Mýty a naděje digitálního světa

Vše, co potřebujete vědět o kryptoměnách, umělé inteligenci a dalších převratných technologiích

Patrick Zandl

Jan Melvil publishing

Patrick Zandl
MÝTY A NADĚJE DIGITÁLNÍHO SVĚTA
Vše, co potřebujete vědět o kryptoměnách, umělé inteligenci a dalších převratných technologiích

V edici Pod povrchem vydalo nakladatelství Jan Melvil Publishing v Brně roku 2022. Žádná část této knihy nesmí být nijak použita či reprodukována bez písemného svolení, s výjimkou případů krátkých citací jako součásti kritických článků a recenzí.

Odpovědná redaktorka Lenka Čížková
Jazykový redaktor Aleš Antošík
Redakční spolupráce Tomáš Baránek, Tomáš Holčík, Vít Šebor, Marek Vlha
Šéfredaktor Marek Vlha
Grafická úprava a sazba David Dvořák
Ilustrace na obálce byla vygenerována pomocí nástroje Midjourney
Obálka Pavel Junk
Jazyková korektura Vilém Kmuníček
Tisk a vazba PBtisk, a. s., Příbram

Vydání první
Jan Melvil Publishing, 2022
Všechny naše knihy najdete na www.melvil.cz

Chyby a připomínky: melvil.cz/chyby
Recenze a pochvaly: melvil.cz/kniha-myty-a-nadeje, libisemi@melvil.cz
Kniha vychází také elektronicky a jako audiokniha.

ISBN 978-80-7555-175-7

Věnováno Antonínu Jaroslavu Liehmovi,
kterému jsem tuto knihu slíbil jakožto rukověť
k pochopení současného světa. Tak jako jeho texty
byly rukovětí k pochopení světa jeho generace.
Vydání knihy se bohužel nedožil.

OBSAH

ÚVOD

Jak jsem se nestal bitcoinovým miliardářem.

Prvních pět let po zjevení Bitcoinu znamenalo zlatý věk pro všechny, kteří uvěřili v jeho vizi, nebo se jen dílem náhody dostali ve správný čas na správné místo. Stal jsem se jedním z nich. Můj příběh kryptoměnového miliardářství však měl skončit na nule…

V roce 2011 se mi ozvali dva známí z Číny s tím, že mají skvělý nápad. Chtěli by prý Bitcoin těžit za pomoci šikovného softwaru. Mělo to však jednu vadu. Potřebovali nakoupit součástky pro těžební stroje, jenže ty jim nikdo nechtěl prodat. A tak je napadlo, že se ozvou mně, bílému člověku z Evropy s kontakty v IT, a objednávka se uskuteční přes mě. Nešlo o podvod. Komponenty jsme zaplatili a sestavili jsme těžební počítače. Jeden z mých čínských partnerů se je pokoušel vtěsnat pod postel, aby mu hned první noc došlo, že pro ten randál a teplo těžbu do svého studentského pidibytečku nevtěsná. Já jsem se stal kryptosáhibem – člověkem, který dojednával dealy. Oni dva „noname Asijci", kterých si euroamerické firmy nevšímaly a považovaly je za pouhé poskoky i v době, kdy jsme objednávali díly za miliony dolarů.

Uplynulo několik roků. Vyrostli jsme a stal se z nás významný těžař nejen Bitcoinu. Naše datová centra byla rozlezlá přes několik čínských provincií. V jednom městě dokonce odpadní teplo z našich kryptofarem vytápělo bazén a školu. V kryptokomunitě, která nebyla zdaleka tak rasistická jako IT firmy, jsme získali dobré renomé a byli jsme na nejlepší cestě stát se bitcoinovými boháči. Už se vlastně nemohlo stát nic myslitelného, aby k tomu nedošlo. Neexistovalo nic, co by mohlo naše diverzifikované kryptoaktivity porazit, protože neporazitelnost je jejich podstatou.

Jenže jednoho krásného dne roku 2018 čínská vláda usoudila, že kryptoměny pro ni představují problém. Vlastně hned několik problémů. Tím prvním bylo, že kryptoměny vytvářely skupinu elitních zbohatlíků, kteří se vzpěčovali komunistické morálce i straně, byli hlasití, nepřehlédnutelní a potenciálně podvratní. Druhý problém spočíval v cenách elektřiny. V Číně se masivně dotují a lidé si tak elektřinu běžně kupují pod nákladovou cenou. Masové „pálení" elektřiny pro těžbu bitcoinů začalo lézt do peněz a navíc nebezpečně destabilizovat distribuční soustavu. A tak bylo celé odvětví ze dne na den jednoduše postaveno mimo zákon a všechny zúčastněné firmy se dostaly na úroveň nepřátel státu.

Už jsem zmiňoval, že nás nemohlo nic porazit? Měli jsme zdroje, peníze, právníky i smlouvy. Nám se přece nemohlo nic stát!

Čínská banka se nás ani neobtěžovala upozornit na to, že už nedisponujeme účtem. To kolegové zjistili až ve chvíli, kdy jim neprošla transakce platební kartou. Realitní společnost, která nám pronajímala pozemky pro datové centrum, se zachovala férověji. Upozornila nás, že se máme do konce měsíce přestěhovat. Chápete? Mysleli si, že za pár dní vystěhujeme obrovskou budovu nadupanou počítači. Odpověděli jsme důrazně a do kopie jsme přidali naši čínskou právní firmu, aby jim ozřejmila, že uzavřená nájemní smlouva má desetiletou výpovědní lhůtu.

Dostalo se nám dvou e-mailových odpovědí. Ta první byla od našeho právníka, jenž nám s okamžitou platností vypověděl pro něj velmi lukrativní kontrakt. Ve druhé nás realitní firma upozornila, že jako společnost nepřátelská vůči státu nemůžeme platnost smlouvy vymáhat. Což se okamžitě potvrdilo.

