máte vytvořenou peněženku, můžete se podívat na její adresu (například adresa zde vytvořené peněženky je 1Li8nim4BvHs4dofnHtaLPxHY9p68qEvU).



Tato adresa, která se vám zobrazuje v panelu „žádost“, 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 „odeslat“. Stačí jen znát adresu toho, komu chcete Bitcoiny poslat a částku, na které jste se domluvili. Zde na obrázku se pokoušíme z 1. peněženky odeslat 42 BTC do peněženky s adresou 153FQSiAs4cd9HcbLeBgNiyFwvaxcjSpxu. Popisek transakce není povinný. Jelikož je v peněžence nedostatek bitcoinů, program odeslání nepovolí.



Důležité je, že posílání není zcela zadarmo a platí se malá 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 transkaci je 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**.

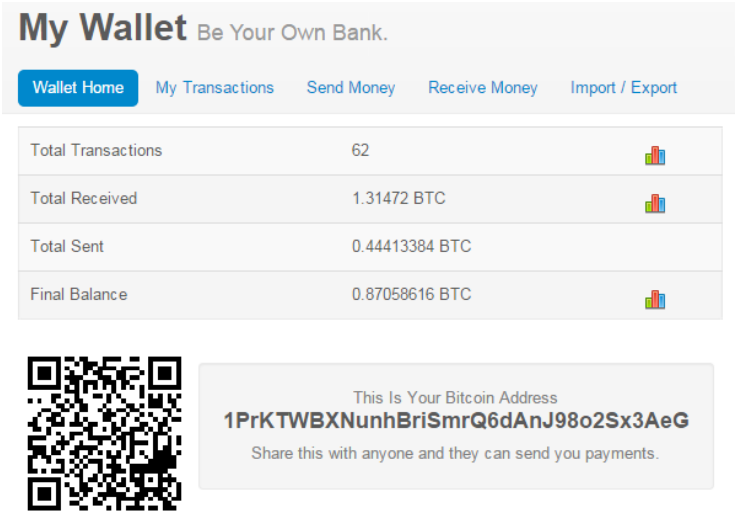
Softwarových peněženek je pochopitelně mnoho. Mezi další oblíbené a fungující na všech operačních systémech patří Electrum, Copay nebo Armory. Za povšimnutí stojí, že se vývojáři přizpůsobují poptávce uživatelů a snaží se zesílit ochranu. Tuto svou snahu tak často vsunou přímo do názvu svého produktu.

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, je zásadní zvolit si důvěryhodného a dobře zabezpečeného poskytovatele. 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.

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 MultiBitu.

Tip: Zaregistrujte se na CoinBase.com



Nyní máte vytvořenu adresu, na kterou si můžete stejně jako v případě MultiBitu 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 naší 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.

Mobilní bitcoin

Blockchain.info a další mají 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 podobně jako MultiBit, avšak své bitcoiny můžete nosit u sebe.

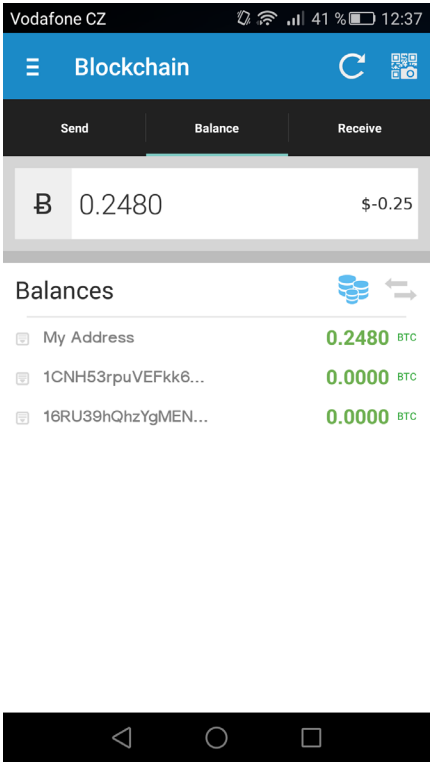
Pro Android patří mezi nejlepší a nejoblíbenější aplikace Mycelium, Coinomi, Copay nebo Blockchain.info. Na iOS potom lze doporučit breadwallet, Copay nebo Bither. Uživatelům Windows Mobile musí stačit Copay a vlastníkům BlackBerry Bitcoin Wallet.

Práce s mobilní peněženkou je intuitivní a mnohem jednodušší než práce s mobilními aplikacemi tradičních bank. Na obrázku je vidět peněženka Blockchain.info, na které je uloženo 0,248 bitcoinu. Ty jsou na jedné adrese v rámci peněženky a na dalších dvou adresách není nic. První adresa je v rámci aplikace pro jednoduchost přejmenována.

Přestože v nastavení v levém horním rohu je k dispozici řada dalších možností, k práci s bitcoinem 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 fotoaparátu před **QR kódem**, címž se aktivuje čtečka QR kódu a po přečtení obrázku se předvyplní adresa a množství. Poté stačí pouze potvrdit odeslání.

QR kód, „Quick Response“ kód je dvourozměrný čárový (spíš „čtverečkový“) kód pro optické strojové zpracování. Je tvořen černými čtverečky v matici o velikosti 21x21–177x177 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 4-úrovňové zabezpečení Reed-Solomon, díky čemuž je odolný proti 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 se tedy na jednom telefonu zmáčknete recieve, vyplníte kolik bitcoinů chcete přijmout, což vygeneruje příslušný QR kód a druhý uživatel kód jednoduše vyfotí a potvrdí. Sestavené celé transakce tak trvá několik sekund.


Vodafone CZ
41 %
12:37
Blockchain
Send
Balance
Receive
Ƀ 0.2480
$-0.25
Balances
My Address
0.2480 BTC
1CNH53rpuVEFkk6...
0.0000 BTC
16RU39hQhzYgMEN...
0.0000 BTC

KDE BITCOIN 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 15000 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 bitcoinu. 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 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.

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 penéze kupovali.

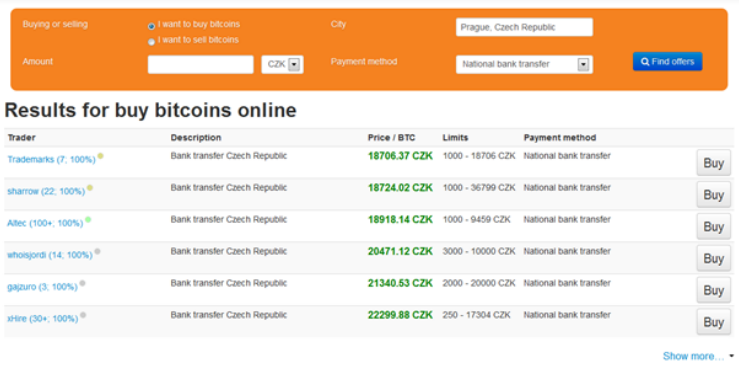
Takových bankomatů je v Čechách několik, v Praze jsou umístěny například v Paralelní Polis, na Arkádách Pankrác, v Centru Nový Smíchov, ve Slovanském domě nebo na Arbesově náměstí. V Brně je bankomat v Galerii Vaňkovka.

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 serverch, 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,

Tip: Kupte si první bitcoiny v bankomatu v Paralelní Polis

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 zpět 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.

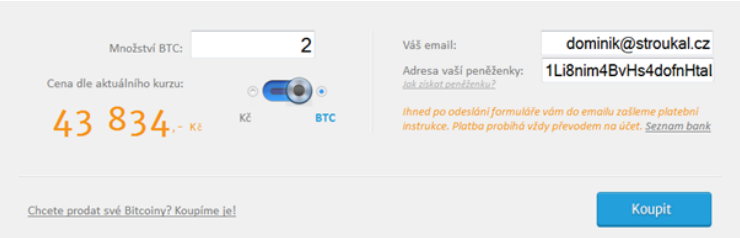
I pokud si ale předáte několikrát nižší částku, ani tak není jednoduché ji vložit na účet. Dle zákona 253/2008 Sb. je obchodem podezřelým z praní špinavých peněz takový obchod, kdy převádíte majetek bez zjevně ekonomického důvodu, provádíte výběry nebo převody na různé účty bezprostředně po hotovostních 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 vysokém rozdílu mezi nákupní a prodejní cenou vydělává.



