Středoškolská technika 2018

Setkání a prezentace prací středoškolských studentů na ČVUT

Bitcoin

Martin Rektoris

Gymnázium, Milevsko, Masarykova 183

Masarykova 183, 399 01

GYMNÁZIUM, MILEVSKO, MASARYKOVA 183

Maturitní práce z IKT pro maturitu JARO 2018

Bitcoin

Martin Rektoris, 4. A

Vedoucí: Ing. Jiří Školník

2017/18

Prohlášení

Prohlašuji, že jsem práci zpracoval zcela samostatně a veškeré zdroje jsem uvedl v seznamu použité literatury.

V Milevsku 25.4.2018 …….

Anotace

Maturitní práce pojednává o technologii blockchain, platebním systému a kryptoměně Bitcoin. Celá tato technologie přináší řadu inovací, jako je například (do jisté míry) anonymita, eliminace potřeby třetí strany (resp. finanční instituce) k zpracování transakcí, zabránění padělávání apod. Práci zaměřuji primárně na vysvětlení principu fungování kryptoměn, zejména Bitcoinu.

Kryptoměny
Blockchain
Těžení
Hash
Blok
Kryptografie
Adresa
peněženka
Klíč
Decentralizace
Proof of Work
Odměna
Nakamoto
Poplatky
nonce
Transakce

Obsah

1 Bitcoin

Ještě před začátkem se musíme naučit rozlišovat pojmy bitcoin a Bitcoin. V první případě se jedná o peněžní jednotku měny, stejně jako je například česká koruna nebo americký dolar. V druhém případě je Bitcoin decentralizovaný platební systém, protokol, který je nezávislý na jakékoliv centrální autoritě, co by se starala o správu a provoz měny. Provozem měny jsou myšleny nezbytné operace, jakými jsou validace transakcí či emise peněžních jednotek dané měny do oběhu.

1.1 Vznik

První zmínka o Bitcoinu pochází z roku 2008, kdy byla zaregistrována doména s jménem bitcoin.org. V listopadu tohoto roku vydal Satoshi Nakamoto dokument s popisem Bitcoinu označený jako Bitcoin: A peer-to-peer Electronic Cash System. Bitcoin je open–source projekt což znamená, že veškeré zdrojové kódy a dokumentace jsou volně dostupné na internetu. Kód této kryptoměny zveřejnil v lednu roku 2009. Tento samý měsíc byl vytěžen první blok bitcoinu v historii blockchainu, také známý jako „Genesis block“. Obecný název „kryptoměna” vznikl spojením slov kryptografie, která je v této technologii značně zastoupena, a měna.

1.2 Satoshi Nakamoto

Satoshi Nakamoto je jméno nebo pseudonym osoby nebo skupiny, která navrhla a vytvořila protokol Bitcoin. Nejsou žádné záznamy o existenci identity Nakamoto před vytvořením Bitcoinu. Satoshi je mužské japonské jméno, jehož význam má různé podoby jako „moudrý“, „jasné myšlení“, „bystrý“, nebo „osoba s inteligentními předky“. Nakamoto je také japonského původu.

Podle domněnek by Nakamoto mohl mít ve vlastnictví zhruba jeden milion bitcoinů. V prosinci roku 2017 by to odpovídalo asi 390 miliardám Kč.

2 Jak Bitcoin funguje

V celé této kapitole se budu snažit přiblížit fungování Bitcoinu z technické stránky. Nahlédneme do kryptografie a vysvětlíme si základní principy Bitcoinu.

2.1 Kryptografie

Úplně jako první se podíváme na kryptografii, která je nedílnou součástí Bitcoinu a spousty dalších digitálních technologií, jako například všem známého internetu (třeba ve formě digitálních certifikátů). Pro pochopení principu digitálního podpisu a jiných pojmů, založených na důvěryhodné archivaci, je nutné získání základní orientace v oblasti kryptografie.

Je to vědní obor, zabývající se metodami utajování (šifrování) obsahu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. Touto znalostí je šifrovací klíč. Na klíče se podíváme detailněji.

Jak bylo v úvodu zmíněno, šifrování je proces, při kterém se z obecně čitelné sekvence dat (např. dokumentu) za použití šifrovacího klíče vytvoří šifrovaná sekvence dat. Zašifrovaný text je bez znalosti šifrovacího klíče zcela nečitelný. Pro komplexnost informací bude v dalším výkladu vysvětlen princip šifrování asymetrických šifer a princip funkce hashovací funkce, konkrétně funkce SHA-256. V případě šifer i hashovacích funkcí se jedná o elementární úvod do problematiky kryptografie.

