ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA ELEKTROTECHNICKÁ

DIPLOMOVÁ PRÁCE

2016 BC. EVA LADOMERSKÁ

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA ELEKTROTECHNICKÁ

KATEDRA EKONOMIKY,

MANAŽERSTVÍ

A HUMANITNÍCH VĚD

DIPLOMOVÁ PRÁCE

DIGITÁLNÍ MĚNY: ANALÝZA ENERGETICKÉ NÁROČNOSTI TĚŽBY BITCOINŮ

VIRTUAL CURRENCIES: ANALYSIS OF THE ENERGY CONSUMPTION OF BITCOIN MINING

VEDÚCI: ING. JÚLIUS BEMŠ, PH.D.

VYPRACOVALA: BC. EVA LADOMERSKÁ

České vysoké učení technické v Praze
Fakulta elektrotechnická

Katedra ekonomiky, manažerství a humanitních věd

ZADÁNÍ DIPLOMOVÉ PRÁCE

Student: Ladomerská Eva

Studijní program: Elektrotechnika, energetika a management
Obor: Ekonomika a řízení energetiky

Název tématu: Digitální měny: Analýza energetické náročnosti těžby Bitcoinů

Pokyny pro vypracování:

- rešerše měnových soustav ve světě
- popis fungování virtuální měny Bitcoin
- porovnání Bitcoin s ostatními kryptoměnami
- analýza energetické náročnosti těžby Bitcoinů

Seznam odborné literatury:

Nakamoto, S. (2009): "Bitcoin: A Peer-toPeer Electronic Cash System".
Chuen D.L.K. (2015) Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data
Ďurša, M. (2011): "Zlatý štandard a jeho potenciál pre nadchádzajúci menový systém"

Vedoucí diplomové práce: Ing. Július Bemš, Ph.D. – ČVUT FEL, K 13116

Platnost zadání: do konce letního semestru akademického roku 2016/2017

L.S.

Prof.Ing. Jaroslav Knápek, CSc.
vedoucí katedry

Prof.Ing. Pavel Ripka, CSc.
děkan

V Praze dne 11.2.2016

Prehlásenie

Prehlasujem, že som predloženú prácu vypracovala samostatne a že som uviedla všetky použité informačné zdroje v súlade s metodickým pokynom o dodržiavaní etických princípov pri príprave vysokoškolských záverečných prác.

V Prahe dňa: ……..…….. ……..……..

Bc. Eva Ladomerská

Poďakovanie

Na tomto mieste by som sa rada poďakovala Ing. Júliusovi Bemšovi, Ph.D. zato, že mi umožnil vybrať si túto tému. Zároveň ďakujem Nickovi Szabovi a Satoshimu Nakamotovi, vďaka ktorým svet objavil decentralizované digitálne kryptomeny.

Anotácie

Cieľom tejto diplomovej práce je pochopenie problematiky digitálnych kryptomien, predovšetkým najznámejšej z nich - bitcoinu. Postupne vysvetľujem základné pojmy ako mining, blockchain, virtuálna peňaženka a iné. Samostatná kapitola je venovaná energetickej náročnosti celej bitcoin siete a je zhodnotená udržateľnosť tohoto nového konceptu.

Summary

The aim of this thesis is the understanding of digital cryptocurrencies, especially the most famous of them - Bitcoin. Keywords like mining, blockchain, virtual wallet and others are explained step by step. A separate chapter is devoted to the energy consumption of the whole bitcoin network and the sustainability of this new concept is evaluated.

Abstrakt

Táto práca predstavuje stručný úvod do pochopenia digitálnej kryptomeny Bitcoin. Bitcoin je najznámejšia a najpoužívanejšia digitálna kryptomena dneška, s ktorou sa bez problémov nakupujú tovary cez internet, ale dá sa ňou zaplatiť aj za obed v reštaurácii. Po vysvetlení základných používaných pojmov je ďalšia časť práce venovaná princípu ťažby. Ťažba alebo mining bitcoinov je proces vytvárania Bitcoinov, pri ktorom ťažobné zariadenie počíta zadanú kryptografickú úlohu, s cieľom vyťaženia nových Bitcoinov. Pri tomto procese zariadenia spotrebúvajú elektrickú energiu. V práci sa sústreďujem aj na ekonomické posúdenie Bitcoinov a vymenúvam jeho najdôležitejšie výhody a nevýhody. Osobitná kapitola je venovaná alternatívnym kryptomenám tzv. altcoinom, ktoré vznikli na báze Bitcoinu, ale snažia sa ho v niečom zdokonaliť a tak isto začínajú hrať dôležitú úlohu vo finančnom svete. Záver práce je venovaný energetickému aspektu celého Bitcoin projektu. V prvej časti si ako potenciálny miner vyberiem zariadenie na ťažbu a stanovím denné náklady na spotrebu elektrickej energie a zároveň aj denné výnosy za vyťažené Bitcoiny pri zvolenom výmennom kurze a pri predpokladanej náročnosti ťažby. Výsledkom je určenie ekonomickej výhodnosti ťažby za sledované obdobie. Druhou úlohou tejto práce je stanoviť energetickú náročnosť Bitcoin siete. Pretože neexistujú žiadne relevantné informácie o spotrebe elektrickej energie touto sieťou, namodelovala som tri typy siete v závislosti na efektivite ťažby (t.j. koľko Joulov sa spotrebuje na vyťaženie Bitcoinu) od najmenej efektívnej, cez priemernú až po najefektívnejšiu. Veľmi dôležitým vstupom bola náročnosť ťažby, ale pretože je zaznamenaná v rôznych databázach a voľne dostupná online, jediným odhadom v celom výpočte bola práve spomínaná efektivita siete. Vo výsledku som dostala číselný interval, v ktorom sa pravdepodobne nachádza aj skutočná hodnota tejto elektrickej spotreby.

Kľúčové slová: digitálne meny, Bitcoin, ťažba, energetická náročnosť, ASIC

Abstract

This thesis represents a brief introduction to understanding digital cryptocurrency Bitcoin. Nowadays, Bitcoin is the most famous and used digital cryptocurrency, which allows buying goods online without problems as well as paying for lunch in a restaurant. After explaining the basic terms used in the text another part of the thesis is devoted to the principles of mining. Bitcoin mining is the process of creating Bitcoins, in which mining equipment is solving cryptographic problem in order to mine new Bitcoins. In this process, mining devices consume electricity. In this thesis I am also focusing on the economic evaluation of Bitcoin and the most important advantages and disadvantages are listed. Separate chapter is devoted to alternative cryptocurrencies called altcoins, which are based on Bitcoin but are trying to improve it and are beginning to play an important role in the financial world. The final part of the thesis is dedicated to the energy aspects of the entire Bitcoin project. In the first part I am selecting mining equipment as a potential miner and setting daily cost of electricity consumption and also daily revenue for mined Bitcoins assuming exchange rate and mining difficulty. The result is the determination of the economic benefit of mining for the specified time period. The second task of this thesis is to determine the energy consumption of Bitcoin network. Because there are no relevant information about electricity consumption of the network, I modelled three types of networks, depending on their efficiency of mining (i.e., how many Joules are consumed to mine a Bitcoin): the least efficient, average and the most effective. Very important input was the difficulty of mining, but since it is recorded in different databases and accessible online, the only assumption in the whole calculation was network efficiency mentioned above. As a result, I got a numeric interval, in which the real value of electricity consumption probably is.

Key words: digital currencies, Bitcoin, mining, energy consumption, ASIC

Obsah

Zoznam obrázkov

Zoznam tabuliek

Zoznam grafov

Úvod

Peniaze a meny vždy boli a sú centrom pozornosti ekonómov, ale aj súčasťou každodenného života. Spravovanie peňazí bolo technicky náročné, až kým internet neumožnil vznik digitálnych mien, ktoré na svoju funkčnosť vyžadovali len počítačovú sieť. Na internete sa postupom času začalo objavovať množstvo digitálnych mien. Určite sa už väčšina z nás stretla s Microsoft bodmi, Facebook kreditmi alebo debetnými a kreditnými kartami. V poslednom desaťročí sa však vznik digitálnych mien exponenciálne zvýšil a narástol aj ich hospodársky význam, pretože vďaka nim prebiehajú obchody v nezanedbateľných finančných čiastkach. Digitálne peniaze sa vymieňajú výhradne elektronicky najmä v internetovom prostredí a môžu, ale nemusia byť kryté zlatom. V tejto práci budem skúmať predovšetkým digitálnu kryptomenu s názvom bitcoin. Dôvodom prečo je bitcoin spomedzi všetkých mien taký výnimočný je jeho úplná decentralizácia. Bitcoiny neriadi žiaden človek, žiadna banka, štát či spoločnosť. Neexistuje žiadna bitcoinová budova alebo firma bitcoinu a dokonca neexistuje ani žiaden centrálny server, ktorý sa dá vypnúť a tak narušiť jeho funkčnosť. Bitcoin teda ako prvý na svete umožňuje online transfer financií medzi dvoma klientmi bez akéhokoľvek zásahu tretej strany.

Do momentu vynájdenia bitcoinu, sa finančný transfer vždy konal prostredníctvom banky, PayPalu alebo iných inštitúcií. Dôvod je úplne jednoduchý. Pre online platbu sa peniaze museli stať digitálnym súborom v počítači, ktorý potom odosielateľ poslal príjemcovi. Pretože ak súbor napr. fotku pošlem z môjho počítača na iný, súbor stále ostane na mojom počítači a nevymaže sa tým, že ho pošlem, tento súbor môžem poslať aj 10 iným ľuďom. V počítačovom prostredí sa tomu hovorí double - spending problem, teda rovnaký obnos peňazí sa môže poslať nekonečne mnohokrát rôznym príjemcom bez toho, aby o tom oni vedeli. Pred bitcoinom tento problém riešila práve tretia strana, ktorá plnila v podstate úlohu veľkej účtovnej knihy, v ktorej boli zaznamenané všetky transfery. Tajomstvo bitcoinu spočíva v tom, že táto účtovná kniha je rozposlaná všetkým účastníkom siete, ktorí ju zaznamenávajú a kontrolujú. Bitcoin je teda prvá úplne decentralizovaná digitálna kryptomena na svete.

Bitcoin ako mena však so sebou prináša aj otázky týkajúce sa základných funkcií peňazí a ich právnej definície. Pretože bitcoin je nový koncept, prirodzene obsahuje aj slabšie miesta a ponúka mnoho možností na vylepšenie svojej funkčnosti. Medzi zásadné obavy a výčitky skeptikov patrí najmä energetická náročnosť získavania bitcoinov. Existuje mnoho publikácií, článkov, ale aj laických výpočtov koľko elektrickej energie vlastne bitcoin sieť spotrebuje, no

takmer všetky tieto údaje spolu nekorešpondujú. Znamená to, že určenie spotreby energie je veľmi náročné a extrémne závisí na zvolených vstupných údajoch

Ťažba bitcoinov sa vo svojej podstate začala veľmi podobať na ťažbu zlata, pretože s pribúdajúcim časom je ich ťažba čoraz viac finančne náročná. Tak ako len zlomok ľudí zbohatol ryžovaním zlata počas kalifornskej zlatej horúčky v roku 1840, tak aj vytvorenie zisku ťažbou bitcoinov v roku 2016. Ťažba si totiž vyžaduje obrovské finančné prostriedky na infraštruktúru, vysoko špecializované vybavenie a v neposlednom rade aj minimálne technické zručnosti. V práci ponúknem prehľad najnovších dostupných technológií a spočítam, či sa ich oplatí kúpiť a začať na nich ťažiť.

Úvodná kapitola tejto práce sa v skratke pozrie na úlohu zlata v našej histórii už od dôb starovekého Egypta. Dôraz kladiem na zlatý štandard, ktorý vznikol v roku 1717 v Británii a naposledy našiel svoje uplatnenie v bretonwoodskom menovom systéme, ktorý fungoval do roku 1971. Následne je vysvetlené fungovanie súčasného menového systému, konkrétne systému čiastočných rezerv a „Quantitative Easing“. Súčasný bankový systém skrýva v sebe mnoho úskalí, ktoré postupne vysvetľujem.

Na začiatku druhej kapitoly som vysvetlila terminológiu, ktorá súvisí s bitcoinom (digitálne meny, kryptomeny, virtuálne meny...) a následne som popísala pojmy ako blok transakcií, blockchain, bitcoin peňaženka, privátny a verejný kľúč a iné. Na jednoduchom príklade som vysvetlila ako funguje transakcia v bitcoin sieti, či existujú transakčné poplatky a koľko bitcoinov je v obehu. V kapitole je detailne vysvetlená ťažba bitcoinov, čo je vlastne proces ich tvorby, je vysvetlený pojem náročnosti ťažby a na grafoch a tabuľkách je ilustrovaný jej časový vývoj. V technickej časti tejto kapitoly sú bližšie špecifikované zariadenia určené na ťažbu bitcoinov od CPU/GPU, cez FPGA až k súčasným ASIC minerom. Na záver sú porovnané technické parametre zariadení z roku 2013 a z roku 2016.

V tretej kapitole zisťujem, či bitcoin spĺňa základnú definíciu peňazí (prostriedok výmeny, uchovávateľ hodnôt a zúčtovacia jednotka). V krátkosti rozoberám veľmi zaujímavý finančný vývoj v Argentíne za posledné roky, ktorý mal za príčinu vznik jednej z najsilnejších bitcoin komunít na svete. Zároveň sú načrtnuté prekážky masového rozšírenia bitcoinov medzi bežnú populáciu ľudí. Na záver tejto kapitoly analyzujem hlavné výhody a nevýhody tejto kryptomeny. Snáď najvyzdvihovanejšie plus bitcoinov – sloboda v platení, je prezentovaná na konkrétnom príklade zo života a to darcovstvom peňazí organizácii WikiLeaks. Okrem toho som poukázala na jednoduchosť a lacnosť bitcoinových transakcií, z ktorých majú prospech aj

podnikatelia, aj ich zákazníci. Z najzávažnejších nevýhod som sa venovala uľahčeniu kriminálnej činnosti, ktoré bitcoin preslávilo pri odhalení nelegálneho trhu s názvom Silk Road. Potom som vysvetlila technický problém dvojitého utrácania a rôzne legislatívne nejasnosti, ktoré vznikli z dôvodu neexistencie jasnej definície bitcoinu.

Kapitola štyri je venovaná ostatným kryptomenám tzv. altcoinom, ktoré sa snažia vylepšiť pôvodný bitcoin protokol najrôznejšími spôsobmi, najčastejšie však zmenou protokolu proof-of-work, ktorý používa bitcoin a má samozrejme aj svoje nevýhody. Z mnohých vylepšení som nakoniec vybrala tie, ktoré zrýchľujú transakcie, využívajú proces ťažby aj na iné účely, riešia deflačný problém a sú viac anonymné. V tejto kapitole sa nachádzajú aj veľmi aktuálne a zaujímavé využitia technológie blockchain mimo bitcoinovej siete. Technológia blockchain si podľa môjho názoru naozaj zasluhuje pozornosť a dala by sa o nej napísať samostatná diplomová práca. Pretože však toľko priestoru nemám, snažila som sa vybrať a popísať tie najzaujímavejšie aplikácie a verím tomu, že mnoho implementácii čaká blockchain ešte v budúcnosti. Na úvod vysvetľujem pojem digitálnych aktív, ktoré veľmi úzko súvisia so smart kontraktmi, ktorým sa venujem tiež. Na záver som ešte spomenula aplikáciu blockchain technológie na trhu s realitami.

Posledná kapitola približuje energetickú stránku celého bitcoin projektu. V prvej podkapitole som sa ako potenciálny miner rozhodla vytvoriť si vlastnú kalkulačku na výpočet výhodnosti resp. nevýhodnosti ťažby bitcoinov. Jednu zo zásadných úloh v tomto výpočte zohráva práve cena za spotrebovanú elektrickú energiu, ktorá je priamo ovplyvnená efektivitou ťažobného zariadenia a cenou elektrickej energie. V práci som prezentovala 2 rôzne varianty výsledku a to raz s optimistickými predpokladmi a raz s predpokladmi pesimistickými. V druhej časti tejto kapitoly som na úvod priblížila rôznorodosť informácií týkajúcich sa spotreby elektrickej energiu celou bitcoin sieťou. Pretože tieto dáta sú značne odlišné a neaktuálne, spočítala som energetickú spotrebu 3 rôznych modelový bitcoin sietí. Na záver som ešte porovnávala náklady na ťažbu bitcoinov, ťažbu zlata a na chod súčasného bankového systému.

Táto diplomová práca poskytuje ucelený pohľad na tému bitcoin, jednu z najaktuálnejších tém dneška.

1 Zlatý štandard a súčasný menový systém

„Peniaze sú zvláštnym merítkom hodnoty. V našej kultúre sú všadeprítomné a tak zásadné pre naše životy, no napriek tomu si málokedy sadneme a zamýšľame sa čo vlastne predstavujú, odkiaľ sú, čo robia a kto ich vlastne kontroluje. Väčšina z nás trávi prevažnú časť svojho času ich naháňaním bez skutočného pochopenia ich podstaty.“ ~ Charles Curtis

Prakticky už od svojho objavenia zlato hralo rolu pri zmene tovarov a stalo sa platobným prostriedkom. Je to vôbec jeden z prvých kovov, ktorý sa vo svete začal ťažiť kvôli tomu, že sa v prírode vyskytuje v rýdzej a ľahko dostupnej forme. Vôbec prvé nájdené ohodnotenie zlata pochádza zo starobylého Egypta, kde faraón Meni určil, že jedna časť zlata je rovnako cenná ako 2,5 rovnakej časti striebra. Ešte aj v dnešnej modernej dobe, je to stále vyhľadávaný artikel pre investorov a hľadaný uchovávateľ hodnoty. Značnou výhodou zlata oproti iným investičným nástrojom je možnosť uložiť si veľký finančný obnos do fyzicky malého objemu látky. Ako už napovedá samotný názov, hodnota meny bola teda odvodená od definovaného množstva zlata. Ďalším dôvodom prečo je zlato tak cenené sú jeho vlastnosti: vysoká trvanlivosť, poddajnosť a trvalý lesk. Okrem toho je zlato zabezpečené aj pred infláciou, pretože jeho ťažba sa stáva čoraz nákladnejšou a ťažšou záležitosťou.

V 17. a 18. storočí sa kvôli nedostatku čistého zlata razili mince s prímesou striebra. Problém bol, že tento bimetalický systém sa nevyrovnal s rôznym pomerom zlata a striebra v minciach, a tak ho nahradil tzv. klasický zlatý štandard. Sir Isaac Newton, vtedajší vedúci britskej Kráľovskej komisie, určil cenu mince (pomer zlata a striebra 1:16) na 21 šilingov. Pretože to znamenalo, že v Británii bolo zlato drahšie ako v zbytku Európy, nastal masový výkup striebra v Európe, ktoré sa následne vymenilo za zlato. Do Británie sa týmto spôsobom dostal dostatočný objem zlata na to, aby sa zrušilo razenie mincí s prímesou striebra a tak vznikol prvý zlatý štandard. Obdobie tohto historicky prvého zlatého štandardu sa udáva od roku 1717 do roku 1797. Počas tohto obdobia, boli všetky peniaze naozaj kryté zlatom, t.j. všetky peniaze v obehu zodpovedali množstvu zlata v bankových trezoroch. [1]

Obrázok 1: Britská zlatá minca z roku 1717.

V Británii bol tento systém znova zavedený v roku 1816 a v USA v roku 1900. Takto sa postupom času zlatý štandard dostal aj do ostatných zemí a vydržal približne do začiatku prvej svetovej vojny. Obdobie medzi rokmi 1871 až 1914 sa nazýva aj obdobím klasického zlatého štandardu. Hodnota amerického dolára bola definovaná ako 1/20 unce zlata. Obchodníci teda mohli plánovať svoju budúcnosť presnejšie, lebo vždy vedeli aký bude výmenný kurz. Zároveň nevznikali ani žiadne ekonomické bubliny a ani žiadne veľké býčie trhy. Dôvodom prečo sa tento systém začal počas vojny oslabovať je jednoduchý - vojna bola príliš drahá a štáty nevlastnili dostatok zlata na krytie svojich výdajov, preto sa postupne opäť začali vydávať peniaze nekryté zlatom. [1]

V medzivojnovom období vznikli pokusy ako napríklad štandard zlatej devízy (meny sa dali vymeniť za libru, dolár a frank, ktoré sa následne dali vymeniť za zlato) alebo štandard zlatého zliatku (peniaze čiastočne kryté zlatom, možnosť vymeniť si ich za zlato bola však limitovaná obrovským objemom - existovali len 12 kg zlaté tehly). Klincom do rakvy zlatému štandardu bola obrovská kríza v roku 1933. Nezamestnanosť v USA dosiahla 28% a americká vláda pod hrozbou pokuty a vezenia odobrala svojim obyvateľom všetko zlato, čo bolo de facto zrušenie zlatého štandardu. Americká verejnosť nemohla vlastniť zlato ešte ďalšie 3 roky, čo bolo vzhľadom na rastúce ceny zlata na burze dosť znevýhodňujúce. 2. svetová vojna návrat k tomuto systému úplne znemožnila. [1]

Posledným menovým systémom, kde zlato hralo prím, bol brettonwoodsky menový systém v rokoch 1945-1971. Pre fungovanie tohto systému vznikli inštitúcie Medzinárodný menový fond a Medzinárodná banka pre obnovu a rozvoj. V tomto systéme bol na zlato priamo naviazaný americký dolár. Ostatné meny mali zafixovaný kurz na dolár a mohli sa zameniť za

zlato len prostredníctvom centrálnych bánk. Jednou z nevýhod tohto systému bolo práve dominantné postavenie dolára a fakt, že systém sa nestal celosvetovým. Hodnota amerického dolára bola definovaná ako 1/35 unce zlata. Rozhadzovačnosť americkej vlády v 70-tych rokoch však aj tento systém pochovala. [2]

Zlatý štandard sa už nikdy viac v histórii nezrealizoval, aj keď k jeho znovuzavedeniu vyzývajú najmä libertariáni a zástanci rakúskej školy ekonómie. V praxi sa teda všetky meny stali nekrytými a jednotlivé vlády si mohli natlačiť toľko vlastnej meny, koľko chceli.

V súčasnosti vystupujú peniaze ako neplnohodnotné peniaze s núteným obehom. Nemajú svoju vlastnú hodnotu a za peniaze sú prehlásené vládou a štát garantuje ich kúpnu silu. Centrálna banka reguluje množstvo peňazí v obehu, čím sa snaží udržiavať stabilnú cenovú hladinu. Rozlišujeme hotovostné peniaze ako mince a papierové bankovky a bezhotovostné peniaze alebo depozitá, ktoré predstavujú prostriedky uložené na účtoch v bankách, či v iných finančných inštitúciách. [3] Pretože došlo k demonetarizácii, t.j. poklesu významu zlata a jeho pôsobenia v technicko-ekonomických funkciách, treba si objasniť ako v súčasnosti peniaze vznikajú. Existujú dva spôsoby vzniku peňazí a obidva vysvetlím v nasledujúcich odstavcoch.

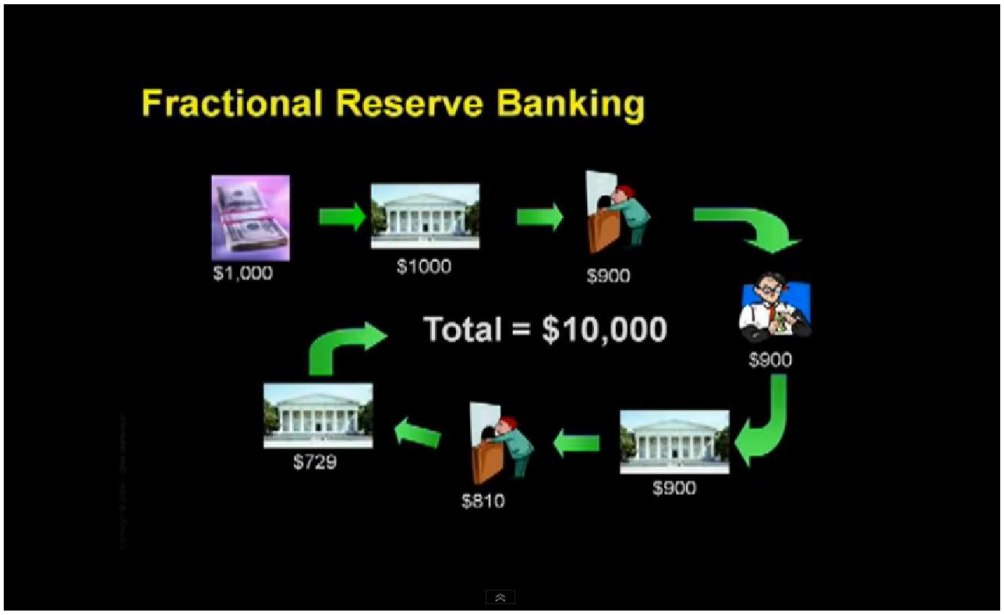
1. Systém čiastočných rezerv

„Proces, akým banky vytvárajú peniaze je tak jednoduchý, že to rozum ani nechce prijať.“ ~ John Kenneth Galbraith

Systém tvorby peňazí je úplne jednoduchý, no zároveň tak bizarný, že je ťažké si ho naozaj osvojiť a akceptovať. Na nasledujúcom príklade ukážem, ako banka vytvorila z 1 000 $ skutočne až 10 000 $. Celý proces je pre zjednodušenie ilustrovaný aj na obrázku 2.

Predpokladajme, že sa nezaujímame odkiaľ sa 1 000 $ na začiatku procesu vzalo. Povedzme, že do mesta príde muž a má 1 000 $ vo svojej peňaženke. Týchto 1 000 $ však nechce nosiť pri sebe a tak ich uloží v nejakej komerčnej banke. V tejto chvíli, má muž majetok v hodnote 1 000 $ (vlastní účet v banke) a banka má záväzok 1 000 $ (ten istý účet). Predpokladajme, že komerčná banka musí držať 10% rezervu u centrálnej banky na krytie svojich pôžičiek (v Austrálii, na Novom Zélande a vo Švédsku je rezerva 0%). Teoreticky banka môže až 90% čiastky z vkladu požičať ďalším ľuďom. Pretože iba časť vkladov musí banka držať ako rezervu, tento proces sa nazýva systémom čiastočných rezerv. Čiže ako môžeme vidieť na obrázku 2, týchto 1 000 $ sa rozdelí na 100 $, ktoré necháva banka ako som

už spomenula u centrálnej banky a zvyšných 900 $ použije na poskytovanie pôžičiek. Povedzme, že náš kamarát si prišiel do tejto banky tých 900 $ požičať a zaplatí za nich svojho účtovníka. Ako možno vydedukovať ďalej z obrázku 2, tak účtovník si týchto 900 $ uložil do svojej komerčnej banky (môže ísť aj o tú istú banku) a jeho banka si týchto 900 $ opäť rozdelí na 90 $ dolárov, ktoré drží u centrálnej banky a zvyšných 810 $, ktoré požičia nejakému subjektu v ekonomike. Ďalšia komerčná banka môže požičať už len 729 $ a ďalšie po nej stále menej a menej až kým sa nedostaneme na nulu, kde sa systém multiplikácie peňazí prostredníctvom komerčných bánk zastaví. Ak spočítame množstvo poskytnutých pôžičiek tak sa dostaneme k číslu 10 000 $, ktoré predstavujú novovytvorené peniaze v obehu. Ako vidíme na tejto schéme, týchto 10 000 $ bolo vytvorených na základe iba 1 000 $ vkladu, t.j. banka si vo forme pôžičiek vyrobila 10-násobne viac peňazí. Jednoducho povedané, banka vytvorí toľko peňazí, koľko sme si ochotní požičať a celkový dlh v ekonomike bude vždy väčší ako množstvo peňazí, ktoré sa dajú použiť na jeho splatenie. [4]



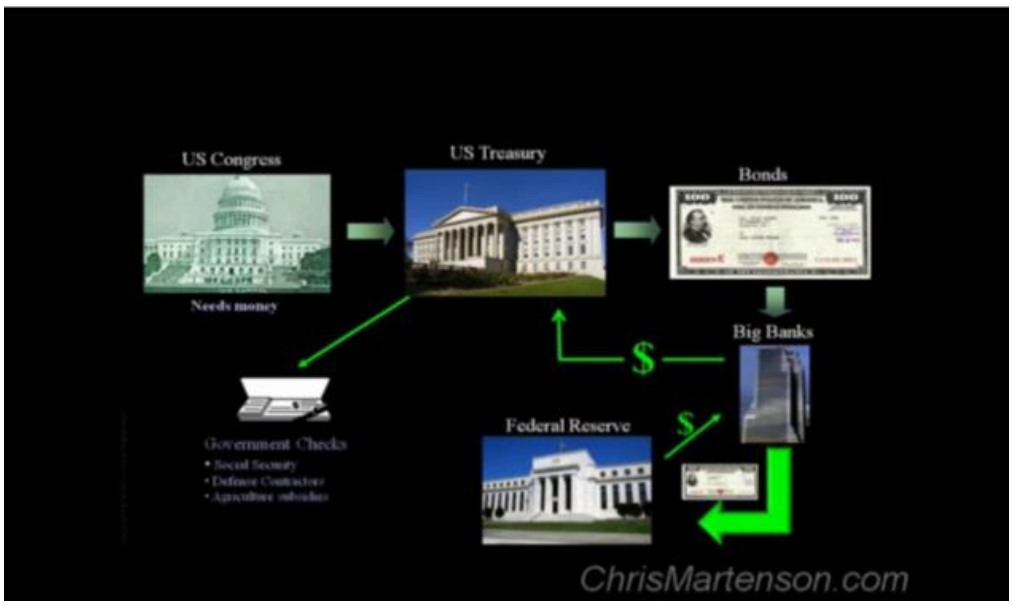
Obrázok 2: Bankový systém čiastočných rezerv, alebo ako sa z 1 000 $ stane vďaka bankám až 10 000 $.

