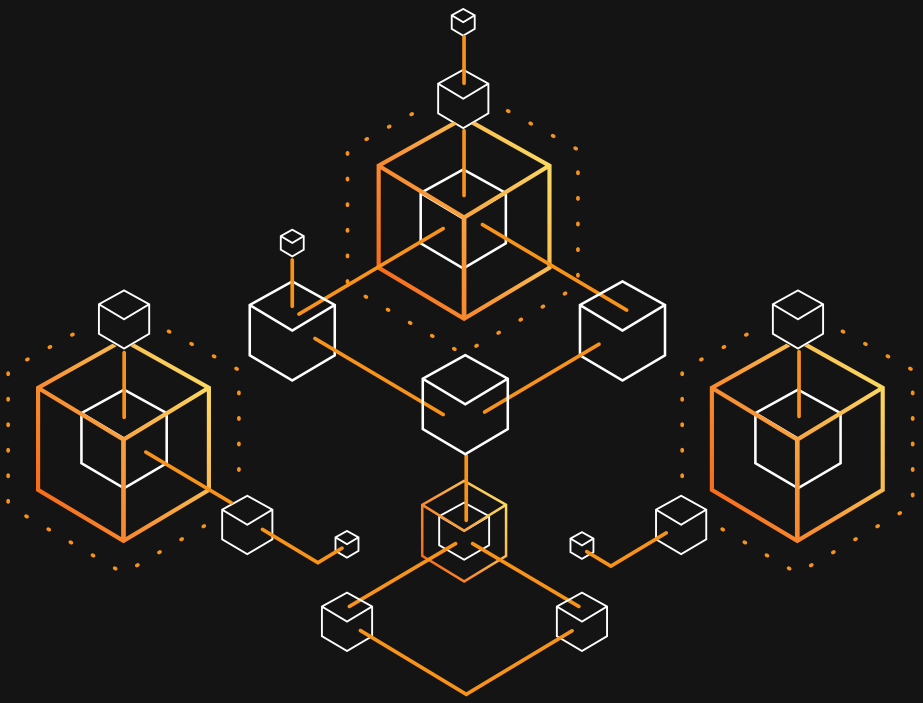
VYNÁLEZ JMÉNEM

BITCOIN



VZNIK A FUNGOVÁNÍ PRVNÍ SKUTEČNĚ VZÁCNÉ A DECENTRALIZOVANÉ MĚNY

YAN PRITZKER

BRAINS Publishing

BRAINS Publishing

ISBN 978-80-907975-0-5

Vynález jménem Bitcoin

Yan Prizker

BRAINS Publishing

BRAIINS

Česká firma působící na globální úrovni, která svými produkty posouvá Bitcoin dopředu. Od operačního systému **Braiins OS** pro ASIC minery, přes **Slush Pool** – první težební pool na světě, až po protokol **Stratum V2**, který zásadním způsobem vylepšuje infrasktrukturu těžby Bitconu.

PROJEKTY BRAIINS

SLUSH POOL

BRAIINS OS+

BRAIINS OS

STRATUM V2

V této knize se dozvíte, na jakých základech Bitcoin stojí a co z něj činí unikátní technologii budoucnosti.

Překlad jsme doplnili glosářem klíčových pojmů v češtině a jejich stručným vysvětlením.

VYNÁLEZ JMÉNEM BITCOIN

VZNIK A FUNGOVÁNÍ PRVNÍCH SKUTEČNĚ VZÁCNÝCH
A DECENTRALIZOVANÝCH PENĚZ

YAN PRITZKER

Aktualizovanou verzi knihy najdete online na inventingbitcoin.com

Tato kniha je věnována mým rodičům Yurymu a Laně, kteří naši rodinu vyvedli z bývalého SSSR, autokratického socialistického režimu se striktní kontrolou kapitálu.

Je taky věnována mé ženě Jessice, která musela vydržet, že jsem nedokázal přestat mluvit o Bitcoinu a chodil jsem spát pozdě, abych tuto knihu dokončil.

Obsah

Úvod

Když lidé prvně slyší o Bitcoinu, často mají sklon si vytvořit názor ještě dřív, než se vůbec pokusí pochopit, o co jde. Všude koluje spousta mýtů a je snadné nabýt mylného dojmu o tom, co Bitcoin je a jak funguje. Ještě před třemi lety jsem byl sám jedním z těch lidí, o kterých mluvím.

Proč jsem se rozhodl napsat tuto knihu? Posledních dvacet let jsem strávil budováním technologických startupů. Každý den se nořím do nových technologií a dobře se v nich orientuju. Přesto mi to od momentu, kdy jsem o Bitcoinu slyšel poprvé, trvalo pět let, než jsem se mu začal snažit porozumět. Mám pocit, že nejsem jediný, kdo s pochopením této inovace, která má potenciál změnit svět, potřebuje pomoct.

Na Bitcoin jsem poprvé narazil v roce 2011 na webu slashdot.org, zpravodajském serveru pro počítačové nadšence. Cena Bitcoinu tehdy dosáhla vrcholu okolo 30 dolarů za minci poté, co prorazila strop v obří bublině. Věděl jsem tehdy jen to, že se nějací lidé na internetu pokoušejí založit jakýsi peer-to-peer platební systém. Přestože jsem netušil, o co jde, jak to funguje, ani jsem neměl ponětí o investičních a burzovních cyklech, rozhodl jsem se tehdy pár mincí koupit, kdyby na tom náhodou něco bylo. Musel jsem k tomu tehdy použít příšerně vyhlížející stránku s názvem Mt. Gox. Později se ukázalo, že se tato směnárna dolarů za Bitcoiny ocitla v platební neschopnosti.

Pomalu jsem sledoval, jak moje investice téměř ztratila hodnotu, když cena spadla ze 30 dolarů na pouhé dva. Postupem času jsem na Bitcoin úplně zapomněl, život šel dál a já jsem dál pracoval ve startupech. Ani nevím, co se s těmi tehdejšími mincemi stalo. Myslím, že klíče k nim jsou uložené na harddisku ze starého laptopu ležícího někde na skládce.

V roce 2013 jsem o Bitcoinu slyšel znovu. Tentokrát byl rozruch v médiích hlasitější a nákup byl o hodně vychytanější. Existovaly aplikace jako Coinbase, které se zdály být zcela legitimní. Oproti Mt. Gox představovaly výrazné zlepšení. Zdálo se mi, že to Bitcoin může opravdu někam dotáhnout.

Pro jistotu, a opět aniž jsem o Bitcoinu cokoliv věděl, jsem tedy na vrcholu té bubliny opět něco nakoupil (Bitcoin tehdy stál okolo 1000 dolarů za minci) a sledoval jsem, jak má investice spadla po poklesu ceny na asi 200 dolarů za minci. Tentokrát jsem si řekl, že to není tak velká částka, aby se ji vyplatilo prodávat, tak jsem to nechal být a úspěšně jsem to ignoroval, zatímco jsem se plně věnoval budování svého dalšího startupu: Reverb.com.

Během následujících čtyř let se Reverb rychle rozrostl a stal se pro hudebníky místem číslo jedna. Měnil jsem svět a přinášel jsem hudbu lidem. Byl jsem technologickým ředitelem vzrušující, rychle se rozvíjející technologické společnosti, dělal jsem práci, která mě bavila, a neměl jsem čas na nějaké hloupé internetové peníze.

Stydím se, že jsem se teprve v létě roku 2016 podíval na první video od Andrease Antonopoulose, které mě konečně donutilo zpozornět. Najednou jsem měl v hlavě spoustu otázek. Odkud Bitcoin pochází? Kdo ho má pod kontrolou? Jak funguje? Jaká je jeho těžba? Jak může Bitcoin měnit svět? Začal jsem číst všechno, co mi přišlo pod ruku, po celý rok a půl jsem každý den poslouchal hodiny podcastů a videí.

Počátkem roku 2018, těsně poté co Bitcoin dosáhl svého dalšího maxima při ceně okolo 20 000 dolarů za minci, jsem se konečně

rozhodl opustit Reverb, abych mohl přispět k šíření povědomí o Bitcoinu. Proč jsem opustil svůj velmi úspěšný startup, abych pracoval na Bitcoinu? Jsem přesvědčen, že Bitcoin je vynález, který se objeví jen jednou za život; možná jednou za mnoho životů.

Pokud Bitcoin uspěje, může být nakonec stejně důležitý jako knihtisk (decentralizované šíření informací), internet (decentralizovaný obsah a komunikace) nebo demokracie založená na trojím typu moci (decentralizovaná vláda). Doufám, že díky pochopení toho, jak Bitcoin funguje, pochopíte, jak může změnit svět k lepšímu. Bitcoin decentralizuje produkci a konzumaci peněz a otvírá tak lidstvu dveře k novým způsobům spolupráce dosud nepředstavitelného rozsahu.

V médiích se z Bitcoinu probírá převážně jeho cena. Jeden den se vyšplhá na milion dolarů, další den padá na nulu ve spirále smrti. Občas se v médiích objeví zpráva o tom, že Bitcoin spotřebuje veškerou světovou energii a v průběhu deseti let zničí planetu. To samozřejmě není pravda, a až se dozvíte, jak funguje, snad vám dojde proč. Porozumíte taky tomu, proč jsou právě cenové bubliny jedním z nejméně zajímavých aspektů Bitcoinu.

V této knížce nehodlám analyzovat ekonomiku Bitcoinu a tvrdých peněz (sound money), přestože se těchto konceptů letmo dotkneme. Nebudu na Bitcoin nahlížet z hlediska investování, ani se vás nebudu snažit přesvědčit, že by měl každý alespoň nějaké Bitcoiny vlastnit. Bezprostředně po přečtení této knihy bych velmi doporučoval knížku od Saifedeana Ammouse *The Bitcoin Standard* (Bitcoinový Standard), pokud jste ji ještě nečetli.

Nebudu se tady ani podrobně zabývat počítačovým kódem, takže pro porozumění této knize znalost informatiky není zapotřebí. Pokud vás zajímá Bitcoin z tohoto hlediska, doporučuji klíčovou publikaci Andrease Antonopoulose *Mastering Bitcoin* a nově vydanou publikaci *Programming Bitcoin* (Programování Bitcoinu) od Jimmyho Songa.

Pro mě osobně bylo (naprosto) klíčovou věcí to, abych pochopil všechno okolo toho, jak Bitcoin funguje. V této knize se s vámi pokusím toto pochopení ve stručné, zjednodušené podobě sdílet. Mým cílem je čtenáře navnadit a nabídnout mu malou ochutnávku z informatiky, ekonomie i teorie her, tedy stránek, které z Bitcoinu dělají jeden z nejzajímavějších a nejvýznamnějších vynálezů naší doby. Doufám, že skrze porozumění fungování Bitcoinu zjistíte stejně jako já, že Bitcoin představuje mnohem hlubší technologii, než se zdá na první pohled, a jeho vynález může mít velký vliv na svět příštích generací.

Při výkladu budeme postupovat krok za krokem. Jen s využitím středoškolské matematiky si postupně projdeme, jak Bitcoin vznikl. Doufám, že se tato kniha pro vás stane pozváním do tajuplného světa Bitcoinu. Tak jdeme na to!

KAPITOLA 1

Co je Bitcoin?

Bitcoin je peer-to-peer elektronická měna, nová forma elektronických peněz, které si mezi sebou můžou lidé či počítače posílat bez jakéhokoliv prostředníka, kterému musí důvěřovat (jakým je například banka), a jejichž vydávání není pod kontrolou nějaké jedné instituce nebo skupiny.

Představte si papírovou bankovku nebo kovovou minci. Když těmito penězi někomu platíte, tato osoba nemusí vědět, kdo jste. Musí jen věřit, že peníze, které od vás dostane, nejsou falešné. To si lidé obvykle ověřují jen pouhým pohledem a pohmatem, v případě vyšších obnosů se pak používá speciální testovací zařízení.

S tím, jak se naše společnost digitalizovala, začala většina našich plateb probíhat přes internet za pomoci prostředníka: může jím být společnost vydávající platební karty, jakou je např. Visa, poskytovatel digitálních pateb, jakým je např. PayPal nebo Apple Pay, nebo nějaká online platforma jako např. čínský WeChat.

Přechod k digitálním platbám s sebou přinesl závislost na centrální autoritě, která musí každou platbu schválit a potvrdit. Je tomu tak proto, že povaha peněz se změnila z něčeho materiálního, co můžete nosit u sebe a sami si kontrolovat, na digitální informaci, která musí být uložena a ověřena třetí stranou, zodpovědnou za převod.

Když se zbavujeme hotovosti ve prospěch pohodlných digitálních plateb, vytváříme tak zároveň systém, v němž dáváme mimořádnou moc těm, kteří se nás můžou pokusit ovládat. Digitální platební platformy se stávají základem dystopických autoritářských systémů kontroly, které využívá např. čínská vláda ke sledování disidentů a k tomu, aby zabránila nákupu zboží a služeb lidí, jejichž chování se jí nelíbí.

Bitcoin nabízí alternativu k centrálně kontrolovaným digitálním penězům. Přináší výhody hotovosti v digitální podobě. Co Bitcoin zahrnuje:

1. Digitální aktivum (obvykle bývá označováno jako bitcoin s malým b), jehož zásoba je omezená, předem známá a neměnná. Představuje zásadní rozdíl oproti papírovým bankovkám a jejich digitálním verzím vydávaným vládami a centrálními bankami, jejichž zásoba nepředvídatelným tempem roste.
2. Skupina vzájemně propojených počítačů (bitcoinová síť), ke které se může pomocí speciální aplikace připojit kdokoliv. Bitcoinová síť slouží k vydávání Bitcoinů, sledování jejich vlastnictví a k jejich převádění mezi účastníky, aniž závisí na jakémkoliv prostředníkovi, jako jsou banky, platební společnosti či vlády.
3. Bitcoinový klient je program, který může kdokoliv spustit na svém počítači a stát se tak součástí sítě. Jedná se o open source software, což znamená, že jeho kód je volně přístupný a každý ho může upravovat či opravovat.

Bitcoin je síť počítačů, na kterých je spuštěn bitcoinový klient.

V následující části se podíváme na to, proč vlastně Bitcoin vznikl.

Kde se vzal?

Bitcoin byl vynalezen někdy okolo roku 2008 člověkem, případně skupinou osob, známým pod pseudonymem Satoshi Nakamoto. Nikdo neví, kdo ve skutečnosti Satoshi Nakamoto je, ví se jen, že zmizel a roky už o něm nikdo neslyšel.

11. února 2009 Satoshi publikoval příspěvek o rané verzi Bitcoinu na internetovém fóru pro tzv. cypherpunkery, kteří se zabývají kryptografickými technologiemi a kterým leží na srdci ochrana soukromí a svobody každého jednotlivce. Přestože tenhle příspěvek není prvním oficiálním oznámením o zrodu Bitcoinu, je v něm dobře shrnuta Satoshiho motivace, proto ho použijeme jako základ pro naši diskusi.

Níže vybíráme relevantní části textu ze zmíněného příspěvku. V následující části si tyto výroky projdeme a zkusíme si ukázat, které nešvary stávajícího finančního systému se Satoshi snažil vyřešit:

Vyvinul jsem nový open source P2P systém e-hotovosti s názvem Bitcoin. Je kompletně decentralizovaný, zcela bez centrálního serveru nebo důvěryhodných třetích stran, protože je všechno založeno na kryptozáznamech, a ne na důvěře. [...]

Problém tradičních měn spočívá v tom, že vyžadují ohromné množství důvěry, aby nějak fungovaly. Musíme důvěřovat centrální bance, že měnu neznehodnotí, historie fiat měn je ovšem plná různých porušení téhle důvěry. Musíme důvěřovat bankám, že budou naše peníze uchovávat a elektronicky je převádět, ale banky naše peníze rozpůjčovávají ve vlnách úvěrových bublin s jen zlomkovou rezervou. Musíme jim důvěřovat, že naše údaje ochrání a že nedovolí, aby nás o úspory obrali zloději identit. Obrovské režijní náklady bank navíc znemožňují mikroplatby.

O generaci dřív měly podobný problém počítačové systémy umožňující synchronní práci většího množství uživatelů. Před zavedením spolehlivého šifrování museli uživatelé k ochraně svých souborů využívat ochranu heslem. [...]

Později došlo k masovému rozšíření spolehlivého šifrování a už nebylo nutné se opírat jen o důvěru. Data bylo možné zajistit způsobem, který fyzicky neumožňoval přístup třetích stran, z žádného důvodu a pod žádnou záminkou, prostě za žádných okolností.

Je načase, abychom zavedli stejné řešení i pro peníze. S pomocí e-měny založené na kryptografickém důkazu a bez potřeby důvěřovat třetím stranám můžou být peníze zabezpečené a transakce snadné. [...]

Bitcoin nabízí řešení v podobě peer-to-peer sítě, která bude zabraňovat dvojím útratám. Ve zkratce, tato síť funguje jako distribuovaný server přidělující časová razítka, který při platbě označí první transakci jako utracenou. Využívá se toho, že informace lze snadno rozšířit, ale jen obtížně se šíření brání. Podrobnější informace o síti Bitcoin najdete v článku na adrese: bitcoin.org/bitcoin.pdf.

- Satoshi Nakamoto

Jaké problémy Bitcoin řeší?

Pojďme si Satoshiho příspěvek rozebrat. V knize se postupně podíváme, jak jsou tyto koncepty implementovány v reálném světě. Nelekejte se, pokud vám něco v této kapitole nebude jasné, později si vše vysvětlíme podrobněji. Teď nám jde jen o to, uvědomit si, jaké měl Satoshi cíle, abychom je pak společně prošli a pochopili Vynález Bitcoinu.

> *Vyvinul jsem nový open source P2P systém e-hotovosti.*

P2P znamená peer-to-peer a je označením pro systém, ve kterém může jedna osoba komunikovat s druhou jako rovný s rovným (peer to peer) bez dalšího prostředníka. Možná si vzpomínáte na P2P technologie sdílení souborů, jakými byly Napster, Kazaa nebo BitTorrent, které lidem jako první umožnily sdílet hudbu a filmy bez jakéhokoliv prostředníka. Satoshi navrhl Bitcoin, aby lidem podobným nezprostředkovaným způsobem umožnil výměnu e-hotovosti neboli elektronické hotovosti.

Software, který Bitcoin využívá, je open source, což znamená, že si každý může přečíst jeho zdrojový kód a upravovat jej.

To je zásadní věc, protože díky ní nestojí celý systém jen na důvěře Satoshimu. Nemusíme věřit ničemu, co Satoshi ve svém příspěvku píše o fungování svého softwaru. Můžeme se prostě podívat na zdrojový kód a sami se přesvědčit, jak funguje. Navíc můžeme funkčnost vylepšovat tím, že budeme kód upravovat.

> *Je kompletně decentralizovaný, zcela bez centrálního systému nebo třetích stran, jimž je třeba důvěřovat.*

Satoshi uvádí, že jeho systém je decentralizovaný, čímž se od centrálně řízených systémů liší. Předchozí pokusy o vytvoření digitální měny, jako např. DigiCash Davida Chauma, byly založené na centrálním serveru, což byl počítač nebo skupina počítačů, které byly zodpovědné za vydávání měny a potvrzování transakcí a zároveň byly pod kontrolou jediné společnosti.

Podobné centrálně řízené soukromé peněžní systémy byly odsouzeny k zániku; lidé nemůžou spoléhat na peníze, které zaniknou, jakmile by společnost, která je vydává, zkrachovala, podlehla útoku hackerů, nebo pokud by této společnosti zkolaboval server nebo snad byla zrušena vládou.

Bitcoin naproti tomu není řízen ani ovládán jedinou společností, ale sítí jednotlivců a společností po celém světě. Vypnout bitcoinovou síť by znamenalo vypnout stovky tisíc počítačů po celém světě, z nichž některé jsou neznámo kde. Připomínalo by to beznadějný hon na krtka, který si vždy udělá novou hromádku na novém místě. Každý takový útok by vedl jen k založení nových síťových uzlů, respektive připojení nových počítačů tvořících síť Bitcoin.

> *[systém Bitcoinu] je založen na kryptografickém důkazu bez potřeby důvěřovat prostředníkům..*

Internet se, stejně jako většina moderních počítačových systémů, zakládá na kryptografii, tedy způsobu skrývání informací takovým

způsobem, aby je dokázal dekódovat jen určitý příjemce. Jak to, že u Bitcoinu není potřeba důvěra? Podrobněji si to ještě probereme později, ale základní myšlenka je následující: Místo abychom věřili někomu, kdo říká „Já jsem Alena" nebo „Mám na svém účtu 10 dolarů", můžeme tato tvrzení vyjádřit pomocí kryptografického záznamu, díky kterému je snadné si je ověřit a který zároveň nelze zfalšovat. Bitcoin je právě na kryptografii založený a účastníci si tak můžou neustále ověřovat chování všech ostatních, aniž by se museli spoléhat na nějakou třetí stranu.

> *Musíme bankám důvěřovat, že ochrání naše údaje a zlodějům identit nedovolí, aby nás obrali o naše úspory.*

Na rozdíl od vašeho bankovního účtu, digitálního platebního systému nebo kreditní karty Bitcoin umožňuje jakýmkoliv dvěma stranám provádět transakce bez uvedení osobních identifikačních údajů. Centralizovaná úložiště spotřebitelských dat v bankách, u společností vydávajících kreditní karty, zpracovatelů plateb a vlád jsou pro hackery téměř jako otevřená truhla s pokladem. Skoro jako důkaz Satoshiho tvrzení došlo v roce 2017 k rozsáhlé zpronevěře dat spravovaných společností Equifax. Hackerům tehdy padly do rukou identifikační údaje a data o financích víc než 140 milionů osob.

Bitcoin odděluje finanční transakce od identit v reálném světě. Konec konců, když někomu platíme v hotovosti, nepotřebuje vědět, kdo jsme, a nemusíme tak mít obavu, že po provedení platby bude moci použít zjištěné údaje k tomu, aby nás o nějaké peníze okradl. Proč bychom neměli mít stejná, nebo dokonce vyšší očekávání od digitálních peněz?

> *Musíme důvěřovat centrální bance, že měnu neznehodnotí, historie fiat měn je ovšem plná různých porušení téhle důvěry.*

Výrazem fiat, což v latině znamená „staniž se", se označuje měna vydávaná vládami a centrální bankou na příkaz vlády. V průběhu historie se jako peníze používaly suroviny, které byly obtížně získatelné, snadno ověřitelné a lehce přemístitelné, například mušle, skleněné korálky, stříbro nebo zlato. Pokaždé, když se něco začalo používat jako platidlo, to vedlo ke snaze vyrábět toho víc. Když se objevila dokonalejší technologie umožňující něco produkovat ve velkém množství, ztrácelo to na hodnotě. Tímto způsobem evropští osadníci obrali Afriku o její bohatství: měnili skleněné korálky, jejichž výroba pro ně byla snadná, za lidské otroky, jejichž výroba snadná není. To je taky důvod, proč bylo zlato tak dlouho považováno za dobré platidlo – bylo obtížné ho produkovat rychle a ve velkém objemu.*

Pomalu jsme se přesunuli od světové ekonomiky, kde se platilo zlatem, k ekonomice, kde se vydávaly papírové certifikáty představující nárok na zlato. Když prezident Nixon v roce 1971 zrušil mezinárodní převoditelnost amerického dolaru na zlato, certifikáty byly úplně odloučeny od jakéhokoliv materiálního základu.

Konec zlatého standardu umožnil vládám a centrálním bankám zvyšovat množství peněz podle potřeby a tím snižovat hodnotu každé bankovky v oběhu. Tomuhle procesu říkáme znehodnocování. Přestože čistou fiat měnu, nesměnitelnou za skutečnou hodnotu, tedy peníze, které všichni známe a denně používáme, vydává vláda, je ve skutečnosti právě ona v lidských dějinách relativně novým experimentem.

Musíme důvěřovat našim vládám, že nebudou tiskárny peněz zneužívat, ale zároveň je známo mnoho případů, kdy byla tato důvěra zklamána. V autokratických a centrálně plánovaných režimech, kde vláda přímo ovládá peněžní systém, jako například

---

* Pro výborný přehled o dějinách peněz doporučuju esej Shelling Out od Nicka Szaboa: nakamotoinstitute.org/shelling-out/.

ve Venezuele, se měna stala téměř bezcennou. Venezuelský bolívar devalvoval ze 2 bolivarů za jeden americký dolar v roce 2009 na 250 000 bolívarů za jeden americký dolar v roce 2019.

V době vzniku této knihy prochází Venezuela kolapsem, který způsobila vláda příšerným řízením ekonomiky.