Obecně existují 2 typy šifer-symetrické a asymetrické. Nám však stačí zabývat se těmi asymetrickými, protože právě ony jsou v oblasti kryptoměn používány.

Již zmíněné asymetrické šifry používají dva klíče. Je to klíč veřejný a klíč soukromý (privátní), které dohromady tvoří klíčový pár. Klíčový pár je na základě matematického algoritmu svázán a oba klíče neoddělitelně patří k sobě. V zásadě platí, že při generování klíčového páru se nejprve generuje klíč soukromý a až po jeho vygenerování se vytvoří klíč veřejný. V případě potřeby lze k privátnímu klíči vygenerovat nový klíč veřejný. Asymetrické šifry v kombinaci s dalšími technologiemi jsou používány zejména pro šifrování, digitální podepisování a ověřování digitálních podpisů a vytváření časových razítek a jejich ověřování. V případě digitálního podpisu a časového razítka je pro podepsání a/nebo vytvoření časového razítka použit klíč soukromý. Pro ověření se v obou případech použije klíč veřejný, který lze volně distribuovat. Tato funkcionalita umožňuje ověření digitálního podpisu komukoliv, kdo má k dispozici veřejný klíč odesílatele.

2.2 Kryptografická hashovací funkce

Bitcoin používá jednosměrnou kryptografickou funkci SHA-256. Je to matematické funkce, která transformuje vstupní data variabilní délky a převádí je na výstupní hash hodnotu o fixním počtu znaků. Hash je obvykle kratší než původní vstupní řetězec (ale nemusí tomu být pravidlem) a i minimální změna ve vstupních datech bude mít za následek absolutně odlišnou hash hodnotu. Jednosměrná hash funkce je funkce taková, která pracuje v jednom směru. Je snadné u ní vypočítat výstupní hodnotu hash ze vstupních dat, ale je velice výpočetně náročný postup opačný, tedy vypočtení vstupní dat z hash hodnoty.

$$\text{SHA256}(\text{“vstup”}) \Rightarrow \text{ řetězec o fixní délce}$$

Jedním z možných formátů výstupu je binární číslo o délce 256 číselných pozic. Máme 256 pozic a na každou pozici připadají dvě možnosti (0 a 1). Existuje tedy 2^{256} různých počtů možností výstupní hodnoty.

2.3 Ledger[1] a digitální podpis

Ledger je účetní kniha nebo počítačový soubor, který zaznamenává historii všech transakcí.

Na úplný začátek si pro zjednodušení představme si skupinu lidí, kteří si navzájem posílají peníze a všechny transakce si sami zapisují do ledgeru. Po uplynutí určitého časového intervalu provedou vyúčtování, vypíší zůstatky, resp. dluhy, a rozdíly si vyrovnají v hotovosti. Jenže problém by byl takový, že kdokoli by mohl do ledgeru zapsat falešnou transakci.

[1] Český ekvivalent anglického slova ledger nevystihuje význam přesně, proto pro autentičnost zachovávám originální znění.

Zde přichází na řadu digitální podpis. Ten se chová podobně jako běžný psaný podpis. Každá transakce zapsaná do ledgeru je digitálně podepsána. Někomu by mohlo přijít, že digitální podpis by mohl být snadno kopírovatelný. Právě proto se každému, kdo provede transakci z bitcoinové adresy (ta se vytvoří každému, kdo vlastní bitcoinovou peněženku), automaticky vygeneruje dvojice asymetrických klíčů, viz bod 3.1. Tyto klíče jsou 256bitová binární čísla, která často bývají pro lepší uchovatelnost znázorňována v jiných číselných soustavách a formách (zapisování 256 nul a jedniček je nepraktické).

Zpět k digitálnímu podpisu. Digitální podpisy se od sebe značně liší, i když potvrzují transakce, které pochází ze stejné bitcoinové adresy. Uvažujme tedy funkci P(x,y), jež výstup vytváří digitální podpis. Řekněme, že je závislá na dvou parametrech-Zprávě (obsah transakce) a Soukromém klíči.