Komerčné banky týmto spôsobom vlastne vytvorili 10-krát viac peňazí skrz pôžičky. Pretože však tieto peniaze vznikli v podstate z ničoho a úplne nezávisle na ekonomickom raste, znížili kúpnu silu všetkých ostatných dolárov na trhu. Tento proces generovania peňazí má v sebe priamo zabudovanú infláciu, ktorej sa teda nedokážeme žiadnym spôsobom zbaviť. Okrem toho sú tu ešte dva zásadné problémy, ktoré sa neriešia. Prvým problémom je, že ak sa

všetci klienti banky naraz rozhodnú vybrať si svoje úspory, banka ich nebude mať z čoho vyplatiť. Druhým závažným problémom je, že ak ktorýkoľvek subjekt v našej schéme skrachuje, nebude mať kto splácať dlhy. Tento zjavne dlhodobo neudržateľný peňažný systém funguje na celom svete od roku 1971. [4]

2. Nákup štátnych dlhopisov prostredníctvom centrálnej banky

Teraz si vysvetlíme odkiaľ sme v predchádzajúcom príklade vzali tých 1 000 $. Predstavme si, že vláda (US Congress) potrebuje viac peňazí, ako v skutočnosti má, a preto o nich požiada ministerstvo financií (US Treasury). Pretože ani ministerstvo financií nemá práve toľko peňazí koľko vláda požaduje, rozhodne sa konať a vydá štátne dlhopisy (Bonds). Povedzme, že nominálna hodnota dlhopisu je 100 $ a úrok je 5%. Tento dlhopis sa zaradí do verejnej aukcie a veľkú väčšinu týchto dlhopisov nakúpia gigantické banky ako J.P Morgan, Commerzbank, ICBC a iné (Big Banks). Peniaze, za ktoré si banky nakúpili dlhopisy, teda putujú od ministerstva financií až k svojmu cieľu do kongresu. Zatiaľ sme teda žiadne nové peniaze nevytvorili, pretože dlhopisy sa nakúpili za peniaze, ktoré už existovali. Peniaze sa vytvoria v momente, kedy centrálna americká banka FED kúpi spomínané dlhopisy od bánk, alebo iných finančných inštitúcií. FED zaplatí bankám za dlhopisy. Banky teda majú peniaze a FED dlhopisy. Kde ale FED zobral peniaze na tieto dlhopisy? Jednoducho si ich vytlačil. Tento proces sa v angličtine nazýva Quantitative Easing. [4] Celý proces je zobrazený na obrázku 3.



Obrázok 3: Operácie na otvorenom trhu pri kúpe štátneho dlhopisu (US Congress - vláda, US Treasury – ministerstvo financií, Bonds – dlhopisy, Federal Reserve alebo FED – centrálna banka USA, Big Banks – veľké banky).

„Ak ja alebo ty vypíšeme šek, musíme mať na účte dostatok peňazí na jeho krytie. Ak vystaví šek FED, neexistuje žiadny bankový vklad, z ktorého by sa peniaze za šek dali uhradiť. Ak FED vystaví šek, vytvoril nové peniaze.“ ~ Putting it Simply, Boston Federal Reserve

Zatiaľ čo bežný Američan si musí svoje peniaze zarobiť a riskovať pri ich zhodnocovaní, FED jednoducho tlačí toľko peňazí koľko potrebuje. Okrem všetkých spomínaných úskalí tohto systému, sme pre jednoduchosť nepočítali s úrokmi na úveroch. Potom môžeme konštatovať, že každý rok musí byť požičané dostatočné množstvo peňazí, aby sa nimi mohli zaplatiť úroky z minulých pôžičiek a samotné dlhy urobené v minulosti. [4]

2 Bitcoiny

2.1 Použitá terminológia

Pri čítaní článkov o bitcoinoch som sa často stretávala s pojmami virtuálne a digitálne meny, pričom sa používali ako synonymá. Nie je to však pravda a kľúčovú úlohu zohráva najmä samotná funkcia danej meny. Ak napríklad počujem pojem digitálna mena, napadnú ma peniaze v elektronickej (bezhotovostnej) podobe, ktoré bežne používame v reálnom živote. Na rozdiel od toho, pri pojme virtuálna mena, väčšinu z nás napadnú peniaze používané v počítačových hrách ako EVE online (ISK), WoW (gold) alebo v online virtuálnych svetoch ako Second Life (Linden) alebo aj Facebook kredity. Zásadný rozdiel medzi týmito menami je, že virtuálne meny sú obmedzené na použitie len v rámci určeného ekonomického systému. Môžu byť zmenené za existujúce reálne meny, ale väčšinou iba jednosmerne t.j. reálne peniaze môžeme zameniť za virtuálne ale nie naopak. Tieto herné peniaze sú preto komoditou a nie médiom výmeny a teda ani nie sú peniazmi v pravom slova zmysle. V tejto práci budem kvôli tomu v súvislosti s bitcoinami používať pomenovanie digitálna mena. [5]

Ďalším dôležitým postrehom je, že pod pojmom bitcoin sa rozumie aj platobný systém (napr. ako PayPal), ale aj samotné platidlo v tomto systéme. V niektorej literatúre sa tieto pojmy rozlišujú malým a veľkým písmenom t.j. Bitcoin je platobný systém a bitcoin je mena. V tejto práci toto rozlišovanie nebudem používať, pretože z kontextu bude vždy jasne vyplývať, o ktorom pojme sa hovorí.

2.2 Technológia v pozadí bitcoinu

Bitcoin platobná sieť je peer-to-peer sieť (P2P, sieť typu klient-klient). Uzlovými bodmi v tejto P2P sieti sú všetky počítačové systémy, ktoré majú nainštalovaný príslušný software. Každý jeden uzol overuje, uchováva a propaguje informácie všetkým ostatným uzlom, ktoré sú pripojené. Týmto spôsobom, sa informácie šíria po celej sieti. Platobná transakcia môže obsahovať ľubovoľný počet vstupov a výstupov. Vstup obsahuje odkaz na výstup z predchádzajúcej transakcie. Výstup obsahuje doručovaciu adresu a príslušnú čiastku. Bitcoinová sieť využíva tzv. proof-of-work protokol (PoW), čo znamená, že systém vyžaduje od užívateľa nejaký výpočet, ktorý stojí čas a softwarovú kapacitu a za to ho odmení. Tento výpočet je úplne náhodný a využíva metódu pokus-omyl. Preto má užívateľ s väčšou výpočtovou kapacitou väčšiu šancu, že sa mu výpočet podarí a za odmenu dostane bitcoiny. [6]

- Čo je to blok transakcií?

Kompletná história všetkých uskutočnených transakcií je uložená u každého minera, takže každý môže overiť, kto je v danej chvíli majiteľom konkrétnych bitcoinov. Transakcie sa združujú do tzv. blokov. Počet transakcií v bloku je rôzny a závisí od veľkosti jednotlivých transakcií. Veľkosť bloku je obmedzená na 1 MB, aby sa zabezpečilo jeho rýchle šírenie bez chýb. Veľkosť jednotlivých transakcií určuje počet ich vstupov a výstupov. Nasledujúca tabuľka 1 reprezentuje blok, ktorý sa skladá z 2 častí: hlavička (žltá farba) a telo (zelená farba). Samotné transakcie sa nachádzajú v tele bloku, zatiaľ čo hlavička pozostáva zo siedmich polí. Prvou transakciou je špeciálna coinbase transakcia, ktorá úspešnému minerovi poskytne bitcoiny ako odmenu za ťažbu. [7]

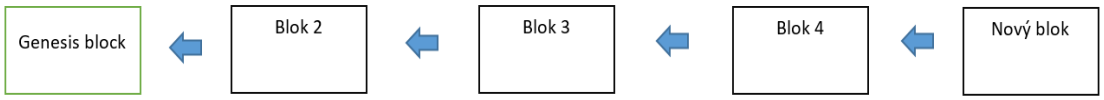
Version	02000000
Previous block hash (reversed)	1798932874gd937464uifj23rt597lk2n34ir93
Merkle root (reversed)	87y45toi5t8734n8h7kgwe5468546805jr749
Timestamp	358b0553
Bits	535f0119
Nonce	48750833
Transaction count	63
Transactions	

Tabuľka 1: Blok transakcií sa skladá z hlavičky (7 položiek, vyznačených žltou farbou) a tela (samotné transakcie, vyznačené zelenou farbou)

Version (verzia bloku) závisí na verzii softwaru, ktorý daný blok vygeneroval. Previous block hash je 256 bitový hash, ktorý slúži ako odkaz na predchádzajúci blok. Merkle root je

hash vytvorený z hashov všetkých transakcií, ktoré sú v bloku. Timestamp obsahuje časový údaj. Bits označuje súčasnú cieľovú hodnotu veľkosti hashu, ktorá sa zmenšuje s náročnosťou riešenia bloku t.j. je nepriamo závislá na zložitosti vytvorenia bloku. Nonce je 4 bajtové pole, ktorého hodnota sa mení tak, aby hash bol pod cieľom Bits. Začína s „0" a zväčšuje sa pre každý hash. Hodnota sa háda až kým sa nenájde hash obsahujúci požadovaný počet núl na začiatku. V predposlednom poli Transaction count je počet transakcií v danom bloku. V poslednom poli Transactions sú zapísané samotné transakcie t.j. adresy a čiastky. [7]

Blockchain je reťazec blokov, v ktorom sa nachádza záznam o všetkých transakciách tak ako napr. v účtovnej knihe. Poradie blokov indikuje poradie, v akom sa transakcie uskutočnili. Na obrázku 4 je znázornený blockchain, ktorý sa skladá z úplne prvého pôvodného bloku (Genesis block), z 3 skôr overených blokov a z najnovšie overeného bloku. Reťazec blokov slúži na potvrdenie toho, že odosielateľ naozaj bitcoiny vlastnil a transakcia sa uskutočnila. Nový blok je pripojený k predchádzajúcemu bloku reťazca zhruba každých 10 minút. [8]



Obrázok 4: Blockchain sa skladá z jednotlivých overených transakcií usporiadaných do blokov.

- Čo je to bitcoin peňaženka?

Aby užívateľ mohol uskutočniť bitcoin transakciu, počítačový program s názvom „peňaženka" mu vygeneruje verejný a privátny kľúč. Nový pár kľúčov je vygenerovaný pre každú jednu transakciu a je úplne nezávislý na predchádzajúcich kľúčoch. V programe peňaženka sú uložené bitcoinové adresy a im prislúchajúce kľúče. Bitcoin adresa je 160 bitový hash verejného kľúča a môžeme ju interpretovať jednoducho ako „číslo účtu". Adresa má 27 až 34 alfanumerických znakov. Bitcoin peňaženka overuje správnosť adresy pred každou transakciou. Adresa okrem toho obsahuje aj kontrolný kód, aby sa predišlo typografickým chybám. Zároveň adresa neobsahuje znaky veľké a malé „o", „l" a číslicu „0", aby nedošlo k chybe. Ak sa užívateľ pri zadávaní adresy pomýli o jeden znak, pravdepodobnosť, že táto adresa bude platná a transakcia sa odošle na spracovanie minerom je 1 ku 4.3 miliardám. [6]

Aj keď pojem bitcoin peňaženka budí dojem, že sú v nej uložené bitcoiny, nie je to pravda. Bitcoin peňaženky uchovávajú privátne a verejné kľúče, pomocou ktorých získava klient prístup k svojej bitcoin adrese a teda prístup k samotným bitcoinom. Privátne kľúče umožňujú bitcoiny utrácať, zatiaľ čo verejné umožňujú bitcoiny prijímať. Peňaženky majú rôzne formy a sú navrhnuté pre rôzne typy zariadení, na ktorých sa budú používať. Tak isto ako aj u fyzických peňaženiek, aj na bitcoin peňaženky resp. na privátne kľúče si treba dávať pozor a chrániť ich pred zlodejmi. Peňaženky môžeme rozdeliť do 5 základných kategórií - softwarová peňaženka, mobilná peňaženka, web peňaženka, papierová peňaženka a hardwarová peňaženka. Aký typ peňaženky si užívateľ zvolí záleží na jeho preferenciách - niektorí uprednostňujú komfort, iní zas bezpečnosť. Pre maximálnu bezpečnosť sa odporúča používať niekoľko typov peňaženiek naraz.

- **Softwarová peňaženka**

Je to vlastne počítačový program, ktorý si užívateľ stiahne a nainštaluje do svojho zariadenia. V tomto prípade, sú všetky kľúče uložené na harddisku daného zariadenia. Prvá originálna softwarová peňaženka má názov Bitcoin Core, a vyvinul ju samotný Satoshi Nakamoto. Je to v súčasnosti najviac preskúmaná a prepracovaná peňaženka na trhu a preto je veľmi dôveryhodná. Je však dôležité si uvedomiť, že Bitcoin Core je plnohodnotný uzol siete a preto vyžaduje, aby bol stiahnutý aj celý blockchain. K dispozícii je pre Windows, Linux, Mac OS a aj pre Personal Package Archives. [9]

- **Mobilná peňaženka**

Aplikácia inštalovaná priamo do mobilného telefónu. Samotné kľúče sú uložené priamo v mobile a s bitcoinami je možné platiť buď použitím skenovania alebo využitím QR kódu. Transakcie prebiehajú cez internet alebo Bluetooth. [10]

- **Webová peňaženka**

Pre užívateľa je najjednoduchšia, pretože informácie sú uložené na webovej stránke poskytovateľa, tzn. nie je to súbor v počítači a prístup k nej má užívateľ vždy a všade. Odpadá teda nutnosť zálohovania v počítači, čo je síce praktické, ale nesie so sebou nebezpečenstvo v podobe sprístupnenia informácii druhej strane. Je teda veľmi dôležité byť opatrný pri výbere poskytovateľa tejto služby, pretože už bolo zaregistrovaných viacero podvodných webových poskytovateľov. Jednou z najpoužívanejších je Coinbase. [10] Coinbase je online bitcoin účet trochu podobný PayPal-u. Má v sebe zabudovanú bitcoin zmenáreň, kde sa dajú kupovať

a predávať bitcoiny a taktiež umožňuje posielať a prijímať bitcoiny priamo z alebo do mailovej adresy. Coinbase je centralizovaný a ukladá všetky bitcoiny na svoju stránku. Samozrejme existujú isté bezpečnostné riziká, pretože prevádzkovatelia tejto služby majú plnú kontrolu nad všetkými bitcoinami, ale zatiaľ k žiadnym problémom nedošlo. K dispozícii už existuje aj ako aplikácia pre Android. [9]

- **Papierová peňaženka**

Je to služba na webovej stránke, ktorá generuje náhodné privátne a verejné kľúče a adresy s QR kódmi, ktoré sa potom vytlačia na papier. Je to teda jedna z najbezpečnejších možností, pretože kľúče nie sú žiadne súbory v počítači alebo na internete. Najpoužívanejšou je BitAddress Paper Wallet. Treba však dodať, že na uskutočnenie akejkoľvek transakcie, sa musí privátny kľúč previesť na digitálnu peňaženku. Preto sa toto riešenie odporúča najmä na dlhodobé držanie bitcoinov, lebo to nie je až tak praktické. [9]

- **Hardwarová peňaženka**

Tento druh peňaženky má podobu flash karty a jedná sa o pravdepodobne najbezpečnejší druh peňaženky. Táto peňaženka pri vytváraní novej adresy vygeneruje 12 slov zo svojej databáze, ktoré reprezentujú privátny kľúč. V prípade straty tejto peňaženky stačí kúpiť novú peňaženku, ktorá cez algoritmus pomocou 12 zadaných slov vypočíta privátny aj verejný kľúč. Je to lepší spôsob ako zapisovať si na papier 256-bitový privátny kľúč. Samotné transakcie sa uskutočňujú tak, že peňaženku treba pripojiť na zariadenie s prístupom na internet. Po tejto akcii vyskočí off-line statická stránka. V tejto statickej stránke sa môžu vytvárať transakcie. Následne vytvorená transakcia putuje do hardwarovej peňaženky, ktorá vyžaduje potvrdenie tlačidlom na peňaženke a zadanie čísel do statickej stránky, ktorá sa objaví na displeji peňaženky. Nasleduje ďalšie potvrdenie a po zadaní hesla sa táto transakcia podpisuje v peňaženke privátnym kľúčom a putuje do siete bitcoin cez pomocný webový server. [11]

- Ako funguje bitcoin transakcia?

Bitcoinové transakcie sú prevody medzi elektronickými bitcoin peňaženkami, ktoré sú kvôli bezpečnosti digitálne podpísané. Každý účastník bitcoin siete vie o všetkých transakciách a celá história transakcií je verejne prístupná až po úplne prvú. Dôležité je uvedomiť si, že tak ako bitcoiny neexistujú vo fyzickej podobe, neexistujú ani v podobe digitálnej na hardwari. Ak by sa užívateľ pozrel na nejakú bitcoin adresu, nevidel by tam žiadne bitcoiny v digitálnej forme, ako je to napríklad s peniazmi na bankovom účte. Namiesto toho existujú len záznamy

o transakciách medzi rôznymi adresami v blockchaine. Ak by užívateľ chcel zistiť zostatok bitcoinov na konkrétnej adrese musel by si ho vypočítať na základe informácií z blockchainu. [12]

Princíp transakcie je najlepšie ilustrovať na konkrétnom príklade. Dajme tomu, že Marika chce poslať bitcoiny Petrovi. Táto transakcia bude obsahovať tri informácie:

1. Vstup - záznam o tom, z ktorej bitcoin adresy sa bitcoiny dostali k Marike = bitcoiny jej poslala Helena.
2. Množstvo bitcoinov, ktoré Marika posiela Petrovi.
3. Výstup - Petrova bitcoin adresa.

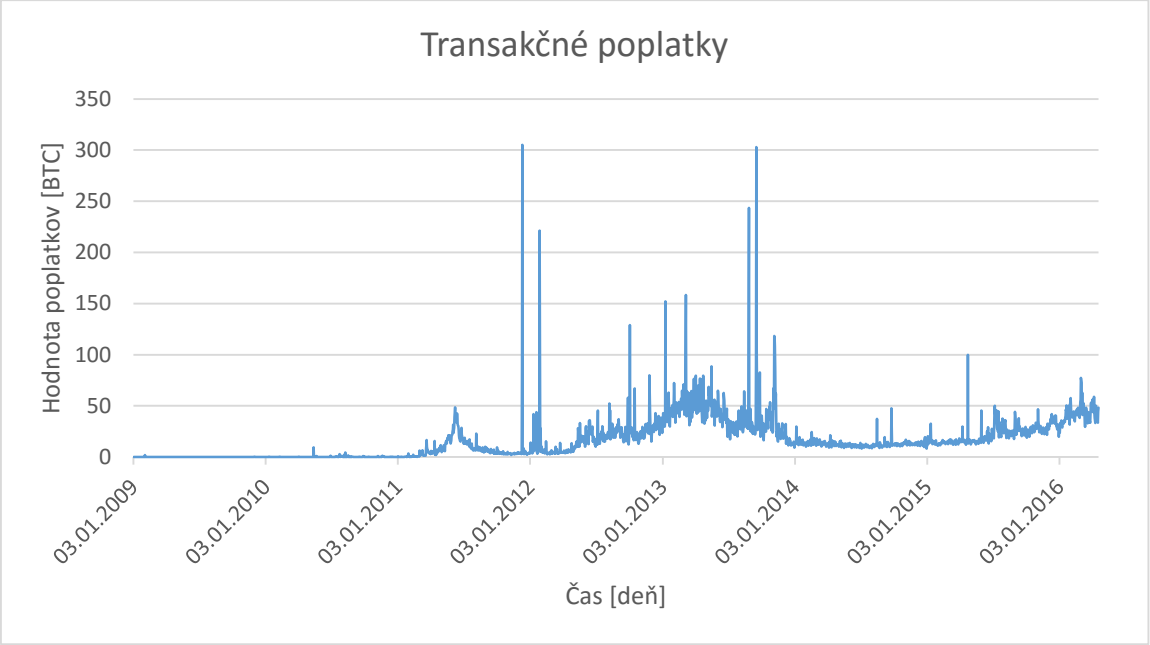
Aby teda Marika mohla poslať bitcoiny Petrovi, musí poznať jeho bitcoin adresu a svoj privátny kľúč. Ako už bolo spomenuté vyššie, adresa aj kľúče sú náhodne vygenerované alfanumerické reťazce. Bitcoin adresu si môžeme predstaviť ako trezor zo skla do ktorého každý vidí a privátny kľúč ako kľúč, ktorým sa tento trezor dá otvárať. Ak Marika pošle bitcoiny Petrovi, použije svoj súkromný kľúč a digitálne sa ním podpíše t.j. vytvorí vstup. Zadá množstvo a Petrovu adresu, čo je výstup. Následne sa táto transakcia zverejní na sieť a mineri ju môžu začať overovať. Vyriešenie bloku transakcií trvá cca 10 minút, takže aj na potvrdenie transakcie sa v priemere čaká takúto dobu. To je samozrejme jedna z nevýhod bitcoinu, pretože platba v hotovosti alebo platobnou kartou je v podstate okamžitá. Podnikateľ, ktorý prijíma bitcoiny môže na potvrdenie čakať, alebo môže zákazníkovi veriť, že tieto bitcoiny sa rýchlo nepokúsi minúť znova.

Pretože bitcoiny existujú len ako záznamy transakcií, na jednu bitcoin adresu môže byť naviazaných veľké množstvo transakcií. Dajme tomu, že Jana poslala Marike 2 BTC, Filip jej poslal 3 BTC a Eva jej poslala 1 BTC v rôznom čase a v rôznych transakciách. Týchto 6 BTC bude mať Marika vo svojej peňaženke ako výsledok týchto transakcií. Ak Marika posiela Petrovi bitcoiny, jej peňaženka sa snaží kombinovať rôzne transakcie tak, aby číslo v súčte dávalo požadovanú čiastku, ktorú chce Petrovi poslať. Šanca, že Marika bude mať presný počet bitcoinov aký chce poslať z nejakej transakcie v minulosti je malá. Predstavme si, že chce Petrovi poslať napr. 1,5 BTC. Pretože ani jedna transakcia (Jana- 2, Filip- 3, Eva- 1) neobsahuje túto sumu a táto suma sa z týchto transakcií ani nakombinovať nedá, musí poslať všetky bitcoiny z niektorej z týchto transakcií a rozdiel sa jej vráti. V tejto platobnej sieti sa teda nedajú deliť sumy v transakciách a musí sa poslať celá suma z danej transakcie. Marika teda pošle

Petrovi 2 bitcoiny, ktoré dostala v transakcii od Jany. Jej peňaženka automaticky vygeneruje 2 výstupy: 1,5 BTC poslať Petrovi a 0,5 BTC poslať na novú adresu, ktorá sa vygeneruje pre Mariku, aby tam mohla mať svoje bitcoiny.

Ďalšou veľmi dôležitou vlastnosťou, ktorú si treba uvedomiť je, že bitcoin transakcie sú nevratné.

Systém nemá zavedené povinné transakčné poplatky. Transakčné poplatky sú okrem odmeny za vyťaženie bloku ďalšou odmenou pre minerov, ktorý danú transakciu overia. Či užívateľ zahrnie do svojej transakcie poplatky závisí len na jeho vôli. Transakcie, ktoré presúvajú peniaze po veľkom počte adries vyžadujú minimálny poplatok, kvôli veľkému dátovému obsahu. Aj tento poplatok je však dobrovoľný, ale pretože mineri sú odmeňovaní aj z transakčných poplatkov, je malá šanca, že dátovo náročné transakcie bude niekto overovať, ak tam nebude žiadna odmena. Poplatok teda odosielateľovi zaručuje, že jeho transakcia bude overená v nasledujúcom vygenerovanom bloku. Niektoré peňaženky umožňujú zadať poplatok manuálne, niektoré bitcoin peňaženky majú v sebe zabudované minimálne poplatky. Treba však poznamenať, že jedna bitcoin transakcia v sebe zahrňuje mnoho výstupov. Znamená to, že môžem poslať bitcoiny na 500 rôznych adries naraz za žiaden alebo minimálny poplatok. [13] Celková suma transakčných poplatkov v jednotlivých dňoch je znázornená na grafe 1.



Graf 1: Výška transakčných poplatkov od vzniku bitcoinu.

- Aký je celkový počet bitcoinov v obehu?

Celý proces generovania bitcoinov vymyslený Nakamotom limituje množstvo vydaných bitcoinov na číslo 21 miliónov. Celkový počet bitcoinov v obehu sa dá jednoducho spočítať pomocou geometrickej rady:

$$\sum_{n=0}^{\infty} \frac{210\,000 \times 50}{2^n} = 210\,000 \times 50 \times \frac{1}{1-\frac{1}{2}} = 21\,000\,000 \qquad (1)$$

Každý blok vygeneruje 50 bitcoinov. Toto číslo (50) sa delí na polovicu po vyťažení každých 210 000 blokov. Index n v sume teda predstavuje počet vyťažených skupín 210 000 blokov.

V roku 2009 Nakamoto vyťažil prvých 50 bitcoinov. V čase písania tohto odstavca t.j. 6.12.2015 je v obehu spolu 14 925 925. Posledný blok, ktorý bude generovať bitcoiny má poradové číslo 6 929 999 a bude vyťažený okolo roku 2140. Väčšina bitcoinov už bude vyťažená v roku 2040. Množstvo bitcoinov v obehu ilustruje graf 2. Po vyťažení posledného bitcoinu sa neprestanú vytvárať nové bloky, ale odmenou za vyriešenie bloku budú už len transakčné poplatky. Tieto transakčné poplatky zachovajú fungovanie celého bitcoin platobného systému. Neexistuje žiaden limit na počet vyťažených blokov v budúcnosti. [14]

Graf 2: Množstvo bitcoinov v obehu.

Pretože počet bitcoinov je obmedzený, má táto mena deflačný charakter. To znamená, že bitcoiny sa od istého času budú už len strácať. Ľudia budú zabúdať svoje privátne kľúče a bitcoiny ostanú na týchto adresách visieť. K týmto bitcoinom nebude mať prístup ich vlastník ale ani nikto iný, takže sa stratia úplne z obehu. Niektorí ekonómovia sa preto domnievajú, že bitcoin sa kvôli tomu nikdy uznávanou menou nestane a sám sa zničí. Pretože s časom bude bitcoinov v obehu stále menej, pravidlá dopytu a ponuky naznačujú, že ich hodnota bude kontinuálne rásť. Bitcoin sa v tomto prípade znova pustí do neprebádaných vôd, pretože nikto v skutočnosti nevie, čo sa stane s menou, ktorá kontinuálne zvyšuje svoju hodnotu. Samozrejme, že deflácia nie je žiaden nevídaný jav, ale konštantná deflácia už áno. Extrémne vysoká deflácia robí z meny veľmi nepraktickú vec. Predstavme si, že za 100 Kč si môžeme kúpiť auto. Ako by sme si potom za české peniaze mohli kúpiť chlieb alebo žuvačky? Bitcoin však proti tomu predstavil veľmi elegantné a jednoduché riešenie a to svoju deliteľnosť. Bitcoin je v súčasnosti deliteľný na veľmi malé čiastky a to konkrétne :

1 BTC (bitcoin) = 1 BTC

1 mBTC (mili bitcoin) = 0.001 BTC

1 μBTC (mikro bitcoin) = 0.000 001 BTC

1 satoshi = 0.000 000 01 BTC

V prípade, žeby ani týchto všetkých $21 \times 10^{(6+8)}$ satoshi nestačilo, existuje možnosť zmeniť deliteľnosť jedného bitcoinu. Ak sa na tom zhodne väčšina klientov, stačí aby jednoducho začali používať jeho novú verziu. [14]

2.3 Ťažba bitcoinov

Ťažba bitcoinov je kľúčovou súčasťou zabezpečenia celej bitcoin siete. Myšlienka spočíva v tom, že bitcoin mineri zaradia skupinu transakcií do bloku a potom opakovane uskutočňujú kryptografickú operáciu nazývanú hashovanie. Aby rozličnί mineri nevyťažili rôzne bloky v tú istú chvíľu naraz, musia hashovať až kým sa im nepodarí nájsť konkrétnu špeciálnu hash hodnotu. V tom momente sa blok tzv. vyťaží a stane sa súčasťou blockchainu. Samotný proces hashovania nevytvorí žiadnu konkrétnu užitočnú vec, ale pretože vyťaženia bloku je extrémne náročné, zabraňuje tým jedincom získať nadvládu nad týmto systémom. Vyťaženie bloku je výpočtovo extrémne náročné, ale zároveň je extrémne jednoduché pre sieť overiť, že sa nejaký blok vyťažil. [15]

Bitcoin využíva hashovaciu funkciu SHA256. Táto funkcia na vstupe vezme dáta s určitou veľkosťou (súbor, obrázok alebo text) a na výstupe z nich spraví 256 bitový alfanumerický reťazec. Tento reťazec sa nazýva hash alebo aj odtlačok a bežne sa používa na bezpečné ukladanie hesiel, alebo pri porovnávaní veľkých súborov. Napr. SHA1 vytvorí hash dlhý 160 bitov t.j. 40 hexadecimálnych čísel alebo 40 znakov.

Napríklad slovo password nám hashovacia funkcia SHA1 prevedie na hash 5baa61e4c9b93f0682250b6cf8331b7eefd8.