Během pár týdnů bylo vymalováno. Odvézt těžební servery? Žádná spediční společnost si to nedovolila. Elektřina? Vypnuta obratem. Zaměstnanci? Do týdne zmizeli všichni – část s omluvou, většina bez ní. Jako poslední věrný nám zůstal bankovní účet na splácení úvěrů, který se měsíc co měsíc dožadoval splátek za zmařené investice. Část z toho všeho jsme nakonec „se štěstím" prodali příbuznému místního komunistického pohlavára, část se prostě vyhodila. Jen malý zbytek se nám povedlo přesunout vláčkem do Hongkongu, kde ještě nevládla tak tuhá kontrola.

Tenhle příběh jsem nikdy nevyprávěl celý a ani tentokrát například neprozradím jméno naší firmy. Mám pro to důvody, včetně vyrovnávání se s vlastním neúspěchem. Snad nejvíc mi ale vadilo, kolik knížecích rad mi ex-post dávali teoretici, kteří ke kryptoměnám přičichli maximálně zpovzdálí a o podnikání v Číně netušili už vůbec nic. A to, jak neotřesitelně tito lidé na svých moudrech trvali.

Nešťastný prožitek byl ale k něčemu užitečný: stál na prahu mého bádání po tom, jakými způsoby se zdánlivě nezdolné systémy a neprůstřelné technologie hroutí. Když se s novými technologiemi potkáváte, děje se tak zpravidla prostřednictvím nadšených článků věrozvěstů, propagátorů a marketérů, kteří nemají důvod rozebírat stinné stránky věci, případně si jich ani nejsou vědomi. Jenže selhávání má své zákonitosti a jsem přesvědčený, že aktuální technologická revoluce otřese mnoha jistotami a svět učiní přinejlepším dočasně křehčím, než doposud byl.

Na následujících stránkách se dozvíte, jak převratné technologie fungují a proč můžeme naopak jiné považovat za nafouknutou bublinu. Měli bychom totiž porozumět jejich možnostem i rizikům, která přinášejí a jež ostentativně odmítáme vnímat, jako by naše víra v pokrok byla slepá.

1

DECENTRALIZACE A KRYPTOMĚNY

Smrt bankéřům a právníkům, sláva programátorům! Nebo ne?

Od osmdesátých let dvacátého po první dvacetiletí našeho století byla určujícím rysem ekonomiky i technologií centralizace. Projevovala se všude, a to nesmírně silně. V průmyslu vznikaly velké výrobní clustery, zejména v Číně. Ve finančním světě se etablovaly centrály jako Londýn nebo Hongkong, ve startupech Silicon Valley. V nových technologiích vznikly a udržely se standardy IBM PC pro osobní počítače, v telekomunikacích mobilní standardy GSM/UMTS/LTE. Každý z těchto převážně centralizovaných přístupů se stal neoddiskutovatelným hegemonem a příčinou, proč jsme začali mluvit o éře globalizace a s ní i o „konci dějin".

Jenže pak se věci začaly měnit. Na internet, který byl sám o sobě technicky decentralizovaný, v praxi však především ekonomicky centralizovaný, začaly přicházet decentralizované služby, z nichž si nejvíce všímáme kryptoměn. Jejich propagátoři totiž decentralizovanost – nezávislost na všech a všem – hlásali jako hlavní výhodu. Kryptoměnová vlna získala masovou pozornost především kvůli ziskům, jež určitému okruhu lidí vygenerovala. Masivní přeskupování kapitálu vždy vzbuzuje zájem, neboť je průvodním jevem revoluce.

V tu chvíli se však ještě zdálo, že půjde jen o menší anomálii. Ano, možná v technologiích vzniknou určité decentralizované služby a budou představovat výjimku z pravidla. Copak je však myslitelná

hybná síla, která by rozbila centralizované výrobní clustery, jež dosud byly rozhodující výhodou v hospodářské soutěži?

Onou hybnou silou se stala pandemie covidu-19 a následně válka na Ukrajině, které zásadně zkomplikovaly dodavatelsko-odběratelské vztahy a rozrušily rozsáhlé výrobní sítě, jež jsou pro výrobu pokročilejších technologií nezbytné. Celý svět začal horečně řešit odolnost proti takovým „černým labutím".* Velké výrobní korporace začaly stahovat svou stěžejní produkci do politicky kompatibilních států, od kterých očekávají ohled na své zájmy. Na prahu dvacátých letech jednadvacátého století se stalo neoddiskutovatelným faktem, že ekonomické sankce, ať přiznané, nebo nepřiznané, se stanou legitimní součástí zápolení o dominanci nebo alespoň o prosazení přípustnosti nějaké politické vize. Politiku strachu tak nahradila ekonomika strachu. Namísto hrůzy z atentátů a masakrů nevinných se společnost začala bát o dodávky energií a pracovní místa.

V době, kdy pracuji na této knize, si ještě nikdo netroufá s určitostí říct, zda ruská invaze na Ukrajinu spolu s pandemií covidu-19 skutečně představují milník, který spouští dlouhodobé stahování průmyslu zpět na Západ. Je možné, že tuto zákrutu během pár let vybereme. Jenže přijdou další. Pravděpodobně se nacházíme před dalšími regionálními konflikty, jež patrně přerostou v celosvětový konflikt. Konflikt ekonomický, nikoli nutně vojenský.

Může v soupeření decentralizačních a centralizačních tendencí dojít k zásadnímu průlomu?

Ukážeme si, že se tyto tendence střídají – lze říct, že trvale oscilují kolem „normálové osy". Oscilace se zpravidla zpomaluje, dokud jí není dodán externí impulz, jímž může být technologický průlom, ohrožení nebo třeba státní regulace. Při takovém impulzu dojde k přeskupení vlivu a kapitálu, což způsobí zesílené kmitání (amplitudu). To mobilizuje obranné mechanismy těch, kteří o vliv a kapitál kvůli změně přicházejí, a snaží se proto přijít s novým průlomem ve svůj prospěch, což zase zvyšuje frekvenci změn.

* Ponechme stranou, že Talebův pojem „černá labuť" není použit správně, neboť ten má označovat situaci nepředvídatelnou. Nikoli takovou, která byla očekávatelná a pravděpodobně musela v brzké budoucnosti nastat.