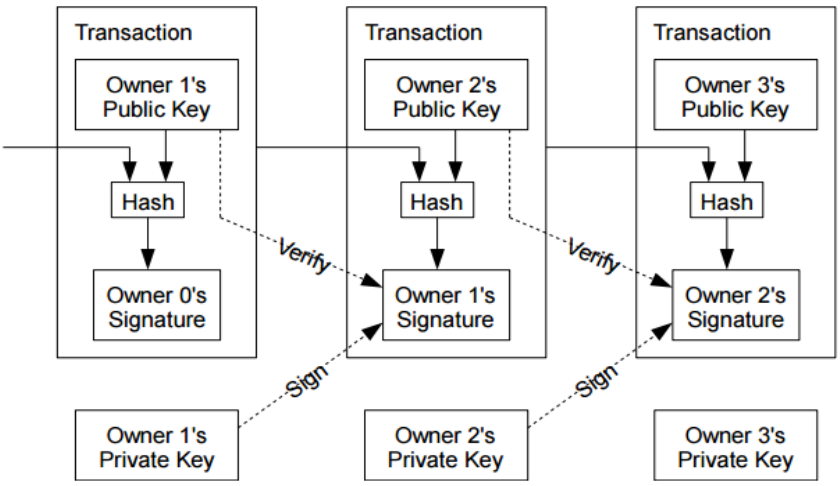
P(Zpráva, Soukromý klíč) = Digitální podpis

Z výše napsaného vyplývá, že kdyby někdo chtěl použít váš podpis na jinou transakci (jiný obsah znamená jinou zprávu) v systému by byl ihned odhalen, protože by ověření podpisu selhalo.

To nás přivádí k další velice užitečné funkci, která se používá k ověřování pravosti podpisu. Funkce O(x,y,z), jež výstup může nabýt dvou hodnot - True nebo False, kontroluje, zda byl podpis vytvořen pomocí soukromého klíče, který je matematicky asociován se správným veřejným klíčem.

O(Zpráva, Dig. podpis, Veřejný klíč) ⇒ True nebo False

Digitální podpis je, stejně jako soukromý a veřejný klíč, číslo reprezentované 256 bity. Existuje tedy celkem 2256 možností. Při výpočetní síle dnešních počítačů je pravděpodobnost uhodnutí správného podpisu v rozumném časovém úseku mizivě nízká.



Obrázek 1: Užití klíčů

Kdyby někdo zkopíroval už úspěšně podepsanou transakci, systém by kopii stejně vyhodnotil jako neplatnou. Kombinace podpisu a zprávy by sice byla správná, ale každá samostatná transakce musí ještě obsahovat jedinečnou informaci, která je přiřazena při podepisování. Z toho vyplývá, že každá řádka v ledgeru vyžaduje kompletně nový podpis.

Digitální podpis odstraňuje velkou část potřebné důvěry třetích stran v ledgeru.

2.4 Decentralizace

Kdybychom pro ověření spoléhali pouze na digitální podpis, znamenalo by to, že všem lidem plně důvěřujeme a spoléháme na to, že se na konci určitého časového úseku vyrovnají v hotovosti. Někdo by si mohl nahromadit veliký dluh a už by se nemusel nikdy ukázat, tj. vytvořil by transakce, ale v hotovosti by se s nikým nevyrovnal. Existuje tedy systém, který zabraňuje utratit více peněz, než máte. Tento způsob zajišťuje, že se nemusíte vyrovnávat v hotovosti. Pokud by se někdo pokusil utratit více, než má, transakce bude vyhodnocena jako neplatná. Neplatná jako kdyby ji nikdy nepodepsal. To znamená, že k potvrzení transakce potřebujeme znát celou historii v ledgeru do současnosti. Zrušení vyrovnávání se v hotovosti odstraňuje propojení mezi ledgerem a fiat měnou.2

Dostáváme se k tomu, že Bitcoin nebo jakákoli jiná kryptoměna jsou zjednodušeně ve skutečnosti historie transakcí, tedy ledger.

[2]Fiat měna je měna peněz s nuceným s nuceným oběhem, fungující jako hlavní státní měna.

Doposud mohl každý přidávat do ledgeru nové řádky. Byl volně přístupný, umístěný na veřejném místě (např. na internetu), což však vyžadovalo důvěru v hostitele sítě a v pravidla o přidávání transakcí. Dalším krokem pro odstranění centralizace je distribuce kopií ledgeru všem uživatelům.

Když by někdo například odeslal bitcoin, tak by vysílal informace o této transakci do všech dostupných kopií ledgerů. Nicméně to takto nefunguje. Nelze předpokládat, že každý uživatel dostane informace a bude používat onu verzi.