Pre bitcoin je správnym hashom ten, ktorý začína na požadovaný počet núl. Tak ako je náročné nájsť telefónne číslo, ktoré by končilo viacerými nulami, rovnako náročné je aj nájsť hash, ktorý začína na viacerými nulami. Napr. 1.4×10^{20} hashov bol ten správny. Inými slovami, nájsť správny 29.09.2014 o 16:16 správny hash musel obsahovať 17 núl na začiatku, takže iba jeden z hash bolo ťažšie ako nájsť konkrétne zrnko piesku na našej planéte. Bitcoin pre dodatočné zabezpečenie používa túto hashovaciu funkciu dva krát. Hashovacia funkcia je vymyslená tak, že neexistujú žiadne skratky, ktoré by viedli k výsledku. Blok sa musí hashovať hrubou silou metódou pokusu a omylu. [15]

Hashrate je počet kalkulácií (hashov) za sekundu, ktoré hardware zvládne, keď sa snaží vyriešiť tento problém. Čím vyšší hashrate má užívateľov hardware oproti zvyšku siete, tým pravdepodobnejšie, že blok vyťaží a získa bitcoiny. [6]

Proces hashovania a overovania bloku transakcií sa teda nazýva ťažba bitcoinov. Miner za to, že obetoval výpočtovú kapacitu svojho počítača na overenie transakcií dostal bitcoiny. Na začiatku bola odmena za vyťažený blok 50 bitcoinov. Približne každé 4 roky (210,000 vyťažených blokov) sa odmena za úspešné overenie bloku delí na polovicu. Od 28.9.2012 až doteraz je odmena vo výške 25 bitcoinov. Ďalšie zníženie bude až v roku 2017. Okrem toho, si miner môže na účet pripísať aj transakčný poplatok, ktorý s popularitou bitcoinu rastie. Tento systém odmeňovania vytvoril v bitcoin komunite veľmi súťaživú atmosféru. Najdôležitejším faktorom určujúcim úspech minera je množstvo výpočtového výkonu (hash rate), ktorý vlastní. Čím väčší je výpočtový výkon, tým väčšia je pravdepodobnosť získania bitcoinov. [6]

Náročnosť ťažby znamená, ako ťažko sa hľadá hash pod stanoveným cieľom. Náročnosť ťažby sa mení každých 2016 blokov v závislosti na čase potrebnom na vyriešenie predošlých 2016 blokov. Pretože 1 blok sa má vyriešiť za 10 minút, overenie 2016 blokov má trvať presne dva týždne. Ak na predchádzajúcich 2016 blokov bolo treba viac času, náročnosť sa zníži, ak

menej tak sa zvýši. Náročnosť môžeme spočítať ak hash, ktorý ma 32 bitov samých núl a zvyšok sú jednotky, podelíme aktuálnym cieľom. Neexistuje žiadna minimálna náročnosť a skutočná maximálna náročnosť je teoreticky nekonečná. [14]

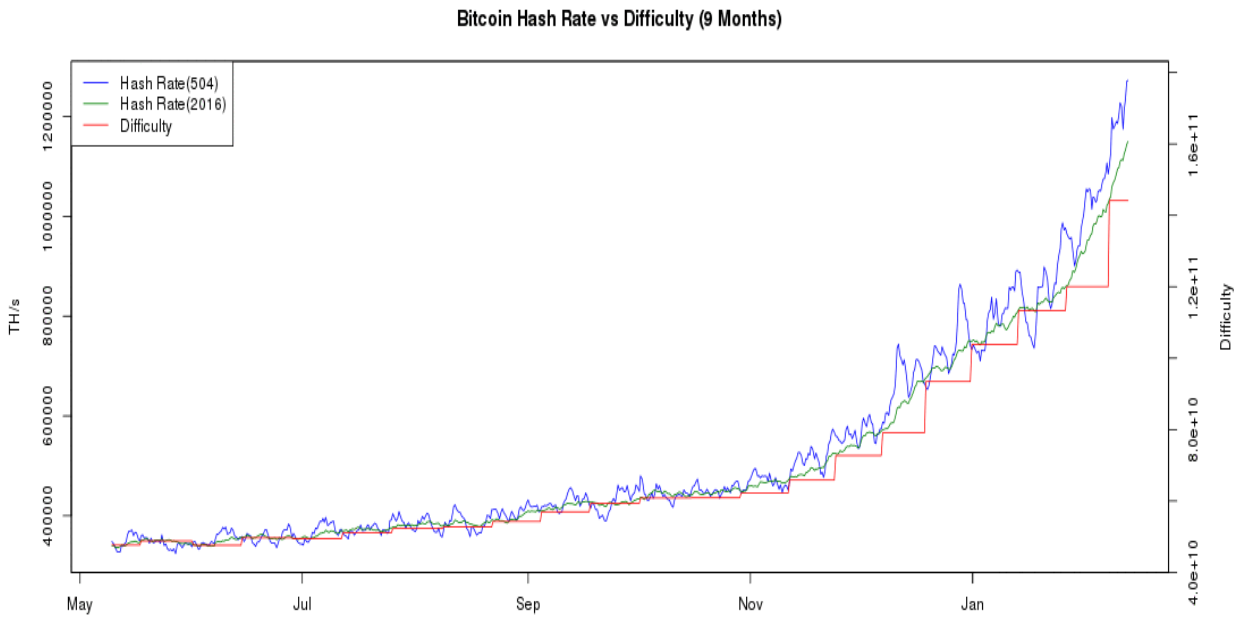
Keď pred pár rokmi bitcoin len začínal, náročnosť ťaženia bola relatívne nízka a viac-menej každý mohol ťažiť bitcoiny len s využitím domáceho počítača (CPU počítačová procesná jednotka). Postupom času, ako sa viac ľudí pokúšalo získať bitcoiny ťažením, začal byť celý proces ťaženia náročnejší. K CPU sa pridali GPU (grafická procesná jednotka), čo sú v podstate vysoko výkonné počítače s drahými grafickými kartami. Ich grafické karty však majú oveľa väčší výkon šifrovania ako CPU. Dnes však máme ešte sofistikovanejšie technológie nazývané ASIC (použitie špecifického počítačového čipu). Toto drahé zariadenie je určené výhradne len pre ťažbu kryptomien. [10] Dôvodom stáleho sťažovanie výpočtovej úlohy je, že každý nový blok má byť vyťažený za 10 minút a celková výpočtová kapacita siete s časom rastie. Uvediem jednoduchý príklad: Predpokladajme, že niekedy v počiatkoch bitcoinu existovalo dokopy 10 minerov a každý z nich mal k dispozícii hash rate napr. 20 MH/s. To znamená, že dokopy mali hash rate 200 MH/s a dajme tomu, že blok by s touto kapacitou vyriešili za požadovaných 10 minút. S postupom času ale počet minerov rástol a tak rástol aj ich celkový výpočtový výkon. Pravdepodobne by blok vyriešili aj za menej ako 10 minút, čo by bolo v rozpore s bitcoin protokolom a preto sa teda náročnosť mení v závislosti na výpočtovom výkone siete.

V čase písania tohto odstavca (12.02.2016, 10:50) je náročnosť 144,116,447,847. Hashrate siete je 1 269 352 217 GH/s a jeden blok sa vygeneruje za 8.4 minúty. Náročnosť sa zmení po vyťažení 1116 blokov čo bude asi o 6.5 dňa a bude približne na úrovni 179,540,826,903, čo je nárast asi o 24.58%. [16] Pre ilustráciu uvádzam v nasledujúcej tabuľke 2 zmeny náročnosti ťažby v čase.

Dátum	Náročnosť	Zmena [%]	Hash rate [GH/s]
7.2.2016	144,116,447,847	20.06	1,031,625,717
26.1.2016	120,033,340,651	5.89	859,232,121
13.1.2016	113,354,299,801	9.12	811,421,684
31.12.2015	103,880,340,815	11.16	743,604,444
18.12.2015	93,448,670,796	18.14	668,931,642
6.12.2015	79,102,380,900	8.77	566,236,898
24.11.2015	72,722,780,643	10.44	520,569,941
11.11.2015	65,848,255,180	5.77	471,360,171
29.10.2015	62,253,982,450	2.25	445,631,364
15.10.2015	60,883,825,480	0.12	435,823,399

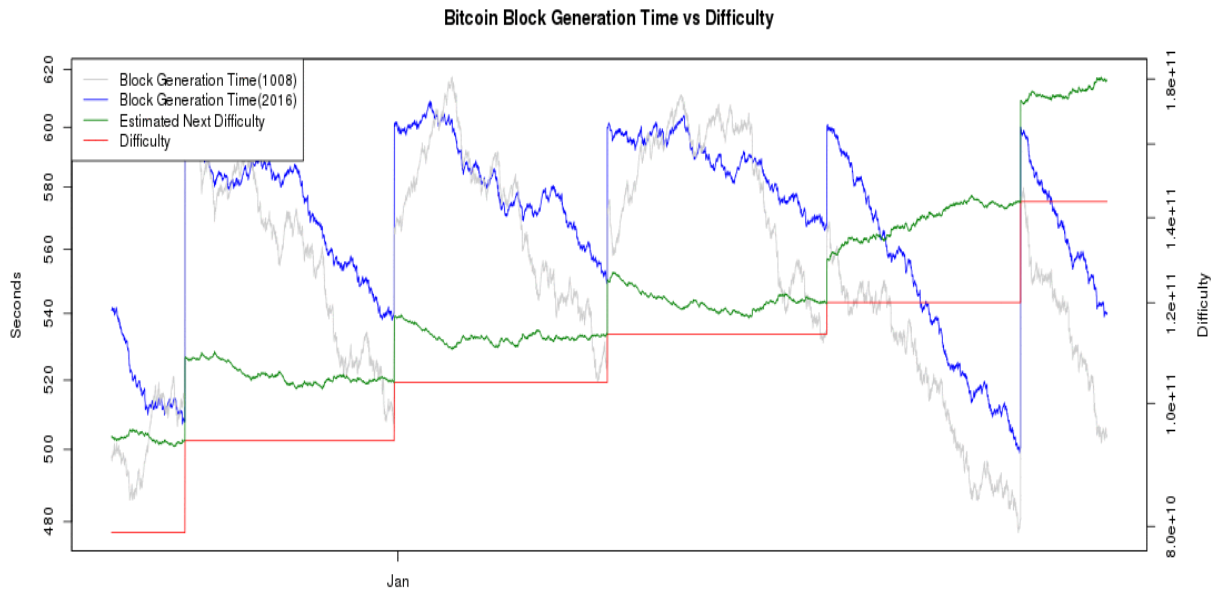
Dátum	Náročnosť	Zmena [%]	Hash rate [GH/s]
1.10.2015	60,813,224,039	2.49	435,318,014
17.9.2015	59,335,351,234	4.17	424,738,988
4.9.2015	56,957,648,455	4.98	407,718,729
22.8.2015	54,256,630,328	2.95	388,384,088
8.8.2015	52,699,842,409	0.81	377,240,166
25.7.2015	52,278,304,846	2.35	374,222,683
11.7.2015	51,076,366,303	3.39	365,618,871

Tabuľka 2: História náročnosti ťažby a hash ratu siete.



Obrázok 5: Porovnanie náročnosti ťažby s aktuálnym hash rateom siete.

Na obrázku 5 je ilustrovaná časová zmena hash ratu siete a náročnosti ťažby. Červenou čiarou je na grafe znázornená skutočná náročnosť ťažby v čase. Zelená čiara znázorňuje najbližšiu náročnosť vypočítanú v každom okamihu. Modrá čiara znázorňuje priemerný čas potrebný na vygenerovanie 2016 blokov, ktorý sa nazýva aj čas na potvrdenie.



Obrázok 6: Porovnanie času potrebného na vygenerovanie bloku a náročnosti ťažby v čase.

Na obrázku 6 je navyše sivou čiarou naznačené množstvo času potrebného na vygenerovanie 1008 blokov. Ak je táto sivá čiara pod modrou, čas na vygenerovanie bloku sa znižuje. Čím nižšie je sivá čiara pod modrou, tým rýchlejšie klesá čas na generovanie bloku. Po 2016 vyťažených blokoch bitcoin sám upraví náročnosť na vypočítanú (bod na zelenej čiare), aby čas potrebný na vyťaženie jedného bloku bol presne 10 minút.

2.4 Možnosti ťažby bitcoinov

Spolu existujú 3 spôsoby ako ťažiť bitcoiny:

1. Ťažba jednotlivca

Ak miner bitcoiny ťaží sám, celá odmena za overenie bloku pripadne len jemu. Pravdepodobnosť, že bitcoiny získa je veľmi malá. Dobre vybavený miner by potreboval v priemere 3 mesiace na získanie odmeny. Proces ťaženia je náhodný proces bez pamäti, takže ak miner nevyriešil blok do konca 3. mesiaca, je rovnako ďaleko od výsledku ako bol úplne na začiatku. Okrem toho, hash rate konkrétneho zariadenia ostáva konštantný, ale náročnosť sa postupom času zvyšuje. Priemerný čas do doby vyriešenia bloku sa dá približne spočítať pomocou vzorca:

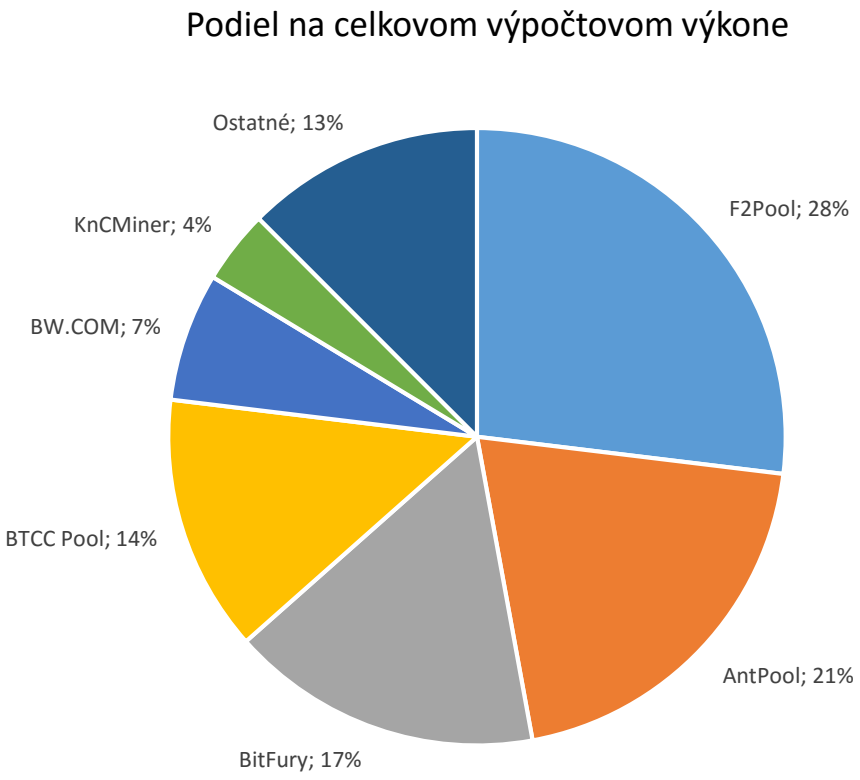
$$\text{čas} = \frac{\text{náročnosť} \times 2^{32}}{\text{hash rate}} \ [s] \qquad (2)$$

Pre zariadenie, ktoré má hash rate 1 GH/s a pri súčasnej náročnosti, ktorá je 72,722,780,643 [16] by trvalo jednotlivcovi s týmto zariadením$72{,}722{,}780{,}643 \times 2^{32} \div 10^9 \div 60 \div 60 \div 24 \div 365 = 9904.3$ rokov na vyriešenie jedného bloku. [6]

2. Ťažba v poole

Mining pool je skupina minerov, ktorá spoločne využíva výpočtové kapacity s cieľom zvýšiť svoj spoločný hash rate. Byť súčasťou poolu znamená väčšiu pravdepodobnosť rýchleho vyťaženia bloku, pričom odmena sa rozdelí medzi minerov v poole podľa toho, akou výpočtovou kapacitou prispeli do systému. Operátor poolu si za svoje služby necháva percentá z celkovej hodnoty vyťaženého bloku. [6]

Mining pool vymyslel český programátor Marek Palatinus, ktorý zároveň od decembra 2010 zastrešuje prvý pool na svete s názvom Slush pool. [17]



Obrázok 7: Rozdelenie výpočtového výkonu medzi jednotlivé mining pooly v percentách ku dňu 11.02.2016.

Pre zaujímavosť uvádzam v nasledujúcej tabuľke 3 top 10 mining poolov s najväčším počtom vyťažených blokov. Najviac vyťažených blokov má pool GHash.IO, pretože sa stal

extrémne populárny okolo roku 2014 a zároveň vytvoril aj mining pool pre iné kryptomeny ako Litecoin, Dogecoin, Auroracoin a Darkcoin.

Názov mining poolu	Počet vyťažených blokov
GHash.IO	22 863
F2Pool	21 596
Slush	15 254
Eligius	11 192
AntPool	9 769
BitFury	7 906
BitMiner	6 308
BTCC Pool	5 846
EclipseMC	5 773

Tabuľka 3: Množstvo vyťažených blokov pre rôzne mining pooly.

3. Kontrakt na ťažbu

Kontrakty na ťažbu sú určené pre jednotlivcov, ktorí chcú investovať do procesu ťažby bitcoinov, ale nechcú si kupovať hardware a nechcú operovať s daným softwarom. Tieto kontrakty zahŕňajú ťažobný servis, kde je zazmluvnený výpočtový výkon a čas, po ktorý bude tento výkon k dispozícii. Takisto je možné zazmluvniť si časť výpočtového výkonu v dátových centrách špecializujúcich sa na ťažbu. V tomto prípade užívateľ potrebuje len počítač na komunikáciu a bitcoin peňaženku. [6]

2.5 Zariadenia určené na ťažbu bitcoinov

V tejto kapitole krátko načrtnem aké významné zmeny sa udiali pri evolúcii výpočtových zariadení prispôsobených na ťažbu bitcoinov. Existujú 3 základné kategórie zariadení určených na ťažbu, ktoré sa líšia svojou cenou a výkonom (CPU/GPU, FPGA a ASIC). Pri výbere hardwaru sú dôležité 2 základné vlastnosti a to hash rate a spotreba elektrickej energie. Hash rate je počet kalkulácií ktoré hardware dokáže uskutočniť každú sekundu pri dešifrovaní matematického problému. Základná merná jednotka je hash za sekundu H/s, ale najčastejšie sa používajú násobky megahash, gigahash a terahash za sekundu (MH/s, GH/s a TH/s). Čím vyšší hash rate (v porovnaní s aktuálnym hash rateom siete) tým väčšia je pravdepodobnosť vyriešenia bloku. Pretože riešenie týchto úloh spotrebúva elektrickú energiu, je dôležité zistiť akú spotrebu dané zariadenie má. Cieľom je neplatiť všetky peniaze za elektrickú energiu na ťažbu bitcoinov, ktoré ani nemusia mať takúto hodnotu. V praxi sa zaviedla merná jednotka, ktorá vyjadruje koľko hashov miner dostane za každý watt energie, ktorá sa spotrebuje. Je to jednoducho podiel hash ratu zariadenia a jeho výkonu. Jednotka je [(GH/s)/W], čo sa dá

upraviť na [GH/J]. Napr. ak miner vlastní zariadenie s hash rateom 500 GH/s a výkonom 400 W, efektivita tohto zariadenia je 1.25 GH/J. V praxi sa často používa aj prevrátená jednotka a teda [J/GH]. Koľko peňazí ťažba stojí v skutočnosti sa miner dozvie až pri pohľade na faktúru za elektrinu. [18]

A. CPU = ťažba 1. generácie

CPU miner je jednoduchý klientský program používaný na ťažbu v poole alebo na individuálnu ťažbu. Hardwarom v tomto prípade je vlastný počítač minera. Program obdrží navrhovaný blok a snaží sa uhádnuť hodnotu, ktorá by blok overila. Zdrojový kód na ťažbu bitcoinov je zverejnený na github-e [19] a je prekvapivo jednoduchý. Základný výpočet:

```
While (1)
HDR[kNoncePos]++;
IF (SHA256(SHA256(HDR))) < (65535 << 208) / DIFFICULTY)
return;
```

môže ovplyvniť existujúce vysoko výkonné knižnice na implementáciu SHA256 hashu. Jedna malá optimalizácia , ktorá sa používa je využitie vyrovnávacej pamäte, ktorá obsahuje počiatočný počet hlavičiek blokov s ktorými pracuje a má konštantnú priemernú hash hodnotu. SHA256 výpočet vezme 512 bitový blok a uskutoční 64 kôl dešifrujúcich operácií, kde každé nasledujúce kolo dešifrovania závisí na kole predchádzajúcom t.j. je to reťaz navzájom závislých operácií. Tento spôsob ťažby sa vyznačuje premrhaním časti výpočtového výkonu a tým aj nízkym využitím elektrickej energie. [20]

B. GPU = ťažba 2. generácie

V októbri 2010 bol na internete zverejnený framework OpenCL, pomocou ktorého sa píšu programy pre GPU. Bitcoin protokol sa začal implementovať do iných programovacích jazykov ako je napr. Java alebo Python. Takto vzniklo mnoho rôznych variantov programov na ťažbu bitcoinov využívajúcich OpenCL knižnicu. Pretože zariadenia sú využívané na nepretržitú ťažbu v období niekoľkých mesiacov, užívatelia často vylaďovali vstupné napätie – znížili ho ak chceli mať menšie náklady na ťažbu alebo ho zvýšili ak chceli dosiahnuť väčší hash rate a znižovali na minimum aj frekvenciu video RAM, pretože pamäť sa nevyužíva a tým sa dajú ušetriť náklady. [20] GPU ťaženie spočíva vo zvýšení hash ratu pridaním grafickej karty do počítača. Hlavnými dodávateľmi GPU boli spoločnosti ATI a Nvidia. Najvýkonnejšie grafické karty môžu stáť desiatky tisíc českých korún, ale zároveň poskytujú minerovi oveľa väčší hash

rate v porovnaní s CPU hash rateom. Napr. grafická karta ATI 5970 poskytuje okolo 800 MH/s, pričom bežné CPU poskytuje hash rate vo výške do 10 MH/s. Ďalšou výhodou GPU ťaženia je možnosť ťažiť aj iné kryptomeny ako je bitcoin. Litecoin využíva iný protokol ako bitcoin s názvom Scrypt, ktorý je však prispôsobenú aj na ťažbu pomocou CPU a GPU. CPU a GPU ťaženie je však v dnešnej dobe už dávno mŕtve. Ťažba bitcoinov sa po uvedení ASIC zariadení stala tak náročná, že s nimi CPU ani GPU nemôžu v žiadnom prípade konkurovať. [18]

C. FPGA = ťažba 3. generácie

FPGA (Field Programmable Gate Array) je integrovaný obvod navrhnutý tak, aby sa konfiguroval až po jeho zostavení. To umožňuje výrobcom nakúpenie rôznych čipov a ich dodatočné prispôsobenie pred uvedením vlastného zariadenia na trh. Vzhľadom na to, že táto technológia je určená priamo na ťažbu, FPGA ponúka zlepšenie výkonu oproti CPU a GPU. Jediný FPGA čip má v prevádzke hashrate okolo 750 MH/s a do zariadenia je možné umiestniť ich rôzne množstvo. [18]

D. ASIC = ťažba 4. generácie

ASIC (Application Specific Integrated Circuits) sú špeciálne navrhnuté tak, aby robili len jednu činnosť a to ťažbu bitcoinov s extrémnou rýchlosťou a relatívne nízkou spotrebou energie. Pretože tieto čipy sú špeciálne navrhované na túto úlohu a sú drahé a časovo náročné na výrobu. Veľmi zaujímavý je fakt, že vývoj tohto zariadenia sa uskutočnil len vďaka fund-raisingu na online fórach, predovšetkým na bitcointalk.org a veľkú zásluhu majú aj fóra v čínskom jazyku. Na týchto fórach spoločnosť Butterfly Labs (BFL) postupne predstavila svoju víziu na vývoj ASICu, zodpovedala na stovky otázok diskutérov ohľadom použitej technológie, biznis modelu spoločnosti a jej dôveryhodnosti. V nasledujúcom odstavci je krátky sumár celého vývoja.

18.7.2012 ASICMINER tím zaregistroval spoločnosť v meste Shenzen v Číne a uzavrel zmluvu so spoločnosťou, ktorá mala čipy vyrábať. 29.7. už bol na svete prvý model s rýchlosťou 1.25 GH/s a príkonom 13.3 W na čip. Ďalšie peniaze získali na online burze GLBSE, kde sa obchoduje v bitcoinoch. Tam sa rozhodli predať časť svojej firmy za 0.1 BTC. Obchodným plánom spoločnosti bolo najprv vlastná ťažba pomocou tohto zariadenia a následná distribúcia zákazníkom. 28.12. toho istého roku bola uverejnená fotka prvého ASIC mineru na svete. Neskôr spoločnosť predala 60 kusov 83 W minerov s hash rateom 10.7 GH/s

a cenou za kus okolo 50-75 BTC (v tom čase 5 000 – 7 500 $). Potom vyvinuli ešte USB minera, ktorý obsahuje jediný ASIC čip a dá sa kúpiť napr. na Amazone za približne 50$. [20]

Obrázok 8: Vľavo je USB ASIC miner (330 MH/s) a vpravo je klasický ASIC miner (10.7 GH/s za 475 $).

Na záver uvádzam v dvoch tabuľkách (tabuľka 4, tabuľka 5) zariadenia dostupné v roku 2014 a v roku 2016. Pretože väčšina zariadení na stránke https://en.bitcoin.it/wiki/Mining_hardware_comparison nie je v súčasnosti dostupná, vybrala som len tie, ktoré sa dajú objednať z Amazonu a Bitmainu. Pomer cena / hash rate sa s pôvodných 3.33 $/(GH/s) zmenšil na dnešných 0.198 $/(GH/s) čo je samozrejme veľké zlacnenie. Ak si napr. porovnám zariadenie AntMiner S5+ s akýmkoľvek ASIC minerom z roku 2014, rozdiely sú až zarážajúce. Zatiaľ čo hash rate zariadenia sa viac ako zdvojnásobil jeho cena bola podstatne nižšia.

Názov zariadenia (rok 2016)	Hash rate [GH/s]	Príkon [W]	Energetická efektivita [J/GH]	Cena za hash rate [$/(GH/s)]	Cena za kus [$]
AntMiner S3	441	355	0.80	1.745	769.36
AntMiner S4+	2570	1500	0.58	0.414	1 064
AntMiner S5 BATCH 5	1 155	590	0.51	0.358	414
AntMiner S5+	7 722	3 436	0.44	0.299	2 307
AntMiner S7 BATCH 10	4 730	1 293	0.27	0.198	935.26
AntMiner U3	63	63	1	0.603	38
BFL Monarch 700 GH/s	700	490	0.7	1.970	1 379

Tabuľka 4: Porovnanie zariadení určených na ťažbu v roku 2016.

Názov zariadenia (rok 2014)	Hash rate [GH/s]	Príkon [kW]	Energetická efektivita [J/GH]	Cena za hash rate [$/(GH/s)]	Cena za kus [$]
KnC Neptune	3 000	2 200	0.73	3.330	9 995
Hashcoins Zeus	3 500	2 400	0.69	3.143	10 999
Cointerra TerraMiner IV	2 000	1 200	0.60	3.000	5 999
Extolabs EX1	3 600	1 900	0.53	2.639	9 499

Tabuľka 5: Porovnanie zariadení určených na ťažbu v roku 2014.

3 Ekonomický význam bitcoinov a jeho výhody a nevýhody

Podľa ekonóma Mankiwa [21] existujú 3 základné funkcie peňazí :

1) prostriedok výmeny

2) uchovávateľ hodnôt

3) zúčtovacia jednotka

Je otázkou ako veľmi bitcoin tieto tri funkcie spĺňa a či v súčasnosti nie je iba špekulatívnou investíciou. Problémom bitcoinu je jeho obrovská volatilita, ktorá ovplyvňuje najmä vlastnosti 2 a 3. Zatiaľ čo napr. česká koruna bude mať o týždeň skoro určite rovnakú hodnotu ako má teraz, bitcoin pravdepodobne nie. V praxi to znamená, že káva zaplatená bitcoinami dnes môže byť oveľa drahšia ako rovnaká káva zakúpená v iný deň. Jediným pravým dôvodom tejto volatility je však podľa niektorých len nízka likvidita trhu s touto menou.

