UNIVERZITA PALACKÉHO V OLOMOUCI

FILOZOFICKÁ FAKULTA

Virtuální měna bitcoin a její budoucnost

Bakalářská práce

Autor: Lucie Habánová

Vedoucí práce: Ing. Zdeněk Puchinger

Olomouc 2016

Prohlášení

Místopřísežně prohlašuji, že jsem bakalářskou práci na téma: „Virtuální měna bitcoin a její budoucnost“ vypracovala samostatně pod odborným dohledem vedoucího diplomové práce a uvedla jsem všechny použité podklady a literaturu.

V Olomouci dne …….. Podpis ……

Obsah

Úvod

Tato bakalářská práce si bere za předmět zpracování téma virtuální měny bitcoinu a jeho budoucnost.

Zpočátku si vysvětlíme principy fungování celého Bitcoin systému, doprovázené vymezením základních pojmů, jejichž pochopení je klíčové pro pochopení celého Bitcoin systému. Zároveň si představíme tvůrce celého systému, přestože jeho identita zůstává až k dnešnímu dni stále skryta, navzdory tomu, že po něm neustále mnozí pátrají. Dále provedeme výčet způsobů nabytí bitcoinů z pohledu uživatele nováčka.

V další kapitole se budeme věnovat srovnání bitcoinu s vybranými měnami, a sice eurem a americkým dolarem. Začneme od pojmu peníze a jejich funkcí a posléze se přesuneme k definici měny a jejím znakům. Srovnáme bitcoin a vybrané měny, zaměříme se na to, zda naplňují zmíněné funkce a znaky, a zda jsou srovnatelné. Zároveň pohlédneme na bitcoin jako na komoditu, abychom zjistili, zda je příhodnější brát jej jako měnu či komoditu.

Následně se budeme věnovat kurzu bitcoinu a jeho vývoji od samotného počátku existence bitcoinu až do současnosti. Zjistíme, zda má spíše stabilní či volatilní vývoj kurzu, a co takový kurz v případě decentralizované, deflační kryptoměny ovlivňuje.

V závěru zhodnotíme, zda má Bitcoin systém v budoucnu své místo na trhu. A zda poslouží jako podnět pro další projekty podobného typu.

1. Fungování Bitcoin systému a vymezení základních pojmů

Počátek celého Bitcoin systému, kterému se budu věnovat ve své bakalářské práci, leží v rukou neznámé osoby či skupiny lidí skrývající se pod pseudonymem Satoshi Nakamoto. Už samotný fakt, že není možné odhalit Nakamotovu identitu je lehce zavádějící, avšak jemu se budeme věnovat až v další podkapitole. Nyní si vysvětlíme, co je to Bitcoin systém a jak funguje.

Byl pátek, 31. října 2008, kdy Satoshi Nakamoto publikoval soubor s názvem „Bitcoin P2P e-cash paper". A sám jej popsal jako nový systém elektronické měny, fungující zcela na *peer-to-peer* bázi, bez existující třetí strany. Tento soubor publikoval na stránce Metzdowd.com, která je sídlem nadšenců do kryptografie a matematických a technických expertů.[1] Následně pak byl Nakamoto otevřený veškerým doplňujícím otázkám ohledně fungování tohoto systému, a až ve čtvrtek, 8. ledna 2009 oznámil spuštění systému Bitcoin. Systému elektronické měny, který užívá peer-to-peer síť, aby zabránila dvojitému užití stejného bitcoinu jedním uživatelem, a který je zcela decentralizovaný.[2]

Teď si vymezíme základní pojmy spojené s Bitcoin systémem, aby následné vysvětlení jeho fungování bylo přehlednější.

- *Peer-to-peer* – Síť fungující na vzájemné komunikaci připojených uživatelů, kde si uživatelé vyměňují informace přímo mezi sebou bez připojení k jakémukoli serveru.[3]
- *Block chain* – Všem uživatelům dostupný, chronologicky seřazený záznam o veškerých transakcích. Nezaznamenává však jména uživatelů, ale adresy jejich *digital wallets.* Je spravován jednotlivými zapojenými uživateli do Bitcoin systému a činí systém transparentním.[4]

[1] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money*. Triumph Books. S. 5.
[2] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 15–16.
[3] *Bezpecne-online.cz*. [online]. Cit. 10. 3. 2016. Dostupné z: http://www.bezpecne-online.cz/surfuj-bezpecne/sosani-a-sdileni-dat/peer-to-peer-site-jak-funguji-a-kde-je-problem.html.
[4] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money*. Triumph Books. S. 31.