Tento jednoduchý ekonomický jev má svůj základ v samotném odměňování penězi a je přirozenou součástí ekonomiky. Dokud bude společenská dominance založená téměř výhradně na dominanci finanční, bude k sinusoidě změn docházet, neboť ji pohání zápas o dominanci. V určité míře není takové kmitání pro život homo economicus špatné. Příliš vysoká amplituda i frekvence změn však způsobují obrovské celospolečenské otřesy, neboť ty se dotýkají stále většího počtu lidí – přinášejí jim nezaměstnanost, nejistotu a strach. Tím současná decentralizační tendence zvyšuje křehkost našeho světa.

V této a následující kapitole si popíšeme, jak tyto centralizačně-decentralizační tendence fungují. Na příkladu kryptoměn a Webu 3.0 uvidíme, jak se služby, jež mají představovat naději pro decentralizaci a absolutní svobodu, v dalším kmitu sinusoidy přibližují centralizovanosti, z níž silně profituje opět jen úzká skupina lidí.

Vedle toho si ukážeme, jak na centralizační tendence reaguje široká společnost, která z nich nemá přímý prospěch. A že klesá víra v ekonomiku a peníze, neboť ty se staly dostupné do té míry, že takřka každému zajistí základní obživu, ale neumožní mu společenský vzestup. Na Západě (a nejen tam) si široké vrstvy společnosti zvykají na fakt, že na vlastnictví základních životních prostředků, jako je bydlení, nikdy nevydělají dost peněz.

Blockchain: koncept s nadějí revoluce

Kde jinde začít povídání o budoucnosti světa a technologií než u kryptoměn. Pro někoho představují Ponziho schéma, pro jiného svobodu a budoucnost. Nezmínit „krypto“ hned na začátku by znamenalo koledovat si o opovržení na obou stranách barikády. Beru to jako příležitost vyrovnat informační manko, které kolem blockchainových technologií vzniká.

Snaha vytvořit digitální měnu, v níž by nemusel existovat prostředník, garant plateb, tu byla dlouho. Jenže narážela na problémy. Jednou z hlavních výzev při navrhování digitální měny je takzvaný problém dvojího utrácení. Pokud je digitální dolar pouhou informací, co lidem brání, aby ho kopírovali a „utratili“, kolikrát chtějí? Tradiční odpověď spočívala v tom, že se použije centrální clearingové

centrum, které bude v reálném čase vést knihu všech transakcí – a zajistí, že pokud někdo svůj poslední digitální dolar utratí, nebude ho moct utratit znovu. Účetní kniha zabraňuje podvodům, ale také vyžaduje důvěryhodnou třetí stranu, která ji bude spravovat. Což tradičně přináší centralizaci a také vliv státu, jenž si může na onu důvěryhodnou třetí stranu došlápnout. Lze najít cestu, jak záznamy v takové účetní knize věrohodně potvrdit kýmkoli? A jak?

V roce 1997 přišel britský kryptograf Adam Back s myšlenkou, že tehdejší ohromně narůstající problém s e-mailovým spamem by mohlo vyřešit počítání „hashe", jakéhosi kontrolního součtu celého e-mailu. Back vycházel z předpokladu, že zatímco běžný odesílatel rád věnuje vteřinu výpočetního výkonu svého počítače na odeslání jednoho e-mailu, spameři si nic takového dovolit nemohou, protože jejich obchodní model stojí na rozesílání milionů e-mailů na všechny strany, a minimalizace nároků na hardware je pro ně tudíž zásadní. Příjemce e-mailu si mohl jednoduše a automatizovaně ověřit, zda hash připojený do hlavičky e-mailu odpovídá hashi, který spočítá jeho vlastní počítač, a tedy zda odesílatel tuto „investici prací" provedl. Tak vznikl koncept proof-of-work (důkaz prací).

Adam Back si svůj objev jako správný kyberpunker nenechal patentovat a v roce 2002 jej publikoval. Pro odhalování spamu se sice hashcash příliš nepoužívá, na Backovu práci však navázal americký vývojář Hal Finney. Ani toto jméno, pokud nejste ponořeni do hlubin kryptosvěta, vám asi mnoho neřekne. Hal Finney byl druhým vývojářem přijatým do společnosti PGP Corporation, kde spolu s Philem Zimmermannem, vývojářem číslo jedna, pracoval na šifrovacím programu PGP, jenž ve své době hodně potrápil a nazlobil americkou vládu.

Hal Finney s využitím konceptu Adama Backa vytvořil „opakovaně použitelný důkaz prací", anglicky reusable proof-of-work (RPoW).* Finney navrhl token podložený právě prací a zamýšlel jej

* Klient RPoW vytvoří token RPoW tak, že zašle řetězec proof-of-work dané obtížnosti podepsaný svým soukromým klíčem. Server pak tento token zaregistruje jako patřící k podepisovacímu klíči. Klient může token předat jinému klíči podepsáním příkazu k převodu na veřejný klíč. Server pak token řádně zaregistruje jako patřící příslušnému soukromému klíči. Tím se řeší možnost dvojího utrácení tokenu. Vlastnictví tokenů je registrováno na důvěryhodném serveru.

užívat k regulaci nadměrného zatěžování služeb. Webová služba by za své využití vyžadovala takovýto token, jejž by vygeneroval počítač uživatele. Zátěž potřebná k výpočtu tokenu by regulovala přístup ke službě. Podstatnou novinkou Finneyho konceptu však byla především „znovupoužitelnost" tokenu. Vytvořený a utracený token bylo možné vyměnit za token neutracený a ten znovu utratit, čímž by se předešlo nutnosti token znovu generovat prostřednictvím práce. Finney navíc kód RPoW zveřejnil pod svobodnou licencí. Do této služby se tak mohl zapojit jakýkoli programátor. S Finnovým kódem si mohl ověřit, zda získal pravý token.

Finneyho služba byla nicméně pro běžné použití komplikovaná a digitální měnu připomínala jen vzdáleně. Faktického rozšíření se nedočkala, inspirovala však jiný experiment, z něhož vzešel Bitcoin. Dne 31. října 2008 byl do jedné kryptografické e-mailové diskusní skupiny zaslán příspěvek nazvaný *Bitcoin: A Peer-to-Peer Electronic Cash System*, jehož autorem byl jakýsi Satoshi Nakamoto. Příspěvek popisoval „systém pro elektronické transakce bez závislosti na důvěře" a mimo jiné používal důkaz prací, vycházející pravděpodobně z Finneyho myšlenek. To byl také jeden z důvodů, proč občas bývá Finney ztotožňován s osobou záhadného Satoshiho Nakamota. Je vcelku jisté, že jméno je přezdívka, takže dodnes není jasné, kdo je skutečným autorem Bitcoinu. Zejména po roce 2015, kdy kurz bitcoinu posílil, se z hledání Nakamotovy identity stala určitá forma posedlosti, podložená především přesvědčením, že zakladatel virtuální měny je pohádkově bohatý.