Bitcoin je taktiež častokrát držaných zo špekulatívnych príčin, preto aj najmenšie faktory môžu viesť k masívnemu predaju, alebo ku kúpe tejto meny. Existuje však predpoklad, že čím viac sa s bitcoinami bude v bežnom živote platiť a čím viac inštitúcií ich začne akceptovať, tým viac bude ich cena stabilná. Bitcoin môžeme vnímať ako alternatívny spôsob online platieb, ktorý je lacnejší a rýchlejší ako zaužívané spôsoby, ale aj ako alternatívu k národným menám. Úspešne môže konkurovať národným menám napríklad v rozvojových krajinách alebo v čase krízy, kedy sa môže zdať hodnovernejšia ako ostatné národné meny. [24]

Národné kryptomeny vznikli z rôznych pohnútok. Napr. Deutsche eMark, Ekrona a eGulden sú tzv. „nostalgické coiny“. Všetky sú pomenované po predchodcoch pred eurom:

nemeckou markou, korunou v dánsku, švédsku a nórsku a holandským guldenom. Vo všetkých spomenutých krajinách je relatívny blahobyt a fungujúca ekonomika, preto sú tieto coiny len nostalgickou spomienkou obyvateľov na časy pred eurom. Druhú kategóriu coinov môžeme nazvať „pokrízové coiny“ a radíme tam SpainCoin, GreeceCoin a GaelCoin. Tieto coiny vznikli v časoch búrlivej finančnej krízy z roku 2008, ktorá postihla najmä spomenuté krajiny (Španielsko, Grécko a Írsko). [6]

Ak sa pozrieme na krajiny mimo Európy, veľmi zaujímavý je príbeh Argentíny, kde je veľmi silná bitcoin komunita. V novodobých dejinách Argentína vyhlásila bankrot 13-krát a inflácia sa pohybuje až v desiatkach percent napr. na konci roku 2014 malo 1 peso o 25% menšiu hodnotu, ako tomu bolo na začiatku toho istého roku. Nesplácanie štátnych dlhov, hyperinflácia a preceňovanie meny je v tejto krajine na dennom poriadku a preto viac ako polovica obyvateľov nepoužíva argentínske banky a ich kreditné karty. Veľmi zaujímavý bol rok 1984, kedy držanie pesos doslova znamenalo stratu peňazí. Vtedy sa bežne stávalo, že ľudia dostali výplatu - dve plné tašky pesos a utekali do obchodu kúpiť si jedlo predtým, ako sa jeho cena úplne zmení. Zamestnanci obchodov celý deň len preceňovali tovar a ľudia kupovali toľko jedla, koľko dokázali uniesť. Dokonca aj bohatí Argentínčania neveria bankám vo svojej krajine a kapitál si radšej ukladajú do amerických bánk. Posilnenie viery v bitcoin nastalo v roku 2012. Argentínsky parlament vtedy nariadil svojim občanom, aby na všetky priame platby medzi sebou používali platobný systém PayPal, čo malo za cieľ spomaliť výmenu pesos za iné stabilnejšie meny. Čoraz viac ľudí začalo uprednostňovať bitcoin, aby sa vyhlo týmto štátnym reštrikciám. Ďalším príkladom je marec roku 2013, kedy vláda povedala, že 1 peso má hodnotu 5 dolárov. To bola rana pod pás podnikateľom, ktorí v tom čase obchodovali s USA, pretože nelegálne zmenárne na uliciach 1 peso menili za 8 dolárov. Tento kurz sa nazýva „dólar blue“ a je ekonómami považovaný za reálny. Ak teda peniaze prišli zo zahraničia tradičnou cestou, banky automaticky peniaze zmenili s nariadeným kurzom a ľudia na každom peso prerobili 3 doláre. Akokoľvek riskantná sa pre Európana javí investícia do bitcoinov, niektorí Argentínčania do nej investujú s cieľom uložiť si do nich hodnotu. Preto v budúcnosti nie je vôbec vylúčené, že v krajinách s veľmi nestabilnou národnou menou, bitcoin úplne tieto národné meny nahradí. [22]

3.1 Bitcoin ako prostriedok výmeny

Prostriedok výmeny je jednou z najdôležitejších funkcií peňazí. Vyjadruje schopnosť peňazí sprostredkovať výmenné transakcie na trhu medzi ekonomickými subjektmi, ktoré majú

o výmenu záujem a je základným predpokladom k tomu, aby peniaze mohli slúžiť ako súčasť finančného systému. Vďaka peniazom sa výmena tovarov a služieb stáva podstatne jednoduchšia. [3]

Ako médium na výmenu bitcoin funguje od roku 2009, odkedy sa dajú nakupovať pomocou neho služby a tovary. Prvý oficiálny nákup uskutočnil floridský programátor Laszlo Hanyecz, ktorý si objednal dve pizze a 22.5.2010 za nich zaplatil 10 000 BTC (v tom čase 41$). 22.5. je teda na počesť tohto aktu nazvaný Pizza Bitcoin Day a obchodníci po celom svete ponúkajú zľavy na nákup pizze pri platbe v bitcoinoch. [23]

Pretože bitcoin nemá žiadnu vnútornú hodnotu, jeho hodnota úplne závisí na tom, ako je pre spotrebiteľa v reálnej ekonomike užitočný. Aj keď stále viac bežných obchodníkov a maloobchodníkov začína prijímať platby v bitcoinoch, väčšinu stále tvoria obchodníci s počítačovým softwarom a hardwarom a burzy určené na špekulatívne obchodovanie s bitcoinami. Realistický pohľad na užívanie bitcoinov je možné získať z univerzálneho záznamu všetkých bitcoin transakcií. [6]

Graf 3: Počet transakcií v bitcoinoch za deň od jeho vzniku v júni 2009 až po súčasnosť.

V čase písania tohto odstavca (14.3.2016) je podľa serveru blockchain.info denný počet transakcií približne 120 000. Otázkou však ostáva, koľko z týchto transakcií sa deje zo špekulatívnych príčin a koľko z nich tvoria platby za tovary a služby. Napríklad Fred Ehrsam, spoluzakladateľ Coinbase, čo je jedna z najčastejšie používaných digitálnych peňaženiek,

povedal v rozhovore z marca 2014, že 80% aktivít spojených s jeho peňaženkou malo špekulatívny charakter, oproti roku pred tým, kedy to bolo až 95%. Ak predpokladáme, že tieto čísla sú obecne platné, tak v danom roku bolo denne na nákup služieb a tovarov použitých 15 000 bitcoinov. Pretože na svete je takmer 7 400 000 000 spotrebiteľov, ktorí robia niekoľko finančných nákupov denne, je bitcoin so svojimi transakciami úplne zanedbateľný. Nákupy pomocou bitcoinov sú teda raritou v celosvetovom meradle, ale aj v samotnej komunite vlastniacej bitcoiny. [6]

Ďalšou veľkou prekážkou pre masové využívanie bitcoinov je pomerne náročný proces ich získavania. Prvou možnosťou, ako si zaobstarať bitcoin je byť úspešným minerom, čo v súčasnosti vyžaduje ťažbu v poole a nemalé finančné prostriedky. Druhou možnosťou je ich nákup priamo na burze alebo od dealera. Tento nákup však samozrejme stojí extra peniaze. Napríklad pre založenie účtu na Bitstamp.net je nutná e–mailová registrácia a následná verifikácia. Pre overenie je potrebné naskenovať identifikačné doklady ako napr. občiansky preukaz alebo pas. Ďalším nevyhnutným dokladom je akýkoľvek dokument, ktorý preukazuje trvalé bydlisko napr. účet za elektrinu, výpis z bankového účtu s adresou alebo výpis z katastra nehnuteľností. V nastaveniach účtu sa potom zadá bankový účet, z ktorého sa budú do Bitstampu posielať peniaze na nákup BTC. Nákup sa teda nedá uskutočniť jednoducho pomocou kreditnej karty alebo PayPalu.

Okrem toho sa bez vlastnenia bitcoinov nedajú nakupovať tovary a služby, čo už je bežná prax aj u maloobchodníkov, ktorí ponúkajú možnosť nakupovať cez spotrebiteľský úver u tretej strany. V súčasnosti neexistuje žiadna bitcoin kreditná karta a tak isto sa v bitcoinoch neposkytujú úvery. [6]

Poslednou prekážkou masového používania bitcoinov v bežnom svete je nutnosť čakať na potvrdenie platby. Zákazník aj obchodník čakajú na 1 potvrdenie transakcie v priemere 10 minút (na úplne potvrdenie transakcie treba čakať 6 overení, teda 60 minút). Táto čakacia doba je spôsobená práve procesom ťažby, pri ktorom sa transakcie overujú. Samozrejme, že obchodník môže veriť zákazníkovi a nečakať na overenie, je však vystavený riziku, že zákazník tie isté bitcoin použije ešte raz pred tým, ako sa transakcia zapíše do blockchainu. [6]

3.2 Bitcoin ako účtovná jednotka

Pre pochopenie tejto funkcie, ktorú musia peniaze splňovať, uvediem jednoduchý príklad. Zákazník musí pri porovnávaní rovnakého druhu tovaru, použiť peniaze ako prostriedok na

porovnanie cien. Napr. ak si kúpi kávu za 80 Kč, tak mu musí byť jasné, že bola 2-krát drahšia ako káva, ktorú si mohol kúpiť u konkurencie za 40 Kč.

Ako som už spomenula v úvode tejto kapitoly, kameňom úrazu bitcoinu je jeho obrovská volatilita. Pretože tržná hodnota bitcoinu sa mení každú hodinu aj o obrovské sumy, obchodníci by museli stále prepočítavať nové ceny tovarov a služieb v bitcoinoch. To by prinieslo samozrejme obrovské množstvo práce a pre zákazníka by to bolo dosť mätúce. V princípe by tento problém vymizol, ak by sa bitcoin používal ako primárna mena, čo však ešte nie je nikde na svete. [6]

Možno však najväčšou prekážkou bitcoinu v plnení funkcie účtovnej jednotky je častokrát nespomínaný a bitcoin fanúšikmi bagatelizovaný fakt, že cena jedného bitcoinu je relatívne veľká oproti cene niektorých tovarov a služieb. To znamená, že obchodník by musel uvádzať ceny s 4-5 desatinnými miestami. Môže sa zdať, že je to iba jednoduchá matematika, ale pre zákazníkov by to mohol byť veľký problém. Napríklad cena sklíčka marmelády by bola 0.01694 BTC , krabička čokolády by stála 0.00529 BTC a popradský čaj by stál 0.05255 BTC. V tomto príklade, je popradský čaj 10-krát drahší ako čokoláda, ale aj človek s vysokoškolským vzdelaním by nemusel dospieť k správnemu výsledku, kvôli dĺžke ceny a počtu začiatočných núl. Toto by samozrejme mohlo spôsobovať aj problém v účtovníctve, pretože väčšina účtovných programov akceptuje len dve desatinné miesta. [6]

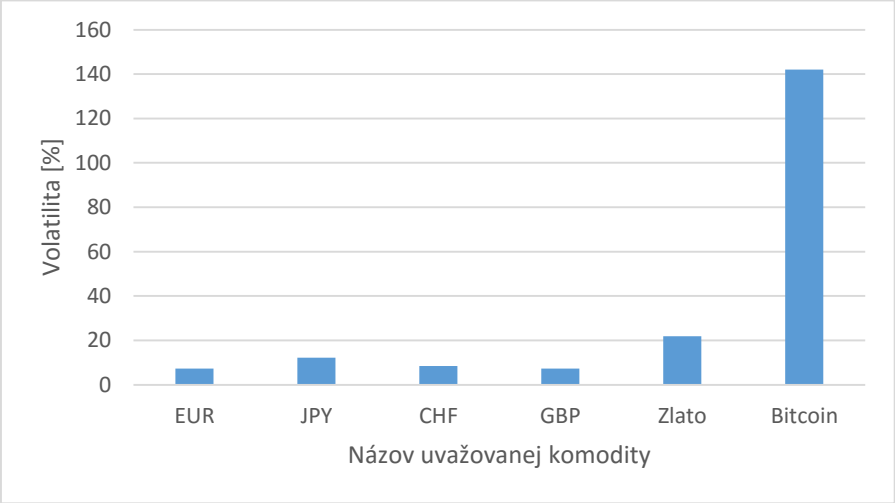
Propagátori bitcoinov však tento nedostatok v bitcoinoch nevidia. Pretože najmenšia existujúca jednotka bitcoinu je 1 satoshi = 0.000 000 01 BTC, fanúšikovia tvrdia, že ak bude cena jedného bitcoinu príliš vysoká, ľudia začnú počítať v milibitcoinoch, mikrobitcoinoch a v satoshi.

3.3 Úložisko hodnoty

Ak peňažná mena funguje ako úložisko hodnoty, zákazník má k dispozícii peniaze v určitom čase a tieto peniaze vymení za tovary a služby niekedy v budúcnosti. Samozrejme očakáva, že za peniaze ktoré minul dostal rovnakú ekonomickú hodnotu, ako mali peniaze v čase keď si ich zaobstaral. Vo svojej podstate a väčšinu času to znamená, že peniaze si človek chráni pred lúpežou a uloží si ich napríklad do banky. Pretože bitcoiny nemajú žiadnu fyzickú hodnotu a sú uložené len v digitálnych peňaženkách resp. na privátnych kľúčoch, hlavnou výzvou bitcoin priemyslu sa stala ochrana týchto údajov. Niektoré digitálne peňaženky už ponúkajú možnosť ochrany a aj jej poistenie. V princípe toto riešenie samozrejme funguje, ale

zákazník musí za tieto služby platiť. Dokonca existuje možnosť odložiť si svoje bitcoiny na externé pamäťové zariadenia, ktoré ešte neboli pripojené k počítaču tzv. „virgin cold storage“ s cieľom zabezpečiť ich maximálnu ochranu. [6]

Ak sa teda užívateľovi podarí bezpečne uložiť si svoje bitcoiny, stále je tu možnosť, že jeho bitcoiny stratia vďake volatilite svoju hodnotu. Na nasledujúcom grafe 4 je vyznačená volatilita kurzu medzi bitcoinom a dolárom v roku 2013. Pre porovnanie sú vyznačené aj volatility zmenných kurzov medzi eurom, jenom, librou, frankom, londýnskou cenou zlata a dolárom v danom roku. Volatilita zmenného kurzu bitcoinu bola v roku 2013 približne 142%, čo je o jeden rád viac ako volatility ostatných mien, ktoré sa pohybovali medzi 7-12%. Volatilita zlata, do ktorého sa investuje s cieľom uchovávať hodnotu, bola 22%. Pre porovnanie treba uviesť, že väčšina obchodovaných akcií má na burzách volatilitu kolo 20-30% a ani najrizikovejšie akcie nevykazujú 100% volatilitu. Z tohto grafu je teda jasné, že držať bitcoiny aj na krátku dobu je veľmi rizikové a teda tento predpoklad na uznanie bitcoinu ako finančnej meny je nesplnený. [6]



Graf 4: Volatilita dennej zmeny kurzu vzhľadom k americkému doláru.

	EUR	JPY	CHF	GBP	Zlato	Bitcoin
EUR	1.00	0.18	0.61	0.64	0.20	-0.50
JPY		1.00	0.33	0.20	0.07	0.01
CHF			1.00	0.42	0.19	-0.04
GBP				1.00	0.21	-0.02
Gold					1.00	-0.06
Bitcoin						1.00

Tabuľka 6: Korelačná matica denných zmien vo výmenných kurzoch mien, zlata a bitcoinu s americkým dolárom.

Tabuľka 6 vychádza zo zaznamenaných denných zmien ceny Londýnskeho zlata, výmenných kurzov eura, jenu, franku a libry voči doláru a ceny bitcoinu (Mt. Gox burza) medzi rokmi 2010 až 2014. Ako vidieť v tabuľke 6, 3 európske meny vykazujú silnú pozitívnu koreláciu. Korelácia medzi eurom a frankom je 0.61; medzi eurom a librou je 0,64 a medzi frankom a librou je 0.42. Jen a cena zlata sú takisto pozitívne korelované s európskymi menami aj keď na nižšej úrovni. Naproti tomu výmenný kurz medzi bitcoinom a dolárom vykazuje skoro nulovú koreláciu s ostatnými menami a zlatom. Táto úplná separácia bitcoinu od ostatných komodít má jasné dôsledky: makroekonomické udalosti, ktoré majú približne podobný efekt na hodnotu rôznych mien a komodít nijako neovplyvňujú hodnotu bitcoinu. To znamená, že je extrémne náročné istiť sa voči riziku, ktoré ohrozuje bitcoin, pretože ani nevieme čo má na bitcoin vplyv. [6]

3.4 Výhody bitcoinov

- **Sloboda v platení**

Uvediem konkrétny príklad zo života. WikiLeaks 28.11.2010 začala v médiách zverejňovať tajné prepisy všetkej komunikácie medzi Ministerstvom zahraničných vecí USA a konzulátmi a veľvyslanectvami z celého sveta. Do 1.9.2011 publikovali všetkých 251 287 needitovaných dokumentov, ktoré zahrňovali aj informácie o vojne v Iraku a Afganistane. Toto všetko sa samozrejme nepáčilo Ministerstvu obrany USA a aj iným politickým predstaviteľom nie len z USA. Verejnosť sa ale rozhodla podporiť WikiLeaks za svoju prácu. Pretože je to nezisková organizácia, dali jej finančnú podporu vo forme daru. Na tomto akte nebolo nič nelegálne, no napriek tomu transfer nebol možný ani cez jednu z možností (VISA, MasterCard, PayPal). Aj keď tieto firmy nič nepotvrdili verejne, boli pod obrovským politickým tlakom a tieto platby proste neuskutočnili. PayPal dokonca zmrazil všetky existujúce účty patriace WikiLeaks, ktorý s nimi potom nemohol nič robiť. Pri bitcoin platbe by sa však nič také nemohlo stať. Samozrejme, že by sa mohlo postaviť darcovstvo WikiLeaks mimo zákon a jedinec by mohol byť po čine potrestaný, ale nikto by štátu nedal moc na zamedzenie uskutočnenia tejto platby, pretože je to principiálne nemožné. Ak sa teraz pozriete na stránku WikiLeaks, darcovstvo je už možné aj v bitcoinoch a aj v inej kryptomene s názvom litecoin. Bitcoiny sú teda imúnne voči akejkoľvek cenzúre. [24]

- **Lacné a rýchle cezhraničné prevody**

Bitcoin bol špecificky vyvinutý pre rýchly a lacný transfer peňazí. Finančné prevody sa môžu uskutočňovať bez poplatkov alebo s minimálnym poplatkom, pričom je na samotnom užívateľovi, či je ochotný minimálny poplatok zaplatiť a tým zrýchliť samotný prevod. Oveľa nižšie náklady na prevody sú možne len vďaka neexistencii tretej strany.

V sektore cezhraničných finančných prevodov existuje pre bitcoin obrovská šanca na presadenie sa, pretože peňažné prevody od obyvateľov vyspelých krajín obyvateľom krajín rozvojových dosiahli do konca roka 2015 objem 515 miliárd amerických dolárov.[6]

Predstavme si, že bohatá americká dôchodkyňa chce poslať peniaze svojmu synovcovi do ČR a nato využije služby americkej spoločnosti Western Union, ktorú mimochodom s obľubou propaguje aj Česká pošta. Predpokladajme, že mu chce poslať 3 000 $. Podľa aktuálneho cenníka [25] za túto službu zaplatí 125 $. V čase, keď človek môže prostredníctvom služby Skype zadarmo telefonovať do celého sveta bez obmedzenia a zadarmo, sa mi tieto poplatky zdajú úplne absurdné.

- **Výhody pre podnikateľov a iných užívateľov**

Existuje niekoľko príčin, pre ktoré je platba bitcoinami pre podnikateľov, ktorí chcú prijímať peniaze online lepšia, ako platobný terminál. Prvou z nich je, že prijať platbu v bitcoinoch je pre nich oveľa menej finančne náročné. Aby získali platobný terminál musia sa zaregistrovať, čo stojí peniaze a čas. Navyše za každú uskutočnenú transakciu platia poplatok. [24]

V ČR je v súčasnej dobe viac bánk, ktoré poskytujú obchodníkom a podnikateľom platobné terminály. Ak si teda obchodník vybaví terminál z banky, ten mu automaticky zriadi podnikateľské konto s nemalými poplatkami za vedenie účtu. Ďalej sa potom z každej transakcie platí cca 1,5% (reťazce) resp. 3,5% (maloobchodníci) z obratu a niekedy dokonca aj nájom za terminál vo výške 300 až 700 Kč za mesiac. Cena platobného terminálu sa pohybuje od 15 do 30 tis. Kč za kus. [26] Preto mnoho malých obchodov a podnikov zákazníkom možnosť platiť online ani neponúka. Tým ale riskuje, že zákazníkov zvyknutých platiť kartou stratí, resp. nikdy nezíska.

Naproti tomu sa pre prijímanie bitcoinov podnikateľ nemusí nikde registrovať, len sa pripojí k sieti čo sa dá úplne zadarmo. Takisto neplatí žiadne poplatky pri transakcii. Pretože tieto poplatky na konci zaplatí aj tak vždy len zákazník, je samozrejme aj v jeho záujme, aby boli čo najnižšie.

Reálny príklad preferovania bitcoinov nad inou menou ponúka napr. obchodný reťazec Subway, ktorý predáva rýchle občerstvenie. Jedna jeho pobočka v Moskve pri Moskovskom inštitúte fyziky a technológie začala akceptovať platbu bitcoinami a zároveň poskytla zľavu 10 % pri platbe touto formou práve pre absenciu obchodných poplatkov. [27]

Obrázok 9: Bitcoin v Subway - pri platení bitcoinami zľava 10%.

Vďaka veľmi nízkym, resp. nulovým transakčným poplatkom existuje aj možnosť uskutočňovať tzv. mikroplatby. Dôležitosť mikroplatieb sa najlepšie rozumie na konkrétnych príkladoch. Predstavte si, že čítate článok na webe, ktorý je zaujímavý, ale voľne prístupná verzia dovoľuje prečítať si len prvú štvrtinu. Na dočítanie celého článku treba zaplatiť poplatok za registráciu a užívateľovi je následne sprístupnený obsah všetkých článkov na danom webe. Formou mikroplatieb by ste si mohli prečítať konkrétny článok za pár centov bez toho, aby ste sa museli registrovať a platiť za obsah celého webu. Ďalšou zaujímavou aplikáciou tohto systému platenia by mohli byť káblové televízie. Namiesto toho, aby zákazník platil za celý balíček programov (napr. 200) si zaplatí len 4-5 programov, ktoré naozaj sleduje. Ďalšou aplikáciou by mohlo byť používanie WiFi signálu. Predstavte si, že idete po ulici okolo rôznych obchodov a reštaurácií a každý ma svoj vlastný hot spot. Mikroplatby by umožňovali pripojiť sa presne k tomu hot spotu, okolo ktorého práve idete a platila by sa presne len cena za spotrebované dáta. Mikroplatby ďalej umožnili odmeňovanie blogerov a autorov článkov aj tak malými sumami ako je 5 centov namiesto tradičných lajkov. [24]

Ďalšou obrovskou finančnou úsporou je možnosť uskutočniť mnoho finančných transakcií za jeden poplatok. Predstavte si, že máte vo firme zamestnaných 500 zamestnancov a na konci mesiaca im z firemného účtu idete poslať výplaty. V praxi musíte uskutočniť 500 rozličných platobných transakcií a za každú treba zaplatiť nemalé poplatky, ktoré by sa dali však vďaka bitcoinu ušetriť.

- **Kontrola majiteľa nad svojimi bitcoinami**

Každú bitcoin transakciu dokáže ovplyvniť jedine majiteľ privátneho kľúča a obchodníci nemôžu žiadnym spôsobom získať dodatočné platby. Na rozdiel od toho, ak sa kreditná karta ocitne v rukách neetického obchodníka, zákazníka pred skrytými platbami nič nechráni.

Na druhú stranu však táto absolútna moc majiteľa nad bitcoinami vedie aj k problémom. Pretože majiteľ privátneho kľúča získava ako jediný kontrolu nad danými bitcoinami, musí si dávať veľký pozor na jeho krádež alebo stratu. V prípade straty privátneho kľúča sú všetky bitcoiny v danej peňaženke nenávratne stratené. Takisto sa už objavili nebezpečné softwary, ktorých úlohou je ukradnúť privátne kľúče. V tomto prípade platí, že majiteľ musí byť dostatočne informovaný o týchto hrozbách a adekvátne si svoj kľúč chrániť. [6]

3.5 Nevýhody bitcoinov

- **Uľahčenie kriminálnej činnosti**

Pretože bitcoin ponúka pseudoanonymitu a jednoduchosť v platení, niet divu, že vlády sa o neho zaujímajú. Jeho sila sa naplno prejavila až v kombinácii s webovým prehliadačom Tor. Tor je anonymizujúci software, ktorý znemožňuje sledovanie užívateľského internetového pripojenia, to znamená, že nikto iný okrem samotného užívateľa nevie aké stránky navštevuje a aká je jeho fyzická poloha. Tor v podstate znemožňuje komukoľvek zistiť IP adresu prístroja, ktorý sa v daný moment používa. Tor bol na scéne trochu dlhšie ako bitcoin, ale až ich spoločná kombinácia umožnila užívateľovi zostať fyzicky anonymný v priestore a robiť transakcie s inými anonymnými užívateľmi bez potreby tretej strany. Táto kombinácia viedla bohužiaľ aj k vzniku nechválne známeho „eBayu podsvetia" Silk Roadu, kde sa obchodovalo s drogami, zbraňami, kradnutými pasmi a inými nelegálnymi vecami. Až po medializácii tohto čierneho trhu sa bitcoin dostal do povedomia širšieho obyvateľstva a pre mnohých sa stal symbolom čierneho obchodu. [24]

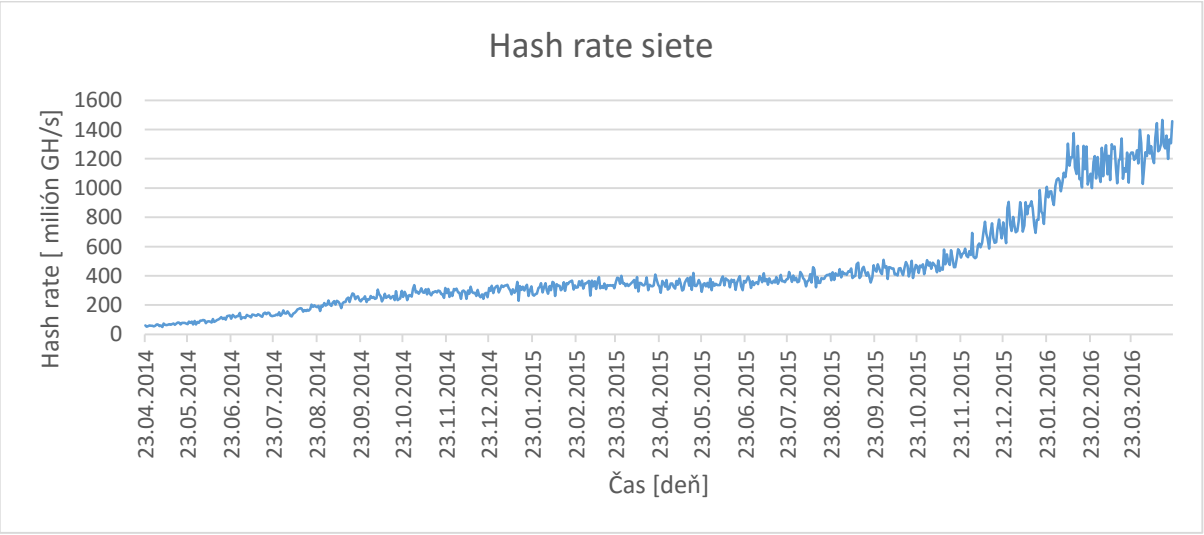
Druhým závažným nelegálnym aktom spojeným s kryptomenami obecne je pranie špinavých peňazí. Tieto podozrenia zosilnili po zrušení súkromnej digitálnej centralizovanej meny Liberty Reserve práve z tohto dôvodu. [24]

Je však dôležité si uvedomiť, že bitcoiny sú peniaze ako všetky ostatné a používajú sa teda aj na činnosti legálne a aj na činnosti nelegálne. Existovalo mnoho iných metód prania špinavých peňazí a finančných zločinov dávno pred vznikom bitcoinov. Teraz už veľa bitcoinových zmenární zavádza opatrenia proti týmto aktom, napr. si uchovávajú dáta o svojich zákazníkoch, čo by malo potenciálnych páchateľov odradiť.

Na druhej strane však bitcoin oproti ostatným peniazom ponúka ochranu voči niektorým formám finančného zločinu. Napr. taký proces ťažby bitcoinov, ktorý spočíva v overovaní transakcií, takmer znemožňuje jeden bitcoin utratiť dvakrát alebo ho sfalšovať. Podvodník by musel nazhromaždiť dostatočný výpočtový výkon, aby prekonal výkon všetkých ostatných účastníkov v sieti a pokúsil sa tak modifikovať súčasné a budúce transakcie predtým, ako by to ostatní účastníci registrovali. [6]

- **51% útok**

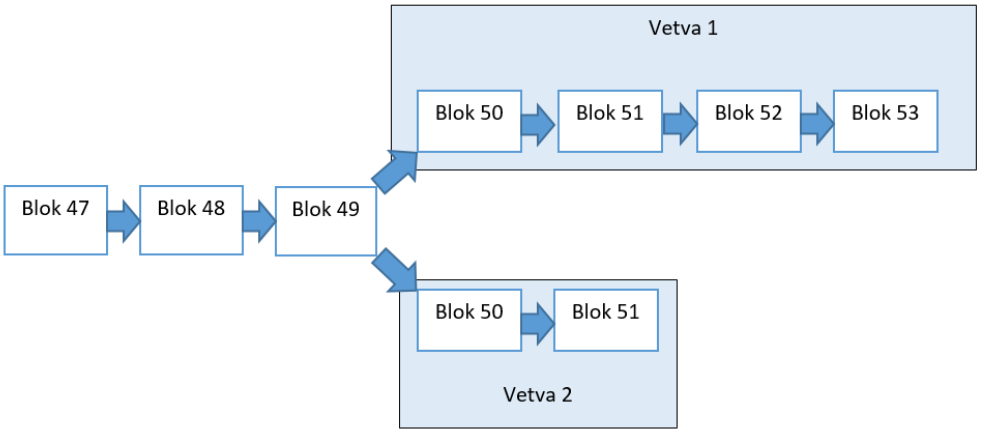
Pretože akákoľvek počítačová sieť môže byť cieľom hackerov, bitcoin sieť nie je žiadnou výnimkou no má svoje špecifiká. Pretože bitcoin je decentralizovaný, neexistuje žiaden centrálny server, ktorý by mohol byť napadnutý. V skutočnosti by musela byť napadnutá viac ako polovica aktívnych počítačov v sieti alebo by sa polovica užívateľov dohodla na tom, že budú utrácať dvojmo. S enormným rastom počtu hardwarov v sieti je to však skoro nereálne.