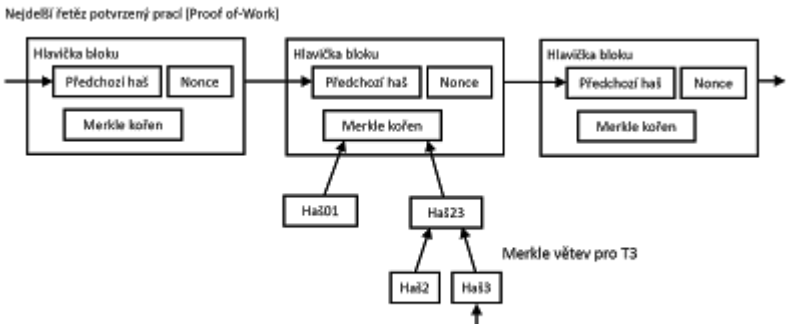
Řešení, které Bitcoin přináší, je věřit ledgeru, na něž byla vyložena největší výpočetní síla. Klíčovým nástrojem je zde kryptografická hash funkce. Hlavní myšlenka je, že bychom použili výpočetní sílu počítače v náš prospěch tak, že by pro schválení a hladký průchod falešných transakcí a rozporných verzí distribuovaných ledgerů byla potřeba neuskutečnitelná výpočetní síla.

2.5 Proof of Work[3]

Řekněme, že najdeme takové speciální číslo nazývané nonce. Když ho přidáme do ledgeru, a pak na celý ledger aplikujeme hash funkci, tak dostaneme hash, jež začíná určitým počtem nul. Jediná možnost, jak číslo nonce najít, je hádat. Pravděpodobnost, že takové číslo uhodneme je $2^{-\,Počet\ hledaných\ nul}$ (pokud je hledané číslo zapsané ve dvojkové soustavě). Nezbývá nám než procházet postupně všechny možnosti a kontrolovat je. A právě to je to, co provádíme. Poté, co nonce najdeme, lze už jednoduše zjistit, zda hash začíná požadovaným počtem nul. Tento způsob ověřování a hledání se jmenuje Proof of Work. Všechna „práce" je vlastně přímo spjata s ledgerem. Pokud bychom změnili klidně i jediné číslo v libovolné transakci z ledgeru. Hash by byl kompletně jiný a my bychom museli znovu projít dalších $2^{Počet\ hledaných\ nul}$ možností, abychom našli nový nonce a prokázali Proof of Work.

Zpět k myšlence volně distribuovaného ledgeru: Každý vysílá svůj záznam transakcí a my chceme, aby se dohodli na tom, jaká verze ledgeru je správná. Jak už jsem zmínil, hlavní myšlenka stojící za originálním Bitcoin whitepaperem je věřit tomu ledgeru, do něhož bylo vynaloženo nejvíce výpočetní síly.

Pro provedení nejdříve systematicky rozdělíme daný ledger do tzv. bloků, kde každý blok obsahuje seznam transakcí, nonce a pár dalších informací. Stejně jako je transakce považovaná za platnou jenom tehdy, pokud má ověřený digitální podpis, tak blok je validní právě tehdy, když obsahuje Proof of Work. Abychom se ujistili, že bloky nejsou náhodně řazeny, každý blok ještě



Obrázek 2:: Proof of Work

[3] V překladu – důkaz o (vykonané) práci.

navíc musí ve své hlavičce obsahovat hash předchozího bloku. Kdybychom nyní změnili informace o libovolné transakci nebo zaměnili pořadí bloků a změnily by se všechny hashe následujících bloků. To by znamenalo dělání celé „práce" odznova. Tj. museli bychom najít nový nonce pro každý blok od začátku.

Protože bloky jsou takto propojeny, tvoří řetězec bloků, který nazýváme blockchain.

2.6 Blockchain[4]

Jako součást našeho aktualizovaného protokolu dovolíme komukoliv na světě vytvořit vlastní blok. Dotyčný tvůrce bude shromažďovat vysílané transakce do bloku, hledat nonce a potvrzovat pomocí Proof of Work. Poté co nonce najdou, platný blok sdílí se všemi ostatními tvůrci. Jakožto odměna za úspěšné nalezení nového bloku se do onoho bloku zapíše speciální transakce určená pro tvůrce bloku, tzv. block reward. Tato odměna se objeví de facto z ničeho nic, od nikoho nepochází, a tudíž nemusí být podepsána. Z toho vyplývá, že s každým novým nalezeným blokem se zvyšuje počet jednotek měny (v našem případě Bitcoinu) v oběhu. Hledání/tvoření nový bloků se v oblasti kryptoměn nazývá těžení (mining). Zřejmě protože to vyžaduje hodně vykonané „práce" a „vyrábí" nové bitcoiny. Těmto „výrobcům" Bitcoinů se říká těžaři (miners). Ve skutečnosti však jenom dávají dohromady transakce, tvoří bloky a dostávají za to odměnu v podobě nových jednotek měny.