- *Block* – Soubor ověřených transakcí, potvrzených uživateli systému a zařazených chronologicky do *block chainu.*[5]
- *Hash/hashing* (hašovací funkce) – Jedná se o převod dat o různé velikosti do kódu a do *blocku* o předem určené velikosti. Ten pak představuje otisk původních dat.[6] V případě změny vstupní informace, dojde ke změně samotného kódu[7].
- *Mining* (dolování) – Cílem počítače je vytvořit *block*, který obsahuje nejnovější transakce a přidělit jim *hash*, který je bude všechny reprezentovat. Zároveň tento *block* musí mít časové označení a to co nejaktuálnější a musí navazovat na předchozí *block*. Následně musí ostatní uživatelé uznat, že *block* splňuje dané podmínky a je platný. Potom je *miner* odměněn v bitcoinech.[8]
- *Digital wallet* (bitcoinová peněženka) – Online způsob uchování uživatelova *public* a *private key*. Má podobu softwaru.[9]
- *Cold storage* – Offline způsob uchování uživatelova *public* a *private key*. Např. na USB klíči, hard disku nebo napsané na papíře.[10]
- *Private key* (heslo pro odchozí platby) – Umožňuje uživateli provádět transakce ze své adresy na adresu jiného uživatele. Tedy umožňuje uživateli přístup k jeho bitcoinům uloženým v *digital wallet*.[11]
- *Public key* (bitcoinová adresa) – Umožňuje uživateli přijímat transakce. Jde o údaj srovnatelný s číslem bankovního účtu.[12]
- BTC – kód měny Bitcoin systému

Celý Bitcoin systém není nekonečný. Omezuje se na množství 21 000 000 BTC, které je možné vytěžit. Vzhledem k tomu, že bitcoiny jsou dolovány řešením matematických

[5] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money*. Triumph Books. S. 32.
[6] (2013). *Wikisofia.* [online]. Cit. 6. 3. 2016. Dostupné z: https://wikisofia.cz/wiki/Bitcoin.
[7] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money*. Triumph Books. S. 40–41.
[8] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money*. Triumph Books. S. 40–44.
[9] KHALIQ, Azzief (2014). *Hongkiat Technology Design Inspiration*. [online]. Cit. 10. 3. 2016. Dostupné z: http://www.hongkiat.com/blog/bitcoin-wallets/.
[10] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money*. Triumph Books. S. 36.
[11] KHALIQ, Azzief (2014). *Hongkiat Technology Design Inspiration*. [online]. Cit. 10. 3. 2016. Dostupné z: http://www.hongkiat.com/blog/bitcoin-wallets/.
[12] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money*. Triumph Books. S. 35.

úkolů, které se s každým dalším získaným bitcoinem ztěžují, lze předpovědět, že poslední bitcoin bude vytěžen až v roce 2140.[13] Velmi podstatné je zmínit, že procesem dolování je shromažďování nejnovějších transakcí do *blocku,* a zároveň ověřování jejich platnosti a správnosti. Především z důvodu hlídání toho, nebyl-li např.: 1 BTC při transakci vykonané jedním uživatelem užit dvakrát. Pak už jen stačí, aby uživatelem vytvořený *block* byl zkontrolován a schválen ostatními uživateli a následně je zařazen do *block chainu*. V současné době, podaří-li se uživateli vyřešit, čí tedy spíše jeho počítači, matematický úkol a vytvořit *block* splňující veškeré podmínky, získá za jeho vyřešení 25 BTC.[14] V roce 2017 tato odměna klesne na pouhých 12.5 BTC.[15]

Bitcoin systém byl zřejmě vytvořený jako odezva na Světovou finanční krizi, která započala odhalením selhání amerických bank v oblasti poskytování hypotečních úvěrů. Jako protipól vytvořil Nakamoto systém, který je zcela v rukou uživatelů a není v něm žádné třetí strany, která by jakkoli zasahovala do průběhu transakcí, tedy nic na úrovni obchodních ani centrálních bank. Touto absencí regulace vytvořil prostředí, ve kterém nemůže dojít k inflaci, jelikož není třetí strana, která by měla moc rozhodovat o chodu vývoje hodnoty bitcoinu a nějakými nástroji do něj zasahovat.