Graf 5: Výpočtová kapacita (hash rate) siete za posledné 2 roky.

Ak by jeden užívateľ alebo organizovaná skupina vlastnili viac ako 50% celkovej výpočtovej kapacity siete, mohli by meniť poradie a vynechávať transakcie podľa vlastného výberu pri neobmedzenom počte ich potvrdení. Mohli by napríklad vrátiť naspäť transakcie, ktoré sami posielali a to by im umožnilo dvojité utrácanie. Ďalej by boli schopní zamedziť transakcii, aby sa začala overovať a zároveň by mohli zabrániť ostatným minerom vo vyťažení bloku. Tento útočník alebo útočníci by si však nemohli posielať mince, ktoré im nepatria, meniť výšku odmeny za vygenerovaný blok alebo získať neobmedzený počet bitcoinov. [28]

Možnosť dvojitého utrácania budem ilustrovať na nasledujúcom príklade a zároveň aj na obrázku 10. Predstavme si, že Martina má doma superpočítač, na ktorom môže ťažiť bitcoiny. Dajme tomu, že ide do reštaurácie a dá si obed za 2 bitcoiny. Táto Martinina transakcia sa dostala do práve riešeného bloku s číslom 50 vo vetve 2. Ako mineri postupne overujú túto transakciu majiteľovi reštaurácie chodia potvrdenia o overení platby. Majiteľ im uverí a pustí Martinu preč. Tá však rýchlo začne ťažiť blok na svojom superpočítači a zaradí do neho svoju transakciu, v ktorej posiela tie isté dva bitcoiny, ktoré utratila za jedlo na svoju inú bitcoin peňaženku t.j. vytvorí z bloku 50 vetvu 1. Tento superpočítač ďalej tajne overuje bloky vo vetve 1 bez toho, aby to Martina zverejnila na sieti. Po vyťažení ďalších troch blokov túto vetvu Martina distribuuje po sieti. Pretože ostatní mineri medzitým vyriešili len jeden blok vo vetve 2, automaticky sa pripájajú k Martininej vetve 1, pretože je dlhšia. Teraz sú všetky transakcie z blokov vo vetve 2 presunuté do fronty na overenie vo vetve 1. Vo vetve 1 je už však Martinina transakcia v hodnote 2 bitcoinov na jej peňaženku a teda majiteľ po obdržaní 2 potvrdení (overenie bloku 50 = 1. potvrdenie, overenie bloku 51 vo vetve 2 = 2. potvrdenie) zistil, že transakcia bola zrušená a peniaze nedostal. Existencia paralelných blockchainov je nízka a exponenciálne klesá s rastom dĺžky reťazca a s počtom nezávislých minerov.



Obrázok 10: Vytvorenie 2 vetiev pri dvojitom utrácaní.

V nasledujúcej tabuľke 7 sú uvedené pravdepodobnosti úspechu dvojitého utrácania pre jednotlivé výpočtové výkony. V prvom stĺpci sú uvedené jednotlivé podiely na celkovom výkone siete v percentách a v prvom riadku je počet potvrdení transakcie t.j. koľko blokov sa od jej potvrdenia vyťažilo.

q	1	2	3	4	5	6	7	8	9	10
2	4	0.237	0.016	0.001	0	0	0	0	0	0
4	8	0.934	0.120	0.016	0.002	0	0	0	0	0
6	12	2.074	0.394	0.078	0.016	0.003	0.001	0	0	0
8	16	3.635	0.905	0.235	0.063	0.017	0.005	0.001	0	0
10	20	5.600	1.712	0.546	0.178	0.059	0.020	0.007	0.002	0.001
12	24	7.949	2.864	1.074	0.412	0.161	0.063	0.025	0.010	0.004
14	28	10.662	4.400	1.887	0.828	0.369	0.166	0.075	0.034	0.016
16	32	13.722	6.352	3.050	1.497	0.745	0.375	0.190	0.097	0.050
18	36	17.107	8.741	4.626	2.499	1.369	0.758	0.423	0.237	0.134
20	40	20.800	11.584	6.669	3.916	2.331	1.401	0.848	0.516	0.316
22	44	24.781	14.887	9.227	5.828	3.729	2.407	1.565	1.023	0.672
24	48	29.030	18.650	12.339	8.310	5.664	3.895	2.696	1.876	1.311
26	52	33.530	22.868	16.031	11.427	8.238	5.988	4.380	3.220	2.377
28	56	38.259	27.530	20.319	15.232	11.539	8.810	6.766	5.221	4.044
30	60	43.200	32.616	25.207	19.762	15.645	12.475	10.003	8.055	6.511
32	64	48.333	38.105	30.687	25.037	20.611	17.080	14.226	11.897	9.983
34	68	53.638	43.970	36.738	31.058	26.470	22.695	19.548	16.900	14.655
36	72	59.098	50.179	43.330	37.807	33.226	29.356	26.044	23.182	20.692
38	76	64.691	56.698	50.421	45.245	40.854	37.062	33.743	30.811	28.201
40	80	70.400	63.488	57.958	53.314	49.300	45.769	42.621	39.787	37.218
42	84	76.205	70.508	65.882	61.938	58.480	55.390	52.595	50.042	47.692
44	88	82.086	77.715	74.125	71.028	68.282	65.801	63.530	61.431	59.478
46	92	88.026	85.064	82.612	80.480	78.537	76.836	75.234	73.742	72.342
48	96	94.003	92.508	91.264	90.177	89.201	88.307	87.478	86.703	85.972
50	100	100	100	100	100	100	100	100	100	100

Tabuľka 7: Úspešnosť dvojitého utrácania v percentách.

Počet potvrdení exponenciálne znižuje pravdepodobnosť dvojitého utrácania. Pravdepodobnosť úspechu ďalej nezávisí na dobe čakania, ale len na počte potvrdení. Čas hraje v neprospech útočníka len v tom prípade, že si nevie udržať svoj výpočtový výkon dosť dlho. Ak útočník vlastní viac ako 50% celkového výpočtového výkonu, žiaden počet potvrdení nezníži jeho pravdepodobnosť na úspech pod 100%. [29]

V súčasnosti je nemožné, aby jednotlivec mal viac ako 50% výkonu siete. Je to možné len pre mining pooly. V júli roku 2014 sa mining poolu GHash.IO reálne podarilo na krátky čas nadobudnúť 50% výkonu siete vďaka svojej popularite. Majitelia však rýchlo zastavili registráciu nových minerov a verejne prehlásili, že v prípade možnosti nebudú vytvárať žiaden

tajný reťazec. Mineri takisto dobrovoľne odišli do iných poolov, aby sa bitcoin nezdiskreditoval na verejnosti. [30]

- **Legislatívne problémy**

Kryptomeny obecne nie sú vydávané žiadnou vládou alebo centrálnou bankou a sú voči ich zásahom skoro imúnne. Na druhej strane však odporcovia tvrdia, že sú menej bezpečné práve preto, že v prípade podvodu nie sú užívatelia chránení a nemajú žiadnu legálnu pomoc. Dôvod je jednoduchý: transakcie kryptomien sa dejú bez vlády, banky, autorizovanej osoby, registrovaného platobného systému alebo regulátora. Navyše všetky transakcie sa dejú skrz internet, užívatelia komunikujú priamo, anonymne a bez zásahu tretích strán z čoho vyplýva aj absencia akýchkoľvek legálnych dôkazov pre súd. Pretože bitcoin je decentralizovaná mena, v ktorej užívateľ môže zostať anonymný (je to však veľmi náročné, preto je namieste skôr hovoriť o pseudoanonymite), často sa užíva na nelegálne činnosti ako je pranie špinavých peňazí a daňové úniky. Vďaka tomu sa viaceré vlády na svete zalarmovali a snažia sa definovať status bitcoinu a aj ostatných virtuálnych kryptomien. Kryptomeny sú legálne v niekoľkých krajinách a aj keď v niektorých krajinách nie sú striktne nelegálne, neznamená to automaticky ich legalitu. Rovnako ak sa v niektorej krajine musí platiť daň za kryptomenu, neznamená to jej legalitu.

Bitcoin a kryptomeny obecne vedú k 5 zásadným legislatívnym problémom a sú to:

1. **Platnosť transakcií** – Všetky národné vlády majú výhradnú právomoc riadiť vlastné finančné meny od ich tlače, uvedenia do obehu až po likvidáciu. Vlády môžu preniesť túto právomoc na centrálne banky alebo na iné autority pod ich kontrolou a dohľadom. Napríklad Reserve Bank of India (RBI) spravuje indické rupije, konkrétne vytvára dizajn bankoviek, určuje ich hodnotu a stanovuje bezpečnostné prvky na bankovke. Tak isto odhaduje množstvo bankoviek, ktoré budú potrebné v obehu. Staré a znehodnotené bankovky má právo zničiť a nahradiť ich novými. Tieto rupije musia byť prijaté akoukoľvek bankou na území Indie na zaplatenie daní, cla a iných verejných príspevkov. Rupija je legálne platidlo na zaplatenie dlhu a všetkých pokút a je to jediné platidlo, v ktorom vláda môže vydávať dlhopisy a zmenky. Všetky vyššie spomínané použitia indickej rupije sa však nevzťahujú na bitcoiny a nikto nemôže osoby alebo vlády prinútiť akceptovať ich. Vláda je autorizovaná menu prehlásiť za neplatnú a všetky transakcii v tejto mene za nelegálne. [6]

2. **Daňová povinnosť** – Ak sú kryptomeny skutočne meny, potom sú to finančné aktíva a všetky transakcie by mali podliehať zdaneniu (daň z príjmu, daň z pridanej hodnoty, dedičná daň, daň z príjmu v zahraničí). Aj keď by bola kryptomena nelegálna, vláda má právo transakcie v tejto mene zdaniť. V marci 2014 Internal Revenue Service v USA (podobné ministerstvu financií) rozhodlo, že pri zdanení sa bitcoin bude posudzovať ako majetok a nie ako mena. To znamená, že príjem vzniknutý z transakcie užívajúcej kryptomenu je zdaniteľný, avšak nerobí tento príjem alebo transakciu legálnou. Znamená to, že akýkoľvek nelegálny prijem musí byť zdanený. [6]

3. **Podanie žaloby v prípade súdneho sporu** – Bitcoin je založený na viere jeho užívateľov, propagátorov a minerov. V prípade porušenia akéhokoľvek zákona, by obeť nemusela byť schopná nazhromaždiť dostatočné množstvo dôkazov, aby sa mohla brániť. Najznámejším súdnym sporom bola žaloba štátnej prokoratúry na šéfa najväčšej bitcoin zmenárne na svete za pranie špinavých peňazí na online drogovom obchode Silk Road v januári 2014. Pretože kryptomeny využívajú IT, mohli by sa na nich vzťahovať aj podobné pravidlá ako napr. na hackovanie a digitálne licencie. Ďalšie vhodné legislatívy by mohli byť bankové právo, majetkové právo vrátane intelektuálneho vlastníctva a právo o ochrane spotrebiteľa. [6]

4. **Status organizácií propagujúcich bitcoiny a užívateľov** - Bežné meny sú riadené vládou resp. centrálnou bankou. Táto autorita je verejná inštitúcia ktorá za ňu nesie zodpovednosť. Kryptomeny sú usmerňované mimovládnymi organizáciami alebo anonymnými propagátormi. Nikto nevie pod akú jurisdikciu spadajú tieto entity a mnohé organizácie nemajú ani právnu formu. Právny rámec týchto organizácii je vďaka decentralizovanej práci jednotlivcov v sieti nedefinovateľný. Súd by tak toto zoskupenie nemusel pokladať za právne a v prípade sporu by stanovenie zodpovednosti bolo v praxi takmer nemožné. [6]

5. **Monetárna a fiškálna politika** – Vládne organizácie kontrolujú množstvo peňazí s cieľom stabilizovať ekonomiku a naštartovať hospodársky rast. V súčasnosti je trh s kryptomenami ešte príliš malý na to, aby mohol výrazne ovplyvniť monetárnu politiku, ale ak narastie množstvo transakcií s kryptomenami, môže to mať priamy

dopad na množstvo iných mien v obehu a znamenať infláciu vplyvom zmenšenia dopytu po týchto klasických menách. [6]

- **Neúplná anonymita**

Úplnú anonymitu má človek len pri platbe hotovosťou. Ak si dohodnem schôdzku cez internetový server s iným užívateľom a stretneme sa, ja si od neho niečo kúpim a dám mu za to hotovosť, táto transakcia je úplne anonymná. Ja neviem jeho meno, on nevie moje meno a neexistuje žiadny písomný záznam o výmene produktu a peňazí. Naopak, ak sa rozhodnem zaplatiť si napr. za izbu na internáte cez svoj bankový účet, banka pozná moje meno, vie komu posielam peniaze a často krát aj vie za akú službu sú peniaze posielané. Banka teda eviduje údaje o čase transakcie, výške prevedenej čiastky a údaje o odosielateľovi a príjemcovi. Bitcoin je niekde medzi. Existuje záznam o čase transakcie a výške finančnej čiastky všetkých potvrdených transakcií v nezašifrovanej forme. Čo však neexistuje je záznam o samotných účastníkoch transakcie. Napriek tomu zostať skutočne anonymný je neuveriteľne náročné. Predstavte si, že mám na účte 100 bitcoinov a chcem si kúpiť produkt u nejakej firmy. Pošlem jej 5 bitcoinov. Každý na sieti si môže zistiť, že som túto transakciu vykonala a že mám v peňaženke už len 95 bitcoinov. Teraz si predstave že si kúpim x ďalších produktov a služieb a pošlem nejaké peniaze svojej mame na účet. Čím viac transakcií z jednej peňaženky vykonám, tým viac informácii o sebe poskytujem každému jednému účastníkovi. Riešením by bolo 100 bitcoinov z jednej peňaženky rozdeliť na rôzne sumy v rôznych peňaženkách a z tých potom posielať platby. Je teda jasné, že udržať si anonymitu dokáže len veľmi sofistikovaný užívateľ. V súčasnosti už kryptografi samozrejme vyvíjajú menu, ktorá by si s anonymitou poradila lepšie. [24]

4 Altcoiny a blockchain

4.1 Klasifikácia alternatívnych mien

a) Token - historickým príkladom môžu byť Britské tokeny používané v 17. až 19. storočí a Scripy používané počas obdobia veľkej krízy v 30. rokoch v USA. Aktuálnym príkladom môžu byť lokálne a komunitné meny ako napr. Zvolenský živec, Bristol pound alebo Salt Spring Dollar v Kanade. Token má nižšiu vnútornú

hodnotu, pretože jeho použitie je viac špecifické a často späté s verejnými dohodami ako napr. výmena za konkrétny tovar alebo službu.

b) Centralizované digitálne meny - príkladom môžu byť vernostné body od finančných, telekomunikačných alebo maloobchodných firiem. Míle od leteckých spoločností a zlato z počítačovej hry Worl of Warcraft sú uzavreté systémy s transakciami len medzi špecifickými subjektami. Už vyššie spomenuté Salt Spring Dollar taktiež spadajú do tejto kategórie. Štruktúra riadenia je centralizovaná.

c) Distribuované a/alebo decentralizované digitálne meny - táto kategória v sebe zahŕňa kryptomeny ako Bitcoin, Litecoin a Dogecoin. Transakcie sa dejú bez tretej strany a štruktúra riadenia je decentralizovaná hlavne kvôli open-source softwaru. Neexistuje žiaden právny subjekt zodpovedný za vykonané aktivity a preto tento typ mien nie je klasicky regulovateľný. [6]

4.2 **Kryptomeny**

Kryptomeny sú podskupinou digitálnych platidiel, ktoré v rámci zvyšovania bezpečnosti používajú na kódovanie transakcií pokročilú kryptografiu. Vo svojej najčistejšej forme je kryptomena peer-to-peer verzia elektronickej hotovosti, teda mena s transakciami typu klient-klient. Umožňuje online platby od jedného subjektu k druhému priamo, bez nutnosti finančnej inštitúcie. Sieť časovo označí danú transakciu použitím kryptografickej funkcie proof-of-work POW (systém potvrdenia práce). Tento koncept, ktorý slúži k odradeniu od servisných útokov a ďalšieho zneužívania služieb ako je napr. posielanie spamovej pošty, prvýkrát predstavili v roku 1993 Cynthia Dwork a Moni Naor a spočíva vo vyžadovaní splnenia práce od žiadateľa o službu. Kľúčom pre fungovanie POW je jeho asymetria: pre žiadateľa o službu musí byť práca dostatočne náročná, ale uskutočniteľná, naopak pre poskytovateľa služieb musí byť kontrola vykonania tejto práce veľmi ľahká. Konkrétne pre bežného používateľa je jednoduché poslať jeden e-mail, pretože práca je jednoduchá avšak ak by ten istý užívateľ chcel poslať spamový mail 10 000 ľuďom, musel by už vlastniť značný počítačový výkon, aby mohol zadanú prácu vykonať. Existujú 2 triedy POW protokolov:

a) Protokol typu výzva-odpoveď (challange - response) predpokladá priame interaktívne spojenie medzi klientom a poskytovateľom služby (serverom). Poskytovateľ služby zvolí zdanie úlohy (výzva) napr. hľadanie určitej položky s konkrétnymi vlastnosťami v celej sade položiek. Klient vyhľadá príslušnú odpoveď, ktorú odošle serveru a ten ju skontroluje.

b) Protokol typu riešenie-overenie (solution - verification) interaktívne spojenie medzi klientom a serverom nepredpokladá to znamená, že úloha sa zadá sama bez toho, aby ju predtým server vyriešil. Preto musí server overiť aj výber problému, aj jeho nájdené riešenie. [31]

Bitcoin užíva proof-of-work funkciu s názvom Hashcash (challange - response) na tvorenie blokov transakcií. Jednoducho povedané ide v podstate o súťaž spočívajúcu v dekódovaní, ktorá motivuje tých ktorí sa jej zúčastnia. Konkrétne účastník, ktorému sa ako prvému podarí rozlúštiť kód, dostane za odmenu novo vytvorené bitcoiny. Táto súťaž takto vytvorí záznam o uskutočnených transakciách.

Ďalšie populárne kryptomeny ako napr. Peercoin alebo BlackCoin zas používajú metódu proof-of-stake (doklad o podiely), ktorej hlavnou úlohou je opäť zabrániť dvojitému utrácaniu. V proof-of-work systéme miner musí opakovane používať hashovacie algoritmy na overenie elektronických transakcií, zatiaľ čo v proof-of-stake systéme musia dokazovať vlastníctvo určitého počtu coinov. V systéme proof-of-work pravdepodobnosť vyťaženia bloku závisí na množstve práce, ktorú vykonal miner. V systéme proof-of-stake je podstatné koľko coinov miner vlastní - miner, ktorý vlastní 1% coinov môže vyťažiť 1% blokov. To znamená, že miner v tomto systéme musí vlastniť coiny, aby mohol ťažiť. Ďalším podstatným rozdielom medzi týmito systémami je energetická náročnosť, pričom proof-of-work je oproti proof-of-stake oveľa viac energeticky náročný. [32]

Vo viacerých prácach a komerčných článkoch sa píše, že bitcoin je prvá kryptomena na svete. To v skutočnosti nie je pravda. Prvou komerčne úspešnou kryptomenou je eCash, ktorého fungovanie popísal David Chaum v protokoloch z roku 1983 a 1992. eCash sa zrealizoval vďaka firme DigiCash, Inc. a použil sa ako systém pre mikroplatby (PayPal definuje ako platby < 12 $, Visa definuje ako platby < 20 $) v americkej banke medzi rokmi 1995 až 1998. V európskych krajinách eCash implementovali Credit Suisse vo Švajčiarsku, Deutsche Bank v Nemecku alebo aj Den norske Bank v Nórsku. Platobné transakcie sa uskutočňovali online alebo offline. Kryptografia sa použila na zamedzenie dvojitého utrácania a tiež sa pomocou nej chránili osobné údaje používateľa. eCash bol teda centralizovaný platobný systém patriaci firme DigiCash, Inc. Na konci 90. rokov bol systém predaný firme InfoSpace a nakoniec skrachoval. [6]

Pri vzostupe globálnej finančnej krízy v roku 2008 sa záujem o kryptomeny znova zvýšil. Americký programátor a kryptograf Nick Szabo na blogu [33] vysvetlil, ako môžu kryptomeny predísť problémom spájaným s peniazmi s núteným obehom a svetu predstavil myšlienku decentralizovanej digitálnej meny zvanej bit gold. Ako už naznačuje samotný názov, predpokladá sa existencia zlata určeného na ťažbu a jeho registrácia v digitálnom registri. Tento digitálny register obmedzil potrebu tretej strany pre transakcie. Jeho myšlienka bola v skutku jednoduchá. Navrhol jednoduchý protokol, ktorý požadoval od účastníkov vynaloženie prostriedkov na ťažbu tohto digitálneho zlata, pričom tieto prostriedky sa využili na overenie tohto verejne prístupného digitálneho registra. Prečo bol jeho nápad úspešnejší ako predošlé formy kryptomien? Jednoducho preto, že tieto myšlienky začal uverejňovať v čase vypuknutia finančnej krízy, kedy ľudia prestávali veriť zaužívanému finančnému systému a zároveň aj kvôli tomu, že ako prvý prišiel s myšlienkou voľne prístupného digitálneho registra. Prvou inováciou bolo navrhnutie odmeny pre minerov, druhou zas voľne prístupný register - blockachain. [6] Aj keď sa bit goldu nakoniec nepodarilo komerčne uspieť, je to bez pochýb priamy predchodca bitcoinu ako ho poznáme dnes.

Už od vzniku bitcoinu v roku 2009 sa mu vyčítali rôzne nedostatky a mnoho ľudí ho považovalo len za pokus, preto na seba vývojárska komunita nedala dlho čakať a snažila sa predstaviť nové algoritmy a riešiť aj sociálno-ekonomické problémy, ktoré bitcoin priniesol. Nové protokoly sa zverejňovali na internetových fórach a čakalo sa, či sa nazbiera dosť priaznivcov a stane sa z nej uznávaná kryptomena. Pre všetky nové kryptomeny však kľúčovým prvkom zostáva blockchain a kryptografia. [6] Všetky údaje uvedené v nasledujúcom odstavci sa vzťahujú ku dňu 13.3.2016.

Najväčšie fanúšikovské bitcoin fórum je na stránke bitcointalk.org a má 787 185 užívateľov a viac ako 14 miliónov príspevkov. Na tejto stránke existuje aj sekcia oznamy (altcoiny) kde sa zverejňuje väčšina nových altcoinov. Prvý altcoin na báze bitcoin protokolu na tejto stránke je registrovaný v roku 2011 a má názov Namecoin. Do konca tohto roka sa už na fóre objavuje ďalších 10 altcoinov. Napríklad softwarový repozitár (miesto z ktorého sa dajú stiahnuť a následne inštalovať softwarové balíčky) bitcoin kódu na stránke github.org má teraz 7 526 rôznych kódov. Každá táto položka má potenciál stať sa novou kryptomenou, aj keď len málo z nich ponúka skutočné riešenia technických problémov. Na stránke coinmarketcap.com je registrovaných 640 alternatívnych mien (tržná kapitalizácia 8 281 880 030 $). To však podľa mňa ani zďaleka neodzrkadľuje ich celkové množstvo, pretože nové kryptomeny vznikajú každý deň, ale sú registrované na rôznych fórach. Bohužiaľ

časť týchto altcoinov nevznikla zo zištných dôvodov a v angličtine sa nazývajú „scamcoins“ (podvodné mince). Častou taktikou je vytvorenie a rýchly nákup lacných coinov, vyvolanie rozruchu na fórach a internetových stránkach s cieľom zvýšiť dopyt a následné bleskové odpredanie za vyššiu cenu. Tieto scamcoiny vznikajú s cieľom obohatiť vynálezcu, ktorý zmizne ihneď, ako nazhromaždí peniaze. Našťastie sa kryptozmenárne rozhodli akceptovať len coiny, ktoré majú verejný blockchain, webovú stránku, unikátny prvotný blok, funkčnú online peňaženku a spĺňajú mnoho iných kritérií. Celý ekosystém kryptomien predstavuje živú kultúru experimentovania, ktorá sa snaží vysporiadať s technickými, sociálnymi a teoretickými problémami inovatívnymi návrhmi.

- Altcoiny zrýchľujúce rýchlosť transakcií

V bitcoin protokole je dané, že vytvorenie nového bloku má trvať cca 10 minút a na úplne zaručenie platnosti transakcie musí byť overených ďalších 6 blokov čo môže trvať do 1 hodiny. Čas na vytvorenie nového bloku bol zámerne vybraný Satoshim Nakamotom tak, aby sa zabránilo zbytočnému a zdĺhavému míňaniu výpočtovej kapacity. Pretože len jeden blok zo všetkých sa nakoniec stane akceptovaným a mineri, ktorí do svojho bloku zaradili iné transakcie môžu začať ťažiť od znova, je 10 minút rozumným časom. Začiatkom roka 2011 sa objavil altcoin s názvom SolidCoin 1.0, ktorý umožňoval overiť blok už za tri minúty. Toto rýchle overovanie blokov však nakoniec vyústilo v jeho nestabilitu a slabú ochranu pred útokmi. Zvýšenie rýchlosti vyťaženia bloku bez porušenia bezpečnosti sa podarilo až Litecoinu. Ten umožňoval generovať nový blok každých 2.5 minúty a dobu potvrdenia transakcie tak skrátil na 15 minút, čo je 4-krát rýchlejšie, ako u bitcoinov. [6] Litecoin je v súčasnosti 3. najpopulárnejšia kryptomena založená v roku 2011 Charlesom Leeom. Litecoin ako prvá kryptomena nahradila SHA-256 hashovacím algoritmom SCRYPT, ktorý umožnil ťaženie aj na domácich počítačoch s grafickými kartami. Odmena za vyťaženie bloku sa zmenšuje na polovicu po vyťažení 840 000 blokov. Najbližšie sa odmena zmenší z pôvodných 25 LTC na 12.5 LTC. Celkové množstvo Litecoinov je 84 000 000. [34]

- Altcoiny znemožňujúce „51% atak” a „zlyhanie trhu”

Pretože mining pooly vznikli až niekoľko rokov po bitcoine, ten ich existenciu vo svojom protokole neuvažuje. Kartel minerov by mohol v poole ovládnuť viac ako polovicu výpočtového výkonu, čo sa aj stalo (GHash.io, 12 hodín v roku 2014), a to by mohlo viesť k dvojitému utrácaniu a cenzúre transakcií. Kroll v práci [35] uvádza, že je veľmi

nepravdepodobné, aby kartel minerov dokázal dvojito utratiť také množstvo bitcoinov, aby si tým pokryl náklady vynaložené na tento útok. Oveľa pravdepodobnejšie však je zablokovanie bitcoinových transakcií s cieľom presadzovať zákony alebo cenzúru. S týmto problémom sa popasovalo viac altcoinov a medzi prvými bol Feathercoin, ktorý predstavil takzvaný pokročilý „checkpoint" mechanizmus, ktorý zabezpečuje nemožnosť prepísať úplne celú históriu reťazca overených blokov. Najstarším použitím tohto mechanizmu nájdeme už paradoxne v genesis bloku bitcoinu, ktorý sa naprogramoval tak, aby sa nemohol prepísať. Tento mechanizmus však viacerí užívatelia skritizovali, pretože programátor vykonávajúci „checkpoint" je vybraný a podporovaný hlavným vývojárom, čo ohrozuje hlavne decentralizovaný charakter týchto mien. Ďalším diskutovaným problémom bitcoinu je, že po vyťažení všetkých bitcoinov už mineri budú profitovať len z transakčných poplatkov. Pretože tie budú jediným zdrojom príjmu, mineri o nich začnú bojovať a výsledkom môže byť zníženie týchto poplatkov na hranicu, kedy by sa ich už ani neoplatilo ťažiť. Výsledkom by bol odchod minerov. S prvým riešením tohto problému prišiel Namecoin. Ten umožňuje ťažbu viacerých blockchainov naraz. V angličtine sa tento spôsob nazýva „merged mining" a ako ďalší ho akceptovali coiny ako Dogecoin. [6]

- Altcoiny zmysluplne využívajúce proces ťažby

Kryptomena Primecoin je prvou kryptomenou na svete, ktorá je naprogramovaná na počítanie reálnych vedeckých problémov. Na rozdiel od bitcoinu, kde hľadanie správneho hashu nemá žiadnu pridanú hodnotu, Primecoin generuje špeciálnu radu prvočísel známu ako Cunninghamova rada. Rozdelenie prvočísel bolo jedným z najzásadnejších objavov aritmetiky a štúdiu rôznych prvočíslených sa rád venoval aj Riemann. Rozdelenie prvočísel nie je len časťou abstraktnej matematiky a Euler dokázal priame spojenie medzi Riemannovou zeta funkciou a rozdelením prvočísel. Zeta funkcia si zas našla aplikácie v mnohých oboroch, ako napr. kvantová mechanika, štatistika a teória pravdepodobnosti. [36]