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 si 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, BTC-e.com, Kraken.com, BTCchina 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.

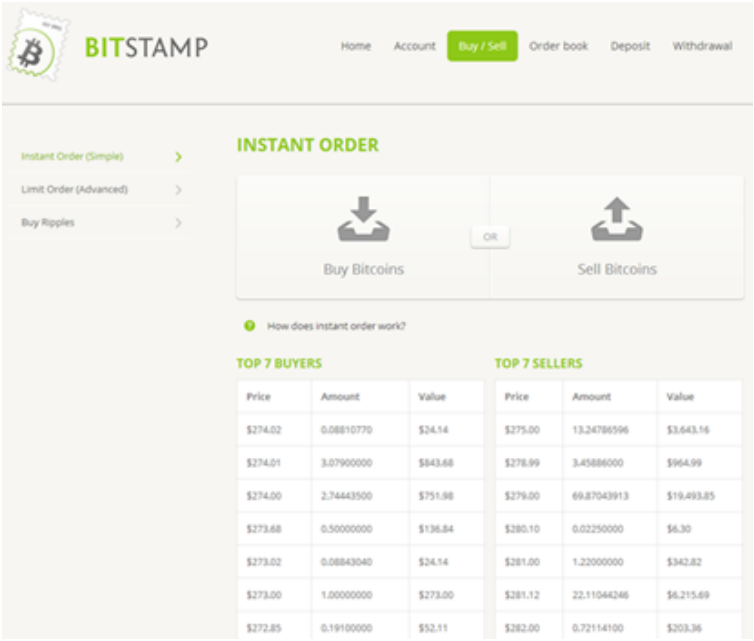
Burza nabízí některé možnosti, které vám Local Bitcoins nebo bankomaty nabídnout nedokážou, ale také má své nedostatky. K tomu, abyste si založili účet na burze, potřebujete v současnosti (postupem času se toto prostředí stále více institucionalizuje) jejich provozovatelům zaslat své osobní údaje. A 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 a dvou týdnech ověřeny, obdržíte e-mail s touto informací a můžete se přihlásit.

Nyní potřebujete na burzu poslat peníze. Korunová burza bitcoinů zatím neexistuje, a tak je nutné zaslat na burzu například 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 výše popsanému ne nepodobnou cestou. 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.

Všem burzám nelze věřit, a o to více po zkušenostech s Mt.Gox. Slušná burza by se neměla stydět ukazovat vlastníka nebo dokonce zemi, v 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 milióny dolarů, už je s nejvyšší pravděpodobností neuvidíte.

Další možnosti

Posledním a nejpříjemnějším způsobem, jak získat bitcoiny, je najít si přátele, které 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) nebo do Baru No. 7 (facebook.com/BarNumberSeven, Na Struze 7, Praha 1) a v Brně se pořádají pravidelné meet-upy na různých místech.

Existovala i doba, kdy se daly bitcoiny koupit pomocí služby PayPal nebo kreditní kartou. Dnes již prakticky nikdo bitcoiny za peníze z PayPalu nebo kreditní karty 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 LocalBitcoins. 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 BITCOIN 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 je 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 zápisu počtem číslic 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.

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 jenáročnější. Když se snažil sám Satoshi Nakamoto vyřešit „nultý" příklad, stačilo mu prakticky pouze zapnout počítač. Byl sám, bitconů bylo vytěženo přesně nula, a tak byla vysoká odměna a extrémně nízkánáročnost úlohy. Postupně se náročnost zvyšovala natolik, že bylo velmi obtížné vytěžit bitcoin 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 5000x 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 (viz dále). 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). Ačkoliv

Potvrzení: **Transakce** se považuje za potvrzenou pokud je obsažena v **blockchainu**. Čím hlouběji je „zabudována"/„pohřbena", tím bezpečnější je pokládat ji za nezvratitelnou. Počet **bloků** mezi blokem zahrnujícím transakci ve svých datech a blokem aktuálně těženým se nazývá 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.

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 je zobrazení z množiny dat obecné délky do množiny dat omezené délky (např. soubor libovolné délky zobrazí do množiny 256-bitových 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 asymetrickou výpočetní složitost (spočítat přímé zobrazení vzor->obraz je snadné, spočítat obecně nejednoznačné inverzní zobrazení obraz->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 upravitelné integrované obvody – hradlová pole typu FPGA, které lze na úrovni hardwaru naprogramovat pro řešení naší úlohy. FPGA je levnější a výkonnější a výnos bitcoinů dokáže oproti GPU až zdesetinásobit.

Skutečnou změnu ale přinesly až kolem roku 2013 zcela specializované integrované obvody typu ASIC. ASIC čip je podstatně dražší, než grafické karty nebo FPGA, ale dosahuje nesrovnatelného výkonu při nízké spotřebě. Výkon ASIC čipů dosahuje až několika miliónů **Mhash/s**, takže srovnání s průměrnou grafickou kartou o výkonu několika stovek Mhas/s neukazuje ani tak řádový nárůst, jako neuvěřitelnou cestu, kterou za pár let bitcoin urazil.

Hashovací rychlost je 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 léty 2009-2013 zvýšil z 1 Mh/s na 10 Ph/s a do konce roku 2015 až na 550 Ph/s (tj. rozdíl o 11 dekadických řádů).

Horníci v bazénu

V dnešním světě tak těží z většiny pouze úzce specializovaní těžaři, kteří zainvestovali statisíce či milióny korun do extrémně výkonných strojů. Sdruženi jsou v několika velkých skupinách – v poolech. Mezi největší pooly patří GHash.IO, F2Pool, AntPool, Eligius, český slushův pool nebo P2Pool. Těžaři tak těží společně a **generující transakce** 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 například GHash.IO nemá žádné poplatky a transakční poplatky sdílí. 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 jeden blok (což bylo zhruba do roku 2013 50 bitcoinů, mezi roky 2013–2016 25 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 0,25 BTC.

Protože má pool 20 % kapacity, v průměru bude úspěšný jednou z pěti pokusů, kdy každý proběhne v průměru jednou za deset minut. Tedy tento těžař by v průměru každých padesát minut získal 0,25 BTC. Pokud by těžil sám, byl by úspěšný jednou z tisíce pokusů, tedy jednou za týden.

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. 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 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.

Na druhou stranu, aby se těžba vyplatila, je dnes zapotřebí investovat do těžby obrovské sumy, mít přístup k levné elektřině

Generující 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 (zhruba 4 roky) se snižuje na polovinu. Toto exponenciální snižování odměny za nově vytěžený blok má za následek omezené množství bitcoinů v kterémkoliv okamžiku. Maximální množtví 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. Generujiící transakce může být jediná transakce zahrnutá v bloku a u prvních desítek tisíc bloků tomu tak bylo.

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 BITCOIN OCHRÁNIT

Bitcoin není jiný

Prolomit bezpečností 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 speciální 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 stejnětak metody útoku jsou dnes 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 MultiBit 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 za-

mykat zase příliš uživatelsky přívětivé. Vznikly tak brzy další metody, jak bitcoin chránit a mnoho vývojářů se snaží právě v této oblasti prosadit tím, že naleznou lepší řešení.

Zpět do reality

Ale stejně jako limit u kreditní karty, tak ani toto řešení není spásné. O zásadní posun se zasadil český startup SatoshiLabs, který vyvinul hardwarovou peněženku zvanou Trezor. Jde o malé zařízení podobné USB donglu, v kterém se skrývá malý jednoúčelový počítač. Trezor zajišťuje, že se při pokusu odeslat bitcoiny z počítače, ke kterému je Trezor připojený, musí ještě fyzicky zmáčknout potvrzovací tlačítko na samotném zařízení. Pokud chcete odeslat bitcoiny vy, potom na Trezoru transakci potvrdíte. Trezor funguje na jednoduchém principu – když chcete poslat z peněženky bitcoiny, škodlivý software může zachytit **privátní klíče** k adresám vašich peněženek, avšak pokud jsou tyto privátní klíče uložené mimo počítač, například v Trezoru, potom není co zachytávat.

Privátní (soukromý) klíč: Jeden z páru klíčů pro **asymetrickou kryptografii** se nazývá soukromý, musí zůstat tajný a majitel ho používá k dešifrování jemu určené zprávy nebo podepisování jím prohlašované zprávy. V bitcoinové síti se pomocí soukromého klíče 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**.

Pokud máte větší množství bitcoinů, je vhodné si hadwarovou peněženku pořídit. Trezor si lze objednat na internetovíé stránce bitcointrezor.com. Po prvním připojení se automaticky stáhne plugin do prohlížeče, který umožňuje snadnou komunikaci

s peněženkou MyTrezor, což je standardní webová peněženka, s jedinou výjimkou. Potvrzování toho, že chcete odeslat bitcoiny, probíhá mimo webovou peněženkou, a to právě v Trezoru. Po připojení a instalaci bude Trezor vyžadovat PIN, bez kterého nelze zapnout. Pokud byste měli už nyní zavirovaný počítač, mohl by virus keylogger číst, jaký PIN zadáváte, proto se PIN zobrazuje na numerické klávesnici na displeji Trezoru a v počítači se zobrazují pouze čtverečky s otazníky. Pořadí čísel na displeji se náhodně mění, a tak není možné, aby případný útočník věděl, jaký PIN jste si zvolili.

Další úrovní ochrany je vytvoření recovery seed, respektive náhodných minimálně dvanácti anglických slov. Tato slova si zapíšete na papír a bezpečně uchováte, protože z nich je možné zpětně obnovit vaše peněženky s uloženými bitcoiny. To je dobrá zpráva, pokud byste svůj Trezor ztratili nebo vám ho někdo ukradnul. Pokud byste chtěli své bitcoiny ještě více ochránit, lze recovery seed ochránit dalším heslem, pokud by někdo například našel onen papír, na který jste si recovery seed zaznamenali.

Následně je vše jednoduché. Pokud odesíláte z MyTrezor peněženky bitcoiny, Trezor vás vyzve k zadání zvoleného PIN tím, že zobrazí náhodně zamíchanou numerickou klávesnici a vy zadáte na monitoru svůj PIN podle toho, jak jsou čísla zrovna zobrazená. Pokud ho zadáte správně, Trezor i počítač vám zobrazí shodnou adresu, na kterou bitcoiny zasíláte. Pokud by se lišily, někdo by ve vašem počítači těsně před odesláním měnil adresu a nechal peníze poslat k sobě. Pokud adresy souhlasí, zmáčknete na Trezoru tlačítko. Následně se Trezor zeptá na částku a pokud i ta sedí, opět zmáčknete tlačítko a transakce se vyšle do sítě.

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.

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 nahackovat, 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. Ta 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 privátní 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 privátní klíč, nebude možné vaše bitcoiny utratit.

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 privátní klíč, který jste si vygenerovali pouze pro sebe, a je stále skryt na papíře. Ve chvíli, kdy chcete

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

skutečně peníze z peněženky odeslat, musíte v dané aplikaci načíst privátní klíč, naskenováním QR kódu v pravé části „bankovky".

Pochopitelně není úplně rozumné použít výše natisknutou adresu, jinak kdokoliv, kdo zde vidí její privátní 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 privátních klíčů je alfou a omegou ochrany bitcoinu.

Papír snese všechno a zdá se, že je to velmi bezpečný způsob uložení privátního klíče. Ale ani zde nelze zaručit, že v počítači není škodlivý software, který privátní klíč zachytil ještě před tím, 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.

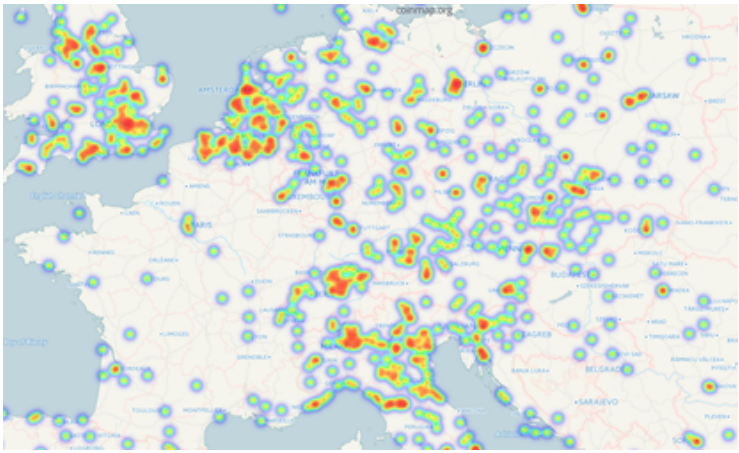
Pro úplnou bezpečnost ale ani to není dostačující a bylo by nutné generovat papírové peněženky z čerstvě instalovaného operačního systému, který by se už nikdy k internetu nepřipojil, a tisk provádět na starých tiskárnách, které není možné napadnout škodlivým programem. Přestože tak lze získat bezpečnou 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

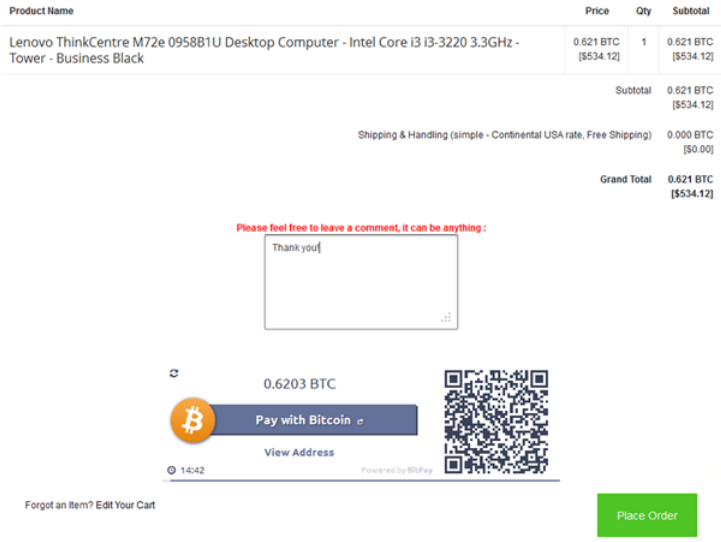
Nyní máme bitcoiny, jsou bezpečně uložené, ale chybí ještě poslední krok. Říká se, že peněz se nenajíme, a u bitcoinu to platí stejně (nebo spíš víc, pokud uvážíme, že papír se sníst dá). Jak se najíst, ošatit a vůbec přežít, pokud jsme všechny zastaralé koruny vyměnili za kryptoměnu? Jde to vůbec?

Nejjednodušším způsobem, jak zjistit, kde je možné utratit své bitcoiny je zavítat na agregující server, například na 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 místech. Pochopitelně však jde jen o zlomek celkového množství.



Tip: Najděte nejbližší obchod na coinmap.org

Podívejme se tedy například na to, jak si koupit za bitcoiny elektroniku. Jako obchod zvolíme například bitcoinstore.com, který nabízí množství různé elektroniky, jako jsou počítače nebo digitální fotoaparáty. 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 MultiBit a další. Pokud máte bitcoiny v telefonu, stačí QR kód naskenovat a platbu potvrdit.



Například peněženka MultiBit se zeptá, zda chcete automaticky předvyplnit adresu a částku. Není důvod programu nevěřit, údaje vyplňuje automaticky a na rozdíl od člověka mu nedělá problém ani dlouhá adresa složená z čísel a velkých a malých písmen. Nyní stačí pouze kliknout na „odeslat" a pokud máte dostatek bitcoinů v peněžence, už si stačí pouze počkat na objednaný počítač.

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

Pokud potřebujete zaplatit z 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 (v našem případě 16jYhCir6GTsq9G7uESdc7RugKpgejWyPY) konkrétní peněženky, kterou systém automaticky vytvořil pro tuto platbu. Obchod tedy očekává, že na tuto adresu dorazí sjednaná suma a nic jiného, přestože by se majitelé privátního 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 bitcoin snadno přijímat?

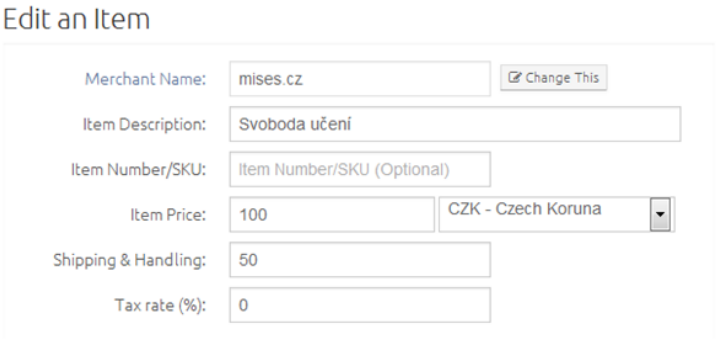
O bitcoinu někteří lidé mluví jako o možném pokořiteli a následníkovi Western Union. Zákazníci Western Union zaplatí za přesun 1000 dolarů 2,5 procenta a musí počkat tři dny, nebo může peníze odeslat okamžitě a zaplatit přes 8 procent, což není zanedbatelná částka ani pro ty, kteří bitcoinu příliš nevěří. 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. 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 až tři 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 je absolutní a ne relativní, 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.

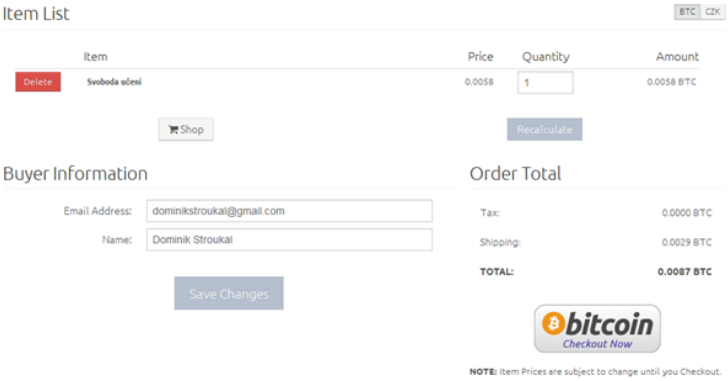
Podívejme se tedy na bitcoin i z druhé strany směny, ze strany obchodníka, který ho přijímá. Pokud chcete za staré rádio v aukci bitcoiny, není nic jednoduššího. Stačí pro aukci vytvořit adresu a čekat na zaplacení.

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 bitcoin, 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.

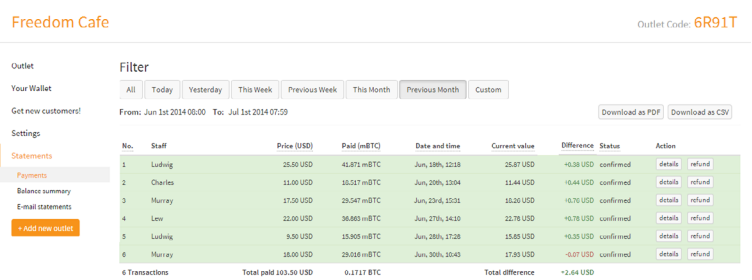


Stačí pouze vložit název a cenu a systém vám automaticky vygeneruje vše potřebné – tedy odkaz, pod nímž se skrývá objednávka. Tento odkaz pak jednoduše vložíte ke svému produktu na stránky. Pokud odkaz sami vyzkoušíte, uvidíte, jak funguje. Stačí vložit požadované informace (které jste si sami zvolili, že chcete

o zákaznících sbírat) a kliknout na velké tlačítko s logem bitcoinu. Po kliknutí se objeví známá obrazovka z předchozího nákupu počítače na bitcoinstore.com. Po kliknutí na „Pay with Bitcoin" se otevře softwarová peněženka a nákup může být dokončen. Vy obdržíte bitcoiny a uživatelé více možností a možná i úplně novou zkušenost.

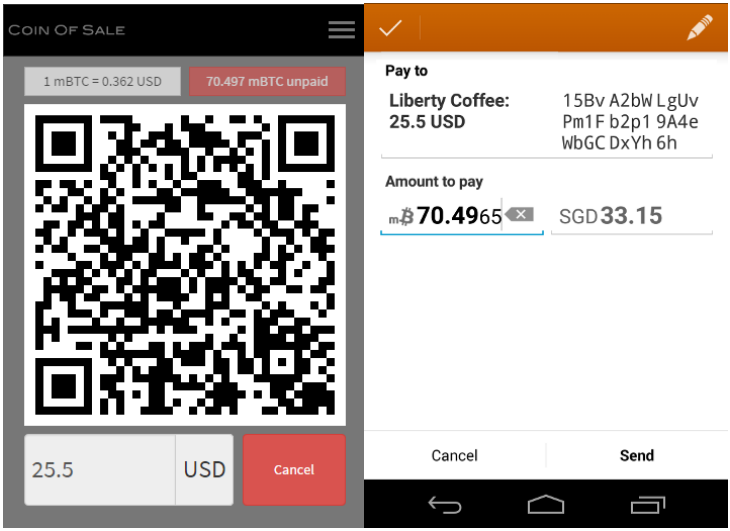


Ve fyzickém obchodě je příjem bitcoinů také velmi snadný, například se službou Coin of Sale. Stačí se zaregistrova na coinofsale.com, založit účty zaměstnancům, kteří mají s peněženkou pracovat a zapsat jim PIN kódy. Pod jejich jmény je poté v aplikaci na webu jednoduše vidět, kdo kdy přijmul kolik peněz, dokonce i s rozdílem proti tržní ceně v dolarech v době příjmu a v současnosti.



Práce s aplikací je pak jednoduchá, stačí v telefonu obsluhy zadat cenu, buď v dolarech nebo v bitcoinech. Cena v dolarech se přepočítá podle aktuálního kurzu. Následně aplikace vygeneruje QR kód, který stačí naskenovat a zákazník ve svém telefonu v mobilní peněžence potvrdí, že chce peníze skutečně odeslat. Úspěšná transakce se ihned projeví na obou telefonech.

Na obrázku níže je vidět nalevo obrazovka obsluhy a napravo obrazovka zákazníka.



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 platiti 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 na začátku roku 2014 výsledky ankety mezi 847 svými členy, z níž vyplývá, že více než polovina lidí měla zcela jistě zájem na možnosti 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.

Největším investiční společností v této oblasti je dnes Grayscale a jejich Bitcoin Investment Trust (www.bitcointrust.co). 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 desíti dolarů. Během roku cena vystoupala až k tisíci dolarům za bitcoin a Winklevossovi udělali ze 400 tisíc 40 miliónů dolarů. Ve světě, kde se výnosy na spořicích účtech blíží k nule, jde o neuvěřitelné zhodnocení.

Anebo 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 ve svém blogu při New York Times nazval jeden z příspěvků jednoduše „Bitcoin je zlo".

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 miliónů 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 vzniknul 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. Příkladem je AidoATP (github.com/aido/AidoATP), který automaticky nakupuje na trhu BTC/USD a prodává na BTC/EUR a naopak, dle toho, kde se rozdíl hladin vytvoří.

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 bitcoinem 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 40 tisíc dolarů, a to v dohledné budoucnosti. 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

peněž uložených v daňových rájích, jeho cena by vzrostla na téměř 3 milióny 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 rychlost. Jednoduše si 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 sílu. 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 výpočetní síly 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 vroste 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 klesla celková výpočetní síla sítě, a to je velmi nepravděpodobné) anebo očekáváte zvýšení ceny bitcoinu na burze. I s menším výnosem se však zbavujete rizika nákupu drahých a rychle zastarávajících těžebních strojů.

Ať už bitcoiny získáte jakkoliv, pokud je budete směňovat na koruny nebo jinou tradiční měnu, musíte počítat s tím, že je dle zákona potřeba zisk řádně zdanit. České zákony příjmy z prodeje bitcoinů klasifikují jako jakýkoliv jiný příjem, přičemž ten je nutné zdanit, pokud přesáhne během zdaňovacího období částku 20 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 máte příjem v bitcoinech, situace je o poznání složitější. Většina finančních a daňových odborníků se shoduje pouze na tom, že je nutné „nějak" bitcoiny ocenit. Jde de facto o barter, tedy nepeněžní směnu, jako když se vymění koláč za maso. Pokud jde o příležitostnou činnost, potom lze předpokládat, že šlo o směnu ekvivalentní, jakkoliv je to nesmyslné, když zjevně obě strany se směnou souhlasily a vydělali tak na ní. Pokud by směna měla probíhat opakovaně, potom je již zapotřebí přijaté bitcoiny ocenit nejlépe dle kurzu jedné z burz a s příjmem pracovat jako kdyby byl korunový. Účetně existují dvě základní možnosti, které nelze kombinovat. První je nechat bitcoiny ležet a 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.

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

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, zejm. při nakládání s většími částkami, a na LocalBitcoins 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 které 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. Bitlaundry.com nebo Bitcoinlaundry.com jsou 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 vědeli, kolik bitcoinů a kdy přes vaši peněženku prošlo. Některé peněženky dokonce mají takové možnosti jako zaškrtávátka s popiskem ve stylu „Vytvořit pro transakci novou adresu". Jde přesně o ten druh anonymity, který máme rádi na každodenních hotovostních platbách.

Vidět všechno

Bitcoin má však 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. Podívámeli se kolem sebe, transparentnost peněz je stále více poptávaná. Charity, dobročinné spolky a neziskové organizace obecně, politické strany a obecní sbírky, ti vše 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, z 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 přimknula pravděpodobně kvůli anonymnímu autorovi, tajemnému Nakamotovi, a ilegálním obchodům na Silk Roadu. Přestože je tedy akcentována spíše možnost anonymity, je to právě transaparentnost, 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 blok Genesis, 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 virtuálních měn

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 187. Historiky ekonomického myšlení je toto považováno za první dílo představující analýzu na základě mezních veličin a tím 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 ekono-

mické 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 Irvingtonu 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 Ludwig von Mises Institut CZ & SK, Liberální institut 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 politiky, které nemohou být prováděny 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 je skupina kryptografických metod, u kterých šifrovací a dešifrovací klíč nejsou stejné (resp. z šifrovacího klíče není možné odvodit klíč dešifrovací). Asymetrie klíčů umožňuje adresátovi šifrované zprávy nesdílet s odesílatelem tajný dešifrovací klíč (viz **Privátní 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 privátního 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, který v srpnu roku 2013 označil bitcoin za formu soukromých peněz a účetní jednotku, čímž explicitně umožnila užívat bitcoiny ve směně. Ovšem ze zákona také podléhají dani,

která se nemusí platit, jsou-li drženy déle než jeden rok. Z právního hlediska tedy bitcoin za peníze lze označit velmi snadno. Ekonomická otázka, zda jde o peníze, je podstatně složitější.

Bitcoin jako peníze

Častou definicí peněz, a to jak ekonomů hlavního proudu 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 je bitcoin 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 300 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 bitconech 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 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 na 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 peněž, 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 současné 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 bitconů 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 neodpovídá 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 vystavených 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 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.

KONKURENČNÍ KRYPTOMĚNY

JEDNA MINCE V MOŘI

Konkurence a bitcoin jsou natolik spjaty, že se nelze divit, když začaly chvíli po bitcoinu vznikat i konkurenční digitální měny založené na podobném, většinou úplně stejném principu. Již brzy se objevil a velké popularity dočkal litecoin, o němž se začalo spekulovat jako o možném nástupci bitcoinu. Nestalo se tak, přesto je litecoin dodnes druhou největší digitální měnou. Vedle litecoinu vznikl brzy feathercoin, novacoin, zerocoin a další. Těmto měnám se začalo říkat altcoiny – alternativní coiny.

Některé z altcoinů se vydaly směrem k jiným arbitrárně zvoleným konstantám (zejména limitu těžby apod.), jiné zkusily vsadit na jiná kryptografická řešení a další začaly hledat svou konkurenční výhodu úplně jinde.

Litecoin přišel oproti bitcoinu s odlišným algoritmem, který mění způsob, jakým se měna těží. Zatímco bitcoin se dnes těží na specializovaných BTC těžebních strojích, litecoin se pokusil učinit dlouhodobě rentabilní i těžbu pomocí grafické karty. Vedle toho vsadil na rychlejší ověřování transakcí. Zatímco u bitcoinu trvá vytěžení jednoho bloku a tedy i ověření transakce v průměru kolem deseti minut, litecoin transakci ověří pod tři minuty. Snaha zvýšit četnost těžby je pochopitelně hnána praktickými důvody, jelikož s desetiminutovým ověřováním je bitcoin jen stěží použitelný pro běžné mikroplatby. Tři minuty ale také nejsou okamžik.

Se zajímavým řešením pseudoanonymity bitcoinu přišla měna zerocoin. Ta se od bitcoinu liší především tím, že není v blockchainu vidět, kterou konkrétní minci z něj vybíráte, ale pouze informace, že jste tak učinili. Historicky druhá měna, namecoin, vsadila na obavy z internetové cenzury a spolu s distribucí mincí obsahuje i decentralizovanou informaci o překladu doménových názvů s příponou .bit na číselné adresy uzlů v internetu. Namecoin navíc umožnil tzv. merge-mining, tedy možnost těžit namecoin současně s bitcoinem.

Inflace měn

Inovace spočívá i v hledání nových možností pro využití blockchainu. S několika zásadními novinkami přišel záhy peercoin. Bitcoin je potenciálně energeticky velmi náročný. Potvrzování transakcí spojené s těžbou vyžaduje stále výkonnější počítače a množství spotřebovávané elektřiny roste s nimi. Peercoin implementoval odlišný způsob ověřování, ke kterému již není potřeba vypočítávat stále složitější úlohy. Množství peercoinů není omezené arbitrárním limitem a může teoreticky růst donekonečna, jelikož dává držitelům mincí za držbu úrok. Nerozděluje tedy nové mince na základě těžby, ale držby a užívání, což je inflační, ale energeticky nenáročné. Na druhou stranu ale z oběhu vyřazuje mince použité jako poplatek za transakci. Odhadnout, zda by v konečném důsledku vedl tento systém k inflačnímu či deflačnímu prostředí nelze, každopádně inflační možnost je pro mnoho uživatelů, kteří deflaci zrovna nefandí, zjevně velmi lákavá. Nižší výpočetní náročnost je na jednu stranu energeticky zajímavá, na stranu druhou je však měna náchylnější k útokům. Autoři si tedy nechali určitou možnost centralizovaných zásahů, což měnu činí bezpečnější, ale je nutné jim důvěřovat. Peercoin tedy není plně decentralizovaný a je otázkou, zda jako takový může mít šanci na úspěch.

Krátkodobým fenoménem se následně stala i kryptoměna, která ve svém názvu konečně vynechala „coin". Quark je virtuální měna, která vsadila na šest různých algoritmů zabezpečení, velmi rychlé ověřování (jen půl minuty) a inflační prostředí. Každý rok je možné vytěžit 0,5 procent dosud vytěžených quarků. Navyšování peněžní zásoby o půl procenta ročně by mělo vést k mírné a předvídatelné inflaci. Quark brzy spadnul až do druhé padesátky největších altcoinů, jeho vliv na další nástupce však byl a stále je silný.

Odlišný model inflace distribuce je základem mnoha nových altcoinů. Někteří ekonomové vyčítají bitconu nerovné rozdělení mincí mezi uživateli. Přestože je obtížné dojít k exaktním číslům, předpokládá se, že z celkového počtu zhruba dvou milionů vlastníků bitcoinu v roce 2013 drželo polovinu všech mincí pouhých tisíc lidí. Na druhé straně kolem 1,9 milionů lidí vlastní pouhých 10 procent veškerých vytěžených bitcoinů. Příjmová nerovnost je nepochybně palčivým tématem ekonomie. Kritika se také snáší na samotného Satoshiho Nakamota. Jeden z investigativních uživatelů Sergio Demian Lerner pomocí sofistikované metody odhadnul, že samotný Satoshi vlastní přes 1 milion bitcoinů. Ze dvou milionů uživatelů tak jeden nejbohatší vlastní stejně, jako 1,9 milionů nejchudších. Na druhou stranu, kdo jiný, než sám Satoshi, by si zasloužil vydělat na vytvoření bitcoinu jmění?

Digitální měně dal také brzy zastřešení i známý člověk. Ryze internetová celebrita Kim Dotcom spustil svůj megacoin – altcoin, který je vedle standardních vlastností ještě „vylepšen" vložením známé značky „mega" do názvu. Kimovi se dařilo s Megaupload.com, méně již s Mega.com, a megacoin se propadl úplně. Nicméně vklad v podobě jeho jména může fungovat. Na jméně populárního amerického kongresmana a kandidáta na prezidenta následně vznikl i RonPaulCoin a recesisté vložili jméno úspěšného amerického rapera Kanye Westa do názvu měny Coinye West. Přestože zpěvákovi

právníci chtěli autory žalovat, tržní kapitalizace rostla. Koneckonců popularitě měny pomáhá i samotná žaloba. Marketing funguje i zde. Nakonec ale jednoho dne strach převládnul, autoři smazali stránky a oficiálně dali od měny ruce pryč. Vydali navíc zprávu, že se distancují i od „všech blbů, kteří se pokusí tuto měnu znovu oživit". Svět kryptoměn ale nefunguje takto jednoduše a „blbové" dále Coinye těží a směňují.

Svou vlastní kryptoměnu si dnes může vytvořit prakticky každý. Vznikl i generátor kryptoměn Coigen.io, kterému stačilo pouze zadat požadovaný limit, algoritmus a název a nechat měnu vygenerovat. Za malý poplatek, pochopitelně v bitcoinech. Nicméně brzy se ukázalo, že šlo o podvod a autoři pouze vytáhli z řady lidí peníze, pravděpodobně si nechali zadní vrátka i v nově generovaných altcoinech a nakonec server zavřeli.

Jednoduchost vzniku konkurenční měny tak nejlépe dokládá spíše altcoin s názvem dogecoin. Doge, překroucený anglický překlad slova „pes", je internetový meme zobrazující japonské plemeno šiba. Jde ve své podstatě pouze o vtip, jehož autor zcela jistě nečekal, že by jeho kryptoměna mohla být reálně používaná. Dogecoin je podobný litecoinu, pouze rychleji potvrzuje transakce a množství mincí je omezeno na sto miliard.

Internet je však nevyzpytatelný stejně jako lidé, kteří ho používají, a dogecoin začal raketově růst. Během několika dní po vzniku se jeho tržní kapitalizace vyšplhala téměř na 300 miliónů korun. A objevila se první poptávka po objednávce pizzy. Navíc komunita uživatelů sponzorovala jednoho jezdce závodů NASCAR a nasbírala 130 tisíc dolarů pro jamajský bobový tým. I dobrý marketing může pomoci. Už na začátku roku 2014 byla registrována čtyři fyzická místa, kde lze dogeconiem zaplatit. Dodnes se toto číslo příliš nezvýšilo. Ale s rukou na srdci, to jsme kdysi vyčítali i Bitcoinu... Kdo ví. A to je to kouzlo.

Zajímavým projektem byla měna auroracoin. Ta vznikla na začátku roku 2014 a od 25. března téhož roku slíbila všem občanům Islandu po 31,8 jednotkách měny. Měna však strmě spadla dolů a v květnu již prakticky přestala existovat. Důvod byl dvojí. Zaprvé autor měnu distribuoval z vlastních zdrojů a uživatelé mu nemuseli věřit, že peníze slíbené ostatním neutratí. Zadruhé si nikdo nebyl jistý tím, kolik mincí je v oběhu.

Bitcoin druhé generace

Budoucnost ale patrně nečeká na jednoduchou kopii bitcoinu nebo litecoinu, které jsou nejčastěji napodobovány. Vývojáři začali hledat bitcoin 2.0.

Vzniklo tak například Ethereum, kryptoměna umožňující smart contrats, složitější podmínky pro další použití některých mincí, přímo ze své podstaty. Jde o myšlenku zabudování kontraktů přímo do blockchainu , kde by se kontrakt uložil, byl ověřován a vynucoval. Může Ethereum nahradit bitcoin? Nejprve by muselo získat obrovskou výpočetní sílu, aby bylo bezpečné. Budou ale lidé důvěřovat natolik komplexnímu altcoinu, který nevznikal pomalu přidáváním dalších vrstev nad bitcoin, ale byl přímo vytvořen jako nástroj na správu prakticky čehokoliv? Ať už Ethereum uspěje či nikoliv, nutí nás přemýšlet nad všemi možnými druhy vztahů, které by bylo lze decentralizovat díky blockchainu.

Jedním z prvních altcoinů druhé generace byl Ripple. Ripple založil Jed McCaleb, jeden z možných adeptů na pravou identitu Satoshiho Nakamota. McCaleb je geniální programátor, jenž vytvořil eDonkey, svého času velmi populární P2P síť pro sdílení souborů, je autorem burzy Mt.Gox, kterou dlouho před bankrotem prodal, a tvůrcem Ripple a Stellar. Ripple nepracuje s ověřováním pomocí těžby, ale s decentralizovaným konsenzem členů sítě. Myšlenkou není

tvorba samotných peněz, ale spíše systému pro P2P infrastrukturu pro přesun nejen finančních prostředků bez nutnosti zúčtovacího centra. I díky tomu Ripple začal zajímat banky, které hledají způsob, jak ho využít. Výsledkem je tržní kapitalizace přes sto milionů dolarů a místo nejdražšího altcoinu a prvního, jenž předběhl litecoin.

Jed McCaleb šel ale ještě dál a založil altcoin Stellar, pracující s multisig (transakci podepisuje více klíčů) a smart contracts, a brzy s ním dobyl první desítku nejúspěšnějších kryptoměn.

Kryptoměn druhé generace je celá řada. Dash (dříve Darkcoin) pracuje s inovativním způsobem anonymizace transakcí, Bitshares se snaží decentralizovat správu jakýchkoliv aktiv, Nxt nadto integroval i vnitřní trh, MaidSafe se pokouší decentralizovat a změnit od základu i celý internet.

Altcoinů je mnoho a bude jich patrně ještě více. Nebude to chaos? Ekonomie ukazuje, že u peněz existuje tendence k převládnutí jedné měny, zejména pak z důvodu snížení transakčních nákladů. O tom, jaká měna se používá, nerozhodujeme ani tak my, drobní nakupující, jako velcí exportéři a importéři, kteří denně operují s částkami v řádech srovnatelných se státními rozpočty. Těm se pochopitelně více hodí, existuje-li jeden měnový standard. A ten pravděpodobně i existovat bude, rozšíří-li se digitální měna ještě více. Za prvních pět let existence bitcoinu vzniklo kolem sedmdesáti perspektivních kryptoměn a třiceti z nich se podařilo překonat tržní kapitalizaci jednoho miliónu dolarů. Po šesti letech je nad jedním milionem stále třicet měn, ale jiných. Altcoinů jsou však již stovky. Přehledný seznam a jejich aktuální kurzy nabízí server coinmarketcap.com.

Možná bude ale cesta k novému bitcoinu úplně jiná. Altcoiny mají řadu problémů. Malá tržní kapitalizace a malá velikost sítě je snadným cílem pro útočníky. Takto skončil například CoiledCoin v roce 2012 a řada dalších altcoinů se potýkala s problémy. Vedle toho je praktický problém s decentralizovanou směnou mezi altcoiny

a bitcoinem nebo mezi samotnými altcoiny. Existuje sice možnost tzv. atomic cross chain swaps, kdy je přímo v síti naprogramována pojistka, aby obě strany skutečně poslaly sumy, na kterých se dohodly, nicméně ta dodnes není využívána. Místo toho jsou pro směnu mezi kryptoměnami používány třetí strany, zejména burzy. Velkým problémem jsou takzvané pump-and-dump altcoiny, kdy se jejich autoři pouze snaží rychle vydělat velké peníze. Postup je jednoduchý. Stačí vytvořit altcoin, udělat mu reklamu a nalákat uživatele, přičemž sám tvůrce (anebo jiný útočník) nakoupí velké množství měny a při první vyšší cenně všechny prodá. U bitcoinu by to již bylo složité, ale malé altcoiny jsou k tomu velmi náchylné. Může to být ale i jen zábava, o kterých všichni dopředu vědí, i takovým způsobem se lidé na přelomu let 2013 a 2014 v altcoinovém boomu bavili.

Málokdo tak chce přecházet z bitcoinu k altcoinům. Vznikly návrhy proof-of-burn, kdy zájem o měnu vyjádříte zničením jednoho bitcoinu. Pokud tak učiníte, získáte jednu jednotku altcoinu. Protože se ale nenávratné ničení nejeví jako vhodný způsob, objevila se alternativa s **escrow** . Pokud chcete jednotku altcoinu, stačí uschovat bitcoin do escrow, kde s ním nemůžete manipulovat. Jedinou možností, jak se k němu zpět dostat, je zničení dané jednotky altcoinu. Ani jedna z těchto možností však uživatele příliš nenadchla.

Tyto problémy se snaží řešit vývojáři, kteří věří, že díky altcoinům půjde vylepšit samotný bitcoin. Altcoiny by teoreticky mohlo jít využít jako boční a spojené řešení pro rychlé mikrotransakce, jiné pro registraci domén apod. Tyto side chains, je však obtížné do bitcoinou implementovat. Bylo by velmi náročné, aby bitcoinová síť ověřovala vedle vlastních transakcí také transakce v dalších altcoinech.

K tomu se dá využít podobný princip, který funguje u mobilních bitcoinových aplikací. Není tak potřeba ověřovat všechny

transakce, ale pouze důvěřovat těžařům, že dělají svou práci. Dobrý návrh ale stále neexistuje, protože i tak může být ověřování velmi pomalé, zejména pokud má altcoin, který chceme využít jako side chain, velmi rychlé připojování dalších bloků. Současné návrhy tak chtějí ověřování ulehčit a umožnit vznik side chainů pomocí pravděpodobnostních funkcí. Návrhy existují, ale na fungující side chainy se stále čeká.

Escrow je 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 a nebo 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 smluv (viz **Transakce**) lze sestavit model pro decentralizovanou směnu digitálních kryptoměn.

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, tak 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 velmi 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 generování by nedávalo žádný smysl. Pro ilustraci může sloužit výpočet, který koluje po internetu jako jednoduchý důkaz. Výpočet je ve skutečnostisofistikovanější, 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 bytu 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 270000000000000000000000000000000000000000000000x 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.

Generování adresy: 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 vygenerovnání 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)

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.

Reálné problémy

Existují i další možné chyby, ale žádná z nich není považována za příliš závažnou. 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 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?

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 bitcoinu 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 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 zatím 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 miliónů 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. 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 se patrně nikdy nestal, ale který se traduje a který krásně ilustruje snahy o regulaci decentralizované měny. Říká se, že 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.

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 stane pravděpodobně i neúspěšným cílem regulačních útoků 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. „pe-

něžní 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 milióny 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 zavřít. 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 zesílil a nadto byl svým způsobem legitimizován, k čemuž není politická vůle. Můžete ale regulovat reálné příjemce bitcoinu. Přijímáte bitcoin? 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 bitcoin 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 bitcoin 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 Egoldu. 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 ano-nymní 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 bitcoinu. 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 bitcoin za komoditu a výnos z jejího prodeje či těžby podléhá dani z kapitálu. V ČR zatím jen Ministerstvo financí doporučuju 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 nepřestali 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 bitcoinu 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".'

Postátnění bitcoinu

Bitcoin se zásadní regulaci patrně nevyhne. Dnešní svět je na vládních zásazích natolik závislý, že k tomu nakonec dojde i konsenzuálně, 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 milióny a miliardami dolarů jen pomocí jednoho kliknutí myši. Když se kupující ze Soulu rozhodne koupit akcie americké firmy za stovky miliónů

dolarů, nemusí do firmy letět a představit se. Může dokonce nakupovat v jednom okamžiku od stovek různých prodejců a nemusí znát jednoho ani 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 bitcoinem, 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 jakoby 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. Pokud si dnes chcete otevřít účet v komerční bance, bude po vás vyžadován doklad totožnosti, většinou i několik. Proč by to tak nemohlo fungovat i u bitcoinových peněženek? Nic tomu nebrání. Pokud by důvěryhodná instituce začala poskytovat peněženky pouze na základě ověřených dokladů totožnosti, nejlépe osobně na pobočkách po celém světě, potom by převody z jedné peněženky do druhé mohly být jasně propojitelné s konkrétním člověkem. Za vedení takové peněženky by si daná instituce pravděpodobně účtovala poplatek, jak je tomu ostatně i dnes. Co však brání podobnému projektu vzniknout již dnes? Především po této službě zjevně není dostatečná poptávka. Vybudovat síť poboček není zadarmo a investice do bitcoinového projektu je značně riziková. Poskytovatel takové služby by si tedy patrně účtoval poplatek, což spolu s nutností osobního kontaktu zvyšuje náklady na zřízení peněženky nad mez, kterou by v současnosti byli uživatelé ochotní akceptovat. Akcie se zatím v digitální měně příliš neobchodují, a tak nemají vlastníci bitcoinů mnoho důvodů pro zřizování podobných účtů, pokud je možné si zadarmo a s minimálními časovými náklady pořídit peněženku anonymní. Ovšem na druhou stranu se akcie bez takové služby obchodovat nezačnou. Zdá se, že jde o začarovaný kruh a nezbývá než doufat, že si na sebe nějaký podnikatel vezme značné riziko a podobný projekt spustí.

Až tomu tak bude, bude bitcoin opět o trochu více propojen se státem. Ačkoliv existují tržní alternativy osobní identifikace, ve vyspělém světě dominují ty státní – občanské průkazy, řidičské

průkazy, pasy, rodné listy apod. Přestože lze tyto dokumenty padělat, hrozí za takové jednání vysoké tresty a často se to neděje. V identifikaci svých občanů jsou státy relativně efektivní, koneckonců je to v jejich nejlepším zájmu, pokud chtějí efektivně vybírat daně. Je tedy nanejvýš pravděpodobné, že by se tyto institucionalizované peněženky přiklonily k identifikaci na základě státních dokumentů.

Takový vývoj může usnadnit i escrow, který se dnes snaží zmenšovat prostor pro podvody při obchodu v bitcoinech. Pokud se instituce zaručí, že zná identitu majitele peněženky, potom je snadné přijít se systémem pozdržených plateb. Pokud si například objednáte pizzu, nemusíte se čekat, až se platba druhý den připíše na účet restaurace, ale banka jednoduše slíbí, že peníze pošle a mezitím je vám zadrží. Obchodník peníze reálně nemá, ale pizzu vám dá rád, jelikož bance věří. Na druhou stranu to však pro stát otevírá nové možnosti v daně a regulaci digitálních měn.

Je otázkou, jestli si lidé zvolí pohodlí zvyku na státem identifikované peněženky a budou stále platit vysoké daně nebo si zvolí takové možnosti postupem času vyhnout úplně a tratit bude státní pokladna.

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 následně i 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". Je sice pravdou, že blockchain není vynálezem Satoshiho Nakamota, ale nelze mu upřít historickou roli v jeho rozšíření a první skutečně masové implementaci. Tato účetní kniha sdílená všemi uživateli může od základů změnit způsob, jakým používáme online služby. Je nepochybné, že systém P2P konsenzu může dát vzniknout inovativním vyhledavačům, sociálním sítím, systémům vlastnických práv k nejen finančním aktivům apod. Meze se kladou pouze fantazii.

Zdánlivě neomezené množství nových možností s sebou nesou takzvané obarvené mince (colored coins). Jde o koncept vystavěný nad původní strukturu 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 privátního 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 svoji transakční historii projde přes smluvenou bitcoinovou adresu.

Decentralizovat převod vlastnictví je možné využitím anonymizačních metod, jako je CoinJoin a další. Majitel bytu 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.

Jde o jednu ze zabudovaných vychytávek bitcoinu, kterou lze realizovat pomocí tzv. skriptů. Skript je v zásadě jednoduchý program, který se spouští, pokud se mají uvolnit existující mince do nové transakce. Síť spuštěním skriptu ověřuje, je-li žadatel transakce skutečně oprávněn k dispozici s určitými mincemi. V prostředí peněž jsou možnosti, které s sebou skriptování přináší, prakticky neomezené (a jejich složitějším použitím vznikají smart kontrakty). Například crowdfunding, stále populárnější způsob financování menších projektů. Kdybychom chtěli vydat tuto knihu pomocí crowdfundingu a bitcoinů, mohli jsme přidat skript, který by říkal, že pokud se na dané adrese, kterou bychom pro tyto účely založili, nashromáždí do konce roku alespoň 5 bitcoinů, potom jsou naše, a pokud méně, tak se všechny vrací zpět a financování našeho projektu nebylo úspěšné. Dnes k tomuto účelu slouží specializované firmy, kterým pošlete na konkrétní projekt peníze a ony hlídají, zda se nashromáždilo požadované množství. Pochopitelně jim je svěřujete do péče a musíte doufat, že v případě nedostatečných financí vám skutečně pošlou vaše peníze zpět a neutečou s nimi. Skript bitcoinu je automatizovaný tak, že se nikdo nemůže rozhodnout, že si peníze nechá a nevrátí vám je.

Vraťme se zpět k příkladu s pronájmem bytu. Co když by nájemník nechtěl byt opustit a neplatil? Skripty pomůžou. 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 jednoduše 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 virtuálních měn. Způsobů, jak využít skripty, byla popsána celá řada. Programátoři jakoby se předháněli v tom, kdo vymyslí něco nového nebo vylepší cokoliv stávajícího. Stačí jen fantazie.

Blockchain je zásadním vynálezem dějin. A nemusí zůstat jen u bitcoinu. Jak bylo ukázáno na příkladu smart kontraktů, blockchain má tendenci přetvořit právo, jak ho známe. Neexistuje žádný ekonomický důvod pro nutnou centralizaci peněz a stejně tak není důvod se domnívat, že by muselo být centralizované právo a zákony. Proč by měl být registr automobilů v papíru či na počítači na jednom úřadě? „Sdílená účetní kniha" může být snadno přetvořena ve „sdílený obchodní rejstřík". Přesuny vlastnických práv jednoho člověka k jinému mohou být stejně snadné a stejně bezpečné, jako přesuny jednotek digitálních měn.

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 miliónů 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 mnohdy 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 si zisky neudrží. 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 pět 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, vyhledavače 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 přemýšlí. 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 bitcoinu 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 má extrémně nízké náklady na převod prostředků a blockchain je natolik robustní, že by banky jeho implementací mohly ušetřit významné sumy.

V říjnu 2015 vydala společnost BitFury ve spolupráci s jedním z nejvýznamnějších vývojářů bitcoinu Jeffem Garzickem článek, ve

kterém polemizují nad tím, zda mají banky vůbec možnost využít pro účely svého podnikání nový blockchain.

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 vydávali omezené povolenky pouze ověřeným těžařům, přestává mít tento model smysl. Blockchain samotný je pouze jiným způsobem ukládání dat v databázi. Banky by tak pouze nahradily své databáze blockchainem, ale bez jeho největší výhody, decentralizace.

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 nebude jednoduše 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 jsou obě zprávy prakticky neúčinné, mění 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.

První týdny roku 2014 přinesly další události, které začaly obracet veřejné mínění. V lednu zatkla americká policie místopředsedu bitcoin Foundation a zakladatele jedné z prvních BTC burz BitInstant Charlieho Schrema. Schrem byl spolu s obchodníkem Robertem Faiellem, známým jako BTCKing obžalováni z praní špinavých peněz a provozování peněžního zprostředkování bez licence. 24 let starému Schremovi hrozilo 25 let a Faiellovi o pět let méně. Podle americké policie Schrem 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 Schrem 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

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 odříznul 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 nic se nezměnilo.

Navíc se bitcoinu začaly čím dál více věnovat velké komerční banky. Bohužel negativně. Jedna z největší bank na světě, americká JPMorgan vydala zprávu, v které kritizuje bitcoin jako „velmi podřadný oproti fiat měnám". Australská Commonwealth Bank zmrazila účet zakladatelům bitcoinové peněženky CoinJar. Vedle toho všeho přišly i problémy BTC burz, zejména krach Mt.Gox.

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 totiž zjistili, že útočníci měli část příjmů v bitcoinech...

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 Schrema nemá nic společného se samotným bitcoinem. Jakkoliv jde o právně otevřený případ, podle zpráv policie Schrem 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.

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."

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 start-upu 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.

Zhroutí se bitcoin někdy v budoucnu a upadne v zapomění?

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 vyhledavačů 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, k zábavě, k 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 vzdálenějšího 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.

Byli jsme svědkem 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?

Ve své zatím krátké epizodě touto cestou dějinami bitcoin zažil své růsty a pády. Zájem o něj však roste. A lidé ho používají čím dál více, a to navzdory tomu, že musí z donucení používat státní alternativu. Na grafu níže je vidět stabilní nárůst denního počtu transakcí v bitcoinové síti.

A tento graf poroste dále. Protože čím více 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.

IDDE děkuje za pomoc v obhajobě myšlenek svobody následujícím lidem a organizacím

liberty.me
mmister.com
stroukal.cz

&

Mises.CZ

Nositel Nobelovy ceny za ekonomii Milton Friedman prohlásil v roce 1999: *„Myslím si, že v omezování role státu bude hrát jednu z hlavních rolí internet. Jedna z věcí, které nám schází, ale brzy se objeví, jsou spolehlivé digitální peníze.“*

Deset let poté byl spuštěn bitcoin.

Lze bitcoin považovat za spolehlivé digitální peníze? Jak se bitcoiny vytváří? Kolik jich je a bude? Kde se dají koupit a jak se s nimi pracuje? Nejde o pyramidovou hru? O bublinu?

Tato kniha je plná odpovědí. Na tyto i na mnohé další otázky. Otevřte ji a naučte se přijímat a odesílat bitcoiny, ponořte se do jejich krátké, ale bohaté historie a prozkoumejte budoucí ekonomické dopady.

Seznamte se s penězi budoucnosti.

Dominik Stroukal vystudoval Národohospodářskou fakultu VŠE v Praze a Fakultu sociálních věd UK, kde se věnoval sociologii médií. Je předsedou Ludwig von Mises Institutu pro Českou a Slovenskou republiku a přednáší ekonomické předměty na Vysoké škole finanční a správní, Vysoké škole ekonomické a několika dalších školách. Profesně s věnuje ekonomii médií, teorii ekonomických systémů a kryptoměnám.

Jan Skalický vystudoval výpočetní techniku na Elektrotechnické fakultě ČVUT. V současnosti pracuje jako analytik a programátor mikropočítačových systémů pro automobilový průmysl. Kromě pozic vývojového specialisty pracoval i v jaderné elektrárně Temelín. Je příznivcem klasického liberalismu a decentralizovaných systémů, mezi něž patří i kryptoměny.

ISBN 9788087733264

@stroukal
@misescz
@IDDEurope

IDDE Institute for Direct Democracy in Europe