Jak funguje Bitcoin?

Po přečtení minulého článku o tom, co je to Bitcoin a proč vznikl, Vás možná napadla (naprosto správná) otázka, a sice, kdo onu účetní knihu, blockchain, spravuje, když má Bitcoin decentralizovanou podobu a žádná jedna entita jej neovládá? A přesně touto otázkou, respektive tím, jak Bitcoin funguje po technické stránce, se v následujících řádcích budeme zabývat. Tento článek bude na pochopení lehce složitější, ale když si jej přečtete, pochopíte základy fungování Bitcoinu a získáte tak konkurenční výhodu oproti naprosté většině světové populace.

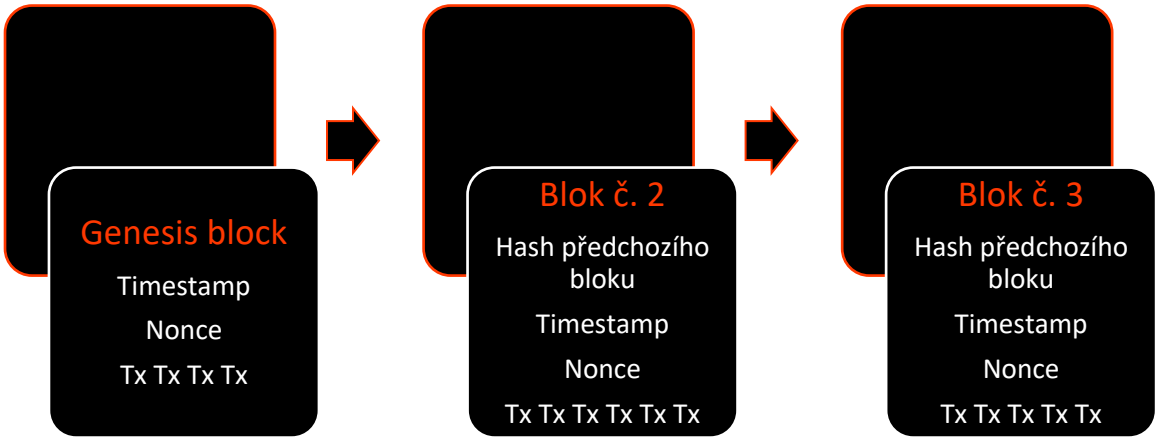
Blockchain (veřejná účetní kniha) je spravován pomocí takzvané *těžby*. Těžbu si lze představit jako jednu velkou loterii. Těžaři (ti, co provádí těžbu) se snaží najít určité číslo – *nonce*, přičemž ten, kdo toto číslo nalezne jako první, získá možnost dostat odměnu v podobě nových bitcoinů. Tedy motivace spravovat veřejnou účetní knihu je primárně finanční, a to v podobě nových mincí a transakčních poplatků od uživatelů *bitcoinové sítě*.

Jakmile těžař nalezne onu správnou nonce, kterou nazýváme *golden nonce*, aplikuje na ni (společně s ostatními údaji v *hlavičče bloku*, jako je *merkle root, časové razítko*, anebo *hash* přechozího bloku) takzvanou *hashovací funkci*. Hashovací funkce je matematická funkce, která převádí zprávu o libovolné délce na otisk, *hash* (nečitelnou kombinaci písmen a čísel) s přesně danou velikostí. Bitcoin využívá hashovací funkci *SHA-256*, tedy výstup hashovací funkce má 256 bitů. Přičemž platí, že drobná změna ve zprávě na vstupu vede k velké změně ve výstupu. Dejme si jednoduchý příklad: Vytvoříme si nějaký vstup, například slovo Bitcoin. Tento vstup vložíme do hashovací funkce SHA-256 a vyjde nám otisk – *b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4*, kdybychom však změnili slovo Bitcoin na Bitcon, vyjde nám zcela odlišný výstup – *dcb05a36f3d9336f77cc7bd59cffabd6f10a0fba48efc7d2ab6cbdd3d8b8d4ca*. U hashovacích funkcí navíc platí, že nejsou obousměrné, symetrické. Z výstupu této funkce je prakticky nemožné zjistit její vstup. Pravděpodobnost, že byste z výstupu zjistili jeho vstup je (díky binární soustavě – 0 nebo 1) 2^{256}, což je zhruba tak stejně velké číslo, jako počet atomů ve vesmíru.