Podstatné však bylo, že příspěvek navrhoval řešení. Bitcoin by se zbavil třetí strany, jelikož by veřejně distribuoval účetní knihu, kterou Nakamoto nazval „blockchain", řetězec bloků. Uživatelé ochotní věnovat výkon procesoru na spuštění speciálního softwaru by se nazývali těžaři a vytvořili by síť, která by blockchain kolektivně udržovala, přičemž by zároveň tímto procesem generovali novou měnu. Transakce by se vysílaly do sítě a počítače se softwarem by soutěžily v řešení nevratných kryptografických hádanek, jež by obsahovaly údaje z několika transakcí. Těžař, který jednotlivou hádanku vyřeší jako první, by získal 50 nových bitcoinů a související blok transakcí by byl přidán do řetězce. Obtížnost každé hádanky by se zvyšovala s počtem těžařů, kteří by udržovali produkci na jednom

bloku transakcí, zhruba každých deset minut. Kromě toho by se velikost odměny za jednotlivý blok snižovala každých 210 000 bloků na polovinu. Nejprve z 50 bitcoinů na 25, pak z 25 na 12,5 atd., až by kolem roku 2140 měna dosáhla svého předem stanoveného limitu 21 milionů bitcoinů. Oním převratným řešením tedy byl blockchain.

Nakamotův příspěvek zprvu nebyl přijat s velkým nadšením. Kryptografové jej zkritizovali a chvíli to vypadalo, že z Bitcoinu nebude víc než nepraktická pracovní hypotéza. A tak se ji Nakamoto rozhodl ověřit praktickou demonstrací.

Začátkem ledna 2009 byla „spuštěna" bitcoinová síť (uvozovky používám proto, že jako spuštění bývá označováno vytěžení nultého bloku bitcoinů, který obsahoval 50 bitcoinů), čímž Nakamoto dokázal funkčnost svého konceptu. A jen o pár dní později vydal pod svobodnou licencí klientský software. Jedním z jeho prvních uživatelů byl Hal Finney, k němuž také směřoval první převod, či chcete-li první bitcoinová transakce na světě. Finney dostal od Nakamota 10 BTC,* v dnešním kurzu asi deset milionů korun. Vskutku slušná testovací platba. Dalšími ranými uživateli a podporovateli se stali Wei Dai, tvůrce předchůdce Bitcoinu B-money, a Nick Szabo, tvůrce dalšího předchůdce Bitcoinu Bit gold. Všichni byli později podezříváni z toho, že jsou Satoshi Nakamoto, a jejich jména je dobré si v kryptokomunitě zapamatovat.

První maloobchodní transakce zahrnující fyzické zboží byla zaplacena 22. května 2010 na Floridě. Šlo o výměnu 10 000 vytěžených BTC za dvě pizzy doručené z místní pizzerie. Tím se 22. květen stal pro fanoušky kryptoměn Dnem bitcoinové pizzy a řada pizzerií, zejména v USA a v Asii, v ten den poskytuje slevu na pizzu zaplacenou bitcoinem. S ohledem na pozdější kurz BTC šlo tehdy na Floridě o pravděpodobně nejdražší pizzy na světě – a jejich kupec Laszlo Hanyecz se tímto nákupem zapsal do historie. Ve skutečnosti přitom nezaplatil přímo pizzerii. Bitcoiny poslal dobrovolníkovi v Anglii, který pak objednávku zadal kreditní kartou…

Zdá se, že Nakamotovo zapojení do aktivit kolem Bitcoinu nepřesáhlo polovinu roku 2010. V dubnu 2011 Nakamoto v komunikaci s jedním z přispěvatelů Bitcoinu připustil, že se „přesunul k jiným

* BTC je zkratka bitcoinu. Používá se také symbol ₿.

věcem“, a od té doby se po něm slehla zem. Zajímavé je, že zhruba milion bitcoinů, které Nakamoto vytěžil v raných dobách této kryptoměny, zůstalo netknuto. Sledování pohybů na pionýrských účtech totiž patřilo k oblíbeným kratochvílím Nakamotových hledačů. Fakt, že původní bitcoinové těžební účty zůstávají netknuté, nahrává domněnce, že Nakamoto někdy po roce 2011 zemřel. Z výše uvedených pánů tuto smutnou skutečnost splňuje jen Hal Finney, jenž v roce 2014 podlehl amyotrofické laterální skleróze. Mezi kandidáty, kteří se mohou skrývat za Satoshiho Nakamota, nicméně zůstává několik desítek osob, živých i mrtvých, včetně Adama Backa.

Dost hledání Satoshiho a vzpomínek na staré časy. To, co se stalo potom, je už historie. Přes několik zakopnutí se Bitcoin stal zakladatelem rodiny kryptoměn, více či méně odvozených z jeho zdrojového kódu a Nakamotových prvotních myšlenek, k nimž se tvůrci jiných kryptoměn vztahovali a vyrovnávali se s nimi. Podstatné je, že za celou dobu existence Bitcoinu se v jeho kódu objevila jen jediná závažná bezpečnostní chyba a ta byla napravena ještě v počátcích.*

Opusťme nyní historii Bitcoinu a podívejme se detailněji na jeho technologické pozadí.

Technologie Bitcoinu

Představuje Bitcoin první virtualizovanou měnu na světě? Určitě ne, viz třeba kamenné disky Rai na mikronéských ostrovech Yap, které se často fyzicky nepřenášejí. Dnes je však obecně známou virtuální měnou.