Každý, kdo chce bitcoin používat jako platební systém, nepřijímá samotné transakce, ale soustředí se na bloky vysílané těžaři a aktualizuje svoji vlastní kopii blockchainu. Klíčová myšlenka tohoto protokolu je, že když někdo uslyší dvě rozdílné větve blockchainu, jejichž historie transakcí jsou v rozporu, přesuneme se k tomu delšímu, na něž bylo vyloženo více „práce". Pokud je v obou větvích shoda, jsou stejně dlouhé, tj. nevíme, který je správný, čekáme na přidání nového bloku k jedné z větví a tu uznáme jako správnou. V některých případech může o správnosti větve rozhodnout až několik přidaných bloků.

Blockchain je relativně odolný proti podvodům. Předpokládejme, že se někdo pokusí zfalšované transakce zahrnout do bloku, který potom se všemi sdílí. V databázi se tudíž vyskytnou rozdílné verze/větve bloků. Čeká se na další bloky, jež potvrdí správnou větev. Osoba, která se pokusila zfalšovat transakce, by musela hledat Proof of Work všech následujících bloků hledat sama. To znamenalo mít více výpočetní síly než všichni ostatní těžaři.

3 Těžba a těžaři

Už jsme si vysvětlili, že existují lidé, kterým se říká těžaři. Jejich prací je hledat nové bloky, za které dostávají odměnu ve formě bitcoinu. Je to jediná možnost přísunu oběhu bitcoinů do oběhu. Pro zajímavost se můžeme podívat na historii transakcí genesis bloku a zjistíme, že neobsahoval žádnou transakci. Jenom odměnu.

Jedním z předmětů jejich hledání je takové číslo nonce, aby výstupní hash začínal požadovaným počtem nul5. Čím větší je požadovaný počet nul, tím je celý proces náročnější. Náročnost

[4] Dosud neexistuje ekvivalent tohoto slova v českém jazyce.
[5] Jedná se o bitové nuly.

je nastavena tak, aby se za dva týdny vytěžilo přesně 2016 bloků. To vychází průměrně na 10 minut na blok. Pokud by bylo za dva týdny vytěženo více než 2016 bloků, náročnost se zvýší a naopak.

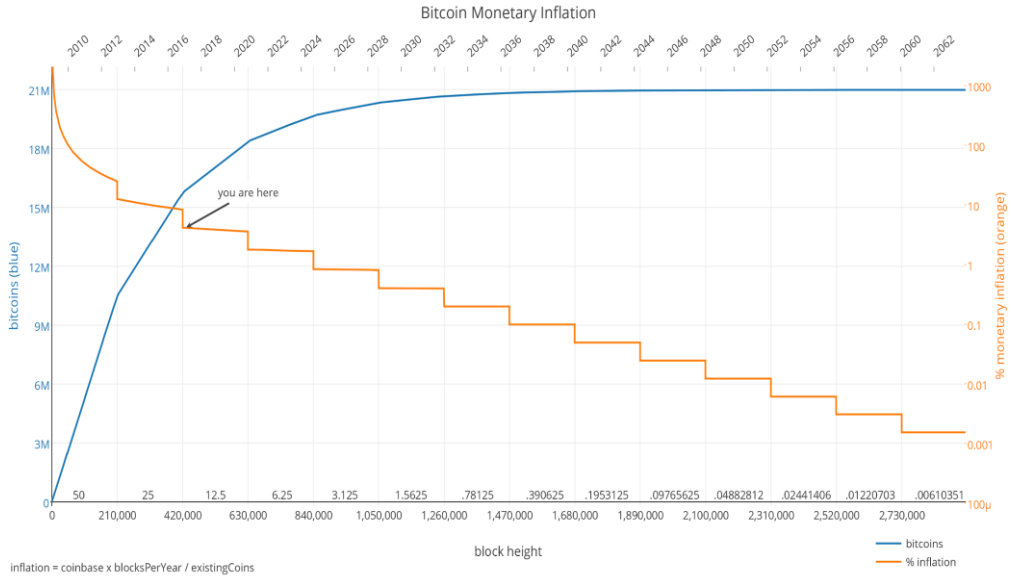
3.1 Odměna

Odměna za jeden vytěžený blok je pevně daná a každých 210 000 vytěžených bloků se půlí. Pro prvním 210 000 odměna činila 50 bitcoinů za blok. Provedením jednoduchého výpočtu dojdeme k závěru, že v oběhu může být maximálně 21 000 000 bitcoinů.

$$210\,000 * 50 * \sum_{n=0}^{\infty} \frac{1}{2^n} = 21\,000\,000$$

Pozn. - V reálném světě nedojde k nekonečnu „půlení", tedy počet bitcoinů se k odhadovanému počtu pouze hodně blíží.