V minulém článku jsem zmínil, že *problém dvojí útraty* byl u Bitcoinu vyřešen pomocí toho, že je mezi všemi uživateli veřejná účetní kniha, avšak to není úplně pravda. A to, jelikož blockchain samotný neřeší problém dvojí útraty, řeší jej v kombinaci s *konsenzuálním algoritmem*. Blockchain je zkrátka pouze veřejná

databáze, ale musíme ještě nějak zajistit, aby do ní nemohl data psát každý, aby kdokoliv nemohl vyhrát loterii.[1]

Bitcoin k tomu používá algoritmus *Proof of Work*. U Bitcoinu totiž onu loterii vyhrává ten, kdo k tomu obětuje nejvíce, kdo utopí největší množství nákladů, a to v podobě elektřiny (celá bitcoinová těžba je postavena na matematické pravděpodobnosti, tudíž vždy nemusí platit, že těžař s největším výpočetním výkonem nalezne správnou nonce jako první, ale má k tomu ze všech největší šanci). K získání odměny je potřeba zahashovat veškeré údaje v *bloku*. Blok je datová struktura, ve které se nachází jednotlivé transakce, časové razítko (*timestamp*), nonce a hash předchozího bloku. Tyto bloky jsou na sebe *kryptograficky* navázány, každý blok potvrzuje blok předchozí, a tím ztěžuje jeho změnu, a tvoří řetězec bloků – blockchain. Ten je právě díky kryptografické návaznosti jednotlivých bloků nezměnitelný (respektive tak tomu je, kvůli možnosti *reorgu*, pouze od určité hloubky *transakce* v bitcoinovém blockchainu). Kdybychom chtěli změnit transakci ve vůbec prvním bloku, který vytěžil samotný *Satoshi Nakamoto, genesis bloku*, hash celého bloku by byl naprosto odlišný od hashe původního, správného bloku (vzpomeňme si, že sebemenší změna ve vstupu hashovací funkce vede k zcela jinému výstupu). Co by to znamenalo? Tento blok by nenavazoval na ostatní bloky a byl by neplatným. Proč? Součástí bloků je hash předchozího bloku, pomocí kterého jsou jednotlivé bloky na sebe navázány. Ve chvíli, kdyby se tento hash změnil, blok by k ostatním blokům jednoduše neseděl.



Řetězec bloků – blockchain

Jak je ale možné získat onu odměnu? Přece jenom, to, že se k získání nových mincí musí zahashovat veškeré údaje v blocích nijak nezaručí to, že je vytěží ten, kdo k tomu obětoval nejvíce zdrojů. A nyní přichází do hry znalost hashovacích funkcí. Bitcoinová síť předem zná takzvané *cílové číslo*. Výsledný hash veškerých údajů v bloku musí být menší nebo stejný jako ono cílové číslo. Komu takto vyjde hash, získá pravomoc uzavřít blok, rozeslat jej mezi uživatele bitcoinové sítě a získat odměnu v podobě nových bitcoinů.

Každé dva týdny (respektive každých *2016* bloků) se cílové číslo mění v závislosti na výpočetní kapacitě (měřeno množstvím hashů za sekundu) bitcoinové sítě vždy tak, aby se blok vytěžil průměrně každých *10 minut*. Tomuto regulačnímu mechanismu říkáme *difficulty algorithm* (algoritmus náročnosti těžby). Díky této technologii můžeme předem vědět, kdy se kolik nových bitcoinů vytěží, jeho *monetární* politika je tak do budoucna známá. To je obrovská výhoda například oproti zlatu, kde růst jeho ceny vede k výhodnější těžbě, a tedy i k větší produkci tohoto drahého kovu. Důsledek růstu nabídky zlata je pak pokles jeho ceny. Bitcoin ale funguje jinak. Růst jeho ceny sice krátkodobě zvýhodní těžbu (dokud nedojde ke změně cílového čísla), ale těžaři nevytěží více bitcoinů (bitcoinový protokol jim to jednoduše neumožňuje), pouze více zabezpečí síť, což má neutrální (respektive někdy dokonce pozitivní) dopad na cenu bitcoinu.