Už zaznělo, že blockchain funguje jako jakási veřejná účetní kniha bitcoinových transakcí. Jde o jednu ze základních technologií

* V srpnu 2010 byl zdrojový kód Bitcoinu zneužit někým, kdo dodnes zůstává v anonymitě. V bloku číslo 74 638 bylo vytvořeno 184 467 440 737,095 516 160 bitcoinů, přičemž dvě adresy obdržely každá něco málo přes 92 miliard bitcoinů. Trvalo pouhých pět hodin, než byl spuštěn soft fork, který blokový řetězec Bitcoinu obnovil do doby před blokem s chybou a obsahoval kód pro odmítnutí transakcí s přetečením výstupní hodnoty. Problémem byla chyba přetečení; kód pro kontrolu transakcí Bitcoinu nefungoval, pokud byly výstupy dostatečně velké, aby při součtu „přetekly“.

kryptoměn a také jeden z hlavních myšlenkových průlomů, s nimiž se můžeme setkat i mimo kryptoměny. Blockchain je veřejná databáze transakcí, která věrohodně identifikuje původce a jeho souhlas s transakcí formou digitálního podpisu, jakož i příjemce transakce. Tuto databázi je možné sdílet, aniž ji kdokoli ze sdílejících může věrohodně modifikovat. Bitcoin pak definujeme jako řetězec digitálních podpisů. Každý majitel převede bitcoin na dalšího tak, že digitálně podepíše hash* předchozí transakce a veřejný klíč** dalšího majitele a přidá je na konec „mince". Příjemce platby pak může podpisy, respektive celý předchozí řetězec vlastnictví ověřit.

Věrohodnost transakce zajišťuje kryptografický podpisový postup, jenž každý záznam spojí s předchozím i následujícím záznamem v blockchainu. Tím vzniká souvislý řetězec záznamů (odtud koneckonců pochází i slovo blockchain), u něhož máte jistotu, že žádný záznam nebyl změněn. Pokud by ke změně došlo, neseděl by kontrolní součet následujícího řetězce, a navíc by se takový záznam lišil v ostatních verzích blockchainu uložených na ostatních nodech neboli uzlech.***

Berme tedy za dané, že operaci můžete jako původce autorizovat a zadat jejího adresáta a že se rovněž vše zaznamená do systému, v němž se informace decentralizovaně rozšíří, takže vaše zaznamenané nároky vidí všichni účastníci systému, aniž je mohou změnit.

Druhým podstatným bodem je, že bitcoin neexistuje fyzicky, ale pouze virtuálně. Nejrůznější mince či papírové kartičky, které se jako bitcoiny tu a tam objevují, jsou buďto marketingové předměty,

---

* Hash je matematická funkce, která převádí libovolně dlouhý vstup na zašifrovaný výstup pevné délky. Nelze z něj zpětně odvodit vstup, ale jeho porovnáním lze ověřit, že dva vstupy jsou stejné. Používá se tedy například pro porovnání dvou souborů, přičemž si původní soubory nemusíte uchovávat. Stačí porovnat jejich hashe.

** Veřejný klíč je kryptograficky odvozený z privátního klíče, jenž z něj není možné zpětně odvodit. Privátním klíčem majitel podepisuje platbu (je tedy obdobou hesla), veřejný klíč je odznakem jeho totožnosti (je tedy obdobou přihlašovacího jména).

*** Node neboli uzel je počítač v bitcoinové síti, který hostí a synchronizuje kopii celého bitcoinového blockchainu. Uzly jsou nezbytné pro udržení chodu kryptoměnové sítě. Existují plné a light verze uzlů, přičemž light verze z bitcoinového blockchainu stahují pouze hlavičky bloků, a neukládají tedy celý blockchain. Jejich jediným úkolem je ověřovat transakce v blockchainu pomocí zjednodušeného ověřování plateb (SPV).

nebo fyzické – a tudíž i poněkud nebezpečné – reprezentace digitální existence bitcoinu. Každý bitcoin je unikátní, má své „sériové číslo" a jeho menší části vznikají vydělením z tohoto původního bitcoinu. Menší části existují jako záznam o vydělení, tedy transakce, z původního bitcoinu. Na první pohled to může znít trochu jako magie, ale o většinu z ní se stará bitcoinová síť, aniž do ní uživatel musí pronikat. Běžná bitcoinová peněženka vám jednoduše ukáže, kolik bitcoinů v ní máte, a nezatěžuje vás technikáliemi, například že vlastníte jednu polovinu tohoto bitcoinu a jednu desetinu tamtoho bitcoinu. Místo toho vám ukáže, že vlastníte 0,6 BTC.

Vlastníkem bitcoinu je ten, kdo disponuje jeho veřejným a privátním klíčem. A protože je Bitcoin postavený na kryptografii, je tento nárok nezvratitelný. Kdokoli je vlastníkem veřejného a privátního klíče, je faktickým vlastníkem dotyčné „peněženky", ať si o tom zákon myslí, co chce. Privátní klíč nelze zpětně zrekonstruovat, takže pokud například soud nařídí vydání bitcoinu, stane se tak pouze vydáním obou klíčů. Pokud privátní klíč ztratíte, neexistuje žádný opravný systémový prostředek k prokázání nároku. Kdo má klíč, má i nárok.

Veřejný klíč je vlastně adresou bitcoinové peněženky a není ho těžké získat: příjemce platby ho musí odesílateli sdělit, aby šlo operaci provést. Zatímco privátní klíč je nutné důsledně chránit, veřejný klíč nikoli. Určitá opatrnost je ovšem namístě. Veřejný klíč umožňuje vidět, kolik bitcoinů je v konkrétní peněžence uloženo. Standardně není zřejmé, kdo je jejím držitelem, ale pokud svou identitu spojíte například na webu s veřejným klíčem, bude jednoduché zjistit, kolik bitcoinů vlastníte.

Při uvažování o blockchainu je tedy nutné si uvědomit několik věcí. Obecně se spojuje s evidencí virtuální měny (typicky bitcoinů), jenže evidovat může vlastně jakoukoli transakci, jak digitální, tak fyzickou. Specializovaným blockchainům se někdy říká sidechain (a v případě měn také altcoiny, někdy hanlivě přezdívané shitcoiny). V knize však budu vždy mluvit obecně o blockchainu a bitcoinech, a to s vědomím, že zjednodušuji ve prospěch pochopení na úkor přesnosti.

Součástí konceptu blockchainu jsou i takzvané chytré smlouvy, tedy ujednání typu POKUD–POTOM, které se v systémech navázaných na daný blockchain automaticky provedou při splnění určitých podmínek. Často uváděným příkladem je „pokud dlužník nezaplatí

za auto (napojené do blockchainu), věřitel získá nejen vlastnické, ale i užívací právo". Kromě situací, kdy je třeba něco potvrdit externě („pošli bitcoiny, pokud poslal eura", což nelze zjistit bez přístupu na účet, a tedy prostředníka, který ho zajistí), tedy nepotřebujete prostředníka. Zároveň však tyto chytré smlouvy znamenají obrovské riziko v případě selhání, chyby či zneužití. Skutečnost, že se nelze odvolat k nejvyšší autoritě a zvrátit například podvod, je velmi frustrující.

Fakt, že transakce je zaznamenána v blockchainu, ještě neznamená, že toto právo obecně uznávají jiné systémy, například policejní, právně-soudní nebo i zločinecký svět. Zejména právní nároky na záznamy v blockchainu jsou v řadě států diskutabilní.

Identifikace je jednoznačná v rámci blockchainového systému, ale ten vás nemusí nijak spojovat s vaším reálným jménem a příjmením. Systém je tedy na první pohled pseudonymní. To však neznamená, že propojením různých databází nelze vaši jinou totožnost s nějakou mírou pravděpodobnosti určit. Vysledování a dohledávání původců plateb v blockchainových systémech je zajímavá a svébytná disciplína, a s jistotou anonymity tedy rozhodně nepočítejte. Některé kryptoměny se nicméně snaží vysokou míru anonymity podporovat. U Bitcoinu to nebylo záměrem.

Transakce v blockchainu jsou zpoplatněny podílem z každé operace. Ostatní účastníky to motivuje potvrzovat transakce v rámci systému a podílet se tak na jeho chodu, ale taky to znamená omezení. Výše poplatků představují minimálně u Bitcoinu problém pro mikrotransakce, přestože řada úprav po roce 2018 už vedla ke značnému zlepšení.

Decentralizace blockchainu znamená běžný provozní stav. Blockchain je standardně uložen v plné či zkrácené verzi na tisícovkách bitcoinových uzlů. Taková decentralizace představuje obranu před ovládnutím či regulací, tedy centralizací. Záleží však na velikosti systému – každý z nich je možné ovládnout získáním nadpoloviční části uzlů stvrzujících transakce. Některé implementace blockchainu se tomu snaží předejít postupy, jako je důsledné rozdrobení uzlů mezi všechny uživatele. Což má rovněž negativní následky (obtížnější implementaci, nižší rychlost či komfort atd.). V každém případě je zřejmé, že decentralizace blockchainu je nákladná; tuto nákladnost má vyvážit hlavní výhoda kryptoměn, tedy fakt, že v nich nefiguruje potenciálně zaujatý prostředník.

Decentralizace sítě není jen její silnou stránkou, ale také výraznou slabinou. Takto navržená síť je totiž náchylná k takzvanému útoku Sybil. Tento druh útoku zapojuje velkou část uzlů sítě, zdánlivě bezpečných a patřících různým lidem, ve skutečnosti však v rámci útoku ovládaných stejnou osobou, která zůstává ve stínu. Během útoku se uzlům podaří celou síť přesvědčit, že dotyčné záznamy v blockchainu mají být legitimně přepsány. Blockchainové sítě se brání zdražováním poplatků za takové operace, takže maximum, které lze při útoku ukrást, je menší než náklady na jeho provedení. Nevyhnutelným důsledkem jsou vysoké náklady. Systém má obří účet za elektřinu, a zanechává tedy i obrovskou uhlíkovou stopu. Tato hluboká neekonomičnost je vlastností, nikoli chybou. Jde o náklad, který udržuje útoky Sybil na uzdě. Neekonomičnost sítě se projevuje i tím, že většina aktivit v blockchainu spočívá pouze v jeho udržování, nikoli v nákupu nebo prodeji kryptoměny. Za jeden den se na sklonku roku 2021 uskutečnilo jen asi 27 000 „ekonomicky smysluplných" transakcí s bitcoiny, přičemž 75 % z nich tvořily meziburzovní transakce. Celkově pouze 2,5 % transakcí s bitcoiny představuje situaci, kdy někdo od někoho něco kupuje. Celosvětově je to méně než pět transakcí za minutu. Na celosvětovou měnu takového rozsahu to rozhodně není mnoho! Tato čísla vzbuzují pochybnosti nad použitelností bitcoinu jako regulérní měny. V těch totiž probíhá nesrovnatelně vyšší počet transakcí.

Díky veřejnému sdílení blockchainu jsou pohyby v něm veřejně přístupné.* Lze tedy odvodit stavy jednotlivých účtů i jejich vzájemné vazby. To je vlastně největší posun finančního paradigmatu ve světě, jak ho známe dnes. Jistě, nikde v blockchainu není zaznamenáno, jakou adresu používáte právě vy, nárok na ni se v systému prokazuje vlastnictvím tajného klíče, a adresy navíc mají být jednorázové. Jenže často nejsou. Stačí, abyste adresu někde veřejně uvedli a spojili se sebou. Adres si sice můžete zdarma vygenerovat mraky, ale problém přetrvává a stává se vlastností, protože jednotlivé adresy na sebe odkazují.

* Veřejné sdílení není úplně nutnost, existují i privátní blockchainy pro pracovní skupiny. Ale princip je opět ten, že všichni uživatelé jej mají plně přístupný.

Blockchain zaznamenává transakce, nikoli saldo (transakce nemusí být platba). To si musíte spočítat vy sami nebo vaše aplikace. Stejně tak je „poněkud" nejisté vlastnictví účtu, jež (připomínám) prokazujete znalostí tajného klíče.

Transakce v blockchainu nějaký čas trvají. Je potřeba, aby se blockchain dostatečně nasdílel a ověřil. Zvláště u Bitcoinu není rychlost zrovna závratná, ostatní systémy se s tím vyrovnávají lépe. (O rychlosti plateb ještě budeme hovořit.) Malé platby lze však provést okamžitě i v Bitcoinu.

Lidé si málo uvědomují, že blockchain Bitcoinu sám o sobě nezná dluhy. Nemůžete do blockchainu zaznamenat, že vám někdo něco dluží. Pokud nějaké systémy půjčují bitcoiny, využívají přitom vlastní evidenční systém. Scénář seriálu *Mr. Robot* (vymazat dluhy u clearingové firmy) je tedy stále možný.

Řadu výše uvedených nevýhod i výhod se snaží různé blockchainové systémy řešit různými způsoby. Na každé ALE bohužel existuje nějaké AVŠAK generující další ALE.

Jak funguje platba bitcoinem

Aleš chce Blance poslat 1 BTC a má svou bitcoinovou peněženku (například na mobilu či Blockchain.com). K tomu, aby peníze poslal, potřebuje Blančin veřejný klíč, respektive adresu (hash veřejného klíče), a svůj privátní klíč. Klíče vypadají jako náhodné shluky alfanumerických znaků.

Blančin veřejný klíč Aleš získá například oskenováním QR kódu, načtením přes NFC nebo prostým opsáním; svůj privátní klíč má uložený v aplikaci a slouží mu jako důkaz vlastnictví peněženky. Proto je dobré si vybrat důvěryhodného dodavatele peněženek, který si klíč nepřivlastní.*

Jak Aleš transakci provede? Zadá platební příkaz, v němž vyplní částku a Blančin veřejný klíč. Peněženka vygeneruje zprávu o transakci obsahující vstupy, částku a výstupy.

Vstupy obsahují informace o bitcoinech, které byly dříve odeslány na Alešovu adresu. Představte si například, že Aleš dříve obdržel

* Je patriotické na tomto místě poznamenat, že největším světovým výrobcem hardwarových krypto-peněženek je česká firma SatoshiLabs.

0,6 BTC od Ctirada a 0,6 BTC od Davida. Nyní, aby bylo možné poslat 1 BTC Blance, musí existovat dva vstupy: jeden vstup 0,6 BTC původem od Ctirada a jeden vstup 0,6 BTC původem od Davida. Protože Alešova peněženka neobsahuje jeden celý původní bitcoin, musejí se do transakce uvést oba vstupy.

Převáděná částka, kterou chce Aleš poslat, je v tomto případě 1 BTC.

Definované jsou také dva výstupy. Prvním je 1 BTC na adresu Blanky. Druhým je 0,2 BTC vrácený Alešovi jako „drobné". Tento druhý výstup se vypočítá jako součet vstupů 0,6 + 0,6 = 1,2 minus částka, kterou chce Aleš poslat, tedy 1 BTC. Vypadá to složitě, ale je to logické a tento postup mimo jiné zajišťuje, aby nebylo možné jeden bitcoin utratit vícekrát.

Tento platební příkaz Alešova peněženka digitálně podepíše jeho privátním klíčem a odešle nejbližšímu nodu – ve skutečnosti to může být cokoliv s implementovaným validačním mechanismem, i běžná peněženka.

Node ověří, zda má Aleš dostatek bitcoinů k provedení transakce – zpětně prohledá všechny záznamy v blockchainu podle ID předchozí transakce (sečte všechny transakce na tomto účtu) – a také zkontroluje Alešův digitální podpis, tedy fakt, že odesílatel zná Alešův privátní klíč. Pokud jsou náležitosti v pořádku, začne node požadavek na transakci posílat na další nody, do takzvaného mempoolu, dokud se nerozšíří do celé sítě. Požadavek na platbu je v tomto okamžiku ve stavu „pending", čekající na vyřízení.

Zde k transakci přistupuje specializovaný node nazývaný miner,* tedy těžař. Ten ověří, že Alešovy klíče mají přístup ke vstupům (tj. k adrese či adresám, odkud předtím obdržel bitcoiny, o nichž tvrdí, že je ovládá). Těžaři také shromáždí seznam dalších transakcí, které byly do sítě vysílány přibližně ve stejnou dobu jako Alešova transakce, a vytvoří z nich blok. Každý těžař, jenž dokončil „důkaz práce", může navrhnout nový blok, který bude „připojen" k řetězci s odkazem na

* Nakamoto původně používal pouze univerzální node – uzel, ale postupem času se i uzly začaly specializovat. Rozlišujeme těžební uzly, uzly pro sázení, autoritativní uzly a master uzly. První tři typy uzlů se používají v závislosti na používaném „důkazu", o typech důkazů i o uzlech ještě bude řeč, nebojte!

poslední blok. Tento nový blok je pak vysílán do sítě. Pokud ostatní účastníci sítě (nody) odsouhlasí, že jde o platný blok (tj. transakce, které obsahuje, se řídí všemi pravidly protokolu a správně odkazuje na předchozí blok), předají jej dál. Nakonec na něj naváže další těžař tím, že na něj při návrhu dalšího bloku odkáže jako na předchozí blok. Všechny transakce provedené v předchozím bloku nyní budou „potvrzeny" dalším těžařem. S přidáváním bloků do řetězce se počet potvrzení Alešovy transakce zvyšuje.

Počet potvrzení je důležitý pro obchodníka přijímajícího platbu. Pouhé jedno potvrzení by teoreticky (za určitých nákladů) bylo možné zfalšovat. Pokud platbu ještě žádný node nepotvrdil, může být zrušena. Jedno potvrzení se považuje za dostatečné pro drobnější platby do tisíce dolarů. U transakcí s žádným a jedním potvrzením je možný podvod zvaný dvojí výdaj (double-spend attack). Dvojí výdaj je postup, při kterém se uživatel pokouší utratit stejné peníze vícekrát. Větší platby potřebují v závislosti na své výši šest potvrzení, ale také třeba šedesát. Počet potvrzení je ovšem věcí obchodníka a jeho důvěry, nesouvisí s bitcoinovou sítí jako takovou. Již při šesti potvrzeních jsou však náklady na útok (a tedy například dvojí utracení bitcoinů) tak vysoké, že se nevyplatí. Proto se šest potvrzení obecně bere za dostačující. Je však třeba pamatovat, že vítězí největší počet potvrzení. Pokud je nějaká verze platby ověřena více nody než ta vaše, dostává přednost a nemáte se jak odvolat.