Z výše uvedeného si lze lehce všimnout, že žádná instituce nemůže ovládat inflaci bitcoinu.



Obrázek 3: Vývoj počtu bitcoinů (modře) a inflace (oranžově)

Po vytěžení většiny bloků a snížení odměny za vytěžení bloku budou těžaři vydělávat pouze na potvrzování transakcí.

3.2 Provedení

Těžení v praxi probíhá několika způsoby. V raném stádiu Bitcoinu byla možnost těžit bitcoiny pomocí procesoru, tzv. CPU mining. S nárustem obtížnosti se cena provozu těžení procesorem zvedla natolik, že tento způsob nebyl dál použitelný. Obecně používanější, rychlejší a efektivnější než CPU mining je GPU mining, tj. těžení za využití grafické karty. Zvýšená poptávka o grafické karty kvůli těžení zapříčinila jejich zdražení.

Rychlost, jakou je matematický problém řešen (hledání nonce), se znázorňuje pomocí hash rate. Měří se v „hashích za sekundu“ (H/s). Další násobky H/s mají předpony stejné jako jednotky soustavy SI.

Asi nejefektivnější možností, jak bitcoiny těžit je ASIC[6]. Jedná o speciálně vyrobené mikročipy pro specifické použití. ASIC určené pro těžení bitcoinu byly poprvé vydány v 2013. Zařízení s těmito mikročipy dosahují hash ratu až 14 TH/s. Pro porovnání, běžný stolní počítač má přibližně 1-100 MH/s.

S postupem času se neměnila pouze zařízení pro těžbu, ale i samotný způsob těžby. Zatímco v počátcích těžili BTC jednotlivci, dnes se tito jedinci spojují do různých uskupení, kterým říkáme mining pools (česky těžařské pooly). Po vytěžení bloku se odměna rozdělí podle dílčího příspěvku výpočetní síly. Přestože většina poolů je soustředěna v Číně, mezi nejpopulárnější patří český SlushPool, který byl oficiálně prvním poolem na světě.

4 Transakce

Velikost jednoho bloku je omezená a tím i maximální počet transakcí za minutu. Satoshi Nakamoto implementoval kód Bitcoinu tak, aby byl jeden blok schopen pojmout maximálně 1 MB informací, což limituje počet transakcí, které můžou být v současném bloku zahrnuty. Při průměrné velikosti transakce 495 Bytů činí průměrný počet transakcí 2020 transakcí na blok. Nalezení nového bloku trvá přibližně 10 minut, z toho nám vychází 3,37 transakcí za sekundu. Pro porovnání - platební systém Visa zpracuje průměrně 1670 transakcí za sekundu, schopný je potvrdit až 56 000 transakcí za sekundu. V současné době se hodně diskutuje o škálovatelnosti Bitcoinu. Je to jeden z jeho hlavní problémů.

Jádro bitcoinové komunity se tento problém snaží vyřešit například implementací tzv. Lighting Network. To by zaručilo téměř instantní provedení transakce. Tato síť by byla schopná zpracovat miliony až miliardy transakcí za sekundu.

4.1 Poplatky

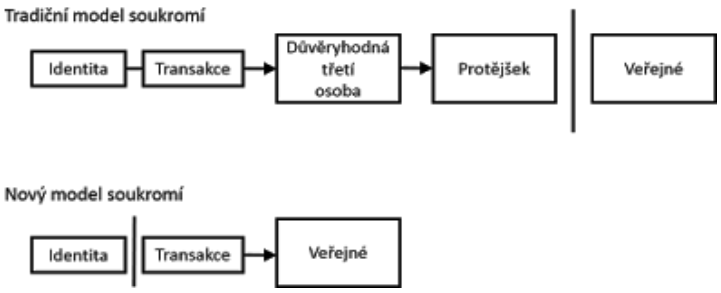
Jak už zde bylo řečeno, velikost jednoho bloku je omezená a tím i maximální počet transakcí za minutu. Uživatelé k transakci navíc připojují poplatek tzv. transaction fee, který jde přímo těžaři do peněženky. Výše tohoto poplatku určuje, jak rychle bude vaše transakce zpracována, potvrzena a zařazena do bloku. Spojením omezení velikosti bloku, doby těžení hledání bloku a zvýšeného zájmu o bitcoin se průměrná cena poplatků vyšplhala v prosinci roku 2017 do řádů desítek amerických dolarů.