Satoshi chtěl nabídnout alternativu k fiat měně, jejíž zásoba stále nepředvídatelně roste. Aby předešel znehodnocování měny, navrhl systém peněz, jejichž zásoba je omezená a které jsou vydávány předvídatelným a neměnným tempem. Nikdy nebude v oběhu víc než 21 milionů Bitcoinů, přestože každý Bitcoin může být rozdělen na 100 milionů jednotek zvaných satoshi. Okolo roku 2140 bude v oběhu nakonec celkem 2,1 biliard satoshi.

Před příchodem Bitcoinu nebylo možné digitální aktiva chránit před neomezeným kopírováním. Zkopírovat digitální knihu, audiosoubor nebo video a poslat je kamarádovi je snadné a nic nestojí. Jedinými výjimkami jsou digitální aktiva kontrolovaná prostředníky. Když si například pronajmete film na iTunes, můžete ho na svém počítači nebo mobilním telefonu sledovat jen díky tomu, že vám to iTunes umožňuje. Po uplynutí nájemní lhůty iTunes tuto možnost opět zruší. Podobně jsou vaše digitální peníze pod kontrolou banky. Banka má za úkol vést záznamy o tom, kolik peněz máte, a když je chcete převést na někoho jiného, banka tenhle převod buď autorizuje, nebo zamítne.

Bitcoin je první digitální systém, který zaručuje určitou hodnotu platidla bez jakýchkoliv prostředníků a je prvním známým aktivem, jehož neměnná zásoba a rychlost vydávání jsou předem dané. Ani vzácné kovy, jako je zlato, tuto vlastnost nemají, protože v případě, že je to nějak výhodné, můžeme vytěžit nějaké další zlato. Zkuste si představit, že by se objevil asteroid, na kterém by bylo víc zlata, než kolik je ho na celé Zemi. Co by to udělalo s cenou zlata, kdyby tímhle způsobem jeho množství vzrostlo? Bitcoin je vůči podobným objevům imunní a jeho množství nelze

v případě potřeby zvyšovat. Je zkrátka nemožné vytvořit Bitcoinů víc a v následujících kapitolách si vysvětlíme, proč tomu tak je.

Povaha peněz a fungování stávajících peněžních systémů jsou složité, v této knize se jimi nebudeme zabývat dopodrobna. Pokud byste se chtěli o povaze peněz ve vztahu k Bitcoinu dozvědět víc, doporučil bych pro začátek knihu Bitcoin Standard od Saifedeana Ammouse.

> *Data bylo možné zajistit způsobem, který fyzicky neumožňoval přístup třetích stran, z žádného důvodu a pod žádnou záminkou, prostě za žádných okolností. […] Je načase, abychom zavedli stejné opatření i v případě peněz.*

Naše stávající systémy úschovy peněz, jako například jejich uložení v bance, jsou založené na tom, že peníze svěřujeme někomu jinému. Důvěřujete-li takovému prostředníkovi, spoléháte se nejen na to, že se nezachová zlovolně nebo nerozumně, ale taky na to, že vláda na prostředníka nebude vyvíjet tlak a vaše finance skrze něj nesebere nebo vám k nim nezablokuje přístup. Opakovaně se totiž ukazuje, že vlády v případě ohrožení přístup k penězům uzavírají.

Někomu, kdo žije ve Spojených státech amerických nebo nějaké jiné zemi s velmi regulovanou ekonomikou, se může představa, že se jednoho dne probudí bez peněz, zdát šílená, ale děje se to dnes a denně. Mně například zablokovali finance na PayPalu jen proto, že jsem účet několik měsíců nepoužíval. Trvalo víc než týden, než se mi opět podařilo přístupu ke „svým" penězům dosáhnout. Mám štěstí, že žiji ve Spojených státech, kde jsem měl v případě blokace účtu ze strany PayPalu alespoň naději na získání peněz zpátky právní cestou a kde můžu věřit, že mě vláda ani banka neokradou.

V méně svobodných zemích se děly a stále dějí i horší věci. Při kolapsu měny v Řecku například došlo k zavření bank, banky

na Kypru navrhly konfiskaci financí svých zákazníků ke splacení vlastních dluhů, v Indii zase vláda prohlásila některé bankovky za neplatné.

V bývalém Sovětském svazu, kde jsem vyrůstal, vedla vládou kontrolovaná ekonomika k rozsáhlému nedostatku různých druhů zboží. Vlastnit cizí měnu, například americké dolary, bylo ilegální. Když jsme chtěli odjet do zahraničí, mohli jsme si koupit jen omezené množství amerických dolarů na osobu, dle oficiálního kurzu určeného vládou, který se diametrálně odlišoval od skutečného tržního kurzu. Vláda nás touto přísnou kontrolou ekonomiky a pohybu kapitálu v podstatě obírala o tu trochu bohatství, kterou jsme měli.

Autokratické země mají sklon zavádět přísná ekonomická opatření, znemožňují lidem vybírání peněz z bank, jejich vyvážení ze země nebo výměnu lokálních peněz na volném trhu za hodnotnější zahraniční měnu, například dolar. To vládě dává volnou ruku k uskutečňování šílených ekonomických experimentů, jakým byl socialistický systém v Sovětském svazu.

> *Bitcoin nespoléhá na důvěru ve třetí stranu, která vaše peníze ochrání. Bitcoin namísto toho neumožňuje přístup k vašim mincím bez speciálního klíče, který máte jen vy, a to z jakéhokoliv důvodu, pod jakoukoliv záminkou, prostě v žádném případě. S Bitcoinem se vám dostává do rukou klíč k finanční svobodě. Bitcoin odděluje peníze od státu.*

Bitcoin nabízí řešení v podobě peer-to-peer sítě, která bude zabraňovat dvojím útratám. Ve zkratce, tato síť funguje jako distribuovaný server přidělující časová razítka, který při platbě označí první transakci jako utracenou.

Síť představuje velké množství propojených počítačů, které si vzájemně můžou posílat zprávy. Slovo distribuovaný znamená, že

není žádný centrální orgán, ale síť funguje na základě společného úsilí všech účastníků.

V systému bez centrální kontroly je důležité vědět, že nikdo nepodvádí. Dvojí útrata spočívá v možnosti utratit jedny peníze dvakrát. V případě fyzických peněz možnost dvojí útraty nepředstavuje problém, protože peníze v okamžiku utracení opouštějí vaši ruku. Naproti tomu digitální transakce můžou být kopírovány stejně jako hudba nebo filmy. Když posíláte peníze bankovním převodem, banka zajišťuje, aby jedny a tytéž peníze nebyly odeslány dvakrát. V systému bez centrální kontroly potřebujeme způsob, jak dvojím útratám, které jsou v podstatě podobné jako padělání peněz, předcházet.

Satoshi popisuje, jak účastníci sítě Bitcoin společnými silami přidělují časová razítka jednotlivým transakcím (tj. jak je uspořádávají), abychom věděli, které transakce se uskutečnily jako první, a mohli proto zamítnout jakékoliv následující pokusy použít už utracené peníze. V následujících kapitolách si tenhle systém popíšeme úplně od začátku. Tenhle systém totiž umožňuje detekovat pokusy o padělání, aniž se musíme spoléhat na nějakého centrálního vydavatele peněz nebo ověřovatele transakcí.

Bitcoin nevznikl na zelené louce. Satoshi ve svém článku zmiňuje několik předchozích důležitých pokusů o vytvoření podobných systémů, jako například b-money od Wei Daie nebo Hashcash Adama Backa. Vynález Bitcoinu stojí na ramenou obrů, nikomu předtím se však nepodařilo spojit ty správné díly dohromady a vytvořit tak první systém vydávání a převádění skutečně vzácné digitální měny bez centrální kontroly.

Aby Satoshi vyřešil problémy tížící stávající peněžní systémy – ochranu soukromí, znehodnocování a centrální kontrolu – musel se vypořádat s řadou technických úkolů:

1. Jak vytvořit peer-to-peer síť, která umožní každému se k ní dobrovolně připojit a podílet se na jejím fungování.

2. Jak může skupina lidí, kteří můžou zůstat v anonymitě a nemusí si navzájem důvěřovat, vést společnou účetní knihu, i kdyby někdo z nich byl nepoctivý.
3. Jak lidem umožnit, aby vydávali svou vlastní nezfalšovatelnou měnu bez nutnosti se spoléhat na centrálního vydavatele a současně zachovávali hodnotu této měny, aby produkce nových jednotek nebyla jen tak dostupná všem a zdarma.

Když byl Bitcoin spuštěn, provozovala ho jen hrstka lidí, kteří měli na svých počítačích spuštěný bitcoinový software a bitcoinovou síť tím napájeli. Většina lidí to v té době považovala za hloupost nebo se domnívali, že se v systému odhalí závažné chyby, kvůli kterým by se stal nefunkčním.

V průběhu času se k síti připojovalo víc a víc lidí, kteří svými počítači posilovali její bezpečnost a zároveň její hodnotu tím, že novou měnu kupovali nebo ji začali přijímat jako platidlo za zboží a služby. Dnes, o deset let později, Bitcoin používají miliony lidí s desítkami až stovkami tisíc počítačových uzlů, na kterých je spuštěn bitcoinový software, který je zdarma a je vyvíjen stovkami dobrovolníků a společností po celém světě.

Pojďme se podívat, jak se takový systém dá vybudovat!

KAPITOLA 2

Pryč s prostředníky

V předchozí kapitole jsme mluvili o tom, že Bitcoin představuje peer-to-peer systém na převádění hodnoty. Než se blíže podíváme, jak to přesně funguje, řekneme si, jak se se sledováním vlastnictví aktiv a převodů vypořádává tradiční banka nebo platební společnost.

Banky nejsou nic než účetní knihy

Jak funguje digitální platba prováděná prostřednictvím vaší banky, PayPalu nebo Apple Pay? Jednoduše řečeno, tito prostředníci fungují jako uctívané účetní knihy se záznamy o účtech a transakcích.

Funkcí banky je uchovávat a chránit vaše vklady. Vklady jsou však v dnešní době spíše elektronické než fyzické v podobě mincí či papírových bankovek. Úkol banky tak spočívá v udržování a ochraně databáze účtů. Protože jsou tato data elektronická, zabezpečení jsou taky většinou elektronická. Banky používají software na detekci neoprávněného proniknutí do systému, provádějí zálohy, aby zabránily ztrátě dat, zajišťují audity třetí stranou, aby se ujistily, že nedochází ke zpronevěře zevnitř, a pro případ, kdyby se náhodou něco stalo, jsou pojištěny.

Na příkladu si ukážeme, jak banky fungují. Budeme používat slovo „banka", ale ve skutečnosti máme na mysli v zásadě jakoukoliv třetí stranu, která zpracovává platby. Začneme s účetní knihou, ve které je zaznamenáno, že Alena a Bedřich si v bance uložili peníze.

Bankovní účetní kniha

1. *Alena: kreditní položka vklad hotovosti +2 $*
2. *Bedřich: kreditní položka vklad hotovosti +10 $*

Když chce Alena Bedřichovi poslat 2 $, zavolá do banky nebo použije webovou či mobilní peněženku, kterou banka vytvořila, v bance se identifikuje svým uživatelským jménem a heslem nebo PIN kódem a potom podá žádost o převod. Banka ho zanese do své účetní knihy.

Bankovní účetní kniha

1. *Alena: kreditní položka vklad hotovosti +2 $*
2. *Bedřich: kreditní položka vklad hotovosti +10 $*
3. *Alena: debetní položka –2 $*
4. *Bedřich: kreditní položka +2 $*

Banka teď zaznamenala nové debetní a kreditní položky a peníze se přesunuly.

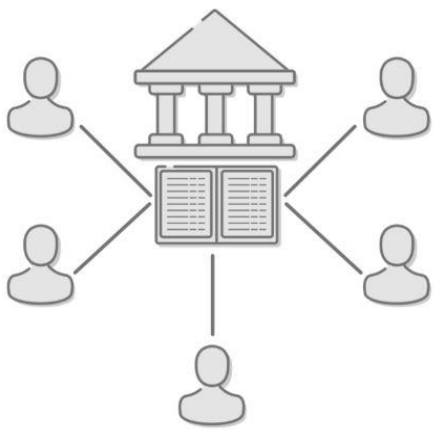
Problém dvojí útraty

Co se stane, když se teď Alena pokusí uvedené dva dolary utratit ještě jednou? Tuto situaci nazýváme problémem dvojí útraty. Alena dá bance příkaz k úhradě, banka jí však sdělí: „Litujeme, ale 2 $ už jste utratila při převodu Bedřichovi. Už nemáte žádné další peníze k útratě."

Pro centrální autoritu, jakou je banka, je jednoduché vám říci, že se pokoušíte utratit peníze, které jste již utratili. Je tomu tak proto, že právě jen banka spravuje účetní knihu a disponuje vnitřními procesy včetně zálohování a auditů, které zajišťují počítače i lidé, a to aby mohla zajistit, že jsou záznamy v knize správné a nikdo s nimi nemanipuloval.

Tomuto systému říkáme centralizovaný, protože je tu jediný centrální orgán, který celý systém řídí.

Banka uchovává účetní knihu, ke které má každý přístup, ale jen prostřednictvím banky.



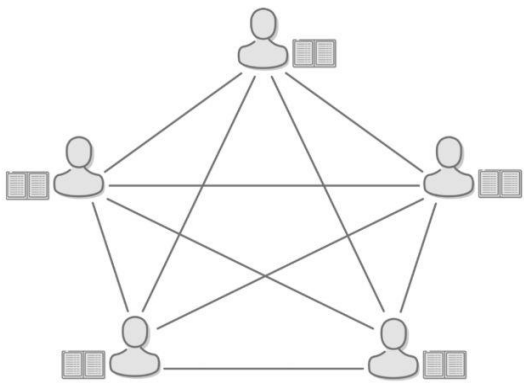
Banka uchovává účetní knihu, ke které má každý přístup, ale jen prostřednictvím banky.

Distribuovaná účetní kniha

První problém, který Bitcoin řeší, je odstranění důvěryhodného prostředníka za pomoci vytvoření peer-to-peer systému. Představme si, že by banky zmizely a my bychom museli celý svůj systém péče o finance vybudovat znovu od nuly. Jak můžeme uchovávat účetní knihu bez centrální autority?

Pokud neexistuje centrální účetní kniha, zavedeme účetní knihu, která bude patřit všem. Ať žije revoluce. Jak budeme postupovat?

Zaprvé, někteří z nás se dohodnou a vytvoří síť. To zatím znamená jen to, že vymyslíme nějaký způsob, jak spolu komunikovat. Například si vyměníme telefonní čísla nebo Snapchat účty. Když Alena bude chtít poslat peníze Bedřichovi, tak místo toho, aby zavolala do banky, řekne svým přátelům: „Posílám Bedřichovi 2 $." Všichni to potvrdí a řeknou: „Ok, bereme na vědomí." Každý si to zapíše do své verze účetní knihy. Obrázek teď vypadá takhle:



Každý má svou kopii účetní knihy, do které může vstupovat nezávisle na ostatních.

Namísto jediné banky tak teď máme kopii účetní knihy v rukou každého. Vždy, když chce někdo převést peníze, musí to oznámit všem svým přátelům. Všichni si transakce zaznamenávají.

Protože účetní kniha už není na jediném místě, říkáme, že je distribuovaná, a protože ji nespravuje žádná centrální autorita, říkáme, že je decentralizovaná. Tímhle způsobem se řeší to, jak odstranit prostředníka.

Když jsme se zbavili prostředníka, jak teď zabráníme dvojím útratám? Kdo nám potvrdí, že peníze, které se chystáme převést, nebyly už předtím převedeny jinam? Protože kopii účetní knihy má každý, musíme se zeptat všech. Tenhle systém se nazývá systémem založeným na konsenzu, protože spočívá v tom, že se všichni musí shodnout na určité konkrétní verzi pravdy.

Když se Alena pokusí podruhé utratit 2 $, které už poslala Bedřichovi, všichni v síti tenhle převod zamítnou: po nahlédnutí do své verze účetní knihy Aleně řeknou, že peníze přece už utratila. Její druhý pokus o převod peněz proto do knihy nezapíšou. Teď tu máme peer-to-peer konsenzuální síť, která zaznamenává vlastnictví a převody prostředků.

Dokud účast v našem distribuovaném systému vyžaduje povolení a my díky tomu můžeme důvěřovat všem jednotlivým účastníkům, systém funguje. Tenhle systém však nemůže být rozšířen na miliony uživatelů po celém světě. Distribuované systémy s náhodnými účastníky jsou ve své podstatě nespolehlivé. Někteří účastníci se můžou čas od času odpojit. To znamená, že se nedozví o některých převodech, o kterých je informujeme. Jiní se nás můžou pokusit úmyslně podvést a tvrdit, že se některé transakce uskutečnily, nebo naopak neuskutečnily. K síti se můžou připojit další osoby a obdržet kopie účetní knihy, které se s těmi existujícími neshodují.

Pojďme se podívat, jakým způsobem by se někdo mohl pokusit podvádět.

Útok s pokusem o dvojí útratu

Pokud budu Alena, můžu se tajně domluvit s jinými účastníky a říct jim: „Až pošlu peníze, nezapisujte to do svých účetních knih. Předstírejte, že jsem žádné peníze neposlala." Takhle Alena může provést útok s pokusem o dvojí útratu.

S počátečním zůstatkem 2 $ Alena provede následující:

1. *Pošle Bedřichovi 2 $ za čokoládovou tyčinku. Na účtu by teď měla mít 0 $.*
2. *David, Eva a Františka jsou s Alenou tajně domluveni a převod do svých účetních knih nezapíšou. Podle jejich verze účetní knihy Alena žádné peníze neutratila a zůstatek na jejím účtu je pořád 2 $.*
3. *Cecílie je poctivá a Alenin převod peněz Bedřichovi zaznamená. V její verzi účetní knihy má Alena na účtu 0 $.*
4. *Hynek byl týden na dovolené a o žádných převodech nebyl informován. Připojí se k síti a vyžádá si aktuální kopii účetní knihy.*
5. *Hynek obdrží 4 falešné kopie (od Davida, Evy, Františky a Aleny) a jednu poctivou kopii (od Cecílie). Jak určí, která kopie je pravdivá? Protože nemá žádnou lepší možnost, důvěřuje většině, a tak přijme falešnou verzi účetní knihy.*
6. *Alena si od Hynka koupí čokoládovou tyčinku za 2 $, které ve skutečnosti nemá. Hynek platbu přijme, protože podle jeho informací, které získal od ostatních účastníků, Alena na svém účtu 2 $ stále má.*
7. *Alena teď má 2 čokoládové tyčinky a v původní účetní knize vznikly 2 $ falešných peněz. Alena se s přáteli rozdělí o tyčinky a zopakují útok ještě 100krát s každým novým účastníkem, který se připojí.*

8. *Alena má teď spoustu tyčinek, zatímco účastníci, od kterých je nakoupila, mají spoustu falešných peněz.*
9. *Když se pokusí těmito penězi zaplatit, David, Eva a Františka, kteří ovládají většinu sítě, tyto platby odmítnou, protože vědí, že peníze jsou falešné.*

Nastalo selhání konsenzu. Účastníci se neshodli na tom, co je pravda. Protože neměli lepší možnost, řídili se pravidlem většiny, což vedlo k ovládnutí sítě nepoctivými účastníky a k převádění neexistujících peněz.

Chceme-li vytvořit otevřený systém, ke kterému se může připojit každý i bez povolení, musí být tenhle systém proti nepoctivým hráčům nějakým způsobem chráněn.

Řešení problému distribuovaného konsenzu

Nyní se pustíme do řešení jednoho z nejobtížnějších problémů informatiky: problému distribuovaného konsenzu mezi stranami, z nichž některé jsou nepoctivé či nespolehlivé. Tenhle problém je známý také pod názvem Problém byzantských generálů a jeho vyřešení je oním klíčem, který Satoshi Nakamoto použil k odemčení vynálezu Bitcoinu. Východiskem takového řešení je myšlenka, že potřebujeme nějak přimět skupinu lidí, aby se na záznamech v účetní knize shodli, aniž by věděli, kteří zapisovatelé zaznamenávali transakce správně a poctivě.

Naivním řešením by bylo poctivé zapisovatele prostě stanovit. Místo toho, aby do účetní knihy mohli zapisovat všichni, zvolíme si skupinu přátel, například Cecílii, Gustava, Filipa a Zuzanu, protože nelžou a je o nich známo, že o víkendech nikdy nechodí na mejdany.

Vždy, když potřebujeme zpracovat transakci, nebudeme to oznamovat všem, ale prostě zavoláme Cecílii a jejímu týmu. Za malý poplatek pro nás účetní knihu rádi povedou. Vždy, když provedou nový zápis do knihy, informují o něm všechny ostatní, kteří si ho zaznamenají do svých kopií knihy, sloužících jako záložní.

Tenhle systém funguje dobře až do chvíle, kdy se jednoho dne objeví vládní agenti a budou chtít vědět, kdo tenhle stínový finanční systém provozuje. Cecílii s jejím týmem zatknou a naše distribuovaná účetní kniha tím skončí. Máme jen nespolehlivé záložní verze, nemůžeme si navzájem důvěřovat, nedokážeme se dohodnout, čí záložní verze má být použita jako základ pro nový systém.

Vláda nemusí naše zapisovatele hned zatknout. Stačí, když jim pohrozí vězením, pokud budou přijímat transakce od Aleny (která je podezřelá z prodeje drog). Systém se tak v podstatě dostal pod centrální kontrolu a už ho nemůžeme pokládat za otevřený – už se k němu nelze připojit bez povolení.

Co kdybychom zkusili demokratický přístup? Najděme skupinu 50 poctivých osob a každý den z nich zvolme jednoho, kdo bude ten den dělat zapisovatele tak, aby se všichni postupně prostřídali. Každý uživatel sítě bude moci v téhle opakované volbě hlasovat.

Tenhle systém bude fungovat skvěle, dokud lidé nezačnou používat násilí nebo finanční nátlak, aby dosáhli takových nepravostí, o kterých jsme mluvili předtím:

1. Přinutit voliče, aby hlasovali pro konkrétní zapisovatele.
2. Přinutit zvolené zapisovatele, aby tvořili falešné záznamy nebo neumožnili některé transakce.

Opět tu vzniká problém. Pokaždé, když zvolíme jako zapisovatele specifické osoby, musíme chovat důvěru v jejich poctivost a nemáme jak zabránit tomu, že je někdo přinutí k nepoctivému jednání a naši účetní knihu tím znehodnotí.

Mylná identita a Sybiliny útoky

Zatím jsme viděli dva způsoby zajištění poctivosti: jedním způsobem bylo stanovení konkrétních zapisovatelů, druhým bylo střídání zapisovatelů na základě volby. Nedostatek obou systémů spočíval v tom, že základ naší důvěry byl spojen s identitou z reálného světa: vždy bylo potřeba identifikovat konkrétní osoby, které by byly za naši účetní knihu zodpovědné. Kdykoliv předpokládáme důvěru v nějakého jednotlivce s konkrétní identitou, umožňujeme tak tzv. Sybilin útok. Není to nic jiného než speciální jméno pro krádež identity; tenhle útok je nazván po ženě s rozdvojenou osobností.

Už se vám někdy stalo, že jste dostali podivnou zprávu od někoho ze svých přátel a později se ukázalo, že tomu člověku někdo předtím ukradl telefon? Jsou-li v sázce miliardy, nebo dokonce biliony dolarů, lidé budou ochotni použít nejrůznější druhy násilí jen proto, aby se třeba telefonu zmocnili a poslali textovou zprávu. Je nezbytné, aby osoby, které udržují naši účetní knihu, nemohly být žádným způsobem k ničemu přinuceny. Jak toho dosáhneme?

Zaveďme loterii

Chceme-li zabránit nebezpečí výhrůžek a podplácení, potřebujeme systém s tolika uživateli, aby bylo prakticky nemožné na ně vyvíjet jakýkoliv nátlak. Ještě lépe, aby ani nebyly známé jejich identity. Stát se členem našeho systému musí být umožněno naprosto komukoliv a nesmíme zavádět žádné hlasování, které by umožnilo nátlak výhrůžkami nebo kupování hlasů.

Co kdybychom zavedli loterii, ve které by byl zapisovatel vždy zvolen náhodně. Tady je prvotní nástin:

1. Uživatelem se může stát kdokoliv na světě. Do naší loterijní sítě o funkci zapisovatele se můžou přihlásit desítky tisíc lidí.

2. Chceme-li poslat peníze, informujeme o transakcích celou síť, stejně jako v předchozím modelu.
3. Namísto toho, aby transakce zapisovali všichni, budeme o právo na zápis transakcí do účetní knihy losovat.
4. Když je stanoven vítěz, zapíše všechny právě oznámené transakce do knihy.
5. Když vítěz do knihy zapíše platné transakce, které odpovídají pravidlům stanoveným všemi ostatními účastníky, dostane odměnu.
6. Kopii účetní knihy uchovávají všichni a do své kopie přidávají vždy ty informace, které do knihy zaznamenal poslední vítěz loterie.
7. Chvíli čekáme, aby všichni měli čas aktualizovat svou verzi knihy až k poslední transakci, a potom spustíme loterii znovu.