Z pohledu uživatele je třeba vysvětlit pojem vlastnění bitcoinu. Jelikož bitcoin je virtuální měnou, nebo též kryptoměnou, která nemá fyzickou formu.

Pojem kryptoměna značí, že se jedná o měnu chráněnou silnou kryptografií neboli šifrováním. Přesněji jde o šifrování SHA256 a ECDSA, které šifruje digitální podpisy všech transakcí.[16]

Jak už jsme zmínili, neexistuje nic jako mince či bankovka, kterou by bylo možné označit jako bitcoin. Jediné, co existuje, jsou bitcoinové adresy a záznamy příjmů a výdajů. Žádný uživatel nemůže ukázat na úsek kódu a říci: „Zde je můj bitcoin.“.

---

[13] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 29.
[14] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 40–44.
[15] FORRESTER, Daniel & SOLOMON, Mark (2014). *Bitcoin Explained: Today´s Complete Guide to Tomorrow´s Currency.* CreateSpace Independent Publishing Platform. S. 58.
[16] HRACH, Jan (2011). *ABC Linuxu – Decentralizovaná kryptoměna bitcoin*. [online]. Cit. 11. 3. 2016. Dostupné z: http://www.abclinuxu.cz/clanky/decentralizovana-kryptomena-bitcoin.

Public key nebo také adresa bitcoinu se jen odkazuje na databázi všech transací, tedy *block chain*, kde leží informace o všech transakcích. A je-li v celém *block chainu* dvakrát zmíněna bitcoinová adresa jednoho uživatele, přičemž první zmínka tvrdí, že obdržel 2 BTC a druhá, že obdržel 3 BTC, potom je uživatel majitelem celkem 5 BTC. Tento systém zároveň zabraňuje padělání bitcoinů. Nebude-li totiž v *block chainu* všemi ověřená a schválená informace o tom, že daný uživatel obdržel bitcoin, pak nikdy nemůžete být jeho majitelem. Sám tvůrce Bitcoin systému, Satoshi Nakamoto, definoval bitcoin jako řetězec digitálních podpisů[17]. A došlo-li by ke zmizení celého *block chainu* a samotné sítě, žádný z uživatelů nevlastní nic a Bitcoin systém přestane zcela existovat.[18]

Uživatel nemusí být vždy majitelem celého bitcoinu. Jako každou jinou měnu, lze 1 BTC rozdělit na menší části, a to až do jednotky zvané satoshi, která je s úctou k tvůrci Bitcoin systému pojmenovaná po samotném Satoshim Nakamotovi.[19] Níže uvádíme tabulku s názvy různých jednotek měny.

1 BTC	bitcoin
0.01 BTC	bitcent
0.001 BTC	mbit (vyslovováno: em-bit)
0.000 001 BTC	ubit (vyslovováno: yu-bit)
0.000 000 01 BTC	satoshi

Obr. 1 Dělení měny
Zdroj: PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 30.

[17] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 39.
[18] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 38.
[19] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 30.

1.1. Tvůrce Bitcoin systému

Jak už bylo v předchozím textu zmíněno, tak zakladatelem celého Bitcoin systém je osoba či skupina osob známá pod pseudonymem Satoshi Nakamoto. Tímto jménem byla zveřejněna první zmínka o systému Bitcoin v roce 2008, a zároveň bylo tímto jménem odpovídáno na otázky ohledně celého systému, než byl 8. ledna 2009 spuštěn. Řada lidí se následně pokoušel odkrýt Nakamotovu totožnost nebo alespoň národnost. Patřili mezi ně i deník *The New Yorker* a *Fast Company*. Avšak nikdo neuspěl, dodnes zůstává zakladatel Bitcoin systému skryt veřejnosti.[20]

Existují i spekulace, že jde o skupinový projekt firem vyrábějících elektronická zařízení, **Sa**msung, **Toshi**ba, **Naka**michi a **Moto**rola.[21]

Jediný, kdo měl alespoň nepatrný úspěch ve spojitosti s pátráním po Nakamotovi, byl programátor Sergio Demian Lerner. Jemu se podařilo odhalit, že Nakamoto si v raných začátcích Bitcoin systému vydoloval přibližně 1 milion BTC, které v dnešní době mají několikanásobně vyšší hodnotu. Výsledky Lernerova pátrání potvrdili i experti z deníku *The Verge*. Zároveň se jim podařilo zjistit, že z celého 1 milionu BTC, které Nakamoto vydoloval v roce 2009, utratil do roku 2013 pouhých 500 BTC.[22] Ovšem tohle je jediná stopa, která nám po existenci Satoshiho Nakamota zbyla.