4.2 Soukromí

Bitcoin je často vnímán jako zcela anonymní síť. Ale ve skutečnosti je Bitcoin asi nejvíce transparentní platební systém na světě. Zároveň však může přinést rozumnou úroveň anonymity, když je správně používán.

[6] *Application Specific Integrated Circuit, česky – Integrovaný obvod pro specifické použití*

Všechny bitcoinové transakce jsou veřejné, vystopovatelné a permanentně skladované v Bitcoin síti-blockchainu. Bitcoinová adresa je jediná informace, která definuje, kde jsou bitcoiny uloženy a kam jsou poslány. Adresa je soukromě vytvořena peněženkou každého uživatele. Avšak už jednou použitá bitcoin adresa obsahuje historii všech transakcí, které s ní byly provedeny. Kdokoli se může podívat na zůstatek nebo provedené transakce jakékoliv adresy. Když někdo chce přijmout nějaké zboží nebo službu, které zaplatí z bitcoin adresy, stejně musí odhalit svoji identitu. Takže bitcoinové adresy nemohou zůstat plně anonymní. Blockchain je permanentní, celá historii transakcí je uložena. To, co je teď nevystopovatelné, se může v budoucnosti s příchodem nových technologií stát lehce vystopovatelné.



Obrázek 4: Model soukromí

5 Způsoby skladování

Bezpečností protokol Bitcoinu je sám o sobě velmi dobrý. Avšak problém je u člověka. Každý, kdo vlastní soukromý klíč má přístup k obsahu dané peněženky, a proto je důležité privátní klíč nikomu nesdělovat. V následujících podkapitolách vás stručně provedu možnostmi skladování bitcoinů.

5.1 Webová peněženka

Způsob uchování Bitcoinu ve webové peněžence je asi nejběžnější, přestože patří k těm nejvíce nebezpečným. Vy ve výsledku soukromý klíč nevlastníte, vlastní ho poskytovatel služby, tj. třetí strana, a vy jí musíte věřit. Tento způsob je velmi vulnerabilní vůči hackerským útokům. Jejich hlavní výhodou je naprostá jednoduchost. S webovou peněženkou totiž nemusíte nic řešit. K jejich obsluze vám většinou stačí znát své přihlašovací údaje, tedy e-mail, heslo, případně ještě nějaké přidělené ID. S nimi se můžete do své peněženky přihlásit z libovolného zařízení přes web nebo dokonce i skrze samostatnou mobilní aplikaci. Tyto peněženky jsou velmi často napojené na kryptoměnové směnárny. Mezi nejznámější patří Coinbase, Binance nebo MyEtherWallet.

5.2 Softwarová peněženka

Další možností je uložení kryptoměn v peněžence v počítači případně v mobilní aplikaci, princip je zde prakticky stejný. Při jejich nastavení si na začátku vždy vygenerujete seed, který si

znovu rovněž někam bezpečně uložíte. Seed přináší peněženkám hlavně pohodlnost pro uživatele, jelikož v případě změny zařízení stačí jen nainstalovat libovolnou peněženku využívající stejného systému, zadat seed a máte plný přístup k vašim penězům.

5.3 Hardwarová peněženka

Hardwarová peněženka je speciální typ bitcoinové peněženky, která uchovává soukromé klíče uživatele v bezpečném hardwarovém zařízení. Riziko odcizení nebo neautorizovaného přístupu k vaší digitální měně je takřka úplně eliminováno. Hardwarové peněženky a trezory pro Bitcoin a jiné kryptoměny jsou mnohem bezpečnější než běžné softwarové peněženky, které jsou nainstalovány v počítači. K němu se připojují většinou přes USB port.

Hlavní výhody:
Jsou imunní vůči počítačovým virům, které se pokouší krást údaje a bitcoiny z klasických softwarových peněženek.
Soukromé klíče jsou uloženy v chráněné oblasti a nemohou být ze zařízení přenášeny v podobě holého textu.
Přístup k zařízení je chráněn PINem.
Potvrzení transakce převodu měny se autorizuje heslem.
Když peněženku ztratíte nebo se rozbije, můžete pro obnovení dat použít seed, který se skládá z 24 náhodných slov a je generován při prvním spuštění peněženky.

Mezi nejvíce používané patří zařízení TREZOR od české společnosti Satoshi Labs a Ledger Nano S od francouzské společnosti Ledger.