Tenhle systém přináší jisté vylepšení. Uživatele v tomto systému není prakticky možné k ničemu přinutit, protože jednak neznáme jejich identitu a jednak nikdy nevíme, kdo loterii vyhraje příště.

Nemáme však jasnou odpověď na otázku, jak provozovat loterii bez toho, aby ji někdo řídil, ani proč bychom měli věřit, že vítěz bude při zapisování do knihy jednat poctivě. K řešení se dostaneme.

KAPITOLA 3

Důkaz o vykonané práci

(Proof of Work)

Systém založený na loterii, který jsme předestřeli, má dva hlavní nedostatky:

1. Kdo bude prodávat losy a vybírat výherní čísla, když jsme si stanovili, že nesmí existovat žádná centrální důvěryhodná strana?
2. Jak zajistíme, aby vítěz loterie do knihy skutečně zapsal správné transakce a nepokusil se nás namísto toho všechny obelstít?

Pokud chceme, aby se k našemu systému mohl připojit kdokoliv bez povolení, musíme ze systému požadavek důvěry odstranit a udělat náš systém plně funkčním i bez důvěry. Musíme tedy vytvořit systém s následujícími vlastnostmi:

1. Pokud nemůžeme důvěřovat žádné centrální autoritě, možnost vygenerovat si svůj vlastní los musí mít každý.
2. Musíme nějak zařídit, aby účast v loterii něco stála, aby si někdo zdarma nevygeneroval velké množství losů

a neovládl tak celou loterii. Jak zařídit, abyste museli za losy utrácet peníze, když se losy od nikoho nekupují? Přimějeme lidi, aby si je kupovali v podstatě od nikoho tím, že budou spotřebovávat elektřinu, velmi nákladný zdroj energie.

3. Pro všechny ostatní účastníky musí být snadné ověřit vaši výhru jen na základě ověření vašeho losu. V loterii Powerball vítěznou kombinaci určují operátoři loterie. Protože v decentralizovaném systému toto možné není, můžeme místo toho zařídit, aby se všichni předem shodli na určitém rozsahu čísel, a když číslo vašeho losu do tohoto rozsahu spadá, vyhráváte. Použijeme k tomu kryptografický trik, kterému se říká hashovací funkce.

Důkaz o vykonané práci: Energeticky náročný asymetrický rébus

Elegantní řešení všech třech těchto problémů se nazývá Důkaz o vykonané práci (Proof of Work). Ve skutečnosti byl vynalezen ještě před Bitcoinem, a to v roce 1993. Celé vysvětlení toho, jak tato loterie funguje, je pravděpodobně tím nejobtížnějším pro pochopení toho, jak Bitcoin funguje. Proto věnujeme několik dalších kapitol podrobnému vysvětlení tohoto řešení.

Losy do loterie musí být „drahé", jinak by si jich lidé mohli vygenerovat nekonečně mnoho. Co je zaručeně drahé, ale nemusí pocházet od centrální autority?

Na tomto místě do Bitcoinu promlouvá fyzika: první pravidlo termodynamiky říká, že energie nemůže být ani vytvořena, ani zničena. Jinými slovy, pokud jde o energii, nic není zadarmo. Elektřina je vzácná vždy, protože si ji buď musíte kupovat od výrobců energie, nebo provozovat vlastní elektrárnu. V každém případě je produkce elektřiny nákladná.

Důkaz o vykonané práci je založen na náhodném procesu podobném hodu kostkou. Namísto šestistěnné kostky má naše kostka tolik stran, kolik je atomů ve vesmíru. K hodu kostkou a vygenerování čísel losů musí váš počítač provést operace, za které platíte elektřinou.

Abyste v loterii vyhráli, musíte vygenerovat číslo, které je matematicky odvozeno od transakcí, které mají být zapsány do účetní knihy, a z hodnoty, která vyšla v hodu kostkou. Abyste našli toto vítězné číslo, musíte kostkou hodit třeba miliardkrát, bilionkrát nebo kvadrilionkrát a utratit při tom tisíce dolarů za elektřinu. Protože je tenhle proces založen na náhodě, je možné, aby kdokoliv získával losy bez nějaké centrální autority, jen s použitím počítače generujícím náhodná čísla a díky seznamu transakcí, které mají být zapsány do účetní knihy.

Přestože nalezení náhodného vítězného čísla vás stálo tisíce dolarů vynaložených za elektřinu, k potvrzení vaší výhry ostatním stačí si ověřit jen pár prostých věcí:

1. Spadá vaše číslo do cílového rozsahu, na kterém se všichni předem shodli?
2. Je číslo skutečně matematicky odvozeno z platné množiny transakcí, které mají být zapsány do účetní knihy?
3. Jsou transakce, které předkládáte, platné podle pravidel Bitcoinu: tj. žádné dvojí útraty, není vytvořen nový bitcoin nad rámec povoleného rozvrhu atd.?

Důkaz o vykonané práci je náhodný proces, který k nalezení vítězného čísla potřebuje mnoho výpočetních operací. K potvrzení správnosti řešení však stačí operace jen jedna.

Představujte si to jako křížovku nebo sudoku. Najít řešení vám zabere dlouhou dobu, ale jeho správnost si pak podle klíče můžete

ověřit rychle. Systém důkazu o vykonané práci je proto asymetrický: je obtížný pro hráče, ale snadný pro ověřovatele.

Protože jste účastí v loterii spotřebovali značné množství energie, a tedy i peněz, máte zájem, aby váš vítězný los všichni přijali. Máte proto motivaci jednat správně a zapsat do účetní knihy jen platné transakce.

Kdybyste se například pokusili utratit peníze, které už byly utraceny, váš „výherní" los by všichni ostatní zamítli a vy byste přišli o všechny peníze, které jste utratili za energii potřebnou k vytvoření losu. Na druhé straně pokud do účetní knihy zapíšete platné transakce, odměníme vás bitcoinem, takže budete moci zaplatit účet za energie a zbytek si ponechat jako zisk.

Systém důkazu práce má důležitou vlastnost, a totiž že je nákladný ve skutečném světě. Pokud byste tedy chtěli podniknout útok na síť přes některé z účastníků, museli byste nejen přijít přímo k nim domů a ovládnout jejich počítače, ale museli byste taky zaplatit jejich účet za elektřinu.

Jakým způsobem účastníci dokazují, že spotřebovali potřebnou energii? Budeme si muset probrat základy dvou pojmů z informatiky: hashování a bity.

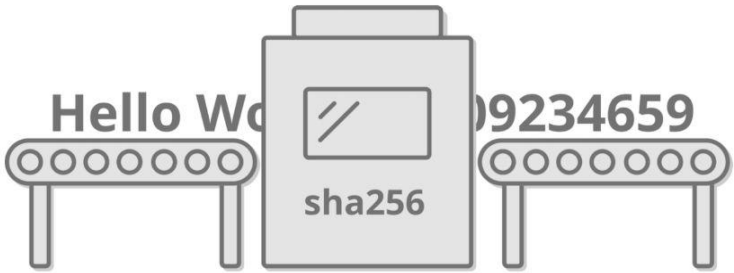
Hashování

Asymetrický rébus důkazu o vykonané práci v síti Bitcoin zahrnuje použití hashovací funkce. Ze základní algebry víme, že funkce je jakási krabička, kam vložíte jako vstup nějakou hodnotu x a jako výstup dostanete hodnotu f(x). Například funkce f(x)=2x bere nějakou hodnotu a násobí ji dvěma. Pro vstup x=2 dá výstup f(x)=4.

Hashovací funkce je speciální funkce, do které vložíte jakýkoliv řetězec písmen, čísel a jiných údajů, například „Hello world", a dostanete obrovské, náhodně vyhlížející číslo:

869913660443924676617831651669733090238071816480247187783135263898928609948 42

Hashovací funkce, kterou jsem použil k zahashování řetězce „Hello world", se nazývá SHA-256 a je to náhodou zrovna ta funkce, kterou používá Bitcoin.



Na jedné straně vstupují údaje, na druhé straně vycházejí nepředvídatelná obrovská čísla.

Hashovací funkce SHA-256 má následující vlastnosti, které jsou pro nás užitečné:

1. Výstup je pevně daný: stejný vstup vždy vyprodukuje stejný výstup.
2. Výstup je nepředvídatelný: změna třeba jen jednoho písmena nebo přidání mezery do řetězce na vstupu radikálně změní výstup, a to tak, že nelze vypozorovat žádnou korelaci se změnou vstupu.
3. Výstup (hash) lze spočítat rychle pro jakoukoliv velikost vstupních údajů.

4. Je nemožné najít dva řetězce, které vyprodukují tentýž výstup.
5. Známe-li výstupní hash funkce SHA-256, je nemožné získat z něj vstupní řetězec. Říkáme, že funkce je jednosměrná (nebo též jednocestná).
6. Výstup má vždy specifickou velikost (u funkce SHA-256 je to vždy 256 bitů).

Stručný úvod do bitů

Číselná soustava, kterou znáte a máte rádi a která používá číslice od 0 do 9, se nazývá desítková, protože používá deset číslic. Počítače naproti tomu upřednostňují číselnou soustavu sestávající z jedniček a nul, které značí přítomnost nebo nepřítomnost elektrického signálu. Této číselné soustavě se říká dvojková nebo taky binární.

V desítkové soustavě se používají jen číslice od 0 do 9. Pomocí jedné číslice můžete vyjádřit deset různých čísel, 0 až 9. Když použijete dvě číslice, můžete vyjádřit 10 × 10 = 100 různých čísel: 00, 01, … až 99. Třemi číslicemi můžete vyjádřit 10 × 10 × 10 = 1000 čísel: 000, 001, … až 999.

Asi už vám začíná být jasné, jak to funguje. Když chceme zjistit, kolik čísel můžeme vyjádřit pomocí n číslic, vynásobíme desítku samu sebou n-krát, jinak řečeno, spočítáme 10n neboli 10 na n-tou.

Binární soustava funguje stejně. Jediným rozdílem je počet dostupných číslic. Zatímco v desítkové soustavě jsme zvyklí pracovat s deseti číslicemi, binární číslice neboli bit může nabývat jen dvou hodnot: jedničky a nuly.

Jestliže jeden bit může vyjadřovat dvě různé hodnoty, pak dva bity mohou vyjadřovat čtyři hodnoty: 00, 01, 10, 11. Můžete si to spočítat, když vynásobíte 2 × 2, protože každá číslice může nabývat dvou hodnot.

Pomocí tří bitů můžeme reprezentovat $2 \times 2 \times 2 = 2^3$ = osm hodnot, tedy 000, 001, 010, 011, 100, 101, 110, 111.

Číslo zapsané v binární soustavě, které je n bitů dlouhé, může vyjadřovat 2^n různých hodnot.

Počet unikátních hodnot, které lze reprezentovat pomocí 256 bitů, což je velikost hashovací funkce SHA-256, je 2^{256}. To je obrovské, skoro nepředstavitelné číslo. Pokud bychom ho zapsali v desítkové soustavě, bylo by to 78místné číslo. Jen pro ilustraci, tohle číslo se přibližně rovná odhadovanému počtu atomů v celém známém vesmíru.

2^{256} = 115 792 089 237 316 195 423 570 985 008 687 907 853 269 984 665 640 564 039 457 584 007 913 129 639 936

Toto je počet možných výstupů při zahashování jakéhokoliv řetězce pomocí funkce SHA-256. V podstatě se nedá odhadnout, jaká bude výsledná hodnota. Bylo by to jako správně předpovědět všechny výsledky 256 hodů mincí nebo uhodnout umístění nějakého konkrétního atomu, který jsem vybral kdekoliv ve vesmíru.

Zápis tohoto čísla zabere opravdu příliš mnoho místa, proto ho budeme propříště označovat jen jako 2^{256}, ale věřím, že vám vždycky, když ho uvidíte, vyvstane na mysli obraz celého vesmíru možností.

Pojďme si zahashovat

Ukážeme si několik příkladů řetězců a jejich hashů vytvořených pomocí funkce SHA-256. Zapsal jsem outputy v desítkové soustavě, ale v počítači by se jednalo o binární řetězce jedniček a nul.

Jde mi o to, ukázat, jak radikálně se výsledné číslo mění při byť jen drobné změně vstupního řetězce. Podle inputu nemůžete předpovídat output hashovací funkce:

„Hello world!"

86991366044292467661783165166973309023807181648024718778313526389892860994842

„Hello world!!"

84940227720695898955447627108840424364390283616735576803008868844073193772558

Neexistuje způsob, jak by kdokoliv, dokonce včetně počítače, mohl na základě výsledného čísla uhodnout, jak byl daný řetězec vytvořen. Jestli si chcete s SHA-256 pohrát sami, můžete si to zkusit na passwordsgenerator.net/sha256-hash-generator.

Jak se prohashovat k výhře v loterii důkazu práce

Teď už jsme připraveni se bavit o tom klíčovém kouzlu celé loterie. Řekli jsme, že je 2^{256} potenciálních výstupních hodnot funkce SHA-256. Aby se to dalo snáze pochopit, představme si, že je těch hodnot jen 1000.

Loterie funguje takhle:

1. Alena oznámí, že chce poslat 2 $ Bedřichovi.
2. Všichni účastníci loterie vezmou transakci „Alena posílá 2 $ Bedřichovi" a na konec přidají náhodné číslo zvané nonce (neboli číslo použité jen jednou). Tak zajistí, že se řetězec, který hashují, liší od řetězců všech ostatních, což jim pomůže najít vítězné číslo.
3. Pokud je výsledný hash menší než cílové číslo (tenhle pojem si vysvětlíme v následující kapitole), vyhrávají loterii.
4. Pokud je výsledný hash větší než cílové číslo, účastníci hashují stejný řetězec znovu s odlišnými noncemi: „Alena posílá 2 $ Bedřichovi nonce = 12345", potom „Alena posílá 2 $ Bedřichovi nonce = 132849012348092134" a tak dále, dokud výsledné číslo hashe není menší než číslo cílové.

Objevit hash, který je menší než cílové číslo, může stát mnoho a mnoho pokusů. Vlastně můžeme stanovit, jak často může někdo v loterii vyhrát, a to tak, že stanovíme pravděpodobnost toho, že najde vítězné číslo. Pokud je 1000 možných hashů a my stanovíme cílové číslo na 100, kolik hashů je menších než cílové číslo?

Je to prostá matematika: 100 z 1000 možných čísel nebo 100/1000 = 10 % hashů je menších než cílové číslo. Když tedy zahashujete jakýkoliv řetězec a vaše hashovací funkce vygeneruje 1000 různých výstupů, potom lze očekávat, že získáte hash menší než cílové číslo 100 v 10 % případů.

Funguje to takhle: Shodneme se na cílovém čísle, potom všichni vezmeme transakce, o kterých jsme byli informováni, a zahashujeme je s tím, že na konec přidáme náhodnou nonci. Jakmile někdo najde výsledný hash, který je nižší než cílové číslo, oznámíme to celé síti:

Ahoj všichni:

- *Vzal jsem transakce: „Alena posílá 2 $ Bedřichovi, Cecílie posílá 5 $ Aleně".*
- *Přidal jsem nonci „32895".*
- *Výsledný hash byl 42, což je méně než cílové číslo 100.*
- *Tady je můj důkaz o vykonané práci: údaje o transakcích, použitá nonce a hash, který je výsledkem těchto vstupních údajů.*

Abych toho dosáhl, mohlo mě to stát miliardy pokusů, tisíce dolarů za elektřinu, ale všichni můžou můj důkaz práce okamžitě ověřit.

Protože jsem jim poskytl jak vstupní údaje (údaje o transakcích a nonci), tak očekávaný výstup (číslo hashe), stačí, aby jen jednou údaje sami zahashovali a ověřili správnost dat, která jsem jim poskytl.

Hashování si můžeme představit jako házení obrovskou kostkou, na které můžou na základě vstupních údajů, které sestávají z transakcí, padnout čísla od nuly až po počet atomů ve vesmíru. Jen hashe pod cílovým číslem vyhrávají a vy musíte doložit údaje, které jste k vypočítání hashe použili.

Jak to souvisí se spotřebou energie? No, už jsme řekli, že množina možných hashů je ve skutečnosti obří číslo, které je asi tak velké jako počet atomů ve vesmíru. Cílové číslo můžeme stanovit tak malé, aby byl platný jen malý zlomek všech hashů. To znamená, že kdokoliv, kdo chce najít platný hash, bude muset hledáním hashe strávit obrovský výpočetní čas, a tedy i spotřebovat velké množství elektřiny.

Čím menší je cílové číslo, tím víc pokusů bude potřeba k nalezení odpovídajícího hashe. Čím je cílové číslo větší, tím rychleji můžeme vítězný hash najít. Pokud jsou naše šance dosažení cíle milion ku jedné, pak tím, že toho cíle nakonec opravdu dosáhneme, prokážeme, že jsme provedli přibližně milion výpočtů.

KAPITOLA 4

Těžba (Mining)

Proces hraní loterie důkazu o vykonané práci, v němž lze vyhrát možnost zapisovat do účetní knihy Bitcoinu, se běžně nazývá těžba. Funguje takhle:

1. Kdokoliv na světě, kdo se chce účastnit, se připojí k bitcoinové síti přes svůj počítač a čeká na informace o transakcích.
2. Alena oznámí svůj záměr poslat peníze Bedřichovi. Počítače na síti si tuto informaci navzájem předávají, až se rozšíří po celé síti.
3. Všechny počítače, které se chtějí zúčastnit loterie, začnou hashovat transakce, o kterých se dozvěděly, a to tak, že k bloku transakcí připojí náhodnou nonci a spouštějí funkci SHA-256.
4. V průměru přibližně každých deset minut některý počítač objeví číslo hashe odvozené od seznamu transakcí, které je menší než cílové číslo, a vyhraje loterii.
5. Tenhle počítač oznámí vítězné číslo, které objevil, a input (transakce a nonci), které použil k jeho výpočtu. Možná mu to trvalo několik hodin, možná taky jen několik minut. Soubor těchto informací (transakce, nonce a hash

důkazu o vykonané práci a hash předchozího bloku) se nazývá blok.

6. Všichni ostatní blok potvrdí tak, že ověří, jestli transakce v bloku společně s noncí skutečně vyprodukují příslušný hash, že je tenhle hash skutečně menší než cílové číslo, že blok neobsahuje žádné neplatné transakce a že historie, kterou obsahuje, není v rozporu s předchozími bloky.
7. Všichni blok zanesou do své kopie účetní knihy, připojí ho k existujícímu řetězci bloků a postupně tak tvoří tzv. blockchain (řetezec bloku).

A to je ono. Vytvořili jsme první blok a udělali jsme první záznam do našich účetních knih.

Možná jste v médiích četli často opakované tvrzení, že těžení Bitcoinu zahrnuje řešení složitých rovnic. Teď už víte, že to vůbec není pravda. Spíše než o řešení rovnic jde při těžení Bitcoinu o opakované házení obří virtuální kostkou, aby byl nalezen hash v určitém předem stanoveném intervalu. Jde prostě o hru náhody, která si žádá spotřebování určitého množství elektřiny.

Jak se razí nové bitcoiny

Zatím jsme mluvili o tom, jak Alena mohla Bedřichovi poslat 2 $. Přestaneme teď mluvit o dolarech, protože Bitcoin s dolary nemá nic společného. Namísto toho tu máme bitcoiny: digitální jednotky, které představují hodnotu v síti Bitcoin.

Abychom se vrátili k našemu příkladu, Alena ve skutečnosti Bedřichovi posílá 2 bitcoiny tak, že oznámí, že převádí bitcoin, který je registrovaný pod jejím „účtem", na Bedřichův účet. Potom někdo vyhraje v loterii důkazu o vykonané práci a smí zapsat její transakci do účetní knihy.

Kde však Alena ty 2 bitcoiny získala? Jak síť Bitcoin vznikla a jak lidé získávali první mince, když ještě neexistovala místa, kde je možné si je koupit za konvenční měnu, jakou jsou například americké dolary?

Když Satoshi zakládal Bitcoin, mohl vytvořit databázi s 21 miliony mincí, které by všechny vlastnil a nabízel by je lidem ke koupi. Lidé by však neměli důvod připisovat hodnotu systému, kde jedna osoba vlastní všechno bohatství. Mohl vytvořit registr, kam by se lidé zapisovali, a mohli tak získat šanci vyhrát nějaké mince pomocí e-mailové adresy, ale tenhle systém by byl náchylný k Sybilinu útoku (krádeži identity), protože vygenerovat miliony e-mailových adres lze téměř zdarma.

V realitě to vypadá tak, že mince vznikají těžením bitcoinu a za ním stojí v celém tom procesu právě hraní loterie důkazu práce a získávání přístupových práv k účetní knize. Když za spotřeby obrovského množství energie objevíte platný blok a najdete výherní číslo, získáte právo do bloku, a tedy i do účetní knihy zapsat všechny transakce, o kterých jste byli informováni. Získáte však taky právo do účetní knihy zapsat jednu velmi specifickou transakci, která se nazývá coinbase transakce. Tato transakce v podstatě říká: „Bylo vyraženo (vyprodukováno, vytvořeno) 12,5 bitcoinů a získala je těžařka Tereza za vynaložení veškeré energie, kterou ji stálo vytěžení bloku."

Takhle tedy vznikají nové bitcoiny. Tenhle proces umožňuje úplně každému na světě, aby začal razit vlastní bitcoiny bez jakékoliv centrální autority a bez osobní identifikace, pokud je ochoten zaplatit cenu elektřiny, která je k účasti v loterii vyžadována. Díky tomu je vydávání bitcoinů odolné vůči Sybilině útoku. Když chcete získat mince, musíte spotřebovat určitou energii a uhradit náklady na těžbu.

Bloková odměna

Osoba, která vyhraje loterii, získá nově vyražené mince. Proč je to jen 12,5 bitcoinu*, a ne 1000? Jak to, že těžařka nemůže systém přelstít a vyplatit si jakoukoliv částku?

Bitcoin je systém založený na distribuovaném konsenzu. To znamená, že se všichni musí shodnout na tom, co bude platit. Činí tak s pomocí softwaru na svých počítačích, který požaduje dobře známá pravidla, o kterých se mluví jako o pravidlech konsenzu Bitcoin. Pro každý blok vyprodukovaný těžařem se ověřuje soulad s těmito pravidly. Pokud pravidla splňuje, každý si ho zapíše do své kopie účetní knihy a přijme jako pravdivý. Pokud pravidla nesplňuje, je zamítnut.

Přestože vyčerpávající seznam pravidel konsenzu je poměrně rozsáhlý, tady je jen pár příkladů:

- Z platného bloku může vzejít určité množství bitcoinů podle rozvrhu vydávání, který je zabudován přímo do softwaru.
- Transakce musí obsahovat platné podpisy dokládající, že jsou tyto transakce patřičně autorizovány těmi osobami, které peníze utrácejí.
- V žádné transakci nesmí být převáděny peníze, které už byly v rámci tohoto posledního nebo kteréhokoliv předchozího bloku utraceny.
- Data v bloku nesmí přesahovat určitou danou velikost.
- Hash vyprodukovaný důkazem o vykonané práci musí být menší než cílové číslo a dokazovat tak statisticky nízkou pravděpodobnost vytěžení tohoto konkrétního

* Po půlení v květnu 2020 činí odměna 6,25 bitcoinu.

bloku jiným způsobem než spotřebováním určitého množství energie.

Když Tereza vytěží blok a rozhodne se vyplatit si něco navíc, všechny ostatní počítače její blok zamítnou jako neplatný, protože v bitcoinovém programu, který je na všech počítačích spuštěn, je příkaz, který říká „Současná bloková odměna je přesně 12,5 bitcoinu. Když uvidíte blok, který někomu vyplácí vyšší částku, nepřijímejte ho."

Když se Tereza pokusí podvádět a vytvoří neplatný blok, ostatní si ho do svých kopií účetní knihy nezapíšou, a ona tak přijde o tisíce dolarů zaplacených za elektřinu k vytvoření něčeho, o co nikdo nestojí: padělku. To dává Bitcoinu nepadělatelnou nákladnost. Tenhle termín zavedl průkopník digitálních měn Nick Szabo ve svém eseji *Shelling Out* (Vypláznout peníze). Intuitivně víme, že kdyby peníze byly snadno padělatelné, neplnily by svou funkci dobře. Bitcoin je v podstatě nezfalšovatelný, protože ho lze otestovat jednoduchým matematickým testem.

Když Satoshi vytěžil první blok, vytvořil tím úplně první bitcoiny. Kód Bitcoinu je open source, což znamená, že se každý může podívat, jak funguje, a ověřit si, že nikde není nějaký skrytý háček. I Satoshi však musel provést miliardy výpočetních operací a zahrát si loterii důkazu o vykonané práci, aby první bloky vůbec vytěžil. Přestože byl tvůrcem celého systému, nemohl peníze padělat tím, že by snad předstíral spotřebu nutné elektřiny.

Každý, kdo se k síti připojil po něm, si mohl dle původního cílového čísla a údajů o transakcích zjistit, které číslo hashe Satoshi vygeneroval. Tak šlo zkontrolovat, že se Satoshi spotřebou určitého množství energie skutečně do cílového čísla trefil. Představte si, že byste mohli v reálném čase takhle přesně ověřovat to, jak bankovní systém vydává tradiční fiat peníze!

Půlení (halving)

Proces těžby vytváří nové bitcoiny. Satoshi však chtěl vytvořit systém, ve kterém nebude docházet ke znehodnocování. Nechtěl, aby zásoba mincí narůstala donekonečna. Místo toho stanovil časový plán vydávání bitcoinů, který měl raketový start a postupně spěje k tomu, že se už žádné nové mince vydávat nebudou.

Na počátku činila bloková odměna 50 bitcoinů. Odměnu za vytěžení prvního bloku získal Satoshi a další lidé, kteří se k síti připojili brzy po jejím vzniku a těžili hned následující bloky.

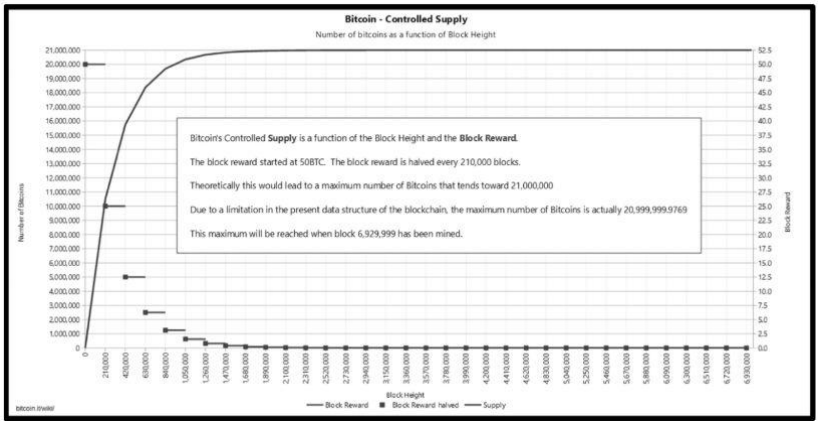
V kódu Bitcoinu je zabudováno půlení blokové odměny, které odměnu přibližně každé čtyři roky o polovinu snižuje. Půlení vychází z počtu vytěžených bloků spíše než z uplynutí určitého času, ale vzhledem k tomu, že zhruba každých deset minut je vyprodukováno stejné množství bloků, vyjde to nastejno.

Bloková odměna byla v roce 2008 50 bitcoinů, v roce 2012 to bylo 25, v roce 2016 12,5. K 8. červnu 2019, bylo vytěženo 579 856 bloků od počátku historie Bitcoinu a odměna je 12,5 bitcoinů za jeden blok.*

Po vytěžení dalších 50 144 bloků, což nastane přibližně koncem května 2020, se odměna sníží na 6,25 bitcoinu za blok, což každoroční nárůst zásoby zvýší asi o 1,8 %. Za dvanáct let, během nichž dojde k dalším třem půlením odměny, bude víc než 99 % bitcoinů vytěženo a jeden blok vytvoří méně než 1 bitcoin. Postup půlení blokové odměny můžete sledovat na stránkách bitcoinblockhalf.com.

---

* Protokol Bitcoinu v podobě tzv. Bitcoin Whitepaperu byl vydán v roce 2008 a jako takový definoval půlení odměny za blok na každé další čtyři roky. Fakticky byl pak první blok vytěžen 3. ledna 2009. Po půlení v květnu 2020 je bloková odměna stanovena na 6,25 bitcoinu.



(Bitcoin: Řízený přírůstek (přísun), Množství bitcoinů v závislosti na výšce bloku, Řízený přírůstek bitcoinů je funkcí (závislý) na výšce bloku a blokové odměně. To teoreticky vede k maximálnímu počtu bitcoinů blížícímu se 21 000 000. Kvůli omezení současné (stávající) datové struktury blockchainu je skutečný maximální počet bitcoinů 20 999 999,9769. Tohoto maxima bude dosaženo po vytěžení bloku 6 929 999.)

Okolo roku 2140 bloková odměna nakonec klesne na nulu a těžaři budou motivováni jen poplatky hrazenými uživateli, kteří provádějí transakce.

Tato čísla týkající se vydávání bitcoinů a blokové odměny jsou zabudována v kódu Bitcoinu – který je, pro zopakování, úplně open source a může být kýmkoliv ověřen – v závislosti na tom, kde v historii Bitcoinu se právě nacházíme. Pokud byste vytvořili blok, který těmto pravidlům neodpovídá, odmítnou vás všichni, kteří mají tato pravidla ve svém kódu vepsána.

Kontrola vydávání a těžebního intervalu

Těžba vyžaduje počítač a elektřinu. Čím víc počítačů, respektive těžebního hardwaru a elektřiny máte k dispozici, tím pravděpodobněji objevíte vítězné číslo dřív než ostatní. Kdyby například síť sestávala ze stovky počítačů se stejnou výkonností a vy byste měli pod kontrolou deset z nich, objevíte vítězný blok v průměru v 10 % případů. Těžba je nicméně proces založený na náhodě a štěstí, v praxi se tedy můžete snažit klidně celé hodiny, nebo dokonce dny, a přesto žádný blok neobjevíte.

Z předchozího oddílu víme, že těžaři si nemůžou přidělit libovolnou blokovou odměnu, protože by ostatní uzly sítě jejich blok odmítly. Co když ovšem spotřebují spoustu energie k urychlení těžby a získají spoustu bitcoinů, čímž poruší záměr systému, podle kterého by rychlost vydávání bitcoinů měla být daná předem?

Vraťme se k příkladu tisíce možných hashů a cílového čísla 100. V 10 % případů získáme číslo, které je menší než 100, a najdeme tak blok.

Řekněme, že výpočet jednoho hashe nám zabere 1 vteřinu. Pokud každou vteřinu „hodíme kostkou" a zahashujeme nejnovější transakce spolu s naší náhodnou noncí a číslo menší než cílové číslo získáme v 10 % případů, potom lze očekávat, že platný hash najdeme v průměru každých 10 vteřin.

Co se stane, když budou loterii hrát dva počítače? Budou hashovat dvakrát tak rychle, očekávaná frekvence nalezení platného hashe tedy bude 5 vteřin. Co když bude hrát 10 počítačů? Libovolný z nich najde vítězný hash v průměru každou vteřinu.

Tady nám vzniká problém: když těží víc lidí, bloky jsou vytvářeny příliš rychle. To vede ke dvěma nežádoucím důsledkům:

1. Narušuje to předem stanovený časový plán vydávání mincí. Chceme, aby každou hodinu bylo vytvářeno

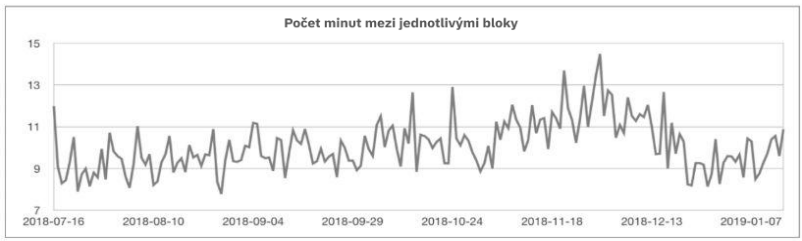
relativně konstantní množství bitcoinů, abychom zajistili, že budou sice všechny vytvořeny do roku 2140, ale ne dřív.

2. Vytváří to problémy v síti: pokud jsou bloky těženy tak rychle, že nemají čas dorazit ke všem uzlům před vytěžením dalšího bloku, nemůžeme se shodnout na lineární historii transakcí, protože víc těžařů může ve svých blocích uvést stejnou transakci, a bloky se tak můžou stát neplatnými, protože obsahují transakce, které jsou už zapsány v jiných blocích.

Když bude těžit méně lidí, může vzniknout zase opačný problém:

1. Bitcoiny jsou vydávány příliš pomalu, což opět narušuje časový plán.
2. Systém se může stát nepoužitelným, protože lidé čekají hodiny, dny nebo ještě déle na zápis transakcí do účetní knihy.

Celkové množství hashů za vteřinu provedených všemi těžaři v síti Bitcoin se nazývá hash rate.



Časové intervaly mezi jednotlivými bloky se liší v závislosti na zrychlování či zpomalování hash rate a na náhodě.

Regulace obtížnosti: Určení cílového čísla

Protože účast v systému Bitcoin je dobrovolná a nevyžaduje povolení a lidé se můžou připojit podle svého přání, aniž je kdokoliv řídí, počet těžařů se s každým okamžikem mění. Potřebujeme proto zajistit, aby rychlost vytváření bloků byla stabilní a nedocházelo ke zrychlování a zpomalování pokaždé, když se připojí noví těžaři, nebo se naopak současní těžaři odpojí.

Jak můžeme zvýšit obtížnost hledání platných hashů, když se k loterii připojí hráčů víc, a jak ji naopak snížit, když hráči loterii opouštějí, tak, aby rychlost vytváření bloků zůstala stabilní?

Připomeňme si, že těžba v síti Bitcoin je loterie, kde se snažíme získat náhodné číslo nižší než číslo cílové:

Snažíme se zasáhnout tuto malou oblast. Počet možných výsledků je obrovský, takže nám na základě náhodných pokusů bude trvat velmi dlouho, než cíle dosáhneme.

Bitcoin tenhle problém řeší regulací obtížnosti těžby. Protože každý používá stejný program se stejnými pravidly a každý má kopii celé historie bloků od počátku až do současného okamžiku, každý může nezávisle vypočítat, jak rychle jsou bloky vytvářeny.

Pokaždé, když vyprodukujeme 2016 bloků, což přibližně odpovídá dvěma týdnům času*, se ohlédneme zpět a zjistíme, jak dlouho nám vyprodukování těchto bloků trvalo. Podle toho upravíme cílové číslo tak, aby buď zrychlilo, nebo zpomalilo produkci bloků.

Každý vezme 2016 posledních bloků a vydělí je časem, který trvalo jejich vytvoření, aby tak získal průměr. Trvalo vytvoření každého bloku v průměru déle než 10 minut? Postupujeme příliš pomalu. Bylo to méně než 10 minut? Postupujeme příliš rychle.

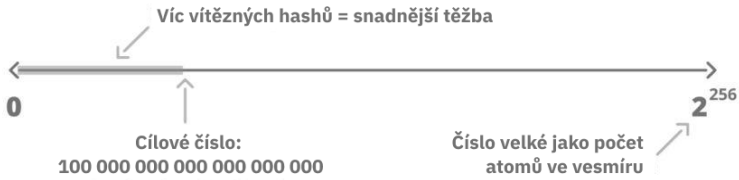
Nyní můžeme upravit cílové číslo tak, aby bylo proporcionálně zvýšeno nebo sníženo vzhledem k tomu, o kolik rychleji nebo pomaleji potřebujeme postupovat, abychom se přiblížili

10minutovému intervalu, který je zabudován do otevřeného zdrojového kódu.

Můžeme cílové číslo zvýšit, vytvořit tak větší interval platných hashů a dát tak těžařům větší pravděpodobnost nalezení vítězného hashe a tím spotřebovat méně energie za nalezený blok. Tomu říkáme snížení obtížnosti.

---

* Vyrovnávací období 2016 bloků bylo zvoleno podle stanoveného intervalu 10 minut na vytvoření jednoho bloku. 10 minut × 2016 bloků dá dohromady dva týdny. Interval mezi jednotlivými bloky Satoshi sice zvolil náhodně, ale je dostatečně dlouhý na to, aby se většina uzlů stihla synchronizovat s nejnovějším blokem. I dvoutýdenní vyrovnávací období bylo zvoleno poněkud náhodně, ale díky němu se zabraňuje případným narušením systému příliš rychlými změnami hash rate.



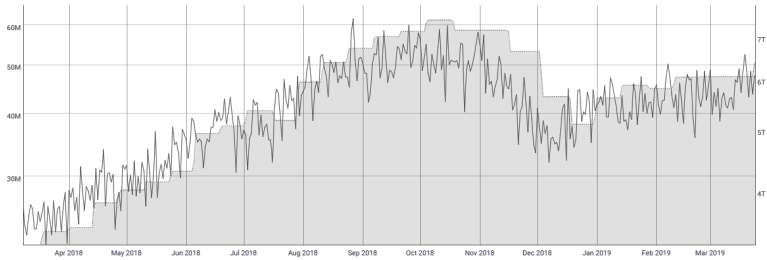
Zvýšení cílového čísla zvětšuje interval, do něhož je nutné se trefit, a zvyšuje tedy pravděpodobnost, že se do něj někdo trefí, při nižším počtu pokusů, čímž zároveň snižuje energetickou nákladnost.

Cílové číslo můžeme naopak snížit, takže bude menší množství vítězných hashů a těžaři budou potřebovat k nalezení hashe platného bloku víc energie. Tomu říkáme zvýšení obtížnosti.

Znamená to, že pro každý oddíl 2016 bloků známe přesné cílové číslo. To nám říká, pod jaký magický práh musí spadat číslo hashe důkazu o vykonané práci pro vítězný los pro každý blok vytvořený v daném období.

Regulace obtížnosti a výpočet cílového čísla jsou možná tou zásadní inovací, kterou Bitcoin přinesl, protože díky nim si může kdokoli ověřovat loterijní čísla v závislosti na cílovém čísle, které si může stejně jako všichni ostatní sám vypočítat. Díky tomu můžeme provozovat loterii, aniž nám kdokoliv sdělí výherní kombinaci.

Následující tabulka znázorňuje v průběhu času hash rate jako linku a obtížnost jako plnou plochu. Obtížnost je znázorněna jako schodiště, protože je upravena vždy po vytvoření 2016 bloků. Vidíme, že pokaždé, když hash rate přesáhne obtížnost, obtížnost vzroste, aby hash rate vykompenzovala. Když hash rate klesne, jako tomu bylo v období říjen až prosinec 2018, klesne i obtížnost. Regulace obtížnosti vždy přichází až podle hash rate za posledních 2016 bloků (dva týdny).



Hasrate a obtížnost
coinmetrics.io/charts/

Protože regulace obtížnosti nastává vždy až se zpožděním po 2016 blocích, může se stát, že výrazné výkyvy v hash rate produkci Bitcoinu ve stávajícím období 2016 bloků urychlí nebo zpomalí, a dojde tak k mírnému narušení časového plánu.

Protože zvýšení hash rate obvykle znamená produkci velkého množství nového hardwaru, výkyvy jsou poměrně neobvyklé a nemají příliš velký dopad. Jakýkoliv vliv výkyvů je omezen na jednotku 2016 bloků, ve které se odehrají, protože následná úprava obtížnosti nás dostává opět na průměr vzniku jednoho bloku za deset minut.

Hash rate a hodnota bitcoinu v dolarech

Bitcoin automaticky přepočítává obtížnost v závislosti na celkové výpočetní síle všech účastníků loterie, jimiž jsou těžaři vynakládající energii na výpočet hashů. Tady se náš digitální svět setkává se světem reálným. Cena bitcoinu, hardwaru a energie a obtížnost daná cílovým číslem vytvářejí řetězec akce a reakce:

1. Spekulanti nakupují bitcoin, protože si myslí, že jeho cena stoupá, a zvyšují tak cenu na X $.
2. Těžaři spotřebují energii a hardware až za X $ a pokoušejí se vytěžit bitcoin.

3. Vysoká poptávka za strany nakupujících způsobí růst ceny a taky to, že víc těžařů těží bitcoin se slušným výnosem.
4. Víc těžařů znamená vyšší hash rate a víc energie spotřebované k produkci bitcoinů, a síť se tak stává dokonce ještě bezpečnější. Kupující mají jistotu, že je bitcoin bezpečný, což někdy vytváří další reakci a vyžene cenu ještě výš.
5. Po vytěžení 2016 bloků zvýšený hash rate způsobí zvýšení obtížnosti.
6. Vyšší obtížnost znamená nižší cílové číslo – těžaři nacházejí bloky s nižší četností – což vede k tomu, že alespoň někteří z nich za vytěžení mince utratí víc než X $.
7. Někteří těžaři přestanou být v plusu, protože spotřebují větší množství energie než kolik můžou vydělat prodejem bitcoinu. Zanechají proto těžby a celkový hash rate klesne.
8. Je vytvořeno dalších 2016 bloků. Obtížnost je znovu vypočítána, aby byla těžba snadnější, protože někteří těžaři se odpojili. Cílové číslo se zvýšilo.
9. Menší obtížnost znamená, že se ti, kterým se těžba už nevyplácela, můžou opět připojit a těžit, nebo se můžou do hry zapojit těžaři noví.
10. A zase od začátku od bodu 1.

Během medvědího trhu se cyklus může pohybovat opačným směrem. Uživatelé se mincí zbavují, cena klesá a těžařům se těžba přestává vyplácet.

Algoritmus regulace obtížnosti zajišťuje rovnováhu mezi cenou a hodnotou hash rate. I kdyby cena radikálně poklesla a hash

rate s ní, díky následné úpravě obtížnosti by se těžba při nové rovnovážné ceně stala znovu výhodnou.

Regulace obtížnosti vede k vyřazování neefektivních těžařů ve prospěch těch, kteří těží s použitím nejlevnější možné energie s nejnižšími celkovými provozními náklady. V průběhu času to těžaře bitconu nutí k tomu, aby těžili v odlehlejších částech světa a používali zdroje energie, které jsou málo využívané nebo zatím ještě úplně nevyužité. Zpráva CoinShares* z roku 2019 odhaduje, že přibližně 75 % těžby bitcoinu probíhá za použití obnovitelných zdrojů energie.

Za posledních pár let cena prudce vzrostla, stejně jako celkový hash rate. Čím vyšší je hash rate, tím obtížnější je podniknout útok na síť, protože abyste mohli ovlivnit, co bude zapsáno byť jen do následujícího bloku, museli byste mít pod kontrolou víc než polovinu energie a hardwaru v celé síti. Energie vynakládaná sítí těžařů bitcoinu je dnes odhadována na ekvivalent spotřeby středně velké země.

Poplatky a odměny na konci bloku

Jak budeme motivovat těžaře, aby vynakládali energii a zapisovali do účetní knihy, až blokové odměny nakonec dojdou? Odpovědí Bitcoinu jsou transakční poplatky. Nejenže transakční poplatky postupem času nahrazují blokovou odměnu, ale taky těžaře motivují, aby do bloků zapisovali transakce a netěžili prázdné bloky jen kvůli odměně.

Výše poplatků je určována systémem volného trhu, kde uživatelé nabízejí cenu za vzácné místo v bloku. Uživatelé, kteří uskutečňují transakce, musejí dát najevo, jak velký poplatek jsou ochotni zaplatit těžařům, a těžaři jejich transakce můžou nebo nemusejí přijmout

---

* O současném stavu těžby se můžete víc dočíst na coinshares.co.uk/bitcoin-mining-cost-june-2019.

podle toho, jestli jim poplatky vyhovují. Když je transakcí k zápisu do následujícího bloku málo, poplatky bývají velmi nízké, protože chybí konkurence. Jak se místo v bloku zaplňuje, uživatelé jsou ochotni platit vyšší poplatky, aby jejich transakce byly potvrzeny dřív. Ti, kteří platit nechtějí, můžou své ceny stanovit nízké a čekat na vytěžení delší dobu, až bude místo v blocích dostupnější.

V tradičních finančních systémech poplatky bývají založené na procentu z převáděné částky. U Bitcoinu hodnota převáděné částky nemá na výši poplatků vliv. Namísto toho je výše poplatků odvozena od vzácného zdroje, který spotřebovávají: místa v blocích. Poplatky jsou vyměřovány v jednotkách satoshi za byte (8 bitů) spotřebovaného místa. Transakce, kterou se převádí milion bitcoinů mezi dvěma osobami, tak může být levnější než transakce, která rozděluje 1 bitcoin mezi deset příjemců, protože ta druhá transakce zabere víc paměti v bloku.

V minulosti byla období, kdy byl Bitcoin velmi žádaný, jako například během obrovského býčího trhu na konci roku 2017. V tomto období byly transakční poplatky extrémně vysoké. Od té doby se do systému zavedlo několik nových prvků, aby se tlak poplatků na síť snížil.

Jedním z těchto prvků je tzv. SegWit (z anglického Segregated Witness, což je volně přeložitelné jako Oddělený svědek). Tenhle prvek mění uspořádání dat v blocích. Transakce, které využívají tohle vylepšení, můžou díky šikovným trikům, které ovšem přesahují rámec této knihy, využívat víc než původní 1 MB místa v bloku.

Co se týká poplatků, další pomoc přišla v podobě sdružování plateb (batchování): burzy a další velkoobjemoví hráči v ekosystému začali spojovat bitcoinové transakce několika uživatelů do jedné transakce. Na rozdíl od tradičních plateb prováděných přes vaši banku nebo PayPal, které se uskutečňují mezi dvěma osobami, bitcoinová transakce může sdružovat velké množství vstupních

dat a produkovat velké množství dat výstupních. Burza, která potřebuje poslat bitcoin k výběru stovce lidí, to může provést v rámci jediné transakce. Je to mnohem efektivnější využití paměti v bloku, a i když se zdá, že za vteřinu proběhlo jen pár bitcoinových transakcí, ve skutečnosti může tahle vteřina obsahovat až tisíce jednotlivých provedených plateb.

SegWit a batchování výrazně snížily potřebu paměti v blocích. Čekají se další vylepšení, která využití paměti v blocích ještě zefektivní. Nicméně protože jsou bloky vzhledem k vysokému zájmu stále plnější a plnější, přijde doba, kdy se bitcoinové poplatky opět zvýší.

Tím jsme vynález Bitcoinu téměř dokončili:

1. Nahradili jsme centrální banku distribuovanou účetní knihou.
2. Zavedli jsme loterii, která určí, kdo bude do účetní knihy zapisovat.
3. Přinutili jsme účastníky loterie, aby při nákupu losů spotřebovávali energii hashováním, a každému jsme umožnili snadno ověřit vítězné losy porovnáním hashů vypočítaných hráči s nezávisle stanoveným cílovým číslem.
4. Řekli jsme hráčům, že pokud nebudou dodržovat pravidla, zamítneme jejich bloky včetně coinbase transakcí, takže v případě výhry nezískají odměnu, a ekonomicky jsme je tak odradili od podvádění, a naopak motivovali k dodržování pravidel.
5. Určili jsme časový plán a umožnili jsme, aby si cílové číslo pro loterii každý mohl nezávisle vypočítat na základě historie posledních 2016 bloků v souladu s pravidly zabudovanými do systému.

6. Zajistili jsme dodržování časového plánu za pomoci regulace obtížnosti, která klesá a stoupá spolu s hash rate.
7. Použili jsme open source kód, aby si každý mohl sám ověřit, že používá stejná pravidla, pokud jde o platnost transakcí, blokovou odměnu a výpočet obtížnosti.

Je konec s centrální autoritou. Máme plně distribuovaný a decentralizovaný systém. Obrázek je téměř kompletní. Zůstává jen jediný problém. Když se někdo připojí k síti a vyžádá si kopie účetní knihy, může od různých uzlů obdržet různé verze knihy. Jak zajistíme jedinou, lineární historii a jak zabráníme těžařům v případném přepisování minulosti?

KAPITOLA 5

Zabezpečení účetní knihy

Zatím jsme mluvili o tom, jak je možné zapisovat do distribuované účetní knihy a uchovávat její kopie pomocí loterijního systému a potvrzování na základě všeobecné shody způsobem, který není ohrozitelný nátlakem či korupcí.

Co když se však vítěz loterie rozhodne udělat něco nekalého? Může těžař změnit historické záznamy v účetní knize? Můžou se naši zločinci Eva, David a Františka domluvit na přepsání historie nebo na změně stavů účtů a dát si mince navíc?

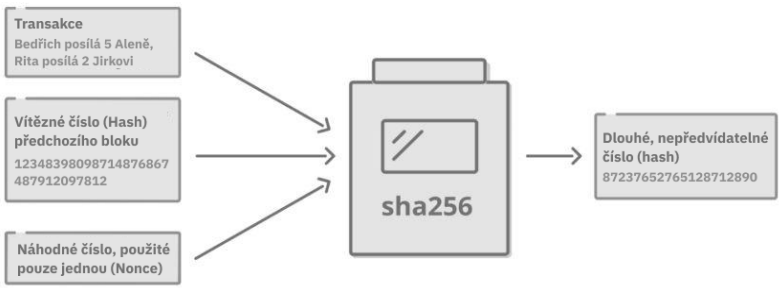
Na scénu přichází řetězec bloků (blockchain). Je to marketingové slovo, které prostoupilo většinu technologického sektoru, a zároveň to není nic víc než myšlenka, že bitcoinové bloky jsou zřetězeny dohromady, takže propojují jednu sadu transakcí s další. Tak vzniká lineární historie vytváření a převádění mincí od chvíle, kdy Satoshi v roce 2009 vytěžil svůj prvotní blok, až dodnes.

V předchozí kapitole jsme v zájmu jednoduchosti neříkali úplnou pravdu. Když těžíte účastí v loterii důkazu o vykonané práci, transakce čekající na zápis do dalšího bloku a náhodná nonce nejsou tím jediným, co se hashuje dohromady. K těmto údajům

přidáváte ještě hash předchozího bloku, čímž se váš blok propojí s předchozím.

Vzpomeňte si, že výsledek hashovací funkce je nepředvídatelný a závislý na všech údajích, které do ní vstupují. Do hashů našich bloků teď vstupují tři různé vstupní údaje:

1. Transakce, které mají být zapsány do účetní knihy.
2. Náhodná nonce.
3. Hash předchozího bloku, z nějž vychází historie naší účetní knihy.



Mezi vstupní údaje, z nichž se vypočítává hash do loterie, teď navíc patří předchozí vítězný hash. Tím se jeden blok propojuje s druhým.

Díky tomu můžeme sestavit historii úplně všech bloků až k prvotnímu bloku, který vytěžil Satoshi. Když do řetězce bloků přidáme další blok, musíme ověřit, že tenhle blok neobsahuje žádné transakce s bitcoiny utracenými už v předchozích blocích.

Když se kterýkoliv ze vstupních údajů změní, tak se zásadně a nepředvídatelně změní i výsledný hash. Když zmanipulujete údaje v jakémkoliv z předchozích bloků, změníte tím jeho hash. Jenže tenhle hash byl zároveň součástí vstupních údajů pro další bloky, takže budete muset změnit i hashe těchto bloků. Hash posledního

bloku v řetězci je propojený se všemi předchozími hashi, a tím funguje jako otisk prstu celé dosavadní historie řetězce bloku!

Důkaz o vykonané práci nelze zfalšovat, protože každý ví, kolik energie stojí vytvoření každého bloku na základě cílového čísla stanoveného pro ten konkrétní blok. Kdyby se kdokoliv pokusil změnit nějaký starší blok v řetězci, musel by přepočítat hash důkazu o vykonané práci nejen pro blok, který mění, ale i pro všechny následující bloky. Taková změna řetězce bloků by byla nejen očividná, ale navíc i extrémně drahá.

Každý nový vytěžený blok tak fakticky zvyšuje zabezpečení předchozích bloků, protože zvyšuje množství elektřiny potřebné k přepočítání hashů důkazu o vykonané práci pro celý předchozí řetězec. Transakci v bloku, po němž následuje šest dalších bloků, dnes většina obchodníků

považuje za potvrzenou. Při dnešním celkovém hash rate by přepočítání hashů posledních šesti bloků stálo neskutečné množstvé energie. A co transakce provedená před 100 bloky? Bez šance.

Když si stáhnete kopii řetězce bloků, každá transakce v každém bloku je zcela průhledná, a hashe důkazu o vykonané práci si můžete sami ověřit, abyste se ujistili, že osoba, která vám účetní knihu poslala, v ní nic neměnila.

Střet bloků

Systému všeobecné shody schází ještě jeden dílek: Jak můžeme všechny udržet na jedné lineární historii transakcí, když těžaři současně vytěží dva bloky a všem je odešlou?

Představte si, že provozujeme celosvětovou síť. K této globální síti jsou připojeni lidé po celém světě od Spojených států až po Čínu a všichni hrají těžařskou loterii důkazu o provedené práci.

Někdo v Chicagu najde platný blok. Oznámí to síti a všechny počítače v Americe začnou blok přijímat. Mezitím někdo v Šanghaji taky najde platný blok, jen pár vteřin po tom chicagském. Jeho sousedé zatím o americkém bloku nevědí, proto k nim čínský blok dorazí jako první.

Oba tyto bloky obsahují transakci, kde Alena odesílá 1 bitcoin Bedřichovi. Bedřich však bitcoin okamžitě po jeho obdržení odešle Cyrilovi. Americký blok tuto transakci kvůli časovému rozdílu obsahuje a Bedřich má na účtu nulu. Číňané však svůj blok vytěžili dřív, než se dozvěděli o převodu od Bedřicha k Cyrilovi. V čínském bloku má Bedřich na účtu 1 bitcoin.

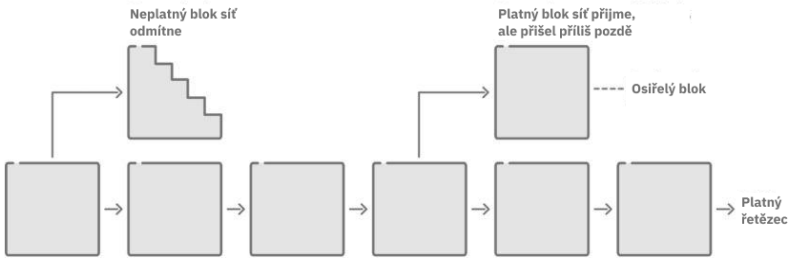
Síť se neshodne na tom, který řetězec bloků je správnou kopií účetní knihy, protože oba bloky obsahují platné transakce propojené s historií ve všech předchozích blocích. Oba bloky obsahují platnou hodnotu důkazu o provedené práci. Této situaci se říká rozštěpení řetězce. Žádná centrální autorita to nerozsoudí. Co s tím?

Bitcoin má jednoduché řešení: prostě počkejme a uvidíme. Těžaři si můžou vybrat, který blok použijí jako základ pro další těžbu. Američané budou těžit na základě bloku, který obdrželi dřív oni, a Číňané budou vycházet ze svého bloku.

V průběhu dalších zhruba deseti minut někdo vytěží další blok. V kódu Bitcoinu je pravidlo, které říká, že ten, kdo vynaložil největší celkovou energii na všechny bloky ve svém řetězci, vyhrává. Toto klíčové pravidlo Bitcoinu, které říká, že máme sečíst celkovou práci v řetězcích a upřednostnit „nejtěžší" řetězec, se někdy na Satoshiho počest nazývá Nakamotův konsenzus.

Řekněme, že Číňané vytěží další blok. Jejich řetězec je teď o jeden blok napřed před americkým řetězcem a obsahuje celkově víc důkazu o vykonané práci. Když svůj blok odešlou do sítě, americké uzly uznají, že čínské uzly vytvořily celkově „těžší" řetězec důkazu o vykonané práci a provedou reorganizaci neboli

reorg. To znamená, že zahodí svůj poslední vytěžený blok a místo něj přijmou poslední dva čínské.



Rozštěpení řetězce je přirozený jev, ke kterému dochází, když víc těžařů najde nový blok ve stejnou chvíli. Řetězec, který je „těžší" důkazem o vykonané práci, je platný, zatímco druhý blok osiří.

Americký blok se teď nazývá sirotek (orphan). Protože byl zamítnut, těžař, který ho vytěžil, nezíská svou odměnu a žádné z transakcí, které blok obsahuje, nejsou zapsány do účetní knihy. Zamítnuté transakce však nejsou ztraceny. Některé z nich se mohly dostat do konkurenčního čínského bloku, a i ty, které se do něj nedostaly, budou zapsány do některého z následujících bloků.

Těžaři uchovávají veškeré transakce, o kterých se dozvědí, na speciálním místě ve svém počítači, kterému se říká mempool. Jakékoliv transakce ze zamítnutého bloku se vrátí do mempoolu. Později je někdo vytěží, pokud nejsou v rozporu s novou historií v účetní knize obsažené v nejnovějším bloku.

Uvědomte si, že ačkoliv jsme mluvili o americkém a čínském uzlu, ve skutečnosti uzly navzájem neznají svou identitu ani zeměpisné umístění. Jediným důkazem platnosti, který potřebují, je to, že někdo má celkově nejtěžší řetězec důkazu o vykonané práci a že transakce v tomto řetězci jsou samy o sobě všechny platné (nejsou to dvojí útraty atd.).

Tenhle typ rozštěpení řetězce je běžný a čas od času k němu v bitcoinové síti dochází. Většinou se vyřeší v rámci následujícího bloku. Díky zdokonalování technologií šíření bloků a síťového propojení mezi těžaři k tomu dochází stále méně často. Dnes (a nejspíš to bude platit i pro dohlednou budoucnost) má v sobě Bitcoin zakódováno omezení množství údajů, které může jeden blok obsahovat. Bitcoin vytváří poměrně malé bloky zhruba každých deset minut mimo jiné právě proto, aby vznikalo co nejméně osiřelých bloků.

Těžba je záležitostí pravděpodobnosti. Někdy jsou od sebe bloky vzdálené deset minut, někdy jen několik vteřin. Kdybychom vytvářeli bloky každou vteřinu nebo měli hodně velké bloky, byla by vysoká pravděpodobnost, že americké a čínské bloky budou v rozporu, protože jsou zeměpisně daleko od sebe a trvá déle, než k sobě dorazí. Kdyby osiřelé bloky vznikaly moc často, blockchain by neplnil svoji funkci. Sirotci by se množili a uzly by neměly čas se shodnout na posledním bloku před vytěžením následujícího.

Bloky musí být malé, aby se zvýšila šance, že celá síť obdrží nejnovější blok, než začne těžit další. Druhý a možná důležitější důvod je to, že když držíme hardwarové požadavky na provoz uzlu poměrně nízko, může vznikat víc uzlů a těžba může být decentralizovaná. Velké bloky by těžaře motivovaly k tomu, aby se sdružovali v datacentrech a v určitých zeměpisných oblastech za účelem vyhnutí se těžbě osiřelých bloků, které negativně ovlivňují ziskovost.

Jediný pravý řetězec

Vraťme se k našemu příkladu z kapitoly 3, kde se Hynek poprvé připojil k síti Bitcoin.

Hynkův uzel se připojí k několika dalším síťovým uzlům, zeptá se jich, jaké další uzly znají, a potom se připojí i k některým těmto dalším uzlům. Tomuto procesu říkáme objevování uzlů.

Některé uzly budou zlé a pošlou Hynkovi falešnou kopii účetní knihy s nesprávnými podpisy u transakcí nebo padělané bitcoiny, které nemají platné hashe důkazu o provedené práci. Tyto kopie budou ihned zamítnuty a příslušným uzlům bude okamžitě znemožněno, aby se k Hynkovu uzlu připojovaly.*

Jiné uzly, ke kterým se Hynek připojí, budou poctivé, ale jejich verze pravdy se bude lišit. Některé z nich se třeba ocitly offline, a můžou tedy být o jeden či dva bloky pozadu. Když Hynek stáhne víc kopií řetězce bloků, z nichž všechny jsou stejně platné, software v jeho uzlu aplikuje pravidlo Nakamotova konsenzu. Změří celkovou váhu důkazu o vykonané práci a nejtěžší řetězec bude považován za jediný pravý řetězec.

Uzly spolu navzájem neustále komunikují, aby se ujistily, že mají nejnovější bloky. Protože se všechny uzly řídí pravidlem nejtěžšího řetězce, panuje všeobecná shoda na tom, jaký je skutečný stav účetní knihy. Hynek se nemusí spoléhat na tvrzení většiny, což by bylo snadno zfalšovatelné, pokud by se většina uzlů přidala na stranu zla.

I když se Hynek připojí k desítkám uzlů, které jsou buď pozadu, nebo mají nekalé úmysly, a jedinému poctivému uzlu, jeho bitcoinový software jedinou správnou kopii knihy rozpozná, protože bude obsahovat největší množství důkazu o provedené práci a bude sestávat z platných transakcí zpátky do historie až k prvotnímu bloku. To je nesmírně důležité. Hynek se nemusí na nikoho spoléhat; jeho uzel sám provede všechna potřebná ověření, která mu dají jistotu, že má ten jediný pravý řetězec.

Dát nějakému uzlu falešnou kopii řetězce bloků je tedy pro útočníky nesmírně obtížné. Příslušný uzel by museli odříznout

---

* Tenhle vynikající esej se do hloubky zabývá tím, jak bitcoin nakládá s neplatnými bloky: hackernoon.com/bitcoin-miners-beware-invalid-blocks-need-not-apply-51c293ee278b

od veškerých poctivých uzlů a propojit ho výhradně s uzly pod nadvládou útočníků.

Vratnost transakcí

Dva konkurenční řetězce většinou vzniknou náhodou a věc se rychle vyřeší. Pokud by se však někomu, kdo chce na síť zaútočit, podařilo ovládnout víc než 50 % celkového výkonu sítě (hash rate), mohl by zneužít Nakamotova konsenzu. Pokud by byl ochotný spotřebovat dost energie, mohl by pak vytvořit řetězec s nejtěžším celkovým důkazem o vykonané práci obsahující transakce podle svého výběru. Kdyby útočník takový řetězec odeslal ostatním uzlům, přijaly by ho jako jediný pravý řetězec. Tomu se říká 51% útok, protože vyžaduje ovládnutí víc než poloviny hash rate.

Je důležité si uvědomit, že v síti Bitcoin nejsou transakce definitivní, protože vždy existuje teoretické riziko 51% útoku nebo náhodného vzniku osiřelých bloků. Z tohoto důvodu příjemci transakcí většinou s uznáním transakce čekají, než bude vytěženo pár dalších bloků. Pak už je vrácení transakce vzhledem k energetické náročnosti nepravděpodobné.

Bloky vytěžené po bloku obsahujícím transakci, o kterou vám jde, se často nazývají potvrzení. Když tedy uslyšíte, že nějaká transakce v bitcoinové síti má šest potvrzení, znamená to, ze na její blok navazuje šest dalších bloků. Když prodáváte digitální knihu, která pro vás jako obchodníka představuje jen zanedbatelné náklady, bude vám možná stačit jedno nebo žádné potvrzení a odkaz ke stažení odešlete hned, jak se transakce na síti objeví. Když prodáváte dům, možná si raději počkáte na dvanáct potvrzení, což odpovídá zhruba dvěma hodinám těžby. Čím déle počkáte, tím víc důkazů o vykonané práci se za blokem s vaší transakcí nahromadí a tím nákladnější v reálném světě bude vrácení transakce. Většina lidí dnes považuje za důkaz o provedení platby šest potvrzení.

Kdyby hash rate v síti Bitcoin výrazně poklesl, což by znamenalo, že každý blok je zajištěn menším množstvím energie, mohli byste zvýšit počet potvrzení potřebných ke konečnému stvrzení transakce. I když vratnost transakcí může být ze začátku zneklidňující, je důležité mít na paměti, že transakce prováděné kreditní kartou můžou být obvykle vráceny až 120 dnů od uskutečnění.

Naproti tomu transakce v síti Bitcoin jsou už po pár blocích prakticky nevratné. Z tohoto hlediska je Bitcoin co do nevratnosti transakcí ve skutečnosti výrazným zlepšením proti většině tradičních platebních sítí, alespoň z perspektivy obchodníka.

Podle současných odhadů se má za to, že pokud byste měli k dispozici energii celé sítě Bitcoin – což je opravdu impozantní představa, protože byste museli mít v ruce tolik energie jako celá jedna středně velká země a každý existující kus bitcoinového hardwaru – stejně by vám přepsání celé historie řetězce trvalo víc než rok. S odhady se můžete blíže seznámit na bitcoin.sipa.be.

KAPITOLA 6

Forky a 51% útoky

Na začátku Satoshi těžil první bitcoiny za pomoci procesoru (CPU) svého počítače. Protože obtížnost těžby byla původně nastavená na nízkou hodnotu, jeho počítač dokázal mince vytvářet s poměrně nízkými náklady.

Postupně lidé začali těžební software přizpůsobovat, aby byl stále efektivnější. Nakonec napsali software, který začal využívat specializované grafické karty (GPU), které se obvykle používají při hraní her.

S grafickými kartami se těžba stala o řád efektivnější než s použitím běžných procesorů. Obtížnost se rychle upravila směrem nahoru, aby se přizpůsobila novému výpočetnímu výkonu grafických karet. Všichni, kdo v této době používali k těžbě běžný procesor, přestali vydělávat, takže s těžbou skončili.

Po nástupu těžby pomocí grafických procesorů se efektivita těžby dále zvyšovala díky produkci ASICů (z anglického Application Specific Integrated Circuit), tedy integrovaných obvodů vyvinutých pro specifické aplikace. Jedná se o hardwarové počítačové čipy, které plní jedinou funkci: počítání algoritmu SHA-256, nic jiného. ASICy specializované na tenhle jeden konkrétní algoritmus byly

v těžbě o další řád efektivnější než grafické procesory a obtížnost se opět upravila směrem nahoru. Grafické procesory tak přestaly vydělávat, stejně jako klasické procesory po příchodu grafických procesorů. Vždycky jednou za pár let přišla nová generace ASICů, která svou efektivitou vyřadila dřívější verze z provozu.

Prvních pár těžařů v síti utratilo za elektřinu na vytváření bitcoinů jen pár korun. Jak cena bitcoinu rostla a připojovalo se čím dál víc těžařů, obtížnost vzrůstala a vytváření bitcoinů se prodražovalo. Dnes se cena pohybuje okolo 8000 $ za jednu minci a lidé na jeden vytvořený bitcoin spotřebovávají elektřinu za tisíce dolarů.

Těžařské pooly

Jeden z problémů těžby bitcoinu spočívá v tom, že je podobně jako hod kostkou nedeterministická. To znamená, že můžete utratit spoustu peněz za elektřinu, a přesto neobjevit žádný platný blok.

V roce 2010 se objevila inovace nazvaná těžařský pool (mining pool), aby vyřešila problém těžařů, kteří vynakládají elektrickou energii na těžbu, ale nezískávají žádnou odměnu. Těžařský pool je fond sdíleného rizika, který funguje podobně jako pojištění.

Všichni těžaři přispívají poolu těžbou a vytvářejí tak dojem jednoho velkého těžaře. Když kdokoliv v poolu objeví platný blok, odměna se dělí mezi všechny těžaře poměrně podle toho, jakým hash rate přispěli. To umožňuje i malým hráčům, jakými jsou jednotlivci, získat nějakou odměnu za malý hash rate, kterým přispívají. Za své koordinační služby si pool nechává část odměny pro sebe.

Těžařské pooly způsobily jistou míru centralizace – jednotliví uživatelé se sdružili do větších skupin. Pořád ale platí, že uživatelé těží pro pooly a že pooly nevlastní veškerý hash rate, který představují. Uživatelé můžou přecházet a taky přecházejí z jednoho poolu do druhého.

V historii máme dokonce precedens odchodu těžařů z poolu, který se stal příliš silným. V roce 2014 představoval pool Ghash.io skoro polovinu veškeré těžební síly. Těžaři viděli, že dochází k přílišné centralizaci, a dobrovolně odešli do jiných poolů.

Přestože dnes existují poměrně centralizované těžařské pooly, stále vznikají nová vylepšení těžební technologie, jako například návrh nazvaný BetterHash, který dává jednotlivým těžařům víc kontroly nad svou vlastní těžbou a omezuje jejich závislost na koordinaci ze strany poolů.

51% útoky

Centralizace těžařských poolů vede k obavám, že by se pár největších poolů mohlo domluvit a podniknout 51% útok na síť. 5 největších známých poolů dnes dohromady ovládá víc než 50 % celkového hash rate. Podívejme se, jak takový útok probíhá a jaká s sebou nese nebezpečí.

Když ovládáte víc než 50 % hash rate, můžete zapisování do účetní knihy ovládnout, protože dokážete vytvořit těžší řetězec než ostatní. Vzpomeňte si na pravidlo Nakamotova konsenzu, které říká, že uzly musí přijmout řetězec s nejtěžším celkovým důkazem o provedené práci, o kterém se dozví.

Tady je příklad, jak lze provést velmi jednoduchý 51% útok:

1. Předpokládejme, že síť jako celek těží bitcoin rychlostí 1000 hashů za vteřinu.
2. Koupíte si spoustu těžebního hardwaru a elektřiny, abyste vytvořili 2000 hashů za vteřinu. Ovládáte teď 66 % celkového hash rate (2000 ze 3000 hashů za vteřinu).
3. Začnete vytvářet řetězec, který obsahuje jen prázdné bloky.

4. O dva týdny později svůj řetězec prázdných bloků rozešlete. Protože těžíte přibližně dvakrát rychleji než poctiví těžaři, váš řetězec bude obsahovat dvakrát větší množství celkového důkazu o vykonané práci. Když řetězec vyšlete všem existujícím uzlům, budou muset provést reorg historie za poslední dva týdny.

Kromě těžby prázdných bloků, která řetězec znehodnocuje, můžete taky podniknout útok s pokusem o dvojí útratu:

1. Pošlete nějaké bitcoiny na burzu.
2. Vyměňte je za dolary a dolary si vyberte.
3. Později rozešlete řetěz, který neobsahuje informaci o převodu bitcoinů na burzu.
4. Přepsali jste historii a teď máte jak původní bitcoiny, tak dolary, které jste za ně získali.

Energetická spotřeba hash rate v síti Bitcoin dnes odpovídá zhruba spotřebě jedné středně velké země. Získat dostatek hardwaru a elektřiny k podniknutí takového útoky by bylo extrémně nákladné. Odhady ukazují, že 51% útok by vás dnes stál zhruba 700 tisíc dolarů za hodinu, a tato cena pořád roste. Tenhle odhad taky nebere v potaz reakci poctivých těžařů na takový útok, která by ho nejspíš prodražila ještě víc. Cenu útoku na síť Bitcoin a jiných kryptoměn můžete prozkoumat na www.crypto51.app.

Je dost těžké zařídit, aby vám tak velký útok s dvojí útratou prošel, aniž byste zanechali stopy, podle kterých by bylo možné vypátrat, kdo jste. Vždyť během útoku byste přece spotřebovávali energii jako středně velká země, nakupovali byste hardware za miliony dolarů a posílali miliony dolarů na burzy.

Ale řekněme, že se nějaká entita s nekalými úmysly a neomezenými prostředky jako například nějaká vláda rozhodla útok podniknout a byla v něm schopná vytrvat tak dlouho, že to přesáhlo úroveň pouhé nepříjemnosti. Síť by se s tím teoreticky mohla vyrovnat

výměnou funkce důkazu o vykonané práci (začala by používat jinou funkci než SHA-256). To by znehodnotilo veškerý útočníkův hardware, protože by byl specializovaný jen na hashování pomocí funkce SHA-256. Jenže změna principu důkazu o vykonané práci je krajní řešení, které by vyřadilo i poctivé těžaře. Síť by však přežila a vstala by ze svého popela.

Kromě toho, že je takový útok v podstatě neproveditelný, ovládnutí většiny hash rate vám stejně nedává právo na dvě věci, na kterých záleží nejvíc:

1. Nemůžete vytvářet bitcoiny z ničeho a mimo stanovený časový plán. To by porušilo pravidlo všeobecné shody o odměně za blok a vaše bloky by byly zamítnuty, i kdyby byly podložené dostatečným důkazem o provedené práci.
2. Nemůžete utrácet bitcoiny, které vám nepatří. Nebyli byste schopni poskytnout platný digitální podpis, což je porušení pravidel.

Uzly, které přijímají bitcoin jako platbu, by udržovaly síť poctivou i v případě, že by většina těžařů byla nepoctivých, a to jen na základě dodržování pravidel sítě Bitcoin. 51% útok je proto spíš drobná nepříjemnost než bezpečnostní riziko. Nejhorší možný scénář je nejspíš stát, který by dal spoustu peněz do pokusu vyřadit síť Bitcoin z provozu. Takový útok však nemůže trvat věčně. Vzpamatováním se z takového útoku by bitcoinová síť opět dokázala svou odolnost a stala by se ještě větším problémem pro případné útočníky.

Přestože síť Bitcoin zatím nebyla 51% útokem nikdy úspěšně napadena, stalo se to jiným blockchainům, které jsou zajištěny velmi nízkým výpočetním výkonem (hash rate). V těchto případech se obětí útoků s dvojí útratou staly burzy a přišly o peníze z mincí s nízkým hash rate, které nejspíš vůbec neměly nabízet.

KAPITOLA 7

Anonymní účty

Vytvořili jsme distribuovanou účetní knihu bez centrální autority, loterijní systém těžení, který určuje, kdo do knihy smí zapisovat, systém odměňování poctivých těžařů a trestání těch, kteří nedodržují pravidla. Taky jsme vytvořili způsob, jak přizpůsobovat obtížnost těžby zajištění konzistentního časového plánu vydávání mincí a jak minimalizovat neshody, a taky systém na ověřování platnosti řetězce založený na prověření celkového důkazu o vykonané práci a historie transakcí.