- Altcoiny, ktoré podporujú obeh mien a riešia deflácia

Podľa Rena [37] je najväčším problémom bitcoinu to, že začína fungovať viac ako digitálny majetok než ako platidlo. Kvantitatívna analýza od Rona [38] ukazuje, že až 55% bitcoinov je nečinných a nebolo použitých medzi rokmi 2010-2013. Táto tendencia bitcoiny šetriť a nie utrácať je spôsobená špekulovaním, že ich hodnota vzrastie vďaka ich limitovanému počtu. V médiách a na rôznych fórach prebiehajú hádky, či toto hromadenie bitcoinov nemôže

zapríčiniť krízu v dopyte a deflačnú špirálu. [39] Okrem toho problém spôsobujú aj tzv. „zombie coins", čo sú coiny, ku ktorým majitelia stratili privátny kľúč a taktiež prispievajú k deflácii. Napr. taký Quarkcoin počíta s ročnou infláciou vo výške 0,5%, aby vyrovnal účinok zombie coinov. Okrem toho je ešte stanovený maximálny počet coinov v prvom roku na 27 miliónov a každý nasledujúci rok na 1 milión. Vďaka hnutiu Occupy Wall Street vznikla ďalšia kryptomena s názvom Freicoin (Jún 2012), ktorá predstavila tzv. poplatok za držanie (4,89%), ktorý mal zabezpečiť cirkuláciu platidla. Freicoin je inšpirovaný ekonomickou teóriou Silvia Gesella a jeho konceptom „Freigeld", ktorý uviedol vo svojom diele „Natural Economic Order". Veril, že separácia dvoch funkcií peňazí – úložiska hodnoty a média na výmenu, zabráni vzniku ekonomických boomov a recesií. Ďalej nasleduje rada inflačných kryptomien ako napr. Peercoin, ktorý nemá stanovený konečný počet jednotiek a ročná inflácia je 1%. Veľmi zaujímavý je však Fluttercoin, ktorý tak isto nemá žiaden strop, ale využíva aj nový koncept proof-of-transaction, v ktorom sú odmeny priznané obidvom účastníkom transakcie (aj príjemcovi, aj odosielateľovi). Fluttercoin odmeny prideľuje teda za ťažbu (proof-of-work), za držanie (proof-of-stake) a za míňanie (proof-of-transaction). [40] Ďalším veľmi zaujímavým počinom je tzv. proof-of-burn od Stewarta. Ten predstavuje alternatívu pre minerov ako získať coiny bez využitia výpočtového výkonu - deštrukcia (burn) iných coinov. Jednou z prvých kryptomien využívajúca túto metódu je XCP. Množstvo XCP coinov priamo závisí na tom, koľko bitcoinov sú ľudia ochotní obetovať a zničiť. Tento nový prístup vyvrátil nutnosť proof-of-work a zároveň bitcoinu narobil ešte väčšiu šarapatu v podobe nových zombie coinov. Tento prístup je na druhej strane veľmi výhodný pre zavedenie novej kryptomeny, pretože jej distribúcia je viac férová a úmerná. [41]

- Anonymizujúce kryptomeny

Aj keď bol bitcoin spočiatku považovaný za veľmi anonymný, ukázalo sa, že vďaka zverejňovaniu všetkých transakcií až tak anonymný nie je. CoinJoin, nápad originálne nachádzajúci sa na fóre bitcointalk.org, sa stal veľmi populárnym vďaka zverejneniu na populárnom webe blockchain.info, kde ho označili ako SharedCoin a neskôr ho implementovali aj do Darkcoinu. Hlavnou myšlienkou CoinJoinu je zlúčenie viacerých účastníkov transakcie a vytvorenie spoločného podpisu, čo znemožňuje vyhľadanie konkrétnych použitých bitcoin peňaženiek. Čím viac užívateľov sa spojí do spoločnej transakcie, tým viac vzrastie ich anonymita. [42] Tento prístup ešte ďalej vylepšil Darkcoin, ktorý k tomu pridal aj decentralizovaný servis „DarkSend", ktorý jednotlivé platby v transakcii rozbíja na ešte menšie

platby, ktoré potom preposiela cez náhodných „Master Nods", ktorí pracujú na základe anonymizujúceho protokolu Tor. Títo master nods dostávajú za túto službu 20% z vyťaženého bloku. Ďalším príkladom je Stablecoin, ktorý sa dal na verejnosť až po vyťažení značného množstva coinov, s cieľom integrovať servis výmeny coinov. [6]

- Kryptomeny, ktoré vznikli vďaka sociálnym sieťam

Existovalo mnoho pokusov, ako k altcoinom prilákať rôznorodé komunity ľudí, nie len programátorov a technokratov. Reddcoin je asi najlepším príkladom. Reddcoin vytvoril tzv. sociálnu peňaženku, ktorá jednoducho umožňuje transakcie na najpopulárnejšie mediálne platformy ako Twitter, YouTube alebo Reddit. Reddcoin bol špeciálne vyvinutý na posilnenie finančného dotovania obsahu - užívateľ má možnosť mikroplatbou podporiť autora článku, blogu, tweetu alebo komentára. Bitcoin sa v skutočnosti ukázal ako nevýhodný pre online príspevok, pretože transakcie menšie ako 0,01 BTC nechcú mineri overovať bez minimálneho poplatku 0,0001 BTC. Ďalšou kryptomenou, ktorá vznikla vďaka sociálnym sieťam je Dogecoin. Ten vznikol len tak pre zábavu ako reakcia na veľmi populárny internetový meme z roku 2013 [43]. Dogecoin sa však stal tak populárny a používaný, že v období medzi decembrom 2013 a februárom 2014 mal najväčší počet transakcií a dokonca predbehol aj samotný bitcoin. [44] Dogecoin sa použil aj na rôzne fundraisingové účely - viac ako 26 miliónov Dogecoinov sa vyzbieralo na pomoc jamajskému bobovému tímu, aby mohol štartovať na zimných olympijských hrách v Soči v Rusku v roku 2014.

Pre lepšie uvedomenie si zásadných hráčov na trhu uvádzam nasledujúcu tabuľku 8, v ktorej sú uvedené základné vlastnosti kryptomien s najväčšou tržnou kapitalizáciou.

Por.	Názov	Vznik	Max. počet	Tržná kapitalizácia [$]	Jednot-ková cena [$]	Množstvo v obehu
1	Bitcoin	2009	21 miliónov	6 523 379 975	436.21	14 954 600
2	Ripple	2012	100 miliárd	294 890 349	0.00879	33 537 439 933
3	Litecoin	2011	84 miliónov	157 435 042	3.61	43 582 685
4	Ethereum	2013	nestanovený	73 255 086	0.97105	75 438 580
5	Dash	2014	18.9 miliónov	15 669 418	2.59	6 057 172
6	Dogecoin	2013	neexistuje	14 865 037	0.00014	102 207 349 283
7	Stellar	2014	neexistuje	9 922 386	0.00205	4 837 356 606

Tabuľka 8: Poradie kryptomien podľa objemu v USD k 13.12.2015.

4.3 Blockchain ako platforma pre budúci vývoj

Blockchain je verejná účtovná kniha všetkých bitcoin transakcií, ktoré sa uskutočnili a ku ktorej majú prístup všetci užívatelia siete. Neustále sa zväčšuje chronologickým pridávaním vyťažených blokov. Analogicky k bankovému systému, môžeme povedať, že je to celá história bankových transakcií a jednotlivé bloky sú vlastne výkazy, ktoré vytvára banka. Je to hlavná technologická inovácia, ktorú bitcoin svetu priniesol aj keď jej neustále zväčšovanie sa mnohí považujú za problém kvôli synchronizácii a ukladaniu. V nasledujúcich podkapitolách zhrniem niekoľko najzaujímavejších možných využití technológie blockchain mimo bitcoin siete.

- **digitálne aktíva**

Technológia blockchain môže byť použitá na tvorbu digitálnych aktív ako napr. akcie, dlhopisy, vlastnícke práva na pôdu a iné. Tieto aktíva sa vytvárajú vďaka nadstavbovému protokolu k bitcoinu. Príkladom môže byť open-source protokol s názvom Colored Coins, ktorý umožňuje pripojiť k bitcoinovým transakciám metadáta. Colored Coins využíva bitcoin infraštruktúru na vydávanie digitálnych aktív, ktoré majú v skutočnom svete svoju hodnotu, a umožňuje aj obchodovanie s nimi. Hodnota tohto digitálneho aktíva je daná prísľubom emitenta, že v skutočnom svete bude môcť tento digitálny token zmeniť za aktívum. Digitálne aktíva, ktoré sú nadstavbou k bitcoinom môžu byť teda použité na vydávanie finančných aktív (cenné papiere ako napr. akcie, komodity ako zlato a nové meny), preukazov o vlastníctve (digitálny kľúč k domu alebo autu, vstupenky na koncert) a môžu slúžiť aj ako úložisko informácií (dokumenty, certifikáty) alebo na vytvorenie smart kontraktov. Výhoda digitálnych aktív je daná tým, že ich základom je blockchain, ktorý je transparentný, nemenný, jednoduchý a nefalšovateľný. Všetky prevody a obchody s digitálnymi tokenmi sú teda veľmi bezpečné a ľahké. [45]

Pre lepšie pochopenie uvediem konkrétny príklad. Predstavme si, že Peter má auto a Jozef ho chce od neho kúpiť. Jozef pošle teda bitcoiny Petrovi a to sa zapíše do blockchainu. S touto bitcoin transakciou sa do blockchainu zároveň zapíše, že Peter Jozefovi predal svoje vlastnícke práva na auto. Zároveň by sa stalo to, že digitálny kľúč od auta by už Petrovi prestal fungovať, ale začal by fungovať kľúč Jozefov. Toto predané auto sa v tomto príklade nazýva aj smart property. S touto myšlienkou môžeme ísť aj ďalej ak ešte pripustíme možnosť mikroplatieb. Predstavte si, že jedno auto by používal človek, ktorý ho práve potrebuje a zdieľal by ho

s ostatnými. Napr. by som sa rozhodla, že nechcem platiť za taxík ani za Uber, ale rada si zašoférujem sama. V meste by som si našla dostupné auto a poslala mikroplatbu za jeho užitie, odviezla by som sa z bodu A do bodu B a auto tam jednoducho nechala. K tomuto autu by zas prišiel niekto iný, poslal mikroplatbu, dostal od neho digitálny kľúč a znova by sa mohol odviesť tam kam potrebuje a nechať auto na tom mieste.

- **blockchain ID**

Blockchain ID je jedinečný identifikátor, ktorý je týmto systémom chránený. Slúži v podstate na to, aby mohol užívateľ kryptograficky spojiť svoje blockchain ID k profilu obsahujúcemu ľubovoľné informácie (meno, odkaz na webovú stránku, verejný kľúč...) bez použitia hesla a bez tretích strán, ktoré by autorizovali prístup do webových stránok alebo aplikácií. Môže slúžiť na zabezpečenie aplikácii určených na sprostredkovanie komunikácie alebo aj ako alternatíva k nezabezpečeným identifikátorom ako je rodné číslo (v USA napr. namiesto Social Security Number). [46]

- **smart kontrakty**

Každý študent práva vie, že kontrakt je dohoda medzi 2 alebo viacerými stranami, v ktorej sa jedna strana zaviaže niečo urobiť (alebo neurobiť) výmenou za niečo iné (peňažná platba, poskytnutie služby, dodávka produktu). Strany, ktoré sú inteligentné, platia svojich právnikov, aby vytvorili komplexné zmluvy, ktoré starostlivo popisujú čo každá strana musí robiť, ako musia byť tieto akcie vykonané, čo sa stane ak nebudú splnené určité predpoklady atď. Smart kontrakty sa od nich odlišujú tým, že sú zakódované a digitálne zaznamenané do blockchainu, čo im, ale poskytuje obrovskú výhodu - smart kontrakty sú nespochybniteľné, autonómne a sebestačné.

Pre pochopenie sa opäť vrátim k Petrovi, Jozefovi a autu. Peter predáva jazdené auto, ktoré chce od neho kúpiť Jozef. Tento obchod predstavuje pre obe strany riziko. Jozef riskuje, že Peter nemá vlastnícke právo na auto, že toto osvedčenie sfalšoval, alebo že na tomto aute je záložné právo a ak Peter nesplatí úver banke, banka mu auto zoberie. Peter riskuje, že auto na Jozefa prepíše, ale ten mu nedá sľúbené peniaze, alebo mu vypíše šek, ktorý neskôr banka z dôvodu nedostatku prostriedkov odmietne preplatiť. Obidve zúčastnené strany môžu znížiť tieto riziká zahrnutím tretej strany (notár, právnik, realitná kancelária), ktorá slúži na vzájomnú kontrolu. To však celý proces predĺži, predraží a skomplikuje. Ak sa teda rozhodnú toto riziko

prijať a nikoho nezainteresovať, musia počítať so zvýšenou pravdepodobnosťou vzniknutia konfliktu a následného súdneho sporu, čo znova bude stáť nemalé peniaze. Teraz tento kontrakt uskutočnia pomocou blockchainu. Prvým rozdielom je to, že namiesto spoliehania sa na papiere vlastníctva vydané políciou, by bolo v blockchaine zapísané pri mene majiteľa VIN číslo vozidla. Tak isto by boli v blockchaine zaevidované všetky záložné práva spojené s týmto VIN číslom. Pomocou tohto systému by mohol Peter predať svoje auto Jozefovi jednoducho pomocou svojho smartphonu. Do blockchainu by Peter nahral ponuku zmluvy o predaji svojho auta Jozefovi výmenou za 30 bitcoinov. Ak by bola táto ponuka Jozefom prijatá, kontrakt by sa sám automaticky spustil. VIN číslo by sa aktualizovalo v blockchaine a zobrazilo by sa pri Jozefovom mene a z Jozefovej do Petrovej peňaženky by sa automaticky previedlo 30 bitcoinov. Okrem toho, ak by Peter týmto autom ručil banke svoj úver, blockchain by automaticky stiahol z tých 30 bitcoinov, ktoré mu prišli, čiastku potrebnú na splatenie úveru. Jozef by po tomto kontrakte dostal svoj digitálny kľúč do smartphonu a mohol by si otvoriť kúpené auto, zatiaľ čo Petrov digitálny kľúč by prestal fungovať. Tento proces eliminuje všetky spomenuté riziká a extrémne zjednodušuje celý proces až tak, že na celú transakciu si vystačia smartphony a ich užívatelia. Tento kontrakt by obidvom stranám ušetril peniaze, ale peniaze by ušetril aj polícii resp. štátu, ktorý by viac nemusel držať evidenciu vozidiel. Takisto by sa výrazne znížil počet podvod súvisiacich s pretáčaním tachometra, pretože vozidlo by do blockchainu neustále zaznamenávalo svoje štatistiky o najazdených kilometroch. [47]

- **trh s realitami**

Ďalším pekným príkladom, kde by blockchain neuveriteľne pomohol je trh s realitami. Zatiaľ čo celé bankovníctvo a inštitúcie poskytujúce finančný servis od začiatku využívajú najnovšie technológie, lebo sú pomocou nich schopné generovať väčšie zisky, trh s nehnuteľnosťami ostal viac menej dlhé roky nemenný a jediná novinka, ktorú som v poslednom čase zaregistrovala, je zverejnenie katastrálnych máp na internete. Využitím blockchainu by sa tento obor mohol rapídne zlepšiť a ušetrili by sa nemalé poplatky a zredukovalo by sa riziko vyplývajúce z neinformovanosti.

Prvým krokom k zefektívneniu tohto systému by bolo nahradenie nášho spoločného právneho systému založeného na zaznamenávaní vlastníckeho práva, hypoték a iných verejných záznamov rôznymi inštitúciami blockchainom. Zakaždým keď sa prepisuje pozemok z pôvodného majiteľa na nového, je nutné znova všetky dokumenty dohľadať, čo zaberá mnoho času a nevyhnutne vedie k riziku, že pri hľadaní sa spraví chyba a nie všetky dokumenty budú

k dispozícii. Okrem toho v mnohých rozvojových krajinách je spoľahlivosť týchto záznamov veľmi diskutabilná aj kvôli nestabilite a korupcii. Ani jeden takýto systém kdekoľvek na svete však nemôže fungovať tak spoľahlivo, ako keby používal blockchain.

Aj keď to môže niektorým pripadať ako sci-fi, honduraská vláda už najala texaskú firmu Factom, aby nahradila súčasný vládny systém za systém pracujúci na blockchaine. Už aj v mnohých krajinách USA vznikajú firmy, ktoré držia záznamy takéhoto typu nezávisle na vládnych úradoch, čo síce stojí peniaze, ale určite zabezpečuje väčšiu informovanosť a istotu.

Vysvetlím to na konkrétnom príklade Petra, ktorý pozemok chce predať a Jozefa, ktorý chce kúpiť práve Petrov pozemok. Je dôležité si uvedomiť, že v systéme blockchain, môže byť zaregistrovaný akýkoľvek predmet pod svojim univerzálnym identifikačným kódom (v prípade auta to bolo VIN číslo) čím sa z neho stane smart property. Blockchain ako taký, teda bude uchovávať informácie o vlastníctve pozemku (alebo aj nehnuteľnosti) a priradí jediné označenie ku každému pozemku. Dajme tomu, že v našom príklade má Petrova parcela priradené označenie A123, čo je jej jednoznačná identifikácia. Aby Jozef zistil, či tento pozemok skutočne patrí Petrovi, len vytiahne svoj smartphone a zadá blockchainu požiadavku na zistenie totožnosti majiteľa pozemku A123. Za pár sekúnd Jozef túto informáciu zistí a nepotrebuje k tomu žiadneho úradníka, žiadne dokumenty a mapy, ale iba smartphone a internet. Okrem toho, že pri parcele číslo A123 bude stáť Petrovo meno, bude tam stáť aj informácia o tom, či je pozemok okamžite k dispozícii a či na ňom nie sú nejaké vecné bremená alebo hypotéky. Všetky tieto informácie sú v blockchaine priamo spojené s daným pozemkom. Druhou dôležitou vecou, ktorú si treba uvedomiť je fakt, že stavy pozemkov sa pomerne dynamicky menia tým že sa delia alebo kombinujú. Tieto zmeny pozemkov by sa v systéme blockchain dali pomerne jednoducho zachytiť, pretože každá novovytvorená parcela by dostala nové univerzálne identifikačné označenie, ale zároveň by si zachovala informáciu o jej vzťahu k pôvodnému pozemku. Napr. naša parcela A123 by sa rozdelila na dve menšie a každá z nich by dostala označenie napr. B112 a B113, ale zobrazila by sa aj informácia, že pozemky vznikli delením pozemku A123. V skutočnosti neexistujú žiadne obmedzenia na informácie, ktoré by mohli byť spojené s pozemkom (napr. by to mohol byť link na fotky alebo na prieskum pozemku, mohla by to byť aj výška dane, ktorú by majiteľ za túto nehnuteľnosť musel zaplatiť po jej kúpe a iné). Akonáhle sa však raz tieto informácie dostanú do blockchainu, sú zabezpečené voči akémukoľvek porušeniu zvonka a teda možnosť podvodov rapídne klesá. Jozef zistil o Petrovej parcele množstvo informácií za pár sekúnd a bez peňazí a už mu nič nebráni uzatvoriť smart kontrakt s Petrom. Namiesto toho, aby teraz obidvaja behali po úradoch

a spisovali zmluvy s právnikmi, dokážu sa dohodnúť veľmi rýchlo, pretože obaja majú k dispozícii všetky informácie. Ak by sa teda obidvaja dohodli, smart kontrakt by sa poslal do blockchainu, kde by ho mineri vyťažili v bloku transakcií a tým by sa stal súčasťou overených transakcií, ktoré zdieľa celá sieť. Pri prevode peňazí z Jozefovej do Petrovej peňaženky, by sa automaticky stal novým vlastníkom pozemku A123 Jozef. [48]

5 Energetická náročnosť ťažby bitcoinov

Spolu existujú 3 samostatné činnosti spojené s bitcoinom, ktoré vyžadujú energiu:

1. **Výroba zariadení určených na ťažbu**: Zahŕňa v sebe energiu spotrebovanú na ťažbu nerastov (predovšetkým medi), z ktorých sa vyrábajú čipy a takisto energiu na samotné zhotovenie zariadenia. V momente kedy minerovi prišiel poštou objednaný ASIC miner sa už spotrebovalo kvantum energie, okrem toho aj energia na dopravu bez toho, aby sa miner vôbec pokúsil vyťažiť svoj prvý bitcoin.

2. **Ťažba bitcoinov**: Podľa Landauerovho princípu každý nevratný výpočet spotrebuje energiu. Minimálna energia potrebná na zmenu jedného bitu je daná vzťahom $k \times T \times ln2$, kde $k = 1.38 \times 10^{-23}$ J/K je Boltzmannova konštanta a T je teplota v Kelvinoch. [49] Spotreba na ťažbu je nevyhnutná, ale môže sa v budúcnosti zmenšiť pri implementácii efektívnejších zariadení.

3. **Chladenie**: Pretože podľa zákona zachovania energie sa energia nestráca len mení svoju formu, v prípade výpočtov na počítači sa mení elektrická energia na teplo, ktoré sa uvoľňuje do okolia. Miner preto musí použiť elektrickú energiu na chladenie zariadenia. Čím viac prístrojov vlastní, tým väčšie náklady na chladenie má.

5.1 Ťažba bitcoinov

Dôležitú otázku, ktorú si kladie každý miner alebo potenciálny miner je, či sa bitcoiny oplatí ťažiť a tým pádom investovať do výpočtových zariadení alebo či sa jeho peniaze dajú zhodnotiť lepšie iným spôsobom.

Tak ako píše Satoshi Nakamoto vo svojej práci [50], každý miner sa snaží potvrdiť uskutočnené transakcie (proof-of-work) a to hľadaním hodnoty pre ktorú platí :

$$H(B.N) < T\ [-] \tag{3}$$

kde T (target) je stanovená cieľová hodnota (256 bitové číslo), B je string reprezentujúci transakcie, N je kryptograficky nonce, znak „.“ je v programovacom jazyku operátor spájania stringových reťazcov a H je bitcoinová hashovacia funkcia. Proof-of-work môže byť dosiahnutý náhodným tipovaním hodnoty N alebo jej systematickým hľadaním, až kým neplatí rovnica (3). Ak sa táto hodnota nájde, blok transakcií je poslaný do siete a napojí sa do blockchainu. Proces hľadania hodnoty N je teda bitcoin ťažba. [51]

Pretože náročnosť ťažby bitcoinu rastie exponenciálne, exponenciálne aj klesá schopnosť zariadenia vyťažiť bitcoiny. Náročnosť je len iná reprezentácia hľadaného cieľa T, aby bola pre ľudí zrozumiteľnejšia a je to jednoducho podiel maximálneho možného cieľa a aktuálne cieľa:

$$D = \frac{T_{max}}{T}\ [-] \tag{4}$$

Ak kapacita na ťažbu siete stúpa tzn. viac výkonnejšieho hardwaru sa zapojí do ťažby, skupina 2016 blokov sa vyťaží rýchlejšie ako za plánované 2 týždne a logicky stúpne náročnosť ťažby. Každé jedno zariadenie, ktoré sa do ťažby zapojilo tak dostane menší podiel z odmeny za ťažbu. V určitom čase sa do ťažby zapojí dostatočné množstvo zariadení a náročnosť sa zvýši tak, že náklady na ťažbu a na zariadenia budú rovnaké ako výnosy za vyťažené bitcoiny. Toto je tzv. bod zvratu (break even point). Pretože však výmenný kurz USD/BTC značne kolíše, výhodnosť ťažby musí fluktuovať tak isto - v čase nízkeho výmenného kurzu sú najneefektívnejšie zariadenia vypojené zo siete a náročnosť ťažby klesne a naopak. [20]

Náročnosť ťažby začala na 1 a nikdy nemôže klesnúť pod túto hodnotu. Po vyťažení 2016 blokov sa zistí aký čas *t* trvalo ich vyťaženie. Chceme, aby sa 2016 blokov vygenerovalo za 2 týždne a ak je naše *t* iné, jednoducho aktuálnu náročnosť vynásobíme faktorom $\frac{2\ týždne}{t}$. Teraz už nájdenie blokov zaberie 2 týždne. Napríklad ak nájdenie blokov trvá 10 dní znamená to, že náročnosť je nízka a musí sa zvýšiť o 40% ($D^{nové} = D^{pôvodné} \times \frac{14}{10} = 1{,}4 \times D^{pôvodné}$).

Náročnosť nemôže byť naraz zmenená viac ako o 4-násobok (nemôže sa zrazu 4-násobne sťažiť alebo zjednodušiť), aby nedošlo k takejto obrovskej neočakávanej zmene. Je možné určiť iba približný odhad nasledujúcej zmeny náročnosti na základe doby trvania vyťaženia predchádzajúcich blokov. Napr. na stránke https://bitcoinwisdom.com/bitcoin/difficulty je

k 23.04.2016 spočítaná nasledujúca náročnosť 187,372,586,478 s presnosťou okolo 5% a zmení sa po spočítaní 699 blokov cca za 4.7 dňa.

Maximálna cieľová hodnota T_{max} je $(2^{16}-1)\times 2^{208} \approx 2^{224}$. Náhodný hash má pravdepodobnosť 2^{-32}, že bude menší ako maximálna cieľová hodnota. [52] Pravdepodobnosť splnenia rovnice (3) je tým pádom:

$$p \approx \frac{1}{D \times 2^{32}}\ [-] \tag{5}$$

Každé hľadanie hodnoty (nonce) je náhodný proces a počet nájdených nonce až po tú správnu má geometrické rozdelenie. Preto je počet hashov potrebných na vyťaženie bloku rovný $D \times 2^{32}$. Ak máme zariadenie, ktoré nám vygeneruje R hashov predpokladaná doba nájdenia bloku je [53]:

$$t = \frac{D \times 2^{32}}{R}\ [s] \tag{6}$$

Napr. ak má miner k dispozícii zariadenie s výkonom 1 MH/s a náročnosť je 158,427,203,767 (15.3.2016) potom $t = \frac{158427203767\times 2^{32}}{10^6} = 6{,}8 \times 10^{14}$ s.

Jednou z veličín, ktorú musíme pri určovaní výhodnosti ťažby započítať je odmena pre minera. Existujú 2 bitcoinové odmeny pre minera a to za vyťaženie bloku (momentálne 25 BTC) a transakčné poplatky.

Transakčný poplatok odosielateľ bitcoinov môže, ale nemusí do transakcie zahrnúť. Pretože sa však tieto poplatky v súčasnosti pohybujú na úrovni satoshi (0,000 000 01 BTC) v porovnaní s odmenou za vyriešenie bloku sú skoro zanedbateľné.

Miner si v prvom rade musí vybrať konkrétny hardware zistiť jeho cenu a náklady na prevádzku. Hash rate zariadenia (udáva rýchlosť vykonania kryptografických operácií) R sa v dnešnej dobe typicky udáva v [GH/s]. Čím väčší hash rate zariadenia, tým väčšia pravdepodobnosť, že sa mu podarí vyťažiť blok. Ak tento hash rate podelíme spotrebou elektrickej energie dostaneme energetickú efektivitu zariadenia ε, ktorá dobre poslúži na porovnávanie rôzneho hardwaru.

$$\varepsilon = \frac{R}{P}\left[\frac{GH}{J}\right] \tag{7}$$

V tabuľke 4 v druhej kapitole som uviedla porovnanie viacerých parametrov rozličných dostupných ASIC zariadení. Ako potenciálny miner som sa rozhodla pre zariadenie AntMiner S7 BATCH 10 (4.5 kg, 4 730 GH/s) z dôvodov, že s pomedzi dostupných zariadení má najvyššiu efektivitu ťažby 0.27 J/GH a najlepší pomer cena / hash rate 0.198 $/(GH/s). Okrem toho je na zariadenie 90 dňová záruka a vyskladnenie je do 5 pracovných dní od uhradenia ceny.

Obrázok 11: Asic miner typu AntMiner S7 BATCH 10.

Okrem ceny 935.26 $ treba ešte zaplatiť prepravu z Číny, ktorá je 55.08 $ cez spoločnosť FedEx. [54]

Tento ASIC potrebuje ešte vlastný napájací zdroj (1 zariadenie = 1zdroj). Riadila som sa odporúčaním výrobcu a vybrala model APW3-12-1600-B2 (2.3 kg, 1 600 W, 140$). [55]

Obrázok 12: Power supply unit APW3-12-1600-B2.

Posledná vec, na ktorú nesmie potenciálny miner zabudnúť, je dodatočné chladenie v podobe ventilátorov a klimatizácie. Pretože ťažba vo veľkom má obrovské nároky na chladenie objavili sa už aj nové technológie chladenia ASIC zariadení a to imersné chladenie olejom. [56] Firma Allied Control so sídlom v Hong-Kongu a zaoberajúca sa ASIC zariadeniami dokonca tvrdí, že ich chladiaci systém môže minerovi ušetriť až 90% spotreby elektrickej energie. [57]

Obrázok 13: Využitie imersného chladenia pri ťažbe bitcoinov.

Táto technológia je však ešte úplne nová a je v podstate vo fáze testovania, takže ako potenciálny miner by som si určite vybrala dostupnú a overenú technológiu napr. ventilátor pre AntMiner S3, S5, S5+, S7 (0.5 kg, 15 $). [58]

Obrázok 14: Ventilátor na chladnenie typ fan for AntMiner S3, S5, S5+, S7.

Po objednaní celého zariadenia minerovi ostáva len dúfať, že všetky komponenty sa dopravia z Číny načas a v nepoškodenom stave. Nefunkčnosť niektorého zo zariadení resp. veľmi neskorá dodávka by výrazne ovplyvnili návratnosť celého ťaženia v minerov neprospech. Je to spôsobené neustálym sa zvyšovaním náročnosti ťažby pri nemennej efektivite zariadenia. To znamená, že čím neskôr začne miner ťažiť tým menej bitcoinov vyťaží. Z osobného rozhovoru s bývalým minerom viem, že nie zriedka sa stalo a stáva, že zariadenie príde aj o dva a kľudne aj o tri mesiace neskôr ako malo. Podľa mňa zásadným problémom v tomto prípade je, že ak výrobca vyvinie vysoko výkonný ASIC miner a je najlepší na trhu, radšej ho sám zapojí do ťažby na istý čas a až potom ho predá ako nové zariadenie ostatným minerom. Uvedomujem si, že toto riziko je veľmi veľké, ale vybrala som si dodávateľa na základe spokojných recenzií zákazníkov a preto budem uvažovať, že zariadenie bude zapojené do ťažby odo dňa, ako bolo v mojom pláne.