5.4 Papírová peněženka

Papírová peněženka patří mezi hojně používané. Její přednosti jsou zabezpečení a jednoduchost. Svoje privátní klíče uchováváte offline mimo dosah hackerů. V podstatě tak přesouváte problematiku obrany ze světa elektronického do světa fyzického.

Je to papírový dokument, na kterém máte uložené svoje soukromé a veřejné klíče, většinou ve formě QR kódu, jenž si vygenerujete na internetu. Pokud chcete vykonat transakci, naskenujete QR a zadáte potřebná hesla do softwarové peněženky.

6 Jiné kryptoměny

V dnešní době existuje více než tisíc kryptoměn. Většina z nich funguje na podobném principu jako Bitcoin. Lišit se můžou používanou hash funkcí, použitím, rychlostí transakcí. Některé kryptoměny dokonce místo Proof of Work používají Proof of Stake. Algoritmus Proof of Stake rozhoduje o tvůrci nového bloku deterministicky, podle jeho bohatství („sázky“7). Všechny kryptoměny mimo Bitcoin bývají označovány jako alternativní kryptoměny (altcoiny).

[7] Anglicky stake – odtud Proof of Stake.

6.1 Ethereum

Ethereum je v současnosti druhá nejznámější a druhá největší (co se trhové kapitalizace týče) kryptoměna. Je to platforma pro tvorbu tzv. chytrých kontaktů. Chytrým kontraktem je označován protokol, jenž zajišťuje, ověřuje a vynucuje provedení smlouvy či dohody takovým způsobem, že eliminuje nutnost skutečné smlouvy uzavřené mezi lidmi. Ethereum využívá kryptografickou funkci SHA-3.

6.2 Litecoin

Litecoin je stejně jako Bitcoin decentralizovaná peer to peer platební síť. Výhoda oproti Bitcoinu je rychlost transakcí. Litecoin dokáže pojmout až 56 transakcí za sekundu.

7 Závěr

Na závěr bych chtěl dodat, že jsem si téma Bitcoin vybral hlavně, protože to byl revoluční nápad a historicky první kryptoměna. Historické prvenství se značně projevuje v jeho problémech. Velká část z novějších kryptoměn dokonce dokáže zpracovat větší počet transakcí za sekundu a jsou tedy vhodnější jakožto platební systém. Dle mého názoru je budoucnost spíše v alternativních kryptoměnách.

.

8 Zdroje

[1] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. In: *Bitcoin.org* [online]. [cit. 2018-04-25]. Dostupné z: https://bitcoin.org/bitcoin.pdf

[2] *Úvod do kryptografie* [online]. [cit. 2018-04-26]. Dostupné z: http://www.earchivace.cz/technologie/uvod-do-kryptografie/

[3] 3BLUE1BROWN. *Ever wonder how Bitcoin (and other cryptocurrencies) actually work?* [online]. In: . [cit. 2018-04-26]. Dostupné z: https://youtu.be/bBC-nXj3Ng4

[4] HUŘŤÁK, Petr. *Analýza virtuální měny Bitcoin* [online]. [cit. 2018-04-26]. Dostupné z: https://vskp.vse.cz/id/1244711. Bakalářská práce. VŠE FIS.

[5] Wikipedie: Otevřená encyklopedie: Satoshi Nakamoto [online]. 2018 [citováno 25. 04. 2018]. Dostupný z WWW: <https://cs.wikipedia.org/w/index.php?title=Satoshi_Nakamoto&oldid=15779226>

[6] *Hardware peněženky* [online]. In: . [cit. 2018-04-26]. Dostupné z: https://www.alza.cz/hardware-penezenky-a-trezory/18862141.html

[7] HRACH, Jan. *Decentralizovaná kryptoměna Bitcoin* [online]. In: . 2011 [cit. 2018-04-26]. Dostupné z: http://www.abclinuxu.cz/clanky/decentralizovana-kryptomena-bitcoin

[8] MIKSA, Martin. *5 způsobů, jak uložit kryptoměny* [online]. In: . [cit. 2018-04-30]. Dostupné z: https://www.zive.cz/clanky/5-zpusobu-jak-ulozit-kryptomeny-od-pohotove-penezenky-po-nedobytny-trezor/sc-3-a-192275/default.aspx#part=2

[9] YOUNG, Joseph. *Bitcoin infaltion* [online]. In: . [cit. 2018-04-30]. Dostupné z: https://cointelegraph.com/storage/uploads/view/1d067f3721f10f0a76439de9860a4e54.png

Seznam obrázků

Rejstřík