Dnes už je Nakamoto od celého systému odcizen, jelikož v dubnu roku 2011, předal celé jeho spravování programátorovi a nadšenci Gavinu Andresenovi. Ten Nakamota kontaktoval již v polovině rou 2010. Nabídl mu své znalosti z oblasti C++ programování a také mu nabídl pomoc se zdokonalením platebního softwaru. To vše jen proto, že ho celý systém nadchnul a chtěl dobrovolně přispět k jeho zdokonalování. Samozřejmě nebyl jediný, kdo se nabídl, že pomůže s jeho údržbou a zdokonalováním, avšak právě jemu svěřil samotný Nakamoto jeho spravování a o sobě prohlásil, že se bude věnovat něčemu jinému. Tím jejich spojení, které mezi sebou měli, výhradně ve formě emailů, skončilo a Andresen se spolu s dalšími dobrovolnými nadšenci stará o Bitcoin systém

[20] GUTTMANN, Benjamin (2013). *The Bitcoin Bible.* Books on Demand. S. 240.
[21] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 25.
[22] GUTTMANN, Benjamin (2013). *The Bitcoin Bible.* Books on Demand. S. 240–241.

dodnes.[23] Mezi jeho nejbližší kolegy, kteří dohromady tvoří skupinu hlavních vývojářů, patří např.: Peter Wuille, Nils Schneider, Jeff Garzik, Wladimir J. van der Laan a Gregory Maxwell.[24]

1.2. Nabytí bitcoinů

Způsoby jakým se běžný uživatel a příznivec Bitcoin systému může stát vlastníkem nějakého bitcoinu jsou dva, i když by se našel i třetí, o kterém si také povíme. Obecně však pro bezúhonného člověka existují jen dvě možnosti, jak se stát majitelem bitcoinu. Jedná se buď o dolování, nebo o nákup.

- Mining (dolování) – Jakýkoliv člověk si může zcela bezplatně vytvořit bitcoinovou peněženku, a to klidně více než jen jednu, a stát se majitelem *public* a *private key,* neboli bitcoinové adresy a hesla pro odesílání plateb. Tímto se zařadí do Bitcoin systému. Následně se může pokusit o samotné dolování. To se však v čase s postupně vydolovanými bitcoiny neustále ztěžuje. Přibližně jednou za 14 dní (nebo po zařazení 2016 *blocků* do *block chainu*) vzroste obtížnost matematických úkolů, které je třeba vyřešit pro zařazení dalšího *blocku* do *block chainu*.[25] Což má za následek potřebu výkonnějšího hardwaru, s co nejnižšími pořizovacími náklady, abyste předstihli ostatní uživatele v dolování. V dnešní době se tak jedná o skutečně velkou investici, jelikož existují centra, která se na dolování specializují a mají vybavení, které je pro běžného uživatele takřka finančně nedostupné. Trvá-li přece jen někdo na tom, že se o dolování pokusí, či se na něm chce alespoň podílet, má následující dvě možnosti:
    - Koupit či vytvořit si vlastní dolovací stanici. Zároveň musí vzít v úvahu, fakt že takováto stanice je energeticky velmi náročná, tudíž jeho spotřeba elektřiny významně vzroste. Taková stanice zahrnuje ideálně

[23] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 21–22.
[24] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 144.
[25] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 33.

několik grafických karet, které urychlí činnost zařízení a kvalitní procesor.[26]

- Přidat se k *mining group*. Což je skupina uživatelů, která se na dolování podílí, a v případě, že se jí podaří zařadit další *block* do *block chainu*, následná odměna je rozdělena mezi všechny členy *mining group*.[27]