Ďalším vstupným faktorom je cena elektrickej energie. Podľa online kalkulačky [59] som stanovila cenu elektrickej energie na 4.156 Kč/kWh. Pretože však beriem pri výpočtoch do úvahy len kurz doláru a bitcoinu a taktiež všetko ťažobné zariadenie sa uvádza prevažne v dolároch, cenu elektrickej energie budem uvádzať tiež v dolároch. 4.156 Kč/kWh dnes zodpovedá 0.17 USD/kWh. [60]

Ďalšou dôležitou úlohou minera je vybrať si pool v ktorom bude ťažiť. Rozhodla som sa pre český pool Mareka Palatinusa s názvom Slush pool, pretože má najdlhšiu históriu, ponúka stabilné odmeny a webové stránky spolu so zákazníckou podporou sú dostupné v českom jazyku 24 hodín denne. Okrem toho má vo svete bitcoinov dobré meno a požiadavky minerov pravidelne implementuje do praxe vývojársky tím.

Teraz už len zostáva zrátať koľko peňazí stojí minera ťažba a koľko peňazí je schopný zarobiť. V nasledujúcom odstavci zhrniem všetky vstupné náklady, ktoré budem mať ako potenciálny miner:

- AntMiner S7 BATCH 10 s cenou 935.26 $
- APW3-12-1600-B2 s cenou 140 $
- fan for Antminer S3, S5, S5+, S7 s cenou 15 $
- cena za prepravu je 55.08 $

Spolu by som za zariadenie zaplatila 1 145.34$ (27 504.17 Kč, prepočítané cez server [60])

Ďalšie vstupné údaje (k 23.04.2016) sú:

- cena elektrickej energie 0.17 $/kWh
- náročnosť pri ktorej začne ťažba 178,678,307,671.69 [64]
- príkon zariadenia je 1 293 W
- hash rate zariadenia je 4 730 GH/s
- zvýšenie náročnosti ťažby 3% resp. 1% 2 krát za mesiac
- aktuálna odmena za vyriešenie bloku je 25 BTC
- odmena za vyriešenie bloku od 10.7.2016 je 12.5 BTC [61]
- doba trvania ťažby 168 dní (začiatok ťažby 23.04.2016)
- výmenný kurz 400.24 $/BTC resp. 500 $/BTC
- poplatok poolu 2%

Vypočítané údaje:

- cena spotrebovanej elektrickej energie za deň $1.293[kW] \times 24[h] \times 0.17[\$/kWh] = 5.28\$$

- doba potrebná na vyťaženie jedného bloku podľa vzorca (6) je $E(t) = \frac{178\,678\,307\,671.69 \times 2^{32}}{4\,730 \times 10^{9}} = 162\,244\,712.04\ s \cong 5.14\ roka$ (5 rokov a necelé 2 mesiace)

- množstvo vyťažených bitcoinov

Aj keď na oficiálnej stránke poolu je postup výpočtu trochu iný a je tam aj link na online kalkulačku, rozhodla som sa využiť len vzorce dostupné na „oficiálnej“ bitcoin stránke www.en.bitcoin.it a všetko spočítať sama.

Pri výpočte budem vychádzať zo znalosti vzťahu medzi hash rateom siete ozn. TNHR (Total Network Hash Rate) a náročnosťou ťažby ozn. D (Difficulty). Počet hashov potrených spočítať na vyťaženie bloku pri určitej náročnosti je [53]:

$$\frac{D \times 2^{256}}{OxFFFF \times 2^{208}}\ [-] \tag{8}$$

0xFFFF v hexadecimálnej sústave reprezentuje číslo 65 535 a teda vzorec (8) sa dá upraviť do tvaru:

$$\frac{D \times 2^{48}}{65\,535}\ [-] \tag{9}$$

Náročnosť D je nastavená tak, aby sa 2016 blokov našlo za 10 minút to znamená, že ak výraz (9) podelíme časom získame hash rate siete:

$$TNHR = \frac{\frac{D \times 2^{48}}{65\,535}}{600}\ \left[\frac{H}{s}\right] \tag{10}$$

To, koľko bitcoinov sme so zariadením schopný vyťažiť, je určené pomerom medzi hash rateom nášho zariadenia ozn. HR a celkovým hash rateom siete. Ak budem počítať počet bitcoinov vyťažených za deň ozn. DR (Daily Revenue), do vzorca ešte zahrniem aktuálnu cenu za vyťaženie bloku ozn. BR (Bitcoin Reward) a dostanem vzťah:

$$DR = \frac{HR \times BR \times 6 \times 24 \times 600 \times 65535}{2^{48} \times D} \left[\frac{BTC}{deň}\right] \quad (11)$$

Člen v čitateli 6×24 je časový faktor a prepočítava 10 minút v TNHR na celý deň. V tomto vzorci je dôležité dosadzovať hodnoty HR a TNHR v jednotkách [H/s]. Po dosadení všetkých neznámych na pravej strane som spočítala, že denne by som na svojom zariadení vyťažila:

$$DR = \frac{4730 \times 10^9 \times 25 \times 6 \times 24 \times 600 \times 65535}{2^{48} \times 178678307671.69} = 0.01331301965926686 \left[\frac{BTC}{deň}\right]$$

Tento počet bitcoinov by som však vyťažila len za predpokladu konštantnej hodnoty náročnosti. V skutočnosti sa však náročnosť mení každých 2016 blokov čo je cca každé 2 týždne. Pretože odhadnúť ako sa náročnosť bude meniť je naozaj ťažké, prečítala som si viacero článkov a štatistík a vyhľadala som si viaceré online kalkulačky. Nakoniec som v pesimistickej variante počítala s 3% prírastkom náročnosti 2-krát za mesiac a vo variante optimistickej som prírastok stanovila na 1% 2-krát za mesiac.

Najdôležitejším, ale zároveň nevyspytateľným faktorom však ostáva cena bitcoinov na burze, teda výmenný kurz bitcoinov a amerických dolárov. Nasledujúci graf 6 ilustruje výmenný kurz medzi americkým dolárom a bitcoinom od jeho vzniku až po dnešok (23.4.2016).

Graf 6: Výmenný kurz USD/BTC.

Odmena za vyťaženie bloku je aktuálne 25 BTC, no pravdepodobne sa zmení na 12.5 BTC dňa 10.7.2016. Od 78. dňa ťažby preto počítam už s touto novou zníženou odmenou.

Na stránke [63] som si v štatistikách vyhľadala, že priemerná cena bitcoinu za posledný polrok (27.10.2015 a 27.4.2016) bola 400.24$. Táto hodnota je trochu nižšia ako je v súčasnosti skutočná hodnota a je tiež nižšia oproti odhadom ekonómov pre budúci vývoj. Vo variante č.2 som počítala s vyšším kurzom v hodnote 500 $/BTC. S týmito fixnými kurzami som sa rozhodla počítať v tejto modelovej situácii kvôli tomu, že odhadnúť percentuálne výkyvy vo výmennom kurze by bolo podľa môjho názoru príliš trúfalé. Výsledky pesimistickej varianty sú v nasledujúcej tabuľke 9:

Deň	Náročnosť	BTC/deň po zaplatení poplatku poolu	Zarobené bitcoiny spolu	Výnos spolu [$]	Spolu za elektrickú energiu [$]
0	178,678,307,671.690	0.013046759			
14	184,038,656,901.841	0.012666757	0.195321386	78.18	-73.86
28	189,559,816,608.896	0.012297822	0.372287044	149.00	-147.71
42	195,246,611,107.163	0.011939633	0.544098361	217.77	-221.57
56	201,104,009,440.378	0.011591877	0.710905466	284.53	-295.42
70	207,137,129,723.589	0.011254249	0.872854111	349.35	-369.28
84	213,351,243,615.297	0.005463228	0.990859831	396.58	-443.14
98	219,751,780,923.756	0.005304105	1.067185896	427.13	-516.99
112	226,344,334,351.468	0.005149616	1.141288872	456.79	-590.85
126	233,134,664,382.012	0.004999627	1.213233509	485.58	-664.71
140	240,128,704,313.473	0.004854007	1.283082671	513.54	-738.56
154	247,332,565,442.877	0.004712628	1.350897391	540.68	-812.42
168	254,752,542,406.163	0.004575367	1.416736925	567.03	-886.27

Tabuľka 9: Výnosy a náklady na ťažbu bez počiatočnej investície, pesimistický variant.

Z tabuľky 9 vyplýva, že hodnota vyťažených bitcoinov nedokáže pokryť náklady na vynaloženú elektrickú energiu a počiatočná investícia sa nesplatí. Náklady za spotrebovanú elektrickú energiu v tomto prípade rastú už cca po mesiaci rýchlejšie ako výnosy z vyťažených bitcoinov. Za sledované obdobie (168 dní) by som ako miner bola v strate –1 145.34 – 886.27 + 567.03 = – 1 464.58 $ (34 943.41 Kč podľa [60]). Dokonca aj v prípade, že by si miner vedel zabezpečiť elektrickú energiu zadarmo (napr. by zariadenie používal na študentskej ubytovni) stále by po 168 dňoch ťažby nedokázal splatiť počiatočnú investíciu a bol by v strate –1 145.34 + 567.03 = – 578.31 $. Slush pool by za sledované obdobie zarobil 201.53 $.

Deň	Náročnosť	BTC/deň po zaplatení poplatku poolu	Zarobené bitcoiny spolu	Výnos spolu [$]	Spolu za elektrickú energiu [$]
0	178,678,307,671.690	0.013046759			
14	180,465,090,748.407	0.012917583	0.195572213	97.79	-73.86
28	182,269,741,655.891	0.012789687	0.376290484	188.15	-147.71
42	184,092,439,072.450	0.012663056	0.555219466	277.61	-221.57
56	185,933,363,463.174	0.012537679	0.732376873	366.19	-295.42
70	187,792,697,097.806	0.012413544	0.907780247	453.89	-369.28
84	189,670,624,068.784	0.006145319	1.038061003	519.03	-443.14
98	191,567,330,309.472	0.006084474	1.124034620	620.61	-516.99
112	193,483,003,612.567	0.006024232	1.209157013	604.58	-590.85
126	195,417,833,648.692	0.005964586	1.293436610	646.72	-664.71
140	197,372,011,985.179	0.005905530	1.376881756	688.44	-738.56
154	199,345,732,105.031	0.005847060	1.459500712	729.75	-812.42
168	201,339,189,426.081	0.005789168	1.541301659	770.65	-886.27

Tabuľka 10: Výnosy a náklady na ťažbu bez počiatočnej investície, optimistický variant.

V tabuľke 10 sú výsledky optimistického variantu. Tempo rastu náročnosti som znížila na 1% a výmenný kurz som naopak zvýšila na 500 $/BTC. Aj v tomto prípade sa však za sledované obdobie nestihne splatiť počiatočná investícia. Výnosy z bitcoinov rastú rýchlejšie ako náklady na elektrickú energiu cca do 4 mesiacov. Po 118. dni ťažby sa však tento trend mení a náklady na elektrickú energiu znova začnú prevyšovať výnosy z bitcoinov viď. tabuľka 11. Spolu by som ako miner za sledované obdobie (168 dní) bola v strate –1 145.34 – 886.27 + 770.65 = – 1 260.96 $ (30 085.24 Kč podľa [60]). Rovnako ako v pesimistickom variante, ak má miner k dispozícii elektrickú energiu zadarmo, po 168 dňoch ťažby stále nedokáže splatiť počiatočnú investíciu a je v strate –1 145.34 + 770.65 = – 374.69 $. Za sledované obdobie by si naopak Slush pool zarobil 294.62 $.

Deň	Náročnosť	BTC/deň po zaplatení poplatku poolu	Zarobené bitcoiny spolu	Výnos spolu [$]	Spolu za elektrickú energiu [$]
110	191,567,330,309.472	0.006084474	1.197048308	598.52	-580.30
111	191,567,330,309.472	0.006084474	1.203132782	601.57	-585.57
112	193,483,003,612.567	0.006024232	1.209157013	604.58	-590.85
113	193,483,003,612.567	0.006024232	1.215181245	607.59	-596.12
114	193,483,003,612.567	0.006024232	1.221205477	610.60	-601.40
115	193,483,003,612.567	0.006024232	1.227229708	613.61	-606.68
116	193,483,003,612.567	0.006024232	1.233253940	616.63	-611.95
117	193,483,003,612.567	0.006024232	1.239278171	619.64	-617.23
118	193,483,003,612.567	0.006024232	1.245302403	622.65	-622.50
119	193,483,003,612.567	0.006024232	1.251326635	625.66	-627.78
120	193,483,003,612.567	0.006024232	1.257350866	628.68	-633.05

Deň	Náročnosť	BTC/deň po zaplatení poplatku poolu	Zarobené bitcoiny spolu	Výnos spolu [$]	Spolu za elektrickú energiu [$]
121	193,483,003,612.567	0.006024232	1.263375098	631.69	-638.33
122	193,483,003,612.567	0.006024232	1.269399330	634.70	-643.60
123	193,483,003,612.567	0.006024232	1.275423561	637.71	-648.88
124	193,483,003,612.567	0.006024232	1.281447793	640.72	-654.15
125	193,483,003,612.567	0.006024232	1.287472025	643.74	-659.43
126	195,417,833,648.692	0.005964586	1.293436610	646.72	-664.71

Tabuľka 11:V optimistickom variante náklady na ťažbu okolo 118. dňa ťažby opäť začali prevyšovať výnosy.

Z mojich výpočtov jasne vyplýva, že ťažba na tomto jedinom zariadení sa nevyplatí. Rozdiel medzi stratou v optimistickom a pesimistickom variante je presne 4 858.17 Kč. Ani v pesimistickom a ani v optimistickom odhade ťažba bitcoinov nedokáže splatiť počiatočnú investíciu a to aj v prípade, žeby bola elektrická energia k dispozícii zadarmo.

5.2 Spotreba elektrickej energie bitcoin sieťou

Pretože tvorba nových bitcoinov, zabezpečenie celej siete a koniec koncov aj validácia transakcií vyžaduje proof-of-work, čo je v podstate výpočet náročný na prevedenie, ale ľahký na kontrolu, je jasné, že pri tomto výpočte sa spotrebuje určitá elektrická energia. Tak ako aj na ťažbu zlata, razenie mincí, fungovanie bánk spotrebujeme kvantum energie, ľudskej práce a prístrojov, tak aj ťažba bitcoinov a udržiavanie funkčnosti siete spotrebúvajú energiu.

Bitcoin už od svojho vzniku neustále čelí obrovskej kritike pre energetickú spotrebu. Mnohí ľudia tvrdia, že bitcoin je z dlhodobého hľadiska neudržateľný projekt vďaka stálemu zvyšovaniu náročnosti ťažby. Veď len ku dnešnému dňu (15.04.2016) je zložitosť ťažby na úrovni 178,678,307,671.69 a hash rate celej siete je stanovený na neuveriteľných 1 394 497 055.66 GH/s [64]. Aj napriek tomu, že náročnosť sa stále zvyšuje a teda by logicky mala rásť aj spotreba elektrickej energie celej siete, mnohí zabúdajú, že nové zariadenia na ťažbu vznikajú každý deň, sú oveľa efektívnejšie a ich spotreba elektrickej energie sa stále zmenšuje.

Po publikovaní mnohých článkov kritických k energetickej náročnosti, z hlavnej stránky, ktorá uverejňuje štatistiky a má názov blockchain.info, zmizli údaje o spotrebe elektrickej energie a najnovšie aj o nákladoch na ťažbu. Jedným z týchto článkov je aj [65]. V tomto článku sa píše, že spotreba elektrickej energie na ťažbu za 24 hodín (16.12.2013) bola podľa serveru blockchain.info 131 019,91 MWh, čo predstavuje podľa autora 19 652 986,38 $. V článku [66] sa však píše, že v ten deň bol hash rate celej siete 7 000 000 GH/s a elektrická spotreba bola 650 W/GH/s. To znamená, že bitcoin mal v skutočnosti spotrebovať len 4,55 GW. Ak to

vynásobíme 24 hodinami dostane, že v ten deň sa spotrebovalo 109,2 GWh elektrickej energie. Prečo však blockchain.info uverejnil, že spotreba bola 131 GWh/deň (čo sa použilo aj vo vyššie spomenutom článku), však nie je jasné, pretože to matematicky nesedí. Podľa môjho názoru server blockchain.info chybne stanovil elektrickú spotrebu na 650 W/GH/s, ktorá síce bola pravdivá v časoch keď sa ťažilo na obyčajných počítačoch, ale s príchodom novej technológie toto číslo rapídne kleslo. Ak bola naozaj spotreba 650 W/GH/s, znamenalo by to že ročná spotreba by bola 39,85 TWh, čo je viac ako spotreboval Bangladéš v roku 2008 [67].

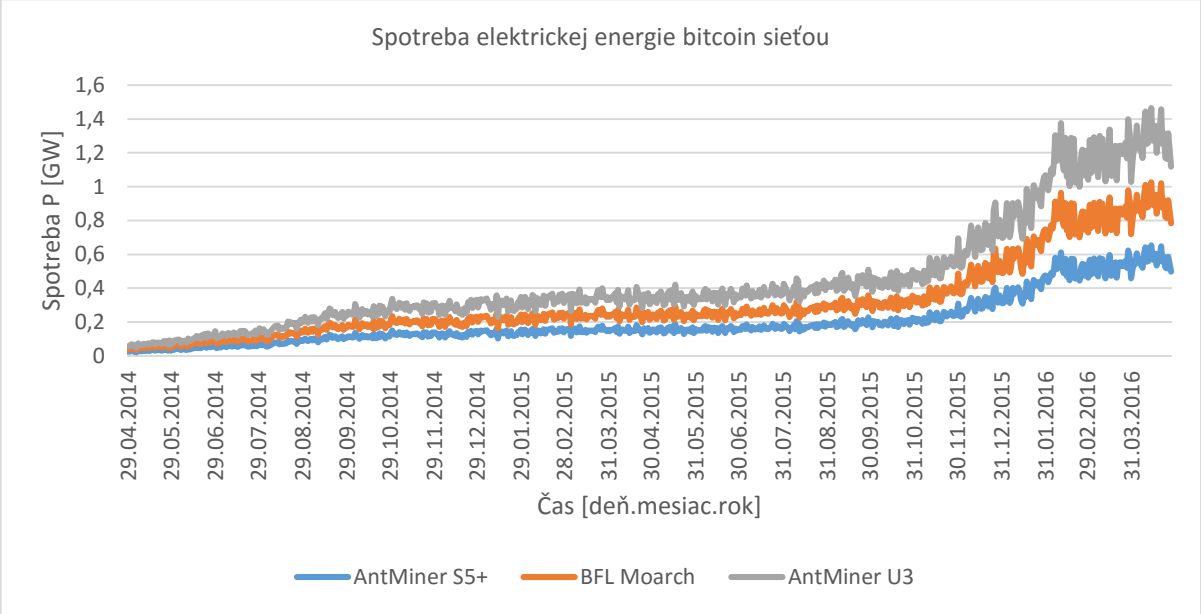
Ďalším „démonizujúcim" článkom bol článok na portály bloomberg [68]. Tento sa znova odvoláva na dáta zverejnené na blockchain.info z dňa 12.4.2013, podľa ktorých spotreba elektrickej energie vyčíslená v peňažnom ekvivalente minerov v tom dni bola 147 000 $, za predpokladu, že el. energia v tom čase stála približne 15 centov za kWh. Denný zárobok za ťažbu bol stanovený na 681 000 $, to znamená, že to bol v tom čase dobrý biznis. V článku sa však spomína, že spotreba el. energie je 982 MWh za deň, čo je spotreba 31 000 priemerných amerických domácností. S týmto problémom sa snažili vysporiadať rôzne iné altcoiny: buď zmenou systému ťažby (z proof-of-work na proof-of-burn alebo proof-of-stake), alebo dodatočným zúžitkovaním spotrebovanej energie (Primecoin a hľadanie špeciálnych prvočísel) alebo zmenou kryptografického hashovacieho algoritmu. Čím viac článkov a príspevkov o energetickej spotrebe som si prečítala tým viac rôznych a nekorešpondujúcich údajov som našla. Bohužiaľ v článkoch autori častokrát nezverejnili postupy výpočtov a ani základné vstupné údaje, preto sú tieto čísla z môjho pohľadu irelevantné a v nasledujúcich odstavcoch sa budem sama snažiť spočítať energetickú spotrebu celej bitcoin siete.

Pretože hash rate bitcoin siete je neustále zverejňovaný na internete, na určenie približnej spotreby elektrickej energie stačí odhadnúť efektivitu zariadení zapojených do ťažby. Samozrejme, že toto číslo sa nedá odhadnúť žiadnym rozumným spôsobom, ale určite môžem vylúčiť možnosti, že miner v dnešnej dobe na ťažbu používa CPU, GPU alebo FPGA. Som si úplne istá a viacero online bitcoinových fór mi potvrdilo, že úplná majorita zariadení sú ASIC zariadenia. Pretože na stránke https://en.bitcoin.it/wiki/Mining_hardware_comparison je v zozname viac ako 70 rôznych ASIC minerov vybrala som len tie, pri ktorých bola zverejnená elektrická spotreba zariadenia, údaj o Mhash/J (t.j. efektivita) a boli aktuálne k dispozícii. Konkrétne teda budem predpokladať, že celá sieť ťaží na resp. má efektivitu ťažby ako: AntMiner S5+ ($\varepsilon = 0.44\, J/Gh$, modrá čiara v grafe 7), BFL Monarch 700 GH/s ($\varepsilon = 0.7\, J/Gh$, oranžová čiara v grafe 7) alebo ako AntMiner U3 ($\varepsilon = 1\ \mathrm{J}/Gh$, sivá čiara v grafe 7). Na stránke blockchain.info sú k dispozícii hash rate siete v každom okamžiku od jej vzniku.

Úpravou rovnice (7) do tvaru:

$$P_{siete} = \frac{R_{siete}}{\varepsilon_{siete}} \; [W] \tag{12}$$

som spočítala spotrebu elektrickej energie v závislosti na čase pre 3 bitcoin siete používajúce len jeden z uvedených typov zariadenia. Pretože ASIC zariadenia sa aktívnejšie začali používať až začiatkom januára v roku 2014 nemá zmysel modelovať spotrebu siete s týmto zariadením pred týmto dátumom.



Graf 7: Spotreba elektrickej energie bitcoin sieťou v prípade že všetci užívatelia majú rovnako efektívne zariadenia typu AntMiner S5+, BFL Monarch 700 GH/S alebo AntMiner U3.

Denná spotreba bitcoin siete sa v prvých 4 mesiacoch roku 2016 podľa mojich výpočtov odhadovo pohybuje medzi 0.4 a 1.5 GW resp. medzi 9.6 GWh a 36 GWh, čo zodpovedá približne výkonu malej elektrárni. Tieto čísla sú skutočne až o 100 GWh menšie ako sa spomínalo v článkoch z roku 2013. Jediné vysvetlenie, ktoré dáva zmysel je, že zariadenia na ťažbu z roku 2013 mali úplne nízku efektivitu oproti tým dnešným v roku 2016.

Preto ak čítam články, v ktorých sa píše, že do roku 2020 bude spotreba bitcoin siete až 14 GW, čo je približne spotreba Dánska, zostávam veľmi skeptická, pretože tak ako nikto v minulosti vo svojich predpovediach nerátal s neuveriteľne efektívnymi zariadeniami typu

ASIC, tak v súčasnosti nikto nemôže vedieť aké technické pokroky sa v najbližšej dobe môžu stať. [69]

Pre zaujímavosť, som ešte skúsila spotrebu bitcoin siete porovnať s celkovou spotrebou elektrickej energie na Slovensku za rok 2014 (najnovšie dostupné). Podľa Správy o výsledkoch monitorovania bezpečnosti dodávok elektriny z júla 2015 [70] je spotreba 28 355 GWh za rok čo je v prepočte približne 3.24 GW za deň. Z mojich výpočtov usudzujem, že energetická spotreba bitcoin siete nie je vôbec tak obrovská, ako sa snažia podsúvať rôzne články a aj keď si uvedomujem, že môj výpočet nie je presný, určite je komplexnejší.

Pre výpočet vypustených emisií do ovzdušia sa mi bohužiaľ nepodarilo nájsť žiadne relevantné dáta. Vo svojej práci [71] Hass McCook síce uvádza spočítané čísla, ale nikde nenapísal detailnejší postup ako sa k nim dopracoval. Jeho prepočty sú za predpokladu, že hash rate siete je 95 000 000 H/s a uvádzam ich v nasledujúcej tabuľke 12.

Priemerná efektivita siete [W/Gh]	Emisie skleníkových plynov [tony CO_2 za rok]
0.5277	263 710
0.9	450 000
1.1	550 000
1.3	650 000
1.5	750 000

Tabuľka 12: Množstvo vypustených skleníkových plynov do ovzdušia v závislosti na hash rate bitcoin siete.

Veľmi veľa ľudí stále často tvrdí, že bitcoin spotrebúva enormné množstvo elektrickej energie. Prečo, ale nikto nevraví o energetickej náročnosti nášho zaužívaného finančného systému? Nestačí len povedať, že bitcoin je náročný, ale treba ho vždy s niečím porovnať. Aby som však neporovnávala jablká s hruškami, budem spotrebu bitcoin siete porovnávať so spotrebou klasického finančného systému. V publikácii [71] som našla porovnanie ekonomických, environmentálnych a socioekonomických nákladov na chod bankovníctva, ťažby zlata, tlače bankoviek, razeniu mincí a na ťažbu bitcoinov a uvádzam ich v tabuľke 13.

	Ročné náklady v hrubom [miliardy $]
Ťažba zlata	105
Recyklácia zlata	40
Tlač bankoviek a razenie mincí	28
Spotreba el. energie bankovým systémom (pri cene 100 $/ MWh)	63.8
Ťažba bitcoinov	0.66

Tabuľka 13: Porovnanie ročných ekonomických nákladov.

	Spotreba energie [GJ]	Emisie skleníkových plynov [tony CO_2]	Vývojový trend
Ťažba zlata	475 miliónov	54 miliónov	stúpajúci
Recyklácia zlata	25 miliónov	4 miliónov	klesajúci
Tlač bankoviek a razenie mincí	39.6 miliónov	6.7 miliónov	stúpajúci
Bankový systém	2340 miliónov	390 miliónov	stúpajúci
Ťažba bitcoinov	3.3 miliónov	0.55 miliónov	klesajúci

Tabuľka 14: Porovnanie ročných environmentálnych nákladov.

Pri ročnej ťažbe zlata (2.7 miliónov kilogramov) sa okrem údajov spomenutých v tabuľke 14 ešte spotrebuje 810 miliárd litrov vody, 400 tisíc ton kyanidu a vyprodukujú sa 4 miliardy odpadového kameňa. [71] Na tlač amerických papierových bankoviek sa ročne použije 1.75 miliárd vody, 7100 ton bavlny, 2300 ton ľanu a 3540 ton farby. [72]

	Zlato	Meny s núteným obehom	Bitcoin
Smrť robotníkov	Viac ako 50 000 historicky zaznamenaných a takmer 100 ročne	0	0
Korupcia	600 miliónov $	1.6 triliónov $	Zanedbateľné
Pranie špinavých peňazí		2.65 triliónov $	
Čierny obchod		1.8 triliónov $	

Tabuľka 15: Porovnanie socioekonomických ročných nákladov.

Pri ťažbe zlata bohužiaľ zomrelo oveľa viac ľudí ako je zdokumentovaných. 50 000 obetí je evidovaných len za minulé storočie a asi nie je prehnané tvrdiť, že obetí bolo niekoľko desiatok tisíc a ďalšie štatistiky o dlhotrvajúcich efektoch ťažby na ľudské zdravie nie sú vyhotovené. [71]

Vo všetkých porovnaniach nákladov jednoznačne víťazí bitcoin. Bitcoin najmä v porovnaní s klasickým bankovým systémom, má až šokujúco nízke náklady, a verím, že v budúcnosti bude aj vďaka tomu jeho veľmi úspešným konkurentom.

Záver

V práci som analyzovala rôzne aspekty digitálnej kryptomeny s názvom bitcoin. Hlavným zámerom bolo určenie výhodnosti ťažby v súčasných podmienkach a približné stanovenie elektrickej spotreby bitcoin sieťou.

Bitcoin je digitálna kryptomena a platobný systém, ktorý vynašiel v roku 2008 Satoshi Nakamoto. Tento systém funguje na báze klient – klient a transakcie prebiehajú medzi užívateľmi priamo bez tretej strany. Tieto transakcie sú overované minermi a sú zaznamenávané do verejne distribuovanej účtovnej knihy s názvom blockchain. Bitcoin často nazývajú prvou kryptomenou aj keď podobné systémy už v minulosti fungovali. Preto je na mieste hovoriť skôr o prvej decentralizovanej digitálnej kryptomene. Bitcoin má najväčšiu tržnú kapitalizáciu spomedzi všetkých kryptomien.

Bitcoiny sa vytvárajú ako odmena za výpočtový výkon poskytnutý minermi. Tento výkon sa používa na overovanie transakcií a ich zápis do blockchainu. Táto činnosť sa nazýva ťažba a mineri sú odmeňovaní transakčnými poplatkami a novo vytvorenými bitcoinami.