Možná jste někdy slyšeli o tom, že těžba je způsob, jak si může kdokoliv vytvořit nové bitcoiny. To však není úplně pravda. Těžba totiž není pro každého. Dnes je to už velice sofistikovaná profesionální činnost, a to právě kvůli algoritmu náročnosti těžby. Dříve bylo možné bitcoiny těžit na procesoru standardního počítače, protože výpočetní síla celé sítě byla malá, a tedy cílové číslo vysoké (čím vyšší je cílové číslo, tím větší je pravděpodobnost nalezení nonce). To se ale časem změnilo. Jak se Bitcoin stával populárnějším, rostlo množství jeho uživatelů i těžařů. Což vedlo k růstu výpočetní síly celé sítě a poklesu hodnoty cílového čísla. Začalo se tak těžit na výpočetně výkonnějších grafických kartách. Náročnost těžby neustále rostla a rostla. Dnes se bitcoiny těží v takzvaných *těžebních poolech*, ve kterých je několik desítek tisíc specializovaných strojů přímo na těžbu bitcoinů – *ASIC minerů*. Tím, že je v daném poolu několik výkonných těžebních strojů, zvyšuje se pravděpodobnost, že právě ona skupina těžařů nalezne golden nonce, pomocí které získají nové bitcoiny. Tyto pooly mají často rozdílné obchodní strategie, ale většina z nich funguje na tom principu, že svoji odměnu rozdělí jednotlivým těžařům (respektive vlastníkům ASIC minerů) podle toho, jak velkým výpočetním výkonem poolu přispěli.

Ale teď zpět ke konsenzuálnímu algoritmu Proof of Work. Proof of Work znamená důkaz vykonané práce, ale co je tím důkazem práce? Je to golden nonce. Samotný fakt, že těžař nalezl správnou nonce, pomocí které mu jako výsledek hashovací funkce vyšel hash menší než cílové číslo, znamená, že k tomu pravděpodobně musel obětovat obrovské množství výpočetního výkonu. Tento důkaz je tak velmi těžké vytvořit, ale naopak naprosto jednoduché ověřit (stačí použít veškeré údaje v bloku jako vstup hashovací funkce SHA-256 a vyjde Vám stejný výstup jako těžařovi). Vzhledem k takto nákladné činnosti nemají těžaři incentivy pro to, aby podváděli, protože by spotřebovali obrovské množství elektrické energie a žádné bitcoiny by nezískali, to jednoduše nedává smysl.

Těžaři získávají svoji odměnu pomocí takzvané *coinbase* (generující) *transakce*. Avšak jsme si říkali, že pomocí těžby se zabezpečuje účetní kniha, respektive zaručuje správnost jednotlivých transakcí. Tak jakou mají těžaři motivaci zabezpečovat transakce? Je to jednoduché, u každé transakce je *transakční poplatek*, které po vytěžení bloku připadá právě jejímu těžaři. Díky tomu není v bloku pouze jediná transakce, generující bitcoiny, ale i transakce běžných uživatelů.