- Nákup bitcoinu (směna) – Patrně nejjednodušší způsob, jak se nováček a zájemce o Bitcoin systém může stát majitelem nějakého bitcoinu. Jediné, co pro to musí udělat, je, že si založí bitcoinovou peněženku a potom má tři možnosti.
  - Směnit daný obnos na bitcoiny pomocí bitcoinových automatů. V České republice jich máme hned několik, avšak pouze ve větších městech, jako: Praha, Plzeň, Brno a Ostrava. Některé tyto automaty jsou dokonce obousměrné a lze v nich bitcoiny prodat. Mají své výhody i nevýhody. Mezi nevýhody patří fakt, že mají o trochu vyšší směnný kurz. Výhodou je fakt, že si můžete v automatu vytvořit bitcoinovou peněženku, nejste-li už jejím majitelem a následně si můžete nechat směněné bitcoiny do ní zaslat. Navíc bitcoinové automaty v České republice nevyžadují ověření totožnosti, jak tomu je u některých zahraničních automatů, zda je tento fakt výhodou či nevýhodou této služby je na uvážení každého z nás.[28]
  - Provést směnu na online směnárnách. V České republice je řada online směnáren, liší se pouze nabízenými kurzy. Můžeme uvést např.: First-bitcoin.cz, Coinhub.cz nebo SimpleCoin.cz.[29]

    Nebo pomocí zahraničních směnáren, mezi největší na celém bitcoinovém trhu patří: Mt. Gox, CryptoXchange a Intersango.[30]

---

[26] FORRESTER, Daniel & SOLOMON, Mark (2014). *Bitcoin Explained: Today´s Complete Guide to Tomorrow´s Currency.* CreateSpace Independent Publishing Platform. S. 60–62.
[27] FORRESTER, Daniel & SOLOMON, Mark (2014). *Bitcoin Explained: Today´s Complete Guide to Tomorrow´s Currency.* CreateSpace Independent Publishing Platform. S. 62.
[28] FILLNER, Karel (2015). *Btctip.cz.* [online]. Cit. 13. 3. 2016. Dostupné z: http://btctip.cz/jak-vyhodne-koupit-a-prodat-bitcoiny/.
[29] FILLNER, Karel (2015). *Btctip.cz.* [online]. Cit. 13. 3. 2016. Dostupné z: http://btctip.cz/jak-vyhodne-koupit-a-prodat-bitcoiny/.

- Využít jedinou bitcoinovou burzu v celé České republice, a sice BitStock. Je na ní možno obchodovat za koruny. Její výhodou je fakt, že převod bitcoinů probíhá přímo mezi uživateli, tudíž nemůže dojít k odcizení bitcoinů během transakce, a také samotná burza nemůže být vykradena hackerem, jelikož nemá žádné bitcoiny v držení.

  Nebo lze využít zahraniční bitcoinovou burzu, kterých je na trhu mnoho. Např.: Bitstamp, BTC-e, Kraken.com, atd.[31]

- Krádež/vydírání – Bohužel i toto je způsob, jak si přivlastnit bitcoiny. Jelikož je ve svém základu celý Bitcoin systém anonymní. Jediné, co je všem uživatelům přístupné jsou bitcoinové adresy, které dokládají transakce uskutečněné s bitcoiny. Kdokoli si může založit bitcoinovou peněženku, a dokonce více než jednu, a k jejímu založení není třeba žádného jména, adresy, telefonního čísla tedy není třeba žádné identifikace. Jedná se o aplikaci, software, který si stáhnete do zařízení a ten vám sám, automaticky vygeneruje první bitcoinovou adresu, pro možnost přijímání bitcoinů[32]. Bitcoinová peněženka vám může vygenerovat těchto adres nekonečně mnoho, jelikož jejich množství je díky jejich složitosti a rozsahu neomezené.

  Zde je příklad bitcoinové adresy: iHcZyBdd53zbtoAUvUGSwiYaqTCLEA4079.[33]

  Zároveň vám bitcoinová peněženka udá vaše heslo, které slouží pro odesílání bitcoinů a je velmi důležité, abyste tuto informaci dobře střežili. Potom už záleží na každém z nás, do jaké míry má zabezpečený počítač a dovede se bránit před napadením hackerem.

---

[30] GUTTMANN, Benjamin (2013). *The Bitcoin Bible.* Books on Demand. S. 65.
[31] FILLNER, Karel (2015). *Btctip.cz.* [online]. Cit. 13. 3. 2016. Dostupné z: http://btctip.cz/jak-vyhodne-koupit-a-prodat-bitcoiny/.
[32] FILLNER, Karel (2015). *Btctip.cz.* [online]. Cit. 13. 3. 2016. Dostupné z: http://btctip.cz/jak-vyhodne-koupit-a-prodat-bitcoiny/.
[33] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 35.