Vzhledem k tomu, že potvrzení se generují po deseti minutách, je na šest potvrzení potřeba čekat hodinu, což rychlost platby značně zpomaluje. Je spravedlivé připomenout, že jiné kryptoměny to mají jinak. Ethereum například doporučuje 12 potvrzení, která jsou k dispozici za tři minuty; Litecoin má šest potvrzení za 15 minut a například Ripple má transakce potvrzené prakticky okamžitě.

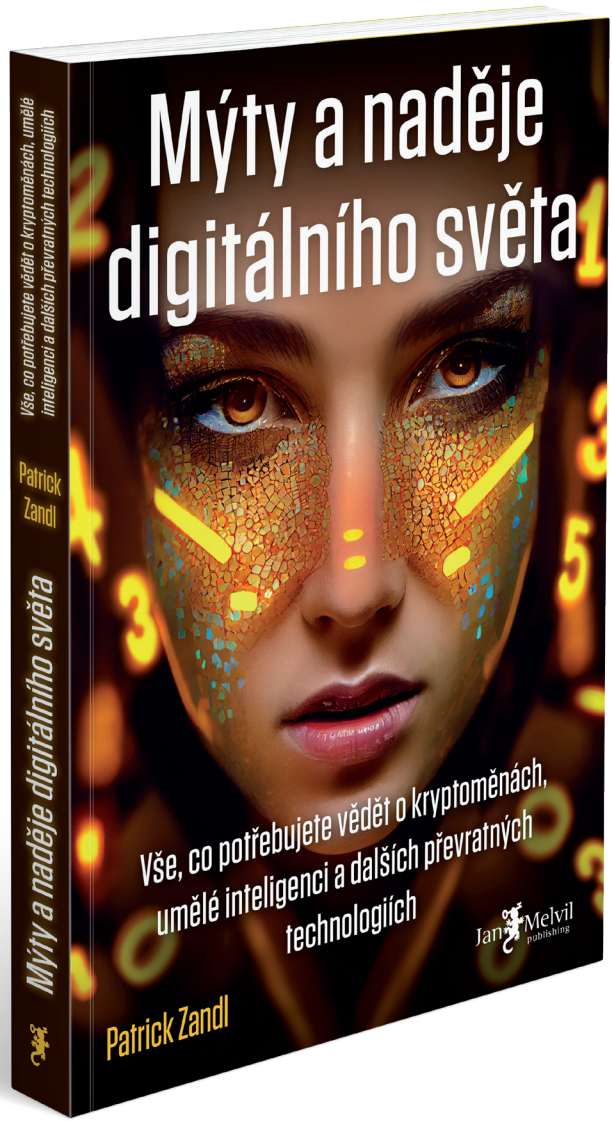
Poplatky za odeslání bitcoinu se mohou pohybovat od několika centů až po sto dolarů. Důvodem velkých rozdílů je skutečnost, že poplatky za bitcoiny jsou závislé jak na nabídce a poptávce (tj. na tom, jak je síť v daném okamžiku přetížená), tak i na velikosti transakce. Pokud má vaše transakce mnoho vstupů, zabere více místa v bloku a bude vyžadovat vyšší poplatek. Chcete-li například poslat 10 bitcoinů, s velkou pravděpodobností bude vaše transakce vyžadovat více vstupů, než když chcete poslat jeden. Transakce v hodnotě

10 BTC se může skládat z 5 + 2 + 1 + 1 + 1 (tedy celkem 5 vstupů), zatímco transakce v hodnotě 1 BTC může mít jen dva vstupy, jako v našem příkladu s Alešem a Blankou. Řada peněžek také umožňuje nastavit velikost odměny za ověření transakce, takže pokud nespěcháte, můžete nastavit poplatek co nejnižší, aby jej těžař zpracoval, až bude síť méně zahlcená. Naopak zvýšením poplatku si můžete zajistit, že vaše transakce budou zpracovány okamžitě.

Celý výše uvedený postup je poněkud složitější a má více verzí. Téhle se říká pay-to-public-key-hash – to proto, že se ve skutečnosti platí na hash veřejného klíče, ne na samotný klíč. Tím se zajišťuje anonymita, či spíše pseudonymita. Je zde také celá řada mechanismů, jež zde nepopisuji a které zajišťují lepší technickou proveditelnost transakce a její vyšší bezpečnost v decentralizovaném prostředí.

Obecně však platí, že blockchainový kryptografický mechanismus zajišťuje, že aby systém správně fungoval, nikdo nemusí nikoho konkrétního znát ani mu důvěřovat. Kryptografické protokoly se postarají, aby byl každý blok transakcí prokazatelně připojen k tomu předchozímu v dlouhém, transparentním a neměnném řetězci, a vytvářejí tak veřejnou účetní knihu. Proces, jenž ji udržuje bez nutné důvěry k třetí straně, se nazývá těžba. Základem sítě uživatelů bitcoinu, kteří mezi sebou obchodují s kryptoměnou, je tedy síť těžařů zaznamenávajících tyto transakce do blockchainu.

Zaznamenat řetězec transakcí je pro moderní počítač triviální, ale samotná těžba je náročná, protože software Bitcoinu tento proces uměle prodlužuje. Bez dodatečné obtížnosti by lidé mohli transakce falšovat, aby se obohatili nebo přivedli jiné lidi na mizinu. Mohli by do blockchainu zapsat podvodnou transakci a navršit na ni tolik triviálních transakcí, že by bylo nemožné podvod rozplést. Ze stejného důvodu by bylo snadné vkládat podvodné transakce do minulých bloků. Síť by se stala nepřehlednou, spamovou změtí konkurenčních účetních knih. Ono umělé prodloužení procesu se jmenuje proof-of-work (PoW), tedy důkaz prací. Kombinace důkazu práce s dalšími kryptografickými technikami byla další průlomovou myšlenkou. Software Bitcoinu upravuje obtížnost, které těžaři čelí, aby síť omezila počet transakcí v novém bloku o velikosti jednoho megabajtu každých deset minut.



Kupte si papírovou nebo elektronickou verzi knihy
za skvělou cenu na
www.melvil.cz