Veškeré transakce, tj. přesunutí bitcoinů z jedné *bitcoinové adresy* na druhou, ukládají *uzly* v bitcoinové síti, *nody*, do takzvaného *mempoolu*. Plnohodnotný uzel v bitcoinové síti je zařízení, které v sobě uchovává celou historii bitcoinového blockchainu (dnes je to zhruba *470 GB*) a ověřuje transakce nové, například pomocí, pro tento účel, nejpoužívanějšího softwaru *Bitcoin Core*. Možná jsem Vás nyní zmátl tím, že uzly ověřují transakce, přece to je práce těžařů, anebo ne? Rozdíl mezi uzly a těžaři je přitom naprosto zásadní. Když někomu odešlete transakci, tato transakce se nejprve rozšíří mezi veškeré uzly, ty ověří, zda neutrácíte již utracené bitcoiny a zda je Vámi poskytnutý *digitální podpis* validní, a následně je zařadí do mempoolu. Z mempoolu pak těžař vybere transakce (samozřejmě vybírá transakce s co nejvyšším transakčním poplatkem), které zařadí do bloku a tím je potvrdí. Tyto bloky pak rozšíří do bitcoinové sítě mezi všechny uzly a ostatní těžaře. Zjednodušeně tak můžeme říci, že uzly ověřují transakce a těžaři je naopak potvrzují. Každý těžař je uzel, ale když máte vlastní bitcoinový node, nemusíte být těžařem.

Zde se přímo nabízí další otázka, a sice, co brání nodům, aby v síti rozšířili transakce, které se ve skutečnosti nestaly? Nyní vstupuje do hry *teorie her*. Vždy, když lidé, jakkoliv jednají, mají k tomu určité *incentivy*, motivace, chcete-li. Jinými slovy, je dobré se pokaždé zamýšlet nad tím, co vede lidi k tomu, aby se určitým způsobem chovali. A Bitcoin je geniální systém incentiv. Jsou zde totiž

jednotliví uživatelé motivováni udržovat celou síť ve správném chodu. Proč tomu tak je? bitcoinoví uživatelé (většinou) drží mince samotného ekosystému – bitcoiny. *Kupní síla* (respektive dnes spíše cena měřená ve státních měnách) by mohla v důsledku útoku na síť totiž výrazně poklesnout (mohla by se snížit poptávka po bitcoinech a to by za jinak stejných podmínek vedlo k poklesu ceny), a to si žádný *Bitcoiner* nepřeje... A naopak by v případě hladkého fungování Bitcoinu mohla jeho cena vzrůst, čímž by se jeho držitelé stali bohatšími. Ekonomické motivace jednoduše fungují.

Navíc dnes celou bitcoinovou síť spravují desítky, ne-li i stovky tisíc (přesná čísla nejsou veřejně známá, protože velká část nodů nemá zveřejněnou IP adresu a zůstává tak v anonymitě) uzlů.[2] Tudíž i kdyby se našlo pár neposlušných nodů, které by chtěli ostatní podvést, většina uzlů by tyto transakce ověřila jako neplatné a nezařadila do mempoolu, potažmo těžaři neumístili do bloku. Falešné transakce by tak byly neplatné. Bitcoin je totiž systém, kde každý kontroluje každého a snaží se zabránit jakýmkoliv podvodům.

Co by se ale stalo, kdyby dva rozdílní těžaři vytěžili a do sítě rozšířili nový blok s validními transakcemi a správným důkazem vykonané práce v jednu a tu samou chvíli? Takováto situace skutečně čas od čase nastane a říkáme jí *fork* nebo také *rozštěpení blockchainu*. Bitcoin tento problém řeší šalamounským způsobem, a sice tím, že počkáme a uvidíme. Vzhledem k tomu, že jsou oba tyto bloky validní, těžaři si mohou vybrat, který blok zařadí do své kopie účetní knihy a použijí jako základ pro další bloky. Čas ukáže, který z těchto bloků bude nakonec tím jediným správným, a to, protože se bitcoinová síť řídí takzvaným *Nakamotovým konsenzem*. Ten spočívá v tom, že uzly musí vždy akceptovat nejsilnější řetězec důkazu o vykonané práci (blockchain s nejvíce platnými bloky), který přitom nijak neporušuje ostatní podmínky bitcoinové sítě.