Ako potenciálny miner som najprv vyčíslila vstupné náklady na nevyhnutné technické zariadenie, ktoré sú spolu 1 145.34 $. Dĺžku ťažby som stanovila na 168 dní. Cenu elektrickej energie som stanovila na 0.17 $ bez zmeny za sledované obdobie. V súčasnosti je ťažba zmysluplná jedine v tzv. poole (zoskupovanie minerov s cieľom zvýšiť spoločnú výpočtovú kapacitu a tým aj pravdepodobnosť vyťaženia bitcoinu). Vybrala som český Slush pool, kde poplatky činia 2% z vyťaženého obnosu. Pretože sa nedá presne namodelovať budúci vývoj náročnosti ťažby a už vôbec sa nedá predpokladať zmena výmenného kurzu $/BTC, ekonomickú efektívnosť tejto investície som spočítala v dvoch variantoch.
V prvom – pesimistickom variante som predpokladala vyšší percentuálny prírastok náročnosti (o 3% 2 krát za mesiac) a výmenný kurz 400.24 $. Tento kurz nie je kurzom aktuálnym, ale je to priemerná hodnota kurzu za posledný polrok. V pesimistickom variante už po mesiaci stojí spotrebovaná elektrická energia viac peňazí ako hodnota vyťažených bitcoinov a počiatočná investícia sa nesplatí nikdy. Za zvolené sledované obdobie by bol miner v strate – 1 464.58 $ a čím dlhšie by ťažil, tým viac v strate by bol. V druhom – optimistickom variante som predpokladala naopak nižší prírastok náročnosti (1% 2 krát za mesiac) a vyšší výmenný kurz v hodnote 500 $/BTC. Za sledované obdobie sa počiatočná investícia nesplatí rovnako ako v pesimistickom variante, ale hodnota vyťažených bitcoinov je väčšia ako cena za spotrebovanú

elektrickú energiu do 118 dňa ťažby. Za sledované obdobie by bol miner v strate – 1 260.96 $. Aj keby v oboch variantoch bola elektrická energia dostupná zadarmo, miner by bol stále v strate.

V oboch modelových prípadoch sa ťažba bitcoinov neoplatí. Z logiky veci vyplýva, že so zvyšujúcou sa náročnosťou ťažby klesá počet vyťažených bitcoinov, pretože ťažobné zariadenie svoju efektivitu nemení. V tomto momente už môže hrať úlohu aj doručovacia doba od termínu objednávky zariadení. Čím neskôr miner začne ťažiť, tým menej bitcoinov má šancu vyťažiť a hoci toto riziko sa nedá vyčísliť jedným číslom (závisí totiž na dĺžke oneskorenia) miner si tohto rizika musí byť vedomý a venovať dostatok času výberu overeného dodávateľa s kladnými hodnoteniami od ostatných zákazníkov.

Bitcoin často čelí obvineniam z vysokej spotreby elektrickej energie potrebnej na svoj chod, ale napriek tomu som nenašla žiadne relevantné výpočty a postupy, ktoré by tomu nasvedčovali. Preto som v druhej časti poslednej kapitoly približne stanovila súčasnú energetickú spotrebu celej bitcoin siete. Prvý parameter, ktorý do výpočtu vstupoval bol výpočtový výkon siete, ktorý je dostupný online. Druhým parametrom bola efektivita siete, ktorá sa nedá vyčísliť, pretože neexistuje žiadna databáza zariadení s danou efektivitou, ktoré sa v danom momente zapájajú do ťažby. Preto som pre výpočet namodelovala tri rôzne efektívne bitcoin siete (tzn. celá sieť má efektivitu ako jedno z troch typovo iných zariadení určených na ťažbu). Po prijatí týchto predpokladov som stanovila elektrickú spotrebu siete v rozmedzí medzi 400 MW až 1 500 MW za deň. Je to ekvivalent jednej menšej elektrárne a je to menej ako v priemere za deň spotrebovala Slovenská republika v roku 2014 (3 240 MW). Oproti číslam, ktoré som našla v rôznych starších článkoch a oproti starším predpovediam budúceho vývoja sú mnou spočítané údaje výrazne menšie. Napríklad dňa 16.12.2013 mala byť spotreba el. energie 131 020 MWh (cca 5 460 MW) čo je o 3 960 MW viac, ako mnou spočítaná horná hranica spotreby na začiatku roka 2016. V inom článku zas písali, že 12.4.2013 bola spotreba 982 MWh za deň tzn. že v rozmedzí 8 mesiacov sa podľa týchto údajov spotreba zmenila takmer o 130 000 MWh za deň. Tieto čísla spolu evidentne nekorešpondujú, čo je podľa môjho názoru spôsobené nepresnosťou týchto výpočtov vplyvom zavedenia zlých predpokladov týkajúcich sa efektivity zariadení zapojených do ťažby v tom čase. V týchto článkoch sa ďalej predpokladá neustály rast spotreby elektrickej energie v budúcnosti a dokonca aj štúdia z roku 2016 tvrdí, že spotreba do roku 2020 vystúpi na 14 GW. Pretože ani staršie predpovede nerátali s technickými pokrokmi (ASIC miner), ktoré výrazne ovplyvnili spotrebu, zostávam skeptická aj voči novým predpovediam do budúcnosti, pretože nikto nevie

čo budúcnosť prinesie. Možno blížiace sa zmenšenie odmeny minerov odradí od ťažby a prestanú túto el. energiu spotrebovávať alebo sa môže objaviť nové super efektívne zariadenie, ktoré bude mať znova významný vplyv na celkovú spotrebu.

Na záver práce ešte uvádzam tabuľku emisií skleníkových plynov v závislosti na efektivite siete. Okrem toho ešte uvádzam porovnanie rôznych nákladov na ťažbu bitcoinov, ťažbu zlata a na chod bankového systému, aby si čitateľ mohol porovnať ich výhodnosť sám. Len za rok sú priame ekonomické náklady na ťažbu a recykláciu zlata spolu 145 miliárd $, na tlač bankoviek a razenie mincí 28 miliárd $ a chod bankového systému je vyčíslený na 63.8 miliárd $. Oproti tomu sú náklady na ťažbu bitcoinov v hodnote 0.66 miliárd $ úplne zanedbateľnou čiastkou.

Aj keď som vďaka písaniu tejto práce narazila na obrovské množstvo problémov spojených s bitcoinom, stále verím, že bitcoin je jedinečný a vynikajúci projekt. Som presvedčená o nezmyselnosti a neudržateľnosti súčasného menového systému a bitcoin je podľa môjho názoru adekvátna náhrada. Napriek tomu, že mnohí tvrdia aký je bitcoin neekologický a extrémne drahý, tieto domnienky sa mi podarilo úspešne vyvrátiť a neostáva mi nič iné, ako popriať bitcoinu veľa užívateľov.

Conclusion

In this thesis I have analysed various aspects of the digital cryptocurrency called Bitcoin. The main object was to determine the profitability of mining in the current circumstances and the approximation of the electrical consumption of the Bitcoin network.

Bitcoin is a digital cryptocurrency and a payment system invented by Satoshi Nakamoto in 2008. The system is peer-to-peer and transactions take place between users directly, without any third party. These transactions are verified by miners and are recorded in a public distributed ledger called the blockchain. Bitcoin is often called the first cryptocurrency, although prior systems existed and it is more correctly described as the first decentralized digital currency. Bitcoin is the largest of its kind in terms of total market value.

Bitcoins are created as a reward for payment processing work, in which miners offer their computing power to verify and record payments into blockchain. This activity is called mining and miners are rewarded with transaction fees and newly created bitcoins.

As a potential miner, I first calculated the initial investment, which is $1 145.34 together. I set the duration of mining on 168 days. I set the electricity price on $0.17 without any change in the observed period. Nowadays, mining is meaningful only in the so-called pool (grouping of miners in order to increase the collective processing power and thus the probability of mining Bitcoin). I chose Czech Slush pool, where the fee is 2% of the mined amount. Because the accurate model of the future development of mining difficulty cannot be made and certainly no assumptions about the exchange rate $ / BTC can be made either, I calculated the economic efficiency of the investment in two scenarios. In the first pessimistic scenario, I assumed a higher percentage increase in difficulty (by 3% twice per month) and the exchange rate of $400.24. This exchange rate is not a current one, but the average exchange rate of the last six months. In this pessimistic scenario, consumed energy is worth more than the value of mined Bitcoins only after one month and the initial investment is never repaid. For the selected observing period the miner would be in a loss - $1 464.58 and the longer he would continue to mine the grater the loss would be. In the second optimistic scenario I assumed lower increase in difficulty (by 1% twice per month) and a higher exchange rate of 500 $/ BTC. The initial investment is not repaid within observed time period alike in pessimistic scenario but the value of mined Bitcoin is greater than the cost of consumed energy until the 118th day of mining. In

the observed period miner would be in a loss - $1 260.96. Even if the electricity was available for free, miner would still be in loss.

In both model scenarios, Bitcoin mining is not worth it. With increasing mining difficulty the amount of mined Bitcoin decreases logically since mining device does not change its effectiveness. In this moment, the duration of shipping time of ordered equipment can play a role. The later miner starts to mine, the less chance to mine a Bitcoin he has. Although this risk cannot be quantified by just one number (because it depends on the length of delay) miner has to be aware of this risk and must give himself sufficient time to select a certified supplier with positive ratings from other customers.

Bitcoin is often accused of large energy consumption needed for its maintenance but still I have not found any relevant method of calculations which would suggest that. That is why I dedicated last chapter in this paper to specifying current energy consumption of the entire Bitcoin network. The first parameter which entered my calculation was processing power of the network, which is available online. The second parameter was the efficiency of the network. This parameter cannot be quantified since there is no database containing mining equipment with its efficiency engaged in mining in that period of time. Therefore, I modelled three different effective Bitcoin network (i.e. whole network efficiency has the same efficiency as one of three different types of mining equipment) for this calculation. After adopting these assumptions, I calculated the network electrical consumption ranging between 400 MW to 1500 MW per day. This is an equivalent to one small power plant and it is less than the average daily consumption of the Slovak Republic in 2014 (3 240 MW). Compared to figures that I found in a variety of older articles and compared to previously predicted future trends my figures are significantly smaller. For example, on 16/12/2013 energy consumption should be 131 020 MWh (about 5 460 MW) which is about 3 960 MW more than upper limit of consumption in early 2016 I computed. Another article says that energy consumption on 12/4/2013 was 982 MWh per day, i.e. according to these data, energy consumption has changed almost by 130,000 MWh per day within eight month period. These numbers clearly do not correspond with each other. In my opinion, it is due to the uncertainty of these calculations caused by computing with bad assumptions made about the efficiency of facilities involved in mining at the time. These articles further expect continuous growth in electricity consumption in the future, and even study from 2016 says that consumption in 2020 will climb to 14 GW. Since even older predictions did not assume technical progress (ASIC miner), which effected energy consumption greatly, I remain sceptical to new predictions for the future, because no

one knows what the future holds. Perhaps the reduction of reward will discourage miners from mining and they will stop this energy usage or maybe someone will find new super-efficient equipment, which will affect energy consumption greatly again.

In the final part of this paper a table of greenhouse gas emissions depending on the efficiency is included. Emissions are depending on the efficiency of the network. I included comparison of different costs of mining bitcoin, gold mining and the banking system so that the reader can compare their advantages for himself. Direct economic costs per year of mining and recycling gold combined are $145 billion, printing of banknotes and minting coins costs $28 billion and the maintenance of the banking system is calculated into $63.8 billion. In contrast, the cost of Bitcoin mining is estimated at 0.66 billion, which is entirely negligible.

Even though I encountered a huge number of problems associated with Bitcoin while writing this thesis, I still believe that Bitcoin is a unique and outstanding project. I am convinced of the absurdity and the unsustainability of the current monetary system and in my view Bitcoin is an adequate replacement. Although many argue that Bitcoin is not ecological and extremely expensive, I was able to disprove these beliefs successfully. There is nothing else for me to say but to wish Bitcoin many users.

Zdroje

[1] *Česká mincovna AURUM* [online]. Dostupné z: http://www.cm-aurum.cz/zpravodajsky-servis-1103/zlaty-standard-a-konec-zlata-jako-meny_987/

[2] ĎURŠA, Miroslav. *Zlatý štandard a jeho potenciál pre nadchádzajúci menový systém*. 2012. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Ing. Pavel Žamberský, Ph.D.

[3] POLOUČEK, Stanislav. Peníze, banky, finanční trhy. Vyd. 1. Praha: C.H. Beck, 2009. xvii, 415. ISBN 978-80-7400-152-9. 47s.

[4] MARTENSON, Chriss. *Crash Course Chapter 7: Money Creation* [online]. 2012. Dostupné z: http://www.peakprosperity.com/crashcourse/chapter-7-money-creation

[5] BRADBURY, Danny. *Is Bitcoin a Digital Currency or a Virtual One?* [online]. 2014. Dostupné z: http://www.coindesk.com/bitcoin-digital-currency-virtual-one/

[6] LEE KUO CHUEN, David. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Singapore: Elsevier, 2015. ISBN 978-0-12-802117-0.

[7] SCHIRRIFF, Ken. *: Bitcoin mining the hard way: the algorithms, protocols, and bytes* [online]. Dostupné z: http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html

[8] GUTTMANN, Benjamin. *The Bitcoin Bible Gold Edition: Books On Demand*. 2014. ISBN 978-3732296965.

[9] KHALIQ, Azzief. *10 Best Bitcoin Wallets For Secure Bitcoin Storage* [online]. Dostupné z: http://www.hongkiat.com/blog/bitcoin-wallets/

[10] COMBS, Brett, MITSOFF, Tom. *Bitcoin decoded: Bitcoin Beginner´s Guide To Mining And The Strategies To Make Money With Cryptocurrencies*. Propellerhead Marketing Group LLC, 2014. 116 s. ISBN 978- 0615955247

[11] RENDLA, Michal. *Analýza digitální měny Bitcoin z hlediska investiční příležitosti*. 2014. Bakalářská práce. České vysoké učení technické v Praze. Vedoucí práce Mgr. Ing. Pavla Nikolovová M.A.

[12] *How do Bitcoin Transactions Work?* [online]. 2015. Dostupné z: http://www.coindesk.com/information/how-do-bitcoin-transactions-work/

[13] KELLEHER, John. *What Is Bitcoin Mining?* [online]. 2014. Dostupné z: http://www.forbes.com/sites/investopedia/2014/05/08/what-is-bitcoin-mining/

[14] *Bitcoinwiki* [online]. Dostupné z: https://en.bitcoin.it/wiki/Help:FAQ

[15] SCHIRRIFF, Ken. *Mining Bitcoin With Pencil And Paper*[online]. 2014. Dostupné z: http://gizmodo.com/mining-bitcoin-with-pencil-and-paper-1640353309

[16] *Bitcoinwisdom* [online]. Dostupné z: https://bitcoinwisdom.com/bitcoin/difficulty

[17] *Slushpool* [online]. Dostupné z: https://slushpool.com/home/

[18] *CoinDesk: How to Set Up a Bitcoin Miner* [online]. 2013.

[19] *BIP9 Implementation* [online]. 2013. Dostupné z: https://github.com/bitcoin/bitcoin/blob/master/src/miner.cpp

[20] TAYLOR, Michael Bedford. *Bitcoin and The Age of Bespoke Silicon*. University of California, San Diego, , 10. ISSN 978-1-4799-1400-5.

[21] MANKIW, Gregory N. *Zásady ekonomie*. GRADA, 1999. ISBN 978-80-7169-891-3.

[22] POPPER, Nathaniel. *Can Bitcoin Conquer Argentina?*[online]. 2015 . Dostupné z: http://www.nytimes.com/2015/05/03/magazine/how-bitcoin-is-disrupting-argentinas-economy.html?_r=1

[23] WALLACE, Benjamin. *The Rise and Fall of Bitcoin*[online]. 2011 Dostupné z: http://www.wired.com/2011/11/mf_bitcoin/

[24] *Everything You Need to Know About Bitcoin: VICE Podcast 027* [online]. 2014 Dostupné z: https://www.youtube.com/watch?v=SNssKmeXrGs

[25] *Poplatky Western Union v CZK* [online]. Dostupné z: http://www.intercash.cz/poplatky.asp

[26] *Platební terminál už nemusí být pro obchodníka trestem ovšem zadarmo to nejde* [online]. [cit. 2016-04-21]. Dostupné z: http://www.bankovnipoplatky.com/platebni-terminal-uz-nemusi-byt-pro-obchodnika-trestem-ovsem-zadarmo-to-nejde-21979

[27] SHUBBER, Kadhim. *Subway sandwich shop in Russia now accepting bitcoin payments* [online]. 2013. Dostupné z: http://www.coindesk.com/subway-sandwich-russia-bitcoin-payments/

[28] *Bitcoinwiki* [online]. Dostupné z: https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

[29] ROSENFELD, Meni. *Analysis of hashrate-based double-spending* [online]. 2012. Dostupné z: https://bitcoil.co.il/Doublespend.pdf

[30] MATONIS, Jon. *The Bitcoin Mining Arms Race: GHash.io and the 51% Issue* [online]. 2014 . Dostupné z: http://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue/

[31] Proof-of-work system. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné z: https://en.wikipedia.org/wiki/Proof-of-work_syste

[32] *Bitcoinwiki* [online]. . Dostupné z: https://en.bitcoin.it/wiki/Proof_of_Stake

[33] SZABO, Nick. *Bit gold* [online]. In: . 2008 . Dostupné z: http://unenumerated.blogspot.cz/2005/12/bit-gold.html

[34] *Litecoin Block Reward Halving Countdown* [online]. Dostupné z: http://litecoinblockhalf.com/

[35] KROLL, J.A., DAVEY, I.C., FELTEN, E.W., 2013. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In: Proceedings of WEIS (vol. 2013)

[36] *About Primecoin* [online]. Dostupné z: http://primecoin.io/about.php#what-xpm

[37] REN, L., 2014. Proof of stake velocity: building the social currency of the digital age. Self-published white paper

[38] RON, D., SHAMIR, A., 2013. Quantitative analysis of the full bitcoin transaction graph. In: Sadeghi, A.R. (Ed.), Lecture Notes in Computer Science: Financial Cryptography and Data Security, vol. 7859. Springer, Berlin, pp. 6-24

[39] SEWARD, Z.M., 2013. Yes, people are hoarding bitcoins. Quartz. Dostupné na adrese : https://qz.com/72118/yes-people-are-hording-bitcoins

[40] *FLUTERCOIN* [online]. Dostupné z: http://fluttercoin.us/

[41] *Bitcoinwiki: Proof of burn* [online]. Dostupné z: https://en.bitcoin.it/wiki/Proof_of_burn

[42] *Bitcoin Forum. CoinJoin: Bitcoin privacy for the real world* [online]. Dostupné z: https://bitcointalk.org/index.php?topic=279249.0

[43] *Know Your Meme* [online]. [cit. 2016-04-21]. Dostupné z: http://knowyourmeme.com/memes/doge

[44] *Bitcoin, Litecoin, Peercoin, Dogecoin Transactions chart* [online]. Dostupné z: https://bitinfocharts.com/comparison/transactions-btc-ltc-drc-ppc-doge.html

[45] Colored-Coins [online]. In: *GitHub* [online]. San Francisco (CA), 2008. Dostupné z: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Introduction

[46] Blockchain id [online]. In: *GitHub* [online]. San Francisco (CA), 2008. Dostupné z: https://github.com/blockstack/blockchain-id

[47] DEWEY, Joe, AMIAL, Shawn. *What is a Smart Contract?* [online]. 2015 . Dostupné z: https://bol.bna.com/what-is-a-smart-contract/

[48] DEWEY, Joe, AMUIAL, Shawn. *The Next Level: mart Contracts and Real Estate Deals* [online]. 2015. Dostupné z: https://bol.bna.com/what-is-a-smart-contract/

[49] Landauer's principle. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001. Dostupné z: https://en.wikipedia.org/wiki/Landauer%27s_principle

[50] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. Dostupné z: https://bitcoin.org/bitcoin.pdf

[51] O'DWYER, Karl J., MALONE, David. Bitcoin mining and its energy footprint. *Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET*[online]. Limerick: IET, , 6 [cit. 2016-04-23]. DOI: 10.1049/cp.2014.0699. Dostupné z: http://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf

[52] *How is difficulty calculated?* [online]. 2013 . Dostupné z: http://bitcoin.stackexchange.com/questions/5838/how-is-difficulty-calculated/5840#5840

[53] *Bitcoinwiki: Difficulty* [online]. Dostupné z: https://en.bitcoin.it/wiki/Difficulty

[54] *Bitmain* [online]. Dostupné z: [https://www.bitmaintech.com/productDetail.htm?pid=00020160129054250700R0OMI3KI061A]

[55] *Bitmain* [online]. [cit. 2016-04-23]. Dostupné z: https://bitmaintech.com/productDetail.htm?pid=00020150504074349691 7U7kGsCm0694

[56] *Bitcoin Forum: Visit of ASICMINER's Immersion Cooling Mining Facility* [online]. 2013. Dostupné z: https://bitcointalk.org/index.php?topic=346134.0

[57] WONG, Joon Ian. *CoinDesk: Cryptocurrency Miners Turn to Exotic Cooling Systems as Competition Heats Up* [online]. 2014 [cit. 2016-04-23]. Dostupné z: http://www.coindesk.com/cryptocurrency-miners-turn-exotic-cooling-systems-competition-heats/

[58] *Bitmain* [online]. Dostupné z: https://www.bitmaintech.com/productDetail.htm?pid=00020160105104607947aoAkWsJK06D0#tab-description

[59] *Cenový kalkulátor ERU* [online]. CYGNI SOFTWARE, a.s., 2016. Dostupné z: http://kalkulator.eru.cz/VstupniUdaje.aspx

[60] *Konverzná kalkulačka* [online]. Dostupné z: http://sk.coinmill.com/CZK_USD.html#CZK=4.156

[61] *Bitcoin Block Reward Halving Countdown* [online]. [cit. 2016-05-22]. Dostupné z: http://www.bitcoinblockhalf.com/

[62] *Currency Stats* [online]. Dostupné z: https://blockchain.info/stats

[63] *BTC/USD Historical Data* [online]. Dostupné z: http://www.investing.com/currencies/btc-usd-historical-data

[64] *Currency Stats: Bitcoin currency statistics* [online]. Luxembourg, 2011. Dostupné z: https://blockchain.info/stats

[65] CARNEY, Michael. *Bitcoin has a dark side: its carbon footprint* [online]. 2013. Dostupné z: https://pando.com/2013/12/16/bitcoin-has-a-dark-side-its-carbon-footprint/

[66] ROTHSTEIN, Adam. *How Much Electricity Does Bitcoin Use?* [online]. 2014 . Dostupné z: https://medium.com/@interdome/how-much-electricity-does-bitcoin-use-c350bd84c64e#.m3abvrnoa

[67] Electric energy consumption. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001. Dostupné z: https://en.wikipedia.org/wiki/Electric_energy_consumption

[68] GIMEIN, Mark. *Virtual Bitcoin Mining Is a Real-World Environmental Disaster* [online]. 2013. Dostupné z: http://www.bloomberg.com/news/articles/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster

[69] DEETMAN, Sebastiaan. *Bitcoin Could Consume as Much Electricity as Denmark by 2020*[online]. 2016 [cit. 2016-05-03]. Dostupné z: http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020

[70] *Správa o výsledkoch monitorovania bezpečnosti dodávok elektriny (2015)* [online]. Ministerstvo hospodárstva Slovenskej Republiky. Dostupné z: http://www.economy.gov.sk/spravy-o-vysledkoch-monitorovania-bezpecnosti-dodavok-elektriny-a-plynu-5851/127536s

[71] MCCOOK, Hass. *An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network: A critical assessment of the Bitcoin mining industry, gold production industry, the legacy banking system, and the production of physical currency* [online]. 2014, , 37. Dostupné z: https://www.scribd.com/doc/228253109/The-Relative-Sustainability-of-the-Bitcoin-Network-by-Hass-McCook

[72] AHLERS, C., MARTIN, M., OLSEN, Ben, P. O. & Jr., M. S., 2010. How Green is Our Green? Sustainability Assessment of U.S. and Australian Currency, Vermont: University of Vermont.

Zdroje obrázkov

Obrázok 1: Britská zlatá minca z roku 1717, Česká mincovna AURUM [online]. Dostupné z: http://www.cm-aurum.cz/zpravodajsky-servis-1103/zlaty-standard-a-konec-zlata-jako-meny_987/

Obrázok 2: Bankovný systém čiastočných rezerv alebo ako sa z 1000$ stane vďaka bankám až 10 000$, MARTENSON, Chriss. *Crash Course Chapter 7: Money Creation* [online]. 2012. Dostupné z: http://www.peakprosperity.com/crashcourse/chapter-7-money-creation

Obrázok 3: Operácie na otvorenom trhu při kúpe štátneho dlhopisu (US Congress - vláda USA, US Treasury – ministerstvo financií, Bonds – dlhopisy, Federal Reserve alebo FED – centrálna banka USA, Big Banks – veľké banky), MARTENSON, Chriss. *Crash Course Chapter 7: Money Creation* [online]. 2012. Dostupné z: http://www.peakprosperity.com/crashcourse/chapter-7-money-creation

Obrázok 5: Porovnanie náročnosti ťažby a aktuálnym hash rateom siete, Bitcoinwisdom [online]. Dostupné z: https://bitcoinwisdom.com/bitcoin/difficulty

Obrázok 6: Porovnanie času potrebného na vygenerovanie bloku a náročnosti ťažby v čase, Bitcoinwisdom [online]. Dostupné z: https://bitcoinwisdom.com/bitcoin/difficulty

Obrázok 7: Rozdelenie výpočtového výkonu medzi jednotlivé mining pooly v percentách ku dňu 11.02.2016, Blockchain [online]. Dostupné z: https://blockchain.info/pools?timespan=24hours

Obrázok 8: Vľavo je USB ASIC miner (330 MH/s) a vpravo je klasický ASIC miner (10,7 GH/s za 475$), Amazon [online]. Dostupné z: [http://www.amazon.com/ASICMiner-Block-Erupter-USB-Sapphire/dp/B00CUJT7TO], Bitcoinrigs [online]. Dostupné z: [http://www.bitcoinrigs.org/product/asicminer-blade-v2-10-7ghs/#prettyPhoto]

Obrázok 9: Bitcoin v Subway - Pri platení bitcoinom zľava 10%, SHUBBER, Kadhim. Subway sandwich shop in Russia now accepting bitcoin payments [online]. 2013. Dostupné z: http://www.coindesk.com/subway-sandwich-russia-bitcoin-payments/

Obrázok 11: Asic miner typu AntMiner S7 BATCH 10, Bitmain: ANTMINER S7 BATCH 10 - Shipped out from Feb. 16~20 [online]. Dostupné z: https://www.bitmaintech.com/productDetail.htm?pid=00020160129054250700R0OMI3KI061A

Obrázok 12: Power supply unit APW3-12-1600-B2, Bitmain: APW3-12-1600-B2 [online]. Dostupné z: https://www.bitmaintech.com/productDetail.htm?pid=00020160129054250700R0OMI3KI061A

Obrázok 13: Využitie imersného chladenia pri ťažbe bitcoinov, Bitcoin Forum: Visit of ASICMINER's Immersion Cooling Mining Facility [online]. 2013. Dostupné z: https://bitcointalk.org/index.php?topic=346134.0

Obrázok 14: Ventilátor na chladnenie typ fan for Antminer S3, S5, S5+, S7, Bitmain: fan for Antminer S3, S5, S5+, S7 [online]. Dostupné z: https://www.bitmaintech.com/productDetail.htm?pid=00020160129054250700R0OMI3KI061A

Zdroje grafov

Graf 1: Výška transakčných poplatkov od vzniku bitcoinu. Dáta odvodené z: https://blockchain.info/charts/transaction-fees?showDataPoints=true&timespan=all&show_header=true&daysAverageString=1&scale=0&format=csv&address=

Graf 2: Množstvo bitcoinov v obehu. Dáta odvodené z: https://blockchain.info/charts/total-

bitcoins?showDataPoints=false&timespan=all&show_header=true&daysAverageString=1&scale=0&format=csv&address=

Graf 3: Počet transakcií v bitcoinoch za deň od jeho vzniku v júni 2009 až po súčasnosť. Dáta odvodené z: https://blockchain.info/charts/n-transactions?showDataPoints=false&timespan=all&show_header=true&daysAverageString=1&scale=0&format=csv&address=

Graf 4: Volatilita dennej zmeny kurzu vzhľadom k americkému doláru. LEE KUO CHUEN, David. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Singapore: Elsevier, 2015. ISBN 978-0-12-802117-0.

Graf 5: Výpočtová kapacita (hash rate) siete za posledné 2 roky. Dáta odvodené z: [https://blockchain.info/charts/hash-rate?timespan=2year&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=]

Graf 6: Výmenný kurz USD/BTC. Dáta odvodené z: https://blockchain.info/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

Zdroje tabuliek

Tabuľka 2: História náročnosti ťažby a hash ratu siete, Dostupné z: https://bitcoinwisdom.com/bitcoin/difficulty

Tabuľka 3: Množstvo vyťažených blokov pre rôzne mining pooly, Dostupné z : https://bitcoinchain.com/pools

Tabuľka 4: Porovnanie zariadení určených na ťažbu v roku 2016, Dostupné z: https://en.bitcoin.it/wiki/Mining_hardware_comparison

https://www.scribd.com/doc/228253109/The-Relative-Sustainability-of-the-Bitcoin-Network-by-Hass-McCook

Tabuľka 15: Porovnanie socioekonomických ročných nákladov, MCCOOK, Hass. *An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network: A critical assessment of the Bitcoin mining industry, gold production industry, the legacy banking system, and the production of physical currency* [online]. 2014, 37. Dostupné z: https://www.scribd.com/doc/228253109/The-Relative-Sustainability-of-the-Bitcoin-Network-by-Hass-McCook