Jak už bylo zmíněno dříve, existují dva typy uložení bitcoinů. Online a offline. Obecně platí, že nejlepší a nejbezpečnější je kombinace těchto dvou možností. Tedy mít především vaše heslo pro odchozí platby uložené offline způsobem, mimo dosah internetu a i mimo počítač. Buď na externím záložním disku či napsaný na papíře, avšak v žádném případě si nepořizujte fotografii tohoto papíru, potom by se opět jednalo o online uložení.[34]

[34] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 37.

2. Srovnání bitcoinu s vybranými měnami – euro, americký dolar

Celý Bitcoin systém a jeho hlavní myšlenka tkví v tom, že se jedná o digitální, decentralizovanou, deflační kryptoměnu, bez jakéhokoli krytí a bez fyzické existence[35]. Má stanovené množství oběživa, které není možné změnit a už vůbec ne navýšit, a zároveň nepodléhá žádné regulaci třetí stranou. Je však vůbec možné nazývat bitcoin měnou a srovnávat jej se zavedenými měnami, které podléhají zcela jiným pravidlům?

Měna je definována jako národní forma peněz, respektive dohodnutá integrační nadnárodní forma peněz a je pojmem užším než pojem peníze[36]. Proto budeme postupovat sestupně a podíváme se nejdříve na pojem peníze a jejich funkce.

Peníze jsou specifický druh zboží. Stejně tak je to jakékoli aktivum, které je všeobecně přijímáno při placení za zboží a služby či při úhradě dluhu, a zároveň u něj lidé věří, že bude přijímáno jinými lidmi při vykonávání platby.[37]

Dále se pak v průběhu let vyvinuly základní funkce peněz, které se odvíjí od jejich definice a doplňují ji. Funkce peněz jsou následující.

- Prostředek směny – Tato funkce navazuje na fakt, že peníze jsou aktivem, které je všeobecně přijímáno. Ať už jde o úhradu zboží, služby či dluhu, musí jít o všemi přijímaný prostředek směny. Jejich forma se během let vyvinula na základě potřeb trhu a to v bankovky a mince o různých nominálních hodnotách, čímž se výrazně snížily transakční náklady – náklady vynaložené na čas strávený úsilím uskutečnit směnu jednotlivých zboží nebo služeb.[38]
- Účetní jednotka – Peníze vyjadřují ceny všech ostatních aktiv. Tato funkce opět trochu navazuje na funkci předchozí. Bez existence peněz, by byla realizace směny nesmírně náročným úkolem a směna třech výrobků by vyžadovala mnoho času pro nalezení ekvivalentní hodnoty pro realizaci směny. S existencí peněz máme jedno aktivum, které vyjadřuje hodnotu zboží a služeb.[39]

[35] KUBIIN (2013). *Svět Bitcoinu*. [online]. Cit. 15. 3. 2016. Dostupné z: http://bitcoin.kubiin.net.
[36] ČERNOHORSKÝ, Jan, TEPLÝ, Petr (2011). *Základy financí.* Praha: Grada. S. 29.
[37] REVENDA, Zbyněk (2011). *Centrální bankovnictví.* Praha: Management Press. S. 60.
[38] REVENDA, Zbyněk (2011). *Centrální bankovnictví.* Praha: Management Press. S. 60.
[39] REVENDA, Zbyněk (2011). *Centrální bankovnictví.* Praha: Management Press. S. 61.

- Uchovatel hodnot – Peníze je možné střádat a držet jako formu majetku. V této funkci vystupují jako součást celkového bohatství každého člověka. Avšak daná míra bohatství přímo závisí na vývoji ekonomiky a na stabilitě kupní síly peněz. Která představuje množství zboží a služeb, které může člověk v různém čase, při daných cenách získat na trhu. Z toho vyplývá, že blíží-li se období růstu cenové hladiny, tedy růst cen zboží a služeb, oslabí to kupní sílu uspořených peněz a jejich držbou po toto období dojde k jejich znehodnocování. I přesto, že inflace úspory znehodnocuje, představují peníze nejlikvidnější způsob držení aktiv. Rozdíl je mezi stupněm likvidity hotovosti a peněz uložených v bance, stále však platí, že je to nejrychlejší způsob jak dostát včas svým splatným závazkům.[40]

Funkce peněz jsme si představili. Není pochyb o tom, že jako euro tak americký dolar všechny tři funkce splňují. Jsou přijímány jako prostředek směny, jsou v nich vyjadřovány ceny zboží a služeb a plní i funkci uchovatele hodnoty.