Pojďme se teď podívat, jak je to s osobními údaji. Když posíláte peníze v tradičním bankovním systému, sdělíte napřed bance svou identitu. Předložíte průkaz totožnosti nebo pin kód v bankomatu nebo zadáte do aplikace uživatelské jméno a heslo. Banka dohlíží na to, aby žádné dva subjekty nesdílely stejnou identitu.

Když v síti Bitcoin nemáme žádnou centrální autoritu, která by o identitách vedla záznamy, jak si v tomto novém finančním systému můžeme zakládat účty? Jak můžeme dostát Satoshiho cíle anonymních finančních transakcí, jak se můžeme vyhnout krádežím identity a svěřování našich osobních údajů třetím stranám? Když Alena oznámí, že chce zaplatit Bedřichovi, jak můžeme zajistit, že je to skutečně ona a že má oprávnění tyto prostředky převádět?

Zakládáme si „bitcoinový účet”

Nemůžeme se spoléhat na centrálního prostředníka, jakým je banka, že povede seznam všech účtů. Co kdybychom každému umožnili zaregistrovat si vlastní uživatelské jméno a heslo? Banka by obvykle ověřila, jestli uživatelské jméno již neexistuje, ale to tady není možné, protože nemáme žádného centrálního aktéra, který by se staral o naše identity. Potřebujeme něco většího, silnějšího a unikátnějšího, než je uživatelské jméno a heslo. Tato technika by nám měla být povědomá z předchozích kapitol. Opět potřebujeme obří náhodné číslo.

Stejně jako jsme všem umožnili kupovat si losy do loterie generováním velkých náhodných čísel, můžeme stejný trik použít na vytváření účtů. K vytvoření „bitcoinového účtu”, který je taky známý jako adresa, nejprve vygenerujeme dvě 256bitová čísla, která jsou matematicky propojena a jsou známa pod názvy veřejný klíč a soukromý klíč. Vzpomeňte si, že 256bitové číslo je zhruba tak velké jako počet atomů ve vesmíru, takže je téměř nemožné, aby dva lidé vygenerovali stejný soukromý klíč. Naši adresu poskytneme komukoliv, kdo nám chce poslat peníze. K poslání mincí námi použijeme soukromý klíč. Funguje to takhle.

Šifrování je metoda skrývání údajů tak, aby je mohl přečíst jen ten, kdo má klíč, jímž může vzkaz dešifrovat. Jako děti si někteří z nás hráli s jednoduchými šifrovacími hračkami, které používaly určitý klíč k převedení nějakého vzkazu do nesrozumitelné řeči a zase zpátky. Tenhle druh šifrování se nazývá symetrický a používá jen jeden klíč. Systém dvojic veřejných a soukromých klíčů je asymetrický, protože jedním klíčem šifrujete, zatímco druhým klíčem dešifrujete.

Svůj veřejný klíč můžete klidně sdílet s celým světem. Lidé, kteří vám chtějí posílat vzkazy, je můžou zašifrovat pomocí vašeho veřejného klíče. Protože soukromé klíče máte jen vy, jste taky jediný, kdo je může dešifrovat.

Podívejme se teď, jak Alena pošle mince Bedřichovi. Aby mohl Bedřich transakci přijmout, vygeneruje si dvojici klíčů a svůj soukromý klíč si nechá pro sebe. Vytvoří adresu, která je velkým číslem vycházejícím z hashe Bedřichova veřejného klíče. Bedřich tuto adresu sdělí Aleně.

Tuto adresu si můžete představit jako poštovní schránku. Namísto dopisů do ní Alena může hodit mince. Jen Bedřich však má soukromý klíč, kterým lze schránku otevřít a získat k mincím přístup.

Když přesouváte peníze v bance, zadáváte své uživatelské jméno a heslo. Když vypisujete šek, podepisujete ho, abyste potvrdili, že jste ho vypsali vy. Když přesouváte bitcoiny, předkládáte důkaz, že vlastníte klíč k adrese, kde jsou bitcoiny uloženy.

Alena potřebuje dokázat, že má soukromý klíč ke své schránce založené na veřejném klíči, ale nechce svůj soukromý klíč odhalit hackerům, kteří by pak mohli její schránku vykrást a mince utratit.

Alenin důkaz vlastnictví se nazývá digitální podpis. Alena vytvoří transakci, což je v podstatě kousek dat, který vypadá přibližně takhle:

Adresa 12345, kde je uloženo 2,5 bitcoinu, posílá 2 bitcoiny na adresu 56789 a 0,5 bitcoinu zpět na adresu 12345.

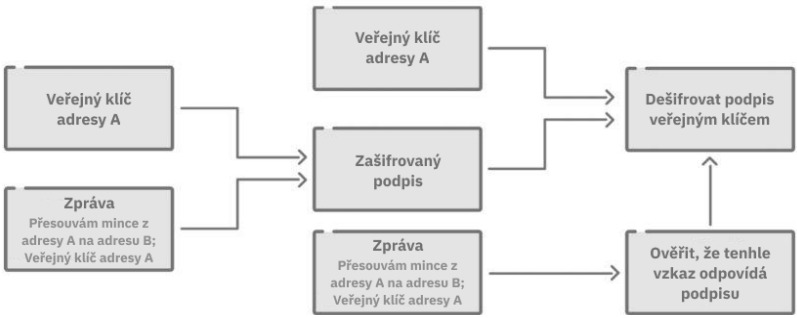
Čísla adres jsou ve skutečnosti velká čísla o 160 bitech. Alena pak transakci zašifruje pomocí svého soukromého klíče a vytvoří tak digitální podpis.

Když svou transakci odešle ostatním uzlům sítě, odhalí veřejný klíč schránky, z níž transakci posílá, a podpis zašifrovaný soukromým klíčem. Alena oznámí následující:

— Posílám mince z adresy 12345.

— Tady je veřejný klíč pro adresu 12345 a můžete si ověřit, že to je opravdu veřejný klíč, když si ho zahashujete a získáte číslo adresy.

— Tady je podpis, který jsem zašifrovala soukromým klíčem odpovídajícím této adrese. Můžete ho dešifrovat veřejným klíčem a ověřit si, že je shodný s údaji posílané transakce.



Transakce, kterou se přesouvají mince, je zašifrovaná soukromým klíčem, čímž vzniká digitální podpis. Je dešifrována veřejným klíčem, který všichni znají.

Protože teď všichni mají Alenin veřejný klíč k adrese její schránky, můžou snadno dešifrovat digitální podpis. Díky tomu, že můžou správně dešifrovat podpis veřejným klíčem k adrese, všichni vědí, že Alena musela použít soukromý klíč k této adrese, aby podpis vytvořila. Jinak by jejich dešifrování neuspělo, protože veřejný klíč může dešifrovat jen vzkazy zašifrované soukromým klíčem. Důležité však je, že nikdo neviděl Alenin soukromý klíč, ale jen důkaz, že ho použila k zašifrování svého podpisu.

Na rozdíl od podpisu na šeku nebo hesla k bankovnímu účtu je digitální podpis vždy specifický pro jedinečná transakční data,

která podepisujete. Proto ho nejde ukrást a znovu použít na jinou transakci. Každá transakce má jiný podpis, i když je uskutečňována ze stejné veřejné adresy a se stejným soukromým klíčem, protože jakákoliv jiná data změní hash podpisu.

Jde soukromý klíč uhodnout?

Pojďme se podívat, jak moc je pravděpodobné, že by se někomu podařilo uhodnout soukromý klíč, který by mu umožnil přesouvat mince z příslušné veřejné adresy. Připomeňme si, že klíč má velikost 256 bitů. Každý bit může nabývat jen dvou hodnot (jedna nebo nula). Každý bit si proto můžete představit jako hod mincí.

Kdybychom měli soukromý klíč o velikosti 1 bit, bylo by to jako hod jedinou mincí. Padne panna, nebo orel, jedna, nebo nula? Máte šanci jedna ku dvěma, že klíč uhodnete.

Zopakujme si rychle základy statistiky: Pravděpodobnost víc událostí zároveň se počítá tak, že vynásobíme pravděpodobnosti všech jednotlivých událostí. Pokud je u hodu mincí pravděpodobnost ½, že padne panna, potom pravděpodobnost, že padne panna dvakrát po sobě, je ½ × ½ = ¼ neboli 1 ku 4.

Pokud byste měli uhodnout výsledek osmi po sobě následujících hodů kostkou, pravděpodobnost by byla $1/(2^8)$ neboli 1 ku 256.

Na poznávací značce auta je 6 písmen a číslic. Základní abeceda má 26 písmen a číslic je 10, to je dohromady 36 znaků. Protože jich na značce máme 6, množství možných poznávacích značek je 36^6. Šance, že uhodnete moji poznávací značku, je tedy jedna ku dvěma miliardám.*

---

* Inspirace pro tenhle oddíl vzešla ze skvělého článku na Medium, který se podrobně zabývá pravděpodobnostmi různých událostí. Doporučuji přečíst si celý článek kvůli kontextu: medium.com/@kerbleski/a-dance-with-infinity-980bd8e9a781.

Kreditní karta má číslo o šestnácti číslicích. Každá číslice může nabývat 10 hodnot a je jich celkem 16, takže pravděpodobnost, že uhodnete číslo mé kreditní karty, je jedna ku 10^{16}, což je jedna ku 10 000 000 000 000 000 neboli zhruba jedna ku deseti kvadrilionům.

Na zemi je okolo 10^{50} atomů. Když si náhodně vyberu jeden z nich, pravděpodobnost, že uhádnete, který to je, je okolo

jedna ku 1 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000.

Soukromý klíč má 256 bitů, což je 2^{256} nebo přibližně 10^{77}. Uhodnout celý klíč by bylo podobné jako uhodnout jeden konkrétní atom v celém vesmíru nebo vyhrát v loterii Powerball devětkrát po sobě:

1 ku 115 792 089 237 316 195 423 570 985 008 687 907 853 269 984 665 640 564 039 457 584 007 913 129 639 936

Co kdybyste však měli supersilný počítač, který by hádal za vás? Nemohu se k tomuto tématu vyjádřit lépe než následující post na Redditu, který doporučuji přečíst si celý: bit.ly/2Dbw9Qd. I když je trochu technický, na základě posledního odstavce si můžete udělat dobrou představu, co by obnášelo vypsat všechny možné 256bitové klíče:

> *Kdybyste tedy mohli použít celou planetu jako harddisk a uložit 1 byte do jednoho atomu, jako palivo používat hvězdy a zapisovat 1 trilion klíčů za vteřinu, potřebovali byste k uložení všech klíčů 37 oktilionů zeměkoulí a 237 miliard Sluncí, abyste dokázali napájet takovýto přístroj, a trvalo by vám to 3,6717 oktodecilionů let.*
>
> ***– u/PSBlake na r/Bitcoin***

Je tedy v podstatě nemožné, abyste uhodli něčí soukromý klíč. * Navíc počet všech možných bitcoinových adres je tak velký, že je na bitcoinové síti zvykem pro každou transakci vytvořit novou adresu s novým soukromým klíčem. Místo toho, abyste měli jeden účet, tak můžete mít tisíce nebo dokonce miliony bitcoinových účtů, jeden pro každou transakci, kterou jste kdy uskutečnili.

Možná vás zneklidňuje, že je váš bitcoinový účet zajištěn jen statisticky, ale na základě výše zmíněné ilustrace je snad už jasné, že je nesrovnatelně bezpečnější než heslo k vašemu bankovnímu účtu, které je uložené na centralizovaném serveru a přístupné případným hackerům.

Zaznamenávání zůstatků

Je načase, abychom opravili poslední malou lež, kterou jsme opakovali v předchozích kapitolách. V účetní knize ve skutečnosti nejsou zaznamenávány žádné zůstatky. Bitcoin namísto toho používá systém nazvaný UTXO z anglického Unspent Transaction Outputs (česky neutracené transakční výstupy). Transakční výstup je prostě jen označení pro mince, které jste obdrželi v rámci nějaké předchozí transakce, ať už vám je někdo poslal, nebo jste je vytěžili v coinbase transakci.

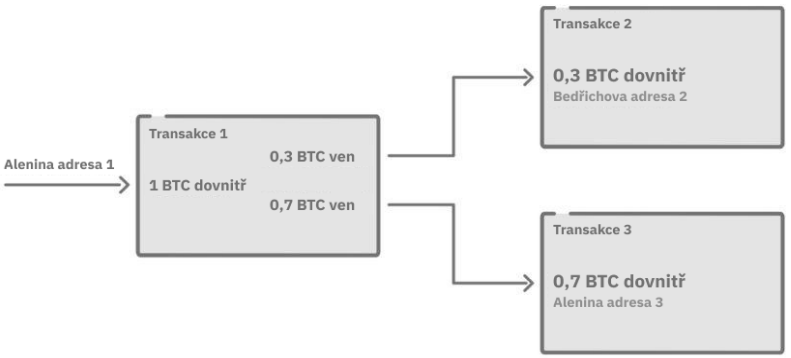
Na rozdíl od kovových mincí, které existují v určitých nominálních hodnotách jako deset korun, dvacet korun, padesát korun atd., lze každý bitcoin rozdělit na 100 000 000 jednotek zvaných satoshi. Podle toho, jaké množství bitcoinů jste na své adresy obdrželi, můžete potřebovat zkombinovat mince z víc adres nebo rozdělit větší UTXO na menší části, které budete moci poslat někomu jinému. Představte si to tak, jako kdybyste vložili hrst mincí do stroje, který je přetaví a vytvoří vám nové mince v jakékoliv hodnotě

---

* V praxi není nutné uhodnout konkrétní soukromý klíč, ale jakýkoliv, který má shodný hash o velikosti 96 bitu.

chcete. Peněženky, o kterých budeme v této kapitole ještě mluvit, pro vás toto všechno zařizují na pozadí, takže jen určujete sumu, kterou chcete poslat.

Řekněme, že Alena má adresu, která obsahuje 1 bitcoin. Chce poslat 0,3 bitcoinu Bedřichovi. Vygeneruje transakci, která ukazuje její adresu s UTXO ve výši 1 bitcoin jako vstup, a dva výstupy: nový UTXO v hodnotě 0,3 bitcoinu na Bedřichově adrese a nový UTXO v hodnotě 0,7 bitcoinu zpátky na Alenině adrese. Vrácené mince můžou přijít zpátky na její původní adresu, ze které mince posílala, nebo jim může pro větší bezpečnost vytvořit novou adresu.



Pokud nemáte UTXO ve stejné výši, kterou chcete poslat, potom se UTXO rozdělí a část mincí bude vrácena. Lze taky spojit víc UTXO do jednoho většího.

Obecně není možné říci, která z adres je Aleny a která Bedřicha. K tomu byste potřebovali znát odpovídající soukromé klíče a spojit je se subjekty v reálném světě. Model založený na UTXO podporuje velmi kvalitní bezpečnostní mechanismus pomocí vytvoření nové adresy při každém přesunu mincí. Někdo tak může vlastnit stovky nebo tisíce adres, pokud poslal nebo obdržel mince mnohokrát. Peněženkový software to za nás vše řeší, takže se nemusíme zabývat detaily.

Abychom zjistili „zůstatek" na nějaké konkrétní adrese, musíme sečíst všechny UTXO, které tuto adresu uvádějí jako výstup. Celkový počet aktuálních UTXO v síti Bitcoin vzrůstá, když lidé posílají z jedné adresy na víc jiných, a klesá, když lidé například provádějí tzv. konsolidační transakce, kterými jsou bitcoiny z mnoha adres převáděny na jedinou.

Model založený na UTXO umožňuje snadné a efektivní ověřování potenciálních dvojích útrat, protože každý výstup UTXO může být utracen jen jednou. Nepotřebujeme znát celou historii převodů z nějakého konkrétního účtu.

Lze taky naráz vytvořit nebo smazat jakékoliv množství UTXO a vytvořit tak komplexní transakce, které kombinují různé vstupy a výstupy.

Toho využívá technika CoinJoin*, při které se víc stran účastní jediné bitcoinové transakce, kde každá strana má některé vstupy a některé výstupy, ale zvenčí není vidět, který výstup pochází z kterého vstupu. Oblíbenost podobných technik stoupá a je důležitá pro zachování anonymity a fungibility, což je termín, který říká, že kterýkoliv jeden bitcoin je ekvivalentní kterémukoliv jinému bitcoinu. Pokud se tedy některé bitcoiny ocitnou u někoho zavrženíhodného, nejsou navěky poznamenané jen proto, že byly jednou použity na něco nekalého.

Peněženky

Vytvoření účtu není ničím jiným než vygenerováním náhodné dvojice 256 bitových klíčů. Takových účtů můžeme vytvořit tisíce nebo miliony, proto potřebujeme způsob, jak je sledovat. V bitcoinové síti se pro jakékoliv zařízení, které sleduje vaše klíče,

---

* en.bitcoin.it/wiki/CoinJoin.

používá termín peněženka. Může to být věc tak prostá, jako je kus papíru, nebo tak složitá, jako je specializovaný hardware.

Původní kód Bitcoinu publikovaný Satoshim zahrnoval i softwarovou peněženku. Tato peněženka generovala adresy, ukládala klíče a vybírala UTXO k utrácení, aby uživatel mohl snadno posílat jakékoliv množství bitcoinů.

Na rozdíl od bankovní peněženky, což je obvykle mobilní nebo webová aplikace, kterou vyvinula banka, je Bitcoin úplně otevřený systém. Existují proto desítky peněženek, z nichž většina je bezplatná, spousta je jich taky open source, existuje několik hardwarových peněženek a další se vyvíjejí. Kdokoliv se znalostí počítačového programování může vytvořit svou vlastní peněženku nebo si překontrolovat zdrojový kód kterékoliv open source peněženky a ujistit se, že nejde o nic nekalého.

Vzhledem k tomu, že váš soukromý klíč je tím jediným, co potřebujete k tomu, abyste mohli převádět mince, musíte ho velmi bedlivě střežit. Když vám někdo ukradne kreditní kartu, můžete zavolat společnosti, která ji vydala, krádež ohlásit a pokusit se získat své peníze zpátky. V síti Bitcoin žádný prostředník není. Když někdo získá váš soukromý klíč, získá přístup k vašim bitcoinům a nikoho se nedovoláte.

Soukromé klíče se taky snadno ztrácejí. Když si uložíte peněženku na vašem počítači a ten pak shoří nebo ho někdo ukradne, máte problém. Pokud dodržujete doporučené postupy a generujete novou adresu pro každou transakci, bezpečné ukládání a zálohování všech soukromých klíčů vám rychle přeroste přes hlavu.

Bitcoinový ekosystém postupně vyvinul řadu řešení tohoto problému. V roce 2012 byl předložen BIP32 (Bitcoin Improvement Proposal neboli návrh na vylepšení Bitcoinu, což je mechanismus, jehož prostřednictvím lidé můžou šířit nápady na vylepšení Bitcoinu), který navrhuje vytvoření hierarchických deterministických peněženek. Myšlenka tohoto návrhu spočívá v tom, že s použitím

jediného náhodného čísla, tzv. seedu, můžeme opakovaně generovat mnoho dvojic klíčů představujících bitcoinové adresy a jejich soukromé klíče.

Když v současné době používáte některou z mnoha běžně dostupných softwarových či hardwarových peněženek, tyto peněženky automaticky generují nové klíče pro každou transakci, přičemž vám umožňují zálohovat jen jediný master klíč (seed).

V roce 2013 se objevil vylepšovací návrh č. 39 (BIP39), který zálohování ještě víc usnadnil. Namísto náhodných čísel se pro generování klíčů používají náhodné sady lidem srozumitelných slov.

Tady je příklad takového seedu:

witch collapse practice feed shame open despair creek road again ice least

S použitím této metody je zálohování klíčů velmi snadné: Seed si můžete zapsat na kousek papíru a uložit si ho do trezoru. Nebo si můžete příslušná slova prostě zapamatovat a v případě totálního kolapsu státu odejít s prázdnými kapsami, aniž by kdokoliv poznal, že si své bohatství nesete v hlavě.

Bitcoinová adresa navíc může k přístupu vyžadovat víc než jeden soukromý klíč. Multisig adresy neboli adresy s více podpisy můžou využívat množství různých zabezpečovacích mechanismů. Dva lidé například můžou sdílet jeden účet pomocí multisigu typu 1 ze 2, u kterého může kterákoliv strana podepisovat transakce a utrácet bitcoiny.

Chceme-li předejít tomu, aby nadvládu nad účtem získala jediná osoba, například jeden z obchodních partnerů, můžeme použít multisig typu 2 ze 2, který vyžaduje k potvrzení transakcí klíče obou stran.

S pomocí multisigu typu 2 ze 3 můžete vytvořit jednoduchý svěřenecký mechanismus (escrow mechanism). Kupující dostane jeden klíč, prodávající dostane druhý klíč a třetí klíč dostane prostředník. Pokud se kupující a prodávající domluví, můžou společně odemknout přístup k penězům. V případě sporu může společně s jednou ze stran přístup odemknout prostředník.

Multisig typu 3 z 5 lze využít k ochraně před ztrátou klíčů. Až 2 z celkem 5 klíčů můžete ztratit a přesto se k prostředkům na účtu dostanete. Dva z klíčů můžete uložit na různých místech, u dvou důvěryhodných přátel, kteří o sobě navzájem nevědí, a jeden klíč můžete uložit u specializované správcovské služby, jakou je např. BitGo, která připodepisuje vaše transakce a ztěžuje tak krádež vašich bitcoinů a zároveň vás chrání před ztrátou klíčů.

Můžete jít ještě dál a vytvořit adresy, které se odemykají za složitých podmínek pomocí programovacích konstrukcí, jako jsou podmínkové příkazy („jestliže X, pak Y"). Mohli byste dokonce bitcoiny uzamknout na nějaké adrese, která bude přístupná až za 10 let, a ani vy sami jako tvůrce této adresy byste si to pak nemohli rozmyslet a změnit kód, abyste se k mincím dostali před stanoveným datem.

Společnosti jako Casa nebo Unchained Capital vyvíjejí další a další částečně správcovská řešení, která vám pomáhají ukládat klíče bezpečným způsobem. Na rozdíl od bank, které vám můžou účet zmrazit, tato částečně správcovská řešení slouží jen jako záloha nebo důvěryhodný připodepisovatel, nemůžou však samy vybrat vaše prostředky bez vašich klíčů. Peněženkové softwary se neustále vyvíjejí, protože k tomu na rozdíl od aplikace vaší banky nepotřebují ničí svolení. Proto se neustále objevují noví hráči a další a další inovace.

Tyhle změny jsou zásadní a přelomové. Až do dneška nebylo možné mít u sebe svůj majetek tak, aby ho nebylo možné nijak zabavit nebo ukrást.

KAPITOLA 8

Kdo určuje pravidla?

V tuto chvíli už máme funkční distribuovaný systém pro sledování a převádění hodnoty. Zopakujme si, co jsme doposud vytvořili:

1. Distribuovanou účetní knihu, jejíž kopii uchovává každý uživatel.
2. Loterijní systém založený na důkazu o vykonané práci a regulaci obtížnosti, který síť chrání před neoprávněnými zásahy a zajišťuje dodržování časového plánu vydávání bitcoinů.
3. Systém všeobecné shody, díky kterému každý účastník sám může ověřovat celou historii řetězce bloků s pomocí open source aplikace zvané bitcoinový klient.
4. Systém identifikace používající digitální podpisy, který umožňuje vytváření schránek podobných účtům, které můžou přijímat bitcoiny bez centrální autority.

Nyní je čas poprat se s jedním z nejzajímavějších a nejpřekvapivějších aspektů Bitcoinu. Odkud pocházejí všechna jeho pravidla, jakým způsobem je zajištěno jejich dodržování, a jak to, že se v průběhu času mění?

Bitcoinový software

V předchozích kapitolách jsme předpokládali, že všichni v síti uznávají stejná pravidla: odmítají dvojí útraty, zajišťují, aby každý blok obsahoval odpovídající množství důkazu o vykonané práci, aby byl propojen s předchozím blokem z konce aktuálního řetězce a aby každá transakce v každém bloku byla řádně podepsaná vlastníkem adresy – a kromě toho dodržují řadu dalších pravidel, na kterých se lidé v průběhu času shodli.

Řekli jsme taky, že Bitcoin je open source software. Open source znamená, že každý může nahlížet do zdrojového kódu a každý může do své kopie přidávat úplně jakýkoliv nový kód. Jak se změny dostanou do bitcoinového softwaru?

Bitcoin je protokol. V oblasti počítačového softwaru se tenhle pojem používá pro označení množiny pravidel, podle nichž příslušný software funguje. Dokud však dodržujete pravidla, která dodržují všichni ostatní, můžete si svůj software modifikovat úplně dle libosti. Když říkáme, že lidé „provozují bitcoinové uzly", ve skutečnosti tím myslíme, že mají spuštěný software, který dodržuje protokol Bitcoinu. Tenhle software může komunikovat s jinými bitcoinovými uzly, vysílat k nim transakce a bloky, objevovat jiné uzly ke spolupráci a tak dále.

Detaily konkrétní implementace bitcoinového protokolu už závisí na každém jednotlivci. Existuje mnoho implementací bitcoinového protokolu. Nejpoužívanějším je Bitcoin Core, což je rozšíření původního softwaru, který vydal Satoshi Nakamoto.

Existují další implementace napsané v jiných programovacích jazycích a udržované různými lidmi. Protože je v Bitcoinu nesmírně důležitá všeobecná shoda, což znamená, že se všechny uzly musí shodnout na tom, které bloky jsou či nejsou platné, většina uzlů používá stejný software Bitcoin Core, aby se předešlo případným náhodným chybám, kvůli nimž by se mohly některé uzly neshodovat

na tom, co je platné. Ve skutečnosti neexistuje úplně kompletní písemná specifikace bitcoinového protokolu. Nejlepším způsobem, jak zavést nový bitcoinový klient, je přečíst si původní kód a neodchýlit se od něj, a to i kdyby obsahoval chyby.

Kdo určuje pravidla?

Pravidla, která tvoří Bitcoin, jsou zakódována v klientu Bitcoin Core. Kdo však rozhoduje, jaká pravidla to budou? Jak můžeme tvrdit, že je Bitcoin vzácný, když může kdokoliv přijít a pozměnit software tak, že se například zvětší celkové množství bitcoinů z 21 milionů na 42 milionů?

Vzhledem k tomu, že jde o distribuovaný systém, musí se na pravidlech shodnout všechny uzly. Pokud jste těžař a rozhodnete se změnit software, aby vám dával dvakrát větší odměnu, než stanoví aktuální nastavení blokové odměny, tak váš blok po vytěžení všechny ostatní uzly v síti zamítnou. Změnit pravidla je extrémně obtížné, protože po světě jsou distribuovány tisíce uzlů, které všechny hlídají dodržování pravidel Bitcoinu.

Systém řízení Bitcoinu je neintuitivní, obzvláště pro ty z nás, kteří žijí v západních demokraciích. Jsme zvyklí na řízení pomocí hlasování – většina lidí může rozhodnout, že se něco udělá, třeba schválit nějaký zákon, a vnutit tak svou vůli menšině. Systém řízení Bitcoinu se však blíží spíš anarchii než demokracii.

Každá osoba, která přijímá bitcoinové platby, se sama rozhodne, co považuje za bitcoin. Když má někdo spuštěný software, který říká, že je 21 milionů bitcoinů, a vy se mu pokusíte poslat bitcoiny vytvořené vaším vlastním softwarem, který tenhle limit neuznává, vaše mince pro něj budou falešné a odmítne je.

Podívejme se na aktéry bitcoinového světa, kteří fungují jako vzájemné brzdy a protiváhy.

Uzly

Každý účastník v síti Bitcoin provozuje uzel. Volí si, který software bude mít na tomto uzlu spuštěný. Většina lidí používá Bitcoin Core, základní implementaci bitcoinového protokolu, kterou jako první vytvořil Satoshi Nakamoto a která je teď vyvíjena stovkami nezávislých vývojářů a společností po celém světě. Pokud by tato implementace začala být záměrně škodlivá a zavedla by například inflaci, všichni by ji přestali používat. Uzly může provozovat každý, kdo přijímá bitcoiny: obchodníci, burzy, poskytovatelé peněženek i obyčejní lidé, kteří používají bitcoiny na cokoliv podle své libosti.

Těžaři

Některé uzly taky těží – vytvářejí bitcoiny, zaznamenávají transakce a díky nim je jakékoliv falšování účetní knihy velmi nákladné. Pokud jsou těžaři jediní, kdo zapisují do účetní knihy, nabízelo by se považovat je za ty, kdo určují pravidla, ale tak to není. Těžaři prostě jen dodržují pravidla daná uzly, které přijímají bitcoiny. Když těžaři začnou vytvářet bloky, které budou obsahovat odměnu navíc, ostatní uzly je nepřijmou, čímž budou tyto mince bezcenné. Každý uživatel provozující uzel se účastní anarchického řízení – volí si, která pravidla musí splňovat mince, kterou považuje za bitcoin, a jakékoliv porušení těchto pravidel ihned odmítne.

Uživatelé/Investoři

Uživatelé jsou lidé, kteří kupují a prodávají bitcoinovou měnu a provozují uzly. Někteří uživatelé dnes neprovozují vlastní uzly, ale spoléhají se na uzly provozované svým poskytovatelem peněženky, přičemž ten funguje jako jistý zmocněnec pro plnění přání uživatele. Uživatelé prostřednictvím nabídky a poptávky určují, jaká je hodnota mince na volném trhu. I kdyby se těžaři a burzy tajně dohodli a zavedli nějakou radikální změnu jako například inflaci, uživatelé by pravděpodobně měnu řídící se těmito

novými pravidly zavrhli, čímž by snížili její cenu, a útočníci by tak přišli o svůj byznys. Menšina uživatelů by tak svým odmítnutím mohla zachránit svou verzi bitcoinu podle původních pravidel.

Vývojáři

Bitcoin Core je nejpoužívanějším bitcoinovým klientem. Vytvořil si okolo sebe bohatý ekosystém stovek nejlepších kryptovývojářů a společností. Projekt Core je velmi konzervativní, protože tenhle software je základem sítě, která má v současnosti hodnotu víc než 100 miliard dolarů. Každý nápad na větší změnu prochází procesem zvaným návrh na vylepšení Bitcoinu (Bitcoin Improvement Proposal)* a jakékoliv změny kódu podléhají přísnému expertnímu posuzování. Proces zlepšovacích návrhů a revizí kódu je naprosto veřejný. Kdokoliv se může zapojit, komentovat nebo předložit kód. Když se vývojáři začnou chovat škodlivě a zavedou něco, co nikdo nebude chtít používat, uživatelé prostě přejdou na jiný software. Možná zůstanou u starší verze nebo začnou vyvíjet něco nového. Proto musejí vývojáři Bitcoin Core dělat jen takové změny, o které uživatelé obecně stojí, jinak riskují, že software ztratí svůj status základní implementace, pokud ho nikdo nebude chtít používat.

Změny pravidel a forky (rozvětvení sítě)

Teď už byste měli mít dobrou představu, jak bitcoinový software zajišťuje dodržování pravidel, na kterých se lidé shodli, a jak se lidé můžou vybírat software a tím upevňovat pravidla, s nimiž souhlasí.

---

* Víc o tom, jak vypadá proces vývoje Bitcoin Core, najdete v textu Jamesona Loppa Who Controls Bitcoin Core?: medium.com/@lopp/who-controls-bitcoin-core-c55coaf91b8a.

Těžaři si volí pravidla, kterými se budou řídit při vytváření bloků, ale musí těžit takové bloky, jaké chtějí uživatelé, jinak riskují odmítnutí svých bloků a tím pádem i ztrátu své odměny.

Víme taky, že bitcoinový software přijímá vždy řetězec s největším platným celkovým důkazem o vykonané práci jako jediný pravý řetězec a že někdy souběžnou produkcí bloků přirozeně vznikají forky (rozvětvení sítě).

Pravidla Bitcoinu byla kvůli velké rozmanitosti účastníků sítě stanovena poměrně pevně už na samém počátku. Jediné upgrady, kterými Bitcoin zatím prošel, jsou zpětně kompatibilní a zachovávají tak základní všeobecně sdílená pravidla i pro uzly bez upgradované verze.

Pojďme se teď podívat na to, jak se pravidla můžou změnit. Úmyslné forky vznikají, když se někteří uživatelé a/nebo těžaři rozhodnou, že nesouhlasí se současnými pravidly Bitcoinu a že je potřebují změnit. Zatím byly zaznamenány dva druhy forků měnících pravidla: tzv. soft forky (měkká rozvětvení), které jsou zpětně kompatibilní, a hard forky (tvrdá rozvětvení), které zpětně kompatibilní nejsou. Nejprve si je popíšeme teoreticky a potom se podíváme na příklady z historie.*

Soft fork je zpětně kompatibilní změna všeobecně sdílených pravidel Bitcoinu, která tato pravidla zpřísňuje. To znamená, že pokud provozujete starý uzel, který nepřešel na nová pravidla, bloky vytvářené podle nových pravidel pro něj budou přesto platné. Jasnější to bude na příkladu.

12. září 2010 bylo do softwaru zavedeno nové pravidlo: Bloky můžou být nanejvýš 1 MB velké. Cílem bylo zabránit spamování v řetězci bloků. Do té doby mohly být platné bloky jakkoliv velké. Podle nového pravidla jsou platné jen menší bloky, pravidla se

---

* Celá historie bitcoinových forků měnících pravidla je rozebrána tady: blog.bitmex.com/bitcoins-consensus-forks/.

tedy zpřísnila. Pokud jste provozovali starý uzel a neupgradovali ho, podle vašich starých pravidel byly nové, menší bloky pořád platné, změna se vás tedy nijak nedotkla.

Soft fork je nenásilným způsobem, jak upgradovat systém, protože umožňuje provozovatelům uzlů upgradovat postupně a dobrovolně v průběhu času. Pokud neupgradují, přesto budou moci zpracovávat všechny nově příchozí bloky jako dřív. Jen těžaři, kteří bloky vytvářejí, musejí upgradovat, aby mohli vytvářet bloky podle nových pravidel. Jakmile těžaři upgradovali na 1MB soft fork, všechny bloky od té chvíle byly maximálně 1 MB velké. Pro uživatele používající starou verzi systému se nezměnilo vůbec nic.

V případě hard forku se zavádí změna, která není zpětně kompatibilní. Hard fork je rozšíření souboru pravidel, podle kterého se původně neplatné bloky nově považují za platné. Staré uzly, které neupgradují, nebudou moci zpracovávat bloky vytvářené podle nových pravidel, protože je budou brát jako neplatné. Pokud neupgradují, uvíznou na starém řetězci.

Hard forky, na kterých by se téměř jednomyslně shodly všechny uzly v síti, by nepůsobily žádné potíže. Každý uzel by okamžitě upgradoval na nová pravidla. Pokud by zůstalo pár opozdilců, nedostávali by žádné nové bloky, zjistili by, že jejich software přestal fungovat, a nezbylo by jim nic než upgradovat. Teoreticky.

V praxi hard forky nikdy neprojdou hladce. Ve skutečně decentralizovaném anarchickém systému nemůžete přesvědčit každého k přijetí nových pravidel. V srpnu 2017 někteří lidé nebyli spokojeni s tím, jak se bitcoinový řetězec vyvíjí ve vztahu k malým platbám. Rozhodli se, že chtějí vytvořit řetězec s většími bloky. V Bitcoinu v té době na základě soft forku z roku 2010 platilo pravidlo, že bloky nesmějí být větší než 1 MB. Někteří lidé chtěli vytvořit nový řetězec s většími bloky. Tenhle fork vstoupil do dějin pod názvem Bitcoin Cash.

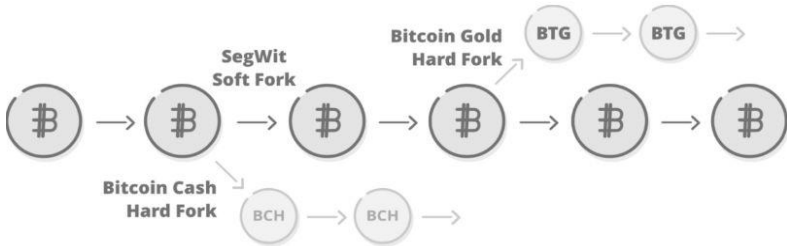
Hard fork bez všeobecné shody, jako je Bitcoin Cash, na který nepřistoupí všichni těžaři a všechny uzly, vytvoří nový řetězec bloků. Tenhle řetězec sdílí historii s původním řetězcem včetně existující sady UTXO (zůstatků účtů) až do chvíle vzniku forku. Avšak mince, které na této větvi vznikly po forku, se už nepovažují za bitcoiny, protože je nepřijímají žádné uzly sítě Bitcoin.

Po forku Bitcon Cash se celý rok vzrušeně debatovalo, co je a co není bitcoin. Někteří lidé na straně Bitcoinu Cash tvrdili, že bitcoin by měl být vymezen podle toho, co píše Satoshi ve svém původním deset let starém článku. Na podporu svého stanoviska z článku vybírali určitá specifická slova. Jenže v systémech založených na všeobecné shodě argumenty autoritou neplatí. Takové systémy fungují na základě kolektivního jednání mnoha jednotlivců včetně rozhodování, jaký software používat a kterou minci prodávat nebo kupovat na volném trhu.

V případě tohoto forku lidé provozující naprostou většinu uzlů – tedy peněženky, burzy, obchodníci a ostatní – nechtěli měnit svůj software za něco podporovaného mnohem menším a méně zkušeným týmem vývojářů, zajištěného mnohem nižším hash rate. Lidé neměli pocit, že by takovýto „upgrade" stál za narušení celého ekosystému. Problém hard forků je v tom, že uspějí jen tehdy, když na ně přejdou všichni. Pokud zůstanou nějací opozdilci, vzniknou dva druhy mincí. Bitcoin proto zůstal bitcoinem, a Bitcoin Cash se stal samostatným druhem mince. Protože všichni, kdo před forkem vlastnili bitcoiny, měli nárok na Bitcoin Cash zdarma, mnoho lidí prodalo mince za „peníze zdarma", což snížilo jejich hodnotu.

Dnes existují desítky dalších větví bitcoinu, jako Bitcoin SV (který sám vznikl rozvětvením Bitcoinu Cash), Bitcoin Gold, Bitcoin Diamond či Bitcoin Private. Každá z nich je zajištěna velmi nízkým hash rate, malou vývojářskou aktivitou a v podstatě žádnou aktivitou na řetězu a likviditou. Jejich nízká likvidita z nich dělá snadné terče pro rychlý nákup a prodej, což často vede k raketovému nárůstu ceny následovanému stejně velkolepým a ničivým pádem.

Mnoho z nich se stalo obětí hackerských útoků na peněženky, terčem 51% útoků a jiných katastrof. Některé z těchto větví jsou vyložené podvody nebo prostě lákadla na gamblery. Většina z nich je v určitém aspektu svého designu částečně centralizována. Webové stránky forkdrop.io v současnosti evidují 74 rádoby Bitcoinů.



Mince ze soft forku můžou být posílány starším uzlům. Hard fork vytváří nové zpětně nekompatibilní UTXO nepřijatelná pro staré uzly.

Podobný kód jako Bitcoin používá i spousta jiných mincí, například Litecoin nebo Dogecoin, ale ty mají svou účetní knihu založenou od prvního bloku a nepřevzaly sadu UTXO z Bitcoinu. Přestože tyto mince mají s Bitcoinem společnou velkou část zdrojového kódu, obvykle se nepovažují za jeho forky, protože nesdílejí jeho historii zůstatků na účtech.

Bitcoinové forky nemají vliv na limit 21 milionů bitcoinů stanovený pro Bitcoin samotný: Představte si, že byste uložili veškeré světové zlato v superzabezpečeném Fort Knoxu s těžce ozbrojenými strážemi. Pak postavíte malou chatrnou boudu s názvem Fort Knox Lite a postavíte před ni jediného strážného. Vezmete nějaké kameny, nabarvíte je nazlato a uložíte je do boudy.

Potom oznámíte světu, že jste vytvořili „rozvětvení zlata", a každému vlastníkovi zlata dáte zdarma stejné množství kamení z vaší boudy.

Bitcoin musí střežit mnoho těžařů, čímž se prodražuje 51% útok. Fork Bitcoinu, který má jen pár těžařů, je podobně jako naše

špatně hlídaná bouda snadno napadnutelný. Jeho zdrojový kód nejspíš nemá solidní strukturu, napsal ho malý nezkušený tým vývojářů a má slabé expertní posuzování, podobně jako vaše bouda. Mince z forků nejsou přijímány žádnými existujícími uzly, protože porušují pravidla Bitcoinu. Stejně tak lidé, kteří mají k dispozici chemické testy zlata, nebudou přijímat obarvené kamení. Cena výroby mincí na forku i kamení je nulová, protože jste je dali všem vlastníkům zadarmo. To všechno snižuje zájem trhu o forky Bitcoinu.

Když se podíváte na ty tisíce vzniklých klonů Bitcoinu, z nichž žádný nemá významnou tržní hodnotu, zamyslete se nad následujícím paradoxem: vytváření bitcoinových forků je bezplatné a snadné. Změnit pravidla Bitcoinu a vytvářet nové bitcoiny je naopak velmi obtížné. Až se vás příště bude někoho s omezenými znalostmi o Bitcoinu ptát, čím je Bitcoin tak jedinečný, budete vědět, co mu odpovědět.

Decentralizovaná povaha ekosystému Bitcoinu vytváří silnou preferenci pro status quo. Velké změny znamenají měsíce nebo roky budování všeobecné shody, diskusi a implementaci expertního posuzování. Je to tak dobře a je to něco, co bychom po systému, který se snaží být globálními penězi, měli chtít. Bitcoin je opatrné našlapování mezi tisíci uživatelů, z nichž každý se chová sobecky, a jejichž zájmy často jdou proti sobě. Je to opravdu anarchický systém volného trhu, který nikdo neřídí.

KAPITOLA 9

Co dál?

Je Bitcoin MySpacem kryptoměn?

Proč jsem napsal knihu o Bitcoinu, když jsem mohl psát o celém ekosystému kryptoměn? Neexistují snad tisíce jiných mincí? Čím je Bitcoin tak zvláštní, kromě toho, že je první decentralizovanou kryptoměnou? Není pomalejší a nemá méně vychytávek než jeho modernější konkurence?

To jsou otázky, které často kladou lidé, kteří se Bitcoinem teprve začali zabývat. Když pochopíte základy fungování Bitcoinu, další logickou otázkou bývá: „Technologie řetězce bloků je zajímavá. Jak můžeme vědět, že se neobjeví lepší verze a nepromění Bitcoin v MySpace kryptoměn?"

Společnosti si vždy snaží vytvořit konkurenční výhodu, která ostatním hráčů ztěžuje boj. MySpace měl obrovskou uživatelskou základnu s přátelskými vztahy. Lidé by nezačali používat konkurenční služby, kdyby na nich už nebyli jejich přátelé. Přestože je dobře propojený sociální graf obrovskou konkurenční výhodou, nezabránilo to Facebooku v tom, aby MySpace během pouhých několika let naprosto převálcoval.

Bitcoin má mnohem, mnohem větší konkurenční výhodu, než měl MySpace. Abychom ji pochopili, podívejme se, co by obnášelo pro některého z konkurentů, aby Bitcoin nahradil.

Prodejnější a likvidnější měna

Nejdřív je potřeba pochopit, že analogie s MySpace a Facebookem kulhá, protože můžete mít bezplatně účet zároveň jak na Facebooku, tak na MySpace. Mnoho lidí to tak taky v přechodovém období z jednoho média na druhé mělo. Když počet lidí na Facebooku překročil určitou kritickou hranici, lidé přestali MySpace používat.

Jenže peníze takhle nefungují. Když máte bitcoiny v hodnotě jednoho dolaru, je to hodnota jiné měny, kterou nevlastníte. Musíte se vědomě rozhodnout jednu měnu prodat a nakoupit jinou. Nemůžete uchovávat stejnou hodnotu v obou měnách zároveň. Teď si položte otázku: proč byste chtěli držet jinou měnu než tu nejlikvidnější a nejšířeji přijímanou? Jedinou možnou odpovědí je spekulace. Pokud se vám nepodaří posunout celou ekonomiku vaším směrem a přimět všechny, aby koupili vaši alternativní minci, není žádný jiný způsob, jak by se mohla stát dominantní.

Likvidita Bitcoinu je v porovnání se všemi jeho konkurenty nepoměrně vyšší. K dnešnímu dni je tržní kapitalizace Bitcoinu (celková hodnota všech bitcoinů) podle messari.io/onchainfx okolo 160 miliard dolarů. Tržní kapitalitace největšího konkurenta Bitcoinu, kterým je Ethereum, je pouhých 30 miliard dolarů. A to ani nebereme v úvahu reálnou likviditu, tedy množství měny, které byste mohli reálně prodat bez výrazného poklesu ceny.

Likvidita je jako sněhová koule. Držení nejlikvidnější měny má za následek zájem ostatních lidí, což opět zvyšuje likviditu. Držením jakékoliv jiné měny než té nejlikvidnější trestáte sami sebe, zatímco čekáte, až všichni ostatní udělají to samé. Ekonomické motivace nehrají ve prospěch přesunu likvidity ke konkurenci ze dne na den.

Dosáhnout zajištění ve výši přes 100 miliard dolarů v průběhu deseti let

Shodou okolností se Bitcoin vyšvihl z bezcenného internetového geekovského experimentu, který nikoho nezajímal, přes koupi pizzy za 10 000 bitcoinů, až na svou vrcholnou cenu 20 tisíc dolarů za bitcoin. Celé se mu to podařilo poměrně nenápadně, aniž by mu kdokoliv šlapal na paty. Během té doby si za léta útoků vybudoval celosvětový imunitní systém a vytvořil největší síť hashovací síly na světě. Za celých deset let, během kterých dosáhl zajištění ve výši víc než 100 miliard dolarů, se ho nepodařilo hacknout.

Dnes je téměř nemožné nenápadně založit novou kryptoměnu. Princip kryptoměn už není žádným tajemstvím a všechny triky jsou už známé. Podívejme se například na alternativní řetězec bloků EOS s hodnotou okolo 10 miliard dolarů při svém vzniku a dnes s hodnotou přibližně poloviční. Dva dny po spuštění úplně zamrzl kvůli chybám ve zdrojovém kódu. Chyby byly opraveny během několika hodin s minimálním dohledem nebo kontrolou. Vložíte 100 miliard dolarů do takové sítě? Možná tu EOS za 10 let ještě bude, ale tou dobou už Bitcoin bude mít za sebou 20 let a bude zajištěn biliony dolarů.

Ubránit se útokům ze strany stávající hashovací síly

Existují tisíce měn, které používají desítky hashovacích algoritmů, a všem novým měnám hrozí 51% útoky ze strany stávající hashovací síly. K útoku již došlo v Bitcoinu Gold a několika dalších měnách.

Nový konkurent musí buď přežít útoky ze strany stávající hashovací síly, nebo používat algoritmus, který nemá žádné specializované ASIC zařízení. Když neexistují žádné ASICy, systém může být snadno napaden s použitím komoditních grafických procesorů, které jsou volně dostupné. Nový konkurent taky nemůže začít zajištěním vysoké hodnoty od prvního dne, jako to udělal EOS, což je lehkomyslné a je to dobrý způsob, jak se dostat do centralizovaného

chování. To tedy znamená, že nový konkurent nemůže vybírat peníze, ale musí začít od nuly podobně jako Bitcoin a pomalu stoupat na hodnotě, aby mohl úměrně tomu budovat svůj bezpečnostní model. Když však poroste pomalu, nemůže kvůli pozdějšímu startu dohnat uživatelskou základnu Bitcoinu ani jeho likviditu.

Být vysoce decentralizovaný

Velká část bezpečnostního modelu bitcoinové sítě vychází z vysoké míry decentralizace. To znamená, že protokol je obtížně změnitelný, a proto lze věřit, že bude ctít vlastnosti přislíbené ve zdrojovém kódu (omezené množství atd.). Tato vlastnost se prokázala, když se mnoho společností a těžařů domluvilo a chtělo prosadit změnu velikosti bloku a posunout protokol určitým směrem.* Uživatelé jejich fork odmítli a celá snaha ztroskotala.

Vysoce decentralizovaným konkurentem jednoduše nemůže být žádná společnost nebo tým založený osobami, jejichž identitu známe, protože by to případného konkurenta ihned učinilo zranitelným a vydíratelným. V úvahu nepřicházejí ani veškeré měny ochotné „postupovat rychle a přes mrtvoly", protože to lze, jen když jste centralizovaní. Jakýkoliv konkurent se buď pohybuje rychle a centralizuje se, nebo se pohybuje pomalu a nikdy Bitcoin nedožene.

---

* Tady si přečtěte víc o forku Segwit2X, který prošel zákulisními dohodami a nakonec byl odvolán: bitcoinmagazine.com/articles/now-segwit2x-hard-fork-has-really-failed-activate.

Přilákat nejlepší vývojáře na světě

Linux vytvořil smršť aktivity, která zabránila ostatním -nixovým systémům* v tom, aby ho předstihly – a Bitcoin udělal to samé. Komunita kolem něj se den za dnem rozrůstá a na základě Bitcoinu vznikají nové společnosti nabízející nové služby. Tomuto exponenciálně se rozrůstajícímu jádru, do kterého patří i desítky společností, vzdělávacích programů a konferencí, by konkurent musel ukrást talentované vývojáře.

Vybudovat celosvětovou finanční síť

Bitcoin je podporován stovkami burz po celém světě, termínovanými komoditami a jinými finančními deriváty u velkých hráčů, jakými jsou Chicago Mercantile Exchange, stovkami investičních fondů a obchodních kanceláří a sítí lidí, kteří Bitcoin již používají jako alternativu k měnám, které selhaly, jako například venezuelský bolívar. Případný konkurent Bitcoinu by všechno toto musel vybudovat, aby Bitcoin překonal.

Instituce jako Chicago Mercantile Exchange nebudou nabízet kdejakou měnu, aniž by byla podepřena velkým objemem probíhajících obchodů. Takové společnosti byste museli přesvědčit, aby tohoto nového konkurenta přijali namísto Bitcoinu. Konkurenta, který je pravděpodobně hůř zajištěný, méně likvidní, má méně schopné vývojáře a už z definice je ve světě méně používaný. To je hodně strmá skála, kterou by musel případný konkurent zdolat.

---

* Operační systémy vycházející ze systému Unix. Jako takové mají většinou otevřený zdrojový kód a tvoří základ mnoha operačních systémů se širokým použitím od datových serverů až po osobní počítače. Prominentním -nixovým systémem je operační systém Linux.

Fungovat jako bezpečnější peníze

Existuje mylný názor, že Bitcoin má být rychlým a levným způsobem, jak posílat peníze. Je jasné, že jím být nemůže už z podstaty svých základních vlastností zahrnujících účetní knihu, jejíž kopie se vytvářejí po celém světě. Nicméně, možnost používat bitcoin jako bezpečné peníze odolné vůči cenzuře byla prokázána a zájem o ni roste.

Cokoliv jiného, jako například zlevnění plateb, je spíš třešničkou na dortu. Většina rádoby konkurentů si pořád myslí, že musí umožnit rychlé platby, což už však dělají desítky centralizovaných společností po celém světě a dělají to docela dobře. Taky to řeší rychle rostoucí Lightning Network budovaná na Bitcoinu.

Soupeřit v oblasti bezpečných peněz vyžaduje naprostou decentralizaci a vlastnosti, které jsou opravdu těžko změnitelné a napadnutelné. Naneštěstí jiné měny v této oblasti soupeřit nemůžou už jen proto, že je většinou vytvořily centralizované týmy a vidina zisku, a ne šťastná náhoda pomalu rostoucího ekosystému vytvořeného cypherpunkery.

Budoucí vývoj Bitcoinu

Zatím jsme společně prošli vymýšlením protokolu. Teď nahlédněme do budoucnosti a podívejme se na některá chystaná vylepšení Bitcoinu.

Bitcoin jsou programovatelné peníze, na nichž můžeme stavět řadu dalších služeb. To je úplně nový koncept a my teprve začínáme poznávat všechny možnosti, které s sebou přináší.

Lightning Network

Bitcoin měl v minulosti potíže s vysokými poplatky, když se prostor v blocích stával stále žádanějším. Dnes Bitcoin zvládá

jen asi 3 až 7 transakcí za vteřinu. Toto číslo je vypočteno podle maximálního počtu transakcí, které se vejdou do jednoho bloku. Nezapomínejte však, že každá transakce může díky sdružování ve skutečnosti představovat platby pro miliony lidí. Přesto kapacita Bitcoinu nestačí na to, aby se stal globální platební sítí.

Naivním řešením by bylo zvýšení velikosti bloku a některé konkurenční měny včetně Bitcoinu Cash tenhle přístup skutečně zkusily. Bitcoin se touto cestou nevydal, protože zvyšování velikosti bloku by negativně ovlivnilo decentralizovanou povahu sítě, jako například počet uzlů a jejich rozptýlení po světě. I kdyby bylo zvětšení bloku možné díky vylepšení hardwaru, pořád by byl problém v tom, že kvůli decentralizované povaze Bitcoinu by hard fork, který by se pokusil změnit velikost bloku, způsobil velké narušení a pravděpodobně odštěpení další měny.

Zvětšení velikosti bloku by navíc doopravdy neřešilo problém vhodnosti Bitcoinu jako celosvětového platebního systému – tak moc by to stejně nepomohlo. Na scénu tak vstupuje Lightning Network: nový protokol a sada softwarových implementací, které vytvářejí bitcoinové transakce mimo řetězec a do řetězce bloků se pravidelně připisují. O Lightning Network by se dala napsat celá kniha, ale my ji probereme jen krátce.

Myšlenka Lightning Network spočívá v tom, že ne všechny transakce musí být zapsány v řetězci bloků. Když si například v baru kupujeme drinky, můžeme si otevřít účet, který vyrovnáme až na konci večera. Nedává moc smysl, abychom platili kartou při každém drinku, protože by to bylo plýtvání časem. V případě Bitcoinu není právě praktické a z hlediska soukromí ani bezpečné, aby každou platbu za kávu nebo pivo zaznamenávaly tisíce počítačů na celém světě s využitím elektrické energie odpovídající spotřebě celé jedné země.

Lightning Network, pokud bude úspěšná, vyřeší několik stávajících nedostatků Bitcoinu:

- Takřka neomezená průchodnost transakcí. Můžete provést stovky tisíc mikroplateb a do řetězce bloků je pak zapsat až jako konečné vyúčtování.
- Okamžité potvrzení platby. Není potřeba čekat na vytěžení dalších bloků.
- Minimální transakční poplatky jsou vhodné pro mikroplatby jako třeba pár korun za přečtení článku na blogu.
- Zvýšené soukromí. O transakci vědí jen její účastníci na rozdíl od transakcí zapisovaných přímo do řetězce, které se vysílají do celého světa.

Lightning využívá koncept platebních kanálů, což jsou skutečné bitcoinové transakce zapisované přímo do řetězce, které zablokují určité množství bitcoinů a zpřístupní je v rámci Lightning Network pro okamžitý, téměř bezplatný přesun. Lightning Network je teprve v počátečním stádiu, ale vypadá slibně. Stránku, která používá mikroplatby založené na Lightning Network pro placení za články, si můžete prohlédnout tady: yalls.org/.

Bitcoin ve vesmíru

Bitcoin je skvělý ve své odolnosti vůči cenzuře a je taky odolný vůči zabavení (můžete ho přenášet ve své hlavě). Jeho převody nepodléhají cenzuře, protože k zaznamenání vašich transakcí stačí jediný poctivý těžař v celé síti (a tím těžařem můžete být vy).

Jenže vzhledem k tomu, že se Bitcoin přenáší přes internet, může podléhat cenzuře na úrovni sítě. Autoritářské režimy, které by chtěly omezit jeho aktivitu, by se mohly pokusit bránit bitcoinovému provozu vstupovat do jejich země a opouštět ji.

Síť Blockstream Satellite je prvním pokusem obejít možnou cenzuru na úrovni jednotlivých zemí a zároveň dosáhnout na místa bez přístupu k internetu. Tenhle satelitní systém umožňuje komukoliv, kdo má satelit a relativně levné vybavení, aby se připojil a stáhl si bitcoinový řetězec bloků. Chystá se i obousměrná komunikace. Existují taky snahy vytvářet netradiční sítě jako například TxTenna. Ve spojení se satelitním připojením by byl podobný systém téměř nezadržitelný.

Kam dál

A je to. Prošli jste si celým vynálezem Bitcoinu a snad jste se vynořili v říši za zrcadlem připraveni na další objevy. Kam tedy dál? Tady je pár zdrojů, které můžete prozkoumat:

Tady se dozvíte víc o ekonomické stránce Bitcoinu:

- The Bitcoin Standard od Saifedeana Ammouse
- Bitcoin Investment Theses od Pierra Rocharda medium.com/@pierre_rochard/bitcoin-investment-thesees-part-1-e9767ob5389b
- The Bulish Case for Bitcoin od Vijaye Boyapatiho medium.com/@vijayboyapati/the-bullish-case-for-bitcoin-6ecc8bdecc1
- Pro děti: Bitcoin Money od Michaela Carase (aka The Bitcoin Rabbi)

Tady se můžete ponořit hlouběji do informatiky:

- The Bitcoin Whitepaper od Satoshiho Nakamota bitcoin.org/bitcoin.pdf
- Mastering Bitcoin od Andrease Antonopoulose
- Programming Bitcoin od Jimmyho Songa
- Seminář Jimmyho Songa na programmingblockchain.com

Tady se dozvíte víc o historii a filozofii Bitcoinu:

- Planting Bitcoin od Dana Helda medium.com/@danheld/planting-bitcoin-sound-monez-72e8oe4off62
- Bitcoin Governance od Pierra Rocharda medium.com/@pierre_rochard/bitcoin-governance-37e8629947of
- Bitcoin Past and Future od Murada Mahmudova blog.usejournal.com/bitcoin-past-and-future-45d92b318of1
- Jakékoliv video od Andrease Antonopoulose, obzvláště Currency Wars a The Monument of Immutability, na youtube.com/user/aantonop

Ohromná část bitcoinového ekosystému žije na Twitteru. Tady je pár lidí (na pořadí nehleďte), které je dobré sledovat. Začněte s těmihle, a určitě objevíte i další:

@lopp	@Excellion
@pwuille	@starkness
@adam3us	@dickerson_des
@danheld	@roastbeef
@TraceMayer	@saifedean
@pierre_rochard	@Melt_dem
@bitstein	@_jillruth
@theonevortex	@giacomozucco
@AlenaSatoshi	@snyke
@WhatBitcoinDid	@aantonop
@stephanlivera	@MustStopMurad
@TheBlock___	@danheld
@TheLTBNetwork	@peterktodd
@real_vijay	@dergigi
@jimmysong	@skwp (to jsem já!)

Víc si ode mě můžete přečíst na yanpritzker.com.

Uvidíme se za zrcadlem.

Poděkování

Mé díky patří všem těm, kteří mi poskytli zpětnou vazbu během přípravy prvního náčrtu této knihy, především Joeovi Leveringovi, Philu Geigerovi, Yurymu Pritzkerovi, Jonathanu Wheelerovi, Walteru Rosenbergovi, Michaelu Santosuossovi a Davidu Hardingovi.

Děkuji Jimmymu Songovi za seminář Programování řetězce bloků, který mě nakopnul k tomu, abych dal dohromady tenhle text.

O autorovi

Yan Pritzker posledních 20 let pracuje jako vývojář a startupový podnikatel. Naposledy byl spoluzakládajícím CTO projektu Reverb.com, kde v letech 2012–2018 řídil technologické oddělení a infrastrukturu. Dnes se věnuje vzdělávání v oblasti Bitcoinu a konzultacím pro začínající startupy.

Yan píše o Bitcoinu a příbuzných tématech na yanpritzker.com.

Můžete ho taky sledovat na Twitteru: @skwp.

Glosář

ASIC

Application-Specific Integrated Circuit (česky též zákaznický integrovaný obvod) je v kontextu Bitcoinu speciální hardware sloužící výhradně jako těžební zařízení. Tyto jednoúčelové stroje jsou navrhnuty k počítání hashovacích algoritmů, odvádějí tak důkaz o provedené práci, který je základem bitcoinového ekosystému. V současnosti představují jediný efektivní způsob těžby Bitcoinu, který nahradil dříve používané grafické karty a klasické procesory.

BIP

(Bitcoin Improvement Proposal) je dokument navrhující zlepšení technologie Bitcoinu. Vzhledem k open source povaze Bitcoinu může návrh na vylepšení vznést kdokoliv, případné změny ale musí projít procesem schvalování, na kterém se podílí celá bitcoinová komunita. Jednotlivé návrhy se číslují ve formátu: BIP a číslo značící pořadí, v jakém byly přijímány, např. BIP 0310.

Bitcoin

Bitcoin (psáno s velkým písmenem na začátku) označuje celou sérii konceptů a technologií, které tvoří bitcoinový ekosystém. Konkrétně zahrnuje samotný bitcoinový protokol, decentralizovanou peer-to-peer síť, veřejnou knihu transakčních záznamů (blockchain),

decentralizovaný matematický a deterministický mechanismus emise nových bitcoinů (distribuovaná těžba a koncept proof-of-work) a decentralizovaný systém ověřování transakcí (transakční skript).

bitcoin

Jednotkou virtuální měny Bitcoin je jeden bitcoin (psáno s malým písmenem). Vzhledem k tomu, že celkový počet bitcoinů je omezen na 21 milionů, používá se ještě pojem satoshi, což je dílčí jednotka o hodnotě jedné stomiliontiny bitconu.

bitcoinový klient / bitcoinový software / program Bitcoin

Program, který si koncový uživatel sítě Bitcoin instaluje na svém zařízení. Klient je program k provozování bitcoinového uzlu a zahrnuje v sobě několik funkcí: předně uchovává kopii transakčních knih (to jest celý blockchain) a slouží tak jako záruka transparentnosti sítě. Některé klienty navíc mohou sloužii jako peněženka. Dnes existují bitcoinové klienty jak pro osobní počítače, tak i pro mobilní zařízení.

blockchain

Blockchain, v překladu řetězec bloků, je kontinuálně budovaná databáze všech transakčních bloků od prvního bloku vytěženého Satoshim až po ten právě těžený. Blockchain je decentralizovaný, jeho kopie jsou uchovány v uzlech rozesetých po celém světě. Vzájemná provázanost bloků znemožňuje zpětnou manipulaci s platbami a dvojí utrácení.

býčí trh (bull market)

Značí trh se vzestupnou tendencí, kdy hodnota daného aktiva stoupá. Trh tak typicky láká nové investory a poptávka převyšuje

nad nabídkou. Příkladem býčího trhu v Bitcoinu je rok 2017, kdy se hodnota jednoho bitcoinu vyšplhala až na 20 000 $.

cypherpunk

Hnutí vzniklé v osmdesátých letech, jehož členové kladli velký důraz na absolutní soukromí zajištěné kryptografickými technologiemi.

časové razítko (time stamp)

Mnoho služeb a produktů online vyžaduje při svém vzniku označení přesným časovým razítkem. Od přesného času vydání příspěvku na blogu, označení digitální fotografie po textový editor evidující, jak změny proběhly v čase. V technologii Bitcoinu se časová razítka přidělují k transakcím v rámci bitcoinové sítě a evidují, kdy byly utracené. Časové razítko zároveň pomáhá zamezit nekalé manipulaci s blockchainem.

dvojí útrata (double spend)

Situace, kdy se ty samé bitcoiny uživatel pokusí utratit vícekrát. Vyřešení problému dvojité útraty tím, že jsou transakce zapisovány do blockchainu, je hlavní technologický přínos Satoshiho Nakamota.

důkaz o vykonané práci (proof of work, PoW)

Data, pro které je možné snadno ověřit, že splňují nějakou specifickou vlastnost, ale pro jejichž vytvoření není známý žádný efektivní postup. Data naopak musíme vytvořit ‘neefektivním’ způsobem, při kterém je vynakládána faktická práce (v podobě času, výpočetního výkonu či elektřiny k němu potřebné). Výsledná data pak lze chápat jako důkaz, že někdo vykonal práci pro nalezení takových dat. Kritickou vlastností mechanismu proof of work je pak právě neschopnost “zjednodušit” si práci například nějakým chytrým trikem nebo zrychleným výpočtem. V případě Bitcoinu

se jedná o počítání hashe hlavičky bloku (číslo), který musí mít menší než stanovenou hodnotu. Je triviální ověřit, že pro konkrétní hlavičku je podmínka splněna – stačí porovnat spočítaný hash s daným číslem. Ale není jednoduché najít takovou hlavičku, pro kterou po zahashování dostaneme očekávaný výsledek, protože výsledek hashovaci funkce se chová zcela náhodně. Při hledání vhodného hashe tak nezbývá nic jiného, než opakovaně zkoušet hashovat různé vstupy.

escrow

Forma kontraktu, ve které figuruje prostředník (escrow agent) zprostředkovávající transakci mezi dvěma stranami, které by si případně nedůvěřovaly. Escrow agent může držet prostředky, dokud se obě strany nedohodnou. V technologii Bitcoinu je tohoto mechanismu použito při ověřování podpisů u multisig adres.

fork

Rozvětvení blockchainu na více paralelních větví, kdy některý z bloků má více než jednoho následovníka. Pojem fork se ale často používá přeneseně jako změna v softwaru nebo pravidlech blockchainu, která vede nebo může vést k rozvětvení blockchainu. Změny v pravidlech blockchainu rozlišujeme tzv. soft forky a hard forky.

hash

Digitální otisk. Otisk je stejně dlouhý pro libovolně dlouhý vstup (a samozřejmě pak více vstupů vede na jiný otisk). U Bitcoinu se používají kryptograficky bezpečné hashe. Ty mají tu vlastnost, že z výsledného hashe nelze zjistit původní vstup, kromě vyzkoušení všech možností. Jedním z důsledků je, že nikdo není efektivně schopen vytvořit dva různé vstupy dávající stejný hash. I když

podobných kolizí samozřejmě existuje obrovské množství, není v praxi možné dva takové vstupy získat.

hash rate

Výpočetní výkon, respektive počet vypočtení hashů za sekundu. Hash rate se uvádí pro jednotlivá těžební zařízení (minery) jako počet hashovacích operací (řešení algoritmu SHA-256) za vteřinu. Výkon všech zapojených zařízení zároveň tvoří hash rate celé bitcoinové sítě.

hard fork

Změna v protokolu, která není zpětně kompatibilní s předchozími verzemi pravidel Bitcoinu. Hard fork tak představuje trvalé rozvětvení sítě na dva separátní blockchainy. Příkladem hard forku je odštěpení Bitcoin Cash v roce 2017.

hierarchická deterministická peněženka (hierarchical deterministic wallet)

Zkracováno též jako HD Wallet, je typ kryptografické peněženky, která soukromý klíč generuje z řetězce náhodných slov, tzv. seedu. K obnovení přístupu tak není nutné peněženku neustále zálohovat, ale stačí si zapamatovat původní seed. Její hierarchický rozměr spočívá v možnosti z původního seedu vytvořit odvozené peněženky s různou mírou přístupových práv.

medvědí trh (bear market)

Trh se sestupnou tendencí, kdy hodnota daných aktiv klesá a investoři trh opouštějí s obavami před ještě větším propadem. Opakem je takzvaný býčí trh (Bull market).

mempool (memory Pool)

Místo v softwarové paměti uzlu, kde bitcoinová transakce po zkontrolování čeká, než si ji vyzvedne nějaký těžař a zařadí do bloku, aby tak byla potvrzena. Ne každá transakce, která čeká v mempoolu, musí být automaticky zařazena do bloku, pokud uzly shledají, že transakce nesplňuje zadaná kritéria, odmítnou ji.

multisig adresa

Multisig neboli adresa s více podpisy má více než jeden privátní klíč. Používá se v případě, kdy k jedné peněžence má přístup více uživatelů. K odeslání transakce je pak potřeba podpis více než jednoho držitele klíče.

nonce

Nonce v kryptografii značí číslo, které se používá jako jednorázová hodnota přinášející náhodný element. Takové hodnotě není přisuzován žádný specifický význam, její role spočívá pouze v její libovolnosti a nemožnosti ji odhadnout. Nonce tvoří součást bitcoinového bloku proto, aby bylo možné tuto hodnotu libovolně měnit a zkoušet tak hledat hash hlavičky splňující podmínku pro platný blok.

open source software

Počítačový program s otevřeným zdrojovým kódem, který jeho vývojáři zveřejňují, a je tak komukoliv k dispozici k nahlédnutí a vylepšení. Bitcoin je typickým příkladem open source projektu, jeho protokol navržený Satoshim Nakamotem je neustále vylepšován komunitou vývojářů, jednotlivé návrhy na vylepšení (BIP) jsou pak celou sítí přijímány a začleňovány do původního protokolu.

peer-to-peer

Typ počítačové sítě, kde spolu přímo komunikují jednotliví uživatelé jako peer-to-peer, tedy rovný s rovným, bez přítomnosti centrálního serveru. Uživatelé či uzly na síti jsou si rovnocenné, není tu přítomna žádná centrální autorita. Bitcoin je od počátku koncipován jako peer-to-peer síť.

peněženka (wallet)

Aplikace sloužící k přijímání, posílání a ukládání bitcoinů. Peněženky, ať již ve své softwarové, nebo hardwarové podobě, uchovávají soukromé klíče sloužící pro generování transakčních adres a zejména podepisování transakcí při posílání bitcoinu.

SegWit

(Segregated Witness, volně přeloženo jako oddělené svědectví) je vylepšení bitcoinového protokolu, které přeuspořádává prvky v transakci tak, aby se část transakce (podpis) dala později vypustit. Konsenzus sítě zní, že tato vypustitelná část méně zatěžuje síť, takže se počítá, jako by byla 4x menší. Což má za následek, že se transakce i o stejné velikosti jen díky přesunu podpisu počítá jako menší. Do bloku se tedy vejde více transakcí.

SHA-256

Ze Secure Hash Algorithm, tedy Bezpečný hashovací algoritmus je kryptografická funkce, která z libovolně dlouhého vstupu vytvoří výstup fixní délky. Z výstupu je proto prakticky nemožné rekonstruovat původní vstup, stejně jako narazit na dvě rozdílné zprávy s totožným výstupem. Číslo 256 značí délku výstupu v bitech.

soft fork

Změna v protokolu, která je zpětně kompatibilní s předchozími verzemi pravidel Bitcoinu. Jelikož po provedení soft forku i uzly, které nemají aktualizovanou verzi, uznají nové bloky jako platné, je soft fork zpětně kompatibilní. V praxi nedochází v případě soft forku k rozvětvení sítě, proto se jedná o preferovaný způsob zavádění nových vylepšení do Bitcoinu. Příkladem soft forku je BIP 0141, který zavedl technologii SegWit.

soukromý klíč (private key)

Soukromý klíč je jedním ze dvou přístupových klíčů v asymetrickém šifrování bitcoinových peněženek, je tvořen náhodně vygenerovaným číslem. Jak již název napovídá, soukromý klíč by měl být známý jen majiteli dané peněženky a slouží k podpisu odchozí transakce.

Sybiliny útoky (Sybil attack)

Hackerský útok, při kterém útočník usilující o ovládnutí sítě uživatelů založené na vzájemné důvěře vytvoří velké množství účtů pod falešnými jmény a použije je k získání většiny sítě. Ovládnutí sítě znamená zejména vytvoření iluze pro konkrétní uživatele, že stav sítě je jiný, než ve skutečnosti je, a takto s uživateli manipulovat. Název pochází ze stejnojmenné knihy pojednávající o psychiatrické pacientce s poruchou osobnosti.

tvrdé peníze (sound money)

Tvrdé peníze, tedy takové, u kterých vláda ani jiná centrální autorita nemůže kontrolovat a manipulovat peněžní zásobu.

uzel (node)

Bitcoinový uzel je integrální součást blockchainu. V systému Bitcoin je uzlem každý počítač či zařízení, které se k síti připojí.

Uchovává typicky kopii celého blockchainu, validuje nové bloky a transakce a je skrze něj možné vyslat transakci k ostatním uzlům v síti. Vzhledem k peer-to-peer povaze bitcoinové sítě jsou si všechny uzly rovny.

UTXO

Bitcoinový blockchain nepoužívá účty, na kterých někdo hlídá účetní zůstatek, ale pracuje s takzvaným modelem UTXO (Unspent Transaction Output – neutracených transakčních výstupů). Jednou z možných analogií, jak si představit udržování přehledu o stavu na jednotlivých adresách, je systém klasické peněženky s bankovkami. Kolik držíme hotovosti, zjistíme jednoduše tím, že se podíváme, kolik bankovek (a jaké hodnoty) v peněžence máme. V případě Bitcoinu pak, kolik UTXO (jaké hodnoty) je asociováno s naší veřejnou adresou nebo bitcoinovou peněženkou. Když chceme provést útratu, použijeme jednu nebo více bankovek (UTXO transakcí asociovaných s naší peněženkou), které předáme protistraně, a možná dostaneme menší bankovku nebo mince zpátky (nový UTXO). Důležité je, že každý UTXO (podobně jako fyzickou bankovku) lze z naší strany utratit pouze jednou.

veřejný klíč (public key)

Druhý z dvojice klíčů v asymetrické kryptografii. Z veřejného klíče se generuje adresa. Veřejný klíč může být vypočítán ze soukromého klíče, avšak nikoliv soukromý z toho veřejného.

BRAIINS Publishing

Yan Pritzker

Vynález jménem Bitcoin

Z anglického originálu *Inventing Bitcoin* přeložila Tereza Wongová
Technická redakce Pavel Moravec a Braiins team
Odborná konzultace Aleš Janda, Andrej Cabaj, Andrej Cibík, Karel Wolf
Jazyková redakce Hana Prokšová a Ondřej Dufek
Odpovědný redaktor Jáchym Černý
Grafická úprava a sazba Rostislav Plachý
Úprava obálky Jiří Chlebus
Vytiskla tiskárna Projects, s.r.o.
114 stran, druhý dotisk prvního vydání

Vydalo nakladatelství Braiins Systems, 2020
braiins.com/publishing

ISBN 978-80-907975-0-5