Další blok tak rozhodne, která verze blockchainu je ta správná. Pokud jej vytěží těžař, který akceptoval blok od těžaře A a vytvoří tak silnější důkaz práce, ostatní těžaři a nody jej musí považovat jako jediný správný blockchain. Ovšem co se stane s blokem těžaře B, který akceptovala část bitcoinové sítě? Odpověď zní jasně, musí provést takzvaný *reorg*, tj. reorganizaci bloků v blockchainu. Z bloku těžaře A se stane blok, který je součástí jediného správného řetězce bloků, jenž musí všechny nody (tedy i ostatní těžaři) uznat platným, zatímco blok těžaře B se stane takzvaným *osiřelým blokem* (*orphan block*). A těžba pokračuje pozvolně dál, dokud nenastane stejná situace znova.

Avšak co se stane s odměnou těžařů A a B? Přece oba tito těžaři vytvořili validní blok s platnou coinbase transakcí, tudíž musí, jak těžař A, tak i těžař B dostat odměnu, anebo ne? Bitcoin je z hlediska technologického fungování naprosto geniální, a i tento problém brilantním způsobem řeší, a to s pomocí takzvaného *maturation time* (doby zrání). Přímo u generující coinbase transakce je nastaven čas, až po kterém bude možné bitcoiny z adresy utratit (takzvaný *timelock*). Tento čas je *100 bitcoinových bloků*, tedy zhruba nějakých 17 hodin. Tedy až po 100 blocích může těžař utrácet svoje nově vytěžené bitcoiny, čímž se eliminují problémy spojené s reorganizací bitcoinocých bloků.

A teď ještě něco k odměně těžařů. Tato odměna byla ze začátku (od genesis bloku, tj. roku 2009) 50 bitcoinů za jeden vytěžený blok. Ovšem každé zhruba *4 roky* (respektive *210 000 bloků*) se tato odměna snižuje, a to přesně o polovinu. Půlení odměny těžařů říkáme *halving*. První halving nastal v listopadu roku 2012 a snížil odměnu na 25 bitcoinů za blok. Dnes činí odměna 6,25 bitcoinů a další halving nastane už v březnu roku 2024. Takto se bude postupně snižovat odměna za těžbu až se dostaneme k roku *2140*, kdy se vytěží poslední *20 999 999,9769.* mince a od této chvíle již nebudou vznikat žádné nové bitcoiny.

1 Respektive blockchain je výsledkem ekonomických motivací tuto databázi zabezpečovat (*security budget – block subsidy* + transakční poplatky), náročností přepsání transakční historie (*PoW*) a kryptografickou návazností jednotlivých digitálních souborů – bloků (*Merkle tree* hashování). Jeho implementace dává smysl pouze s využitím těchto technologií. Bohužel se ze slova **blockchain** stal v posledních letech obrovský *buzzword*, téměř vždy se jedná pouze o marketing. Blockchain sám o sobě nedává smysl a je to pouze neefektivní, vysoce nákladná databáze (výjimkou jsou projekty, které využívají technologií, jež jsem zmiňoval výše).

2 Takto obrovským množstvím nodů je zajištěna decentralizace bitcoinové sítě. Stačí, aby byla na jednom jediném nodu uchována transakční historie a Bitcoin může fungovat (sice nedobře, ale přece). Vzhledem ke geografické různorodosti nodů není možné Bitcoin „vypnout“. Musela by se totiž celosvětově vypnout elektřina (čímž by dále nemohla pokračovat těžba), což je ale v dnešním relativně svobodném světě takřka nemožné, pokud by se nepřihodila obrovské přírodní katastrofa. Výpadek elektřiny by však zničil i současný bankovní systém (přes 92 % všech peněz je v podobě bankovních depozit [digitální peníze] a pouze zlomek peněžní zásoby tvoří oběživo neboli hotovost [fyzické peníze]) a celou spoustu dalších, pro dnešní nastavení společnosti naprosto klíčových odvětví. Navíc hned, co by elektrická energie začala na libovolném území opět fungovat, Bitcoin by byla ta první síť, která by byla obnovena. Dokud bude Bitcoin decentralizovaný, nebude možné jej zničit jakýmikoliv (státními) zásahy.