Nyní se podíváme, zda bitcoin splňuje základní funkce peněz. Bitcoin umožňuje uživatelům platit za zboží a služby. Avšak je tomu tak pouze na některých místech. Vztáhneme-li první funkci jen na Českou republiku. Bude člověk, který chce platit pouze bitcoiny odkázán jen obchodníky přijímající platbu v bitcoinech. Jejich kamenné obchody bývají označené tímto symbolem.

Obr. 2 Označení kamenných obchodů
Zdroj: SINGHA. *Bitcoin – česká grafika*. [online]. Cit. 15. 3. 2016. Dostupné z: http://bitcoin.singha.cz/ceska-grafika.

Je pravdou, že během let se seznam obchodníků, kteří přijímají bitcoiny rozrostl. Dnes je možné nakoupit různé zboží a služby u obchodníků. Největší koncentrace těch, kteří na území České republiky přijímají bitcoiny je v Praze (38 firem), Ostravě (4 firmy)

[40] REVENDA, Zbyněk (2011). *Centrální bankovnictví.* Praha: Management Press. S. 61.

a Brně (4 firmy)[41]. Dostupné je zboží jako: oblečení, elektronika, káva, čaje, víno, umělecká keramika, atd. A ze služeb jde třeba o: kadeřnictví, hodinový manžel, 3D tisk a skenování, fotografování, kurz na výuku psaní všemi deseti, servis PC, atd.

V zahraničí je pak seznam zboží a služeb, které lze pořídit za bitcoiny delší. Tedy obecně lze říci, že bitcoin slouží jako prostředek směny.

Účetní jednotka. Tato funkce opět navazuje na tu předešlou. Přijímá-li nějaký obchod, ať už internetový či kamenný platbu v bitcoinech, potom musí být schopný uvést cenu za zboží či službu v bitcoinech. Tedy tuto funkci bitcoiny také splňují.

Poslední funkcí je uchovatel hodnot. Vzhledem k tomu, že spotřebitelé si spoří peníze, které tím představují složku bohatství, je těžké říci, zda bitcoin plní tuto funkci. Jak už bylo zmíněno, podstatnou roli tu hraje kupní síla peněz a míra inflace. Vzhledem k tomu, že bitcoin je decentralizovaná, deflační kryptoměna[42], není jeho vývoj nijak a ničím regulován. Tedy jeho kupní síla se může změnit ze dne na den. Zatím se tedy spokojíme s tím, že bitcoin není stabilním uchovatelem hodnot a více se budeme této otázce věnovat v pokračování této kapitoly, která se věnuje znakům měny.

A teď se vrátíme k již zmíněné měně, která spadá pod pojem peníze a vyznačuje se dvěma základními skupinami znaků.

Každá měna má své technické a ekonomické znaky[43]. My prozatím budeme na bitcoin nahlížet jako na měnu a podíváme se, zda tyto znaky splňuje.

[41] *Bitperia s.r.o. – Spojujeme digitální světy.* [online]. Cit. 15. 3. 2016. Dostupné z: http://bitperia.cz/katalog/.
[42] KUBIIN (2013). *Svět Bitcoinu*. [online]. Cit. 15. 3. 2016. Dostupné z: http://bitcoin.kubiin.net.
[43] ČERNOHORSKÝ, Jan, TEPLÝ, Petr (2011). *Základy financí.* Praha: Grada. S. 29.

Níže jsme zařadili znaky do tabulky, pro větší přehlednost.

	euro	americký dolar	bitcoin
Technické znaky			
Název měny	√	√	√
Hotovostní druhy (mince a bankovky)	√	√	x
Dělení a kumulace (na poloviny, desetiny x na desítky, sta)	√	√	√
Výlučnost měny - jen určitá měna musí být akceptována na vytyčeném území	√	√	x
Způsob stanovení měnového kurzu - stanovení hodnoty měny k ostatním měnám	√	√	√
Ekonomické znaky			
Charakter emise peněz - jak jsou peníze vydávány a stahovány z oběhu	√	√	x
Způsob zajištění měnové stability - kdo, jak a do jaké míry zajišťuje stabilitu měny	√	√	x

Obr. 3 Technické a ekonomické znaky měny.
Zdroj: ČERNOHORSKÝ, Jan, TEPLÝ, Petr (2011). *Základy financí.* Praha: Grada. S. 29.

Z tabulky vyplývá, že jak euro tak americký dolar splňují veškeré technické i ekonomické znaky měny. Mají svůj název – euro, americký dolar. Jsou v oběhu ve formě jak mincí, tak bankovek. A to v různých nominálních hodnotách, tedy obě měny splňují i znak dělení a kumulace. Znak výlučnosti měny, který znamená, že jen určitá měna musí být akceptována na vymezeném území, tedy zákonné platidlo na daném území[44], též splňuje jako euro tak americký dolar. Poslední technický znak, způsob stanovení měnového kurzu, obě měny jak euro tak americký dolar jsou měnami volně směnitelnými. U volně směnitelných měn existují tři režimy měnových kurzů[45].

- Volně pohyblivé kurzy – Kurz kolísá v reakci na poptávku a nabídku po měně. Centrální banka do něj nijak nezasahuje.
- Řízené pohyblivé kurzy – Centrální banka využívá nástrojů měnové politiky, aby udržela kurz měny v daném fluktuačním pásmu.

[44] ČERNOHORSKÝ, Jan, TEPLÝ, Petr (2011). *Základy financí.* Praha: Grada. S. 29.
[45] ŠMACH, Radek. *Kurzy měn ČNB.* [online]. Cit. 25. 3. 2016. Dostupné z: http://www.kurzymencnb.cz/Menovy-kurz.php.

- Kurzy vázaných měn – Hodnota měny je navázána na jinou významnou měnu.[46]

Jak euro tak americký dolar jsou měnami, které podléhají řízenému pohyblivému kurzu. Tedy centrální banky, Evropská centrální banka i Federální rezervní systém, využívají nástrojů měnové politiky, aby udrželi kurz měny ve fluktuačním pásmu. Zároveň tak plní svůj základní úkol, a sice udržení cenové stability.

Vzhledem k tomu, že už jsme zmínili existenci Evropské centrální banky a Federálního rezervního systému, což jsou centrální banky pro měny – euro a americký dolar, je zřejmé, že právě tyto dvě instituce, které jsou nezávislými samosprávnými orgány, jsou vykonavateli ekonomických znaků měny. Rozhodují o emisi a stahování peněz z oběhu, prostřednictvím měnových nástrojů, a tím se snaží dosáhnout určitých cílů, a sice měnové stability[47].

V souhrnu jak euro tak americký dolar splňují jak technické tak ekonomické znaky měny. Nyní se podíváme, blíže na bitcoin.

První znak, název měny, je bez problému splněn. Hned druhý však splněný není. Bitcoin nemá hotovostní druhy, nemá vůbec fyzickou podobu, a to ani v podobě bankovek ani mincí. Na trhu jsou k vidění mince bitcoinů, jde však o maketu či něco, co reprezentuje bitcoinovou peněženku a má v sobě skryté heslo pro transakce odchozí a bitcoinovou adresu pro transakce příchozí[48]. Znak dělení a kumulace bitcoin naplňuje, jelikož jsme v první kapitole zmínili, že bitcoin lze dělit až na hodnotu 0.000 000 01 BTC, která se jmenuje, s úctou k tvůrci celého systému, satoshi[49]. Jelikož je bitcoin virtuální měnou, jinak také kryptoměnou, je otázka splnění znaku výlučnosti měny trochu náročnější. Dle mého názoru není možné říci, že ji plní, protože není daného území, kde by byl výluční měnou jako zákonné platidlo. Co se způsobu stanovení měnového kurzu týče, spadá bitcoin do skupiny směnitelných měn, a podléhá pouze a jen volnému pohyblivému kurzu. Tedy zákonu poptávky a nabídky

[46] ŠMACH, Radek. *Kurzy měn ČNB.* [online]. Cit. 25. 3. 2016. Dostupné z: http://www.kurzymencnb.cz/Menovy-kurz.php.
[47] REVENDA, Zbyněk (2011). *Centrální bankovnictví.* Praha: Management Press. S. 79.
[48] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 38.
[49] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 30.

na trhu bez jakýchkoliv zásahů jiné instituce. Z ekonomických znaků je více méně jasné, že bitcoin nesplňuje ani jeden, protože jde o měnu decentralizovanou, tedy osvobozenou od kontroly vládou či centrální bankou. Celý Bitcoin systém funguje na *peer-to-peer* síti, tedy za komunikace mezi uživateli a není třetí strany, která by do něj zasahovala, tedy nemůže docházet ani k regulaci peněz v oběhu ani k zajišťování stability měny.

Můžeme tedy vůbec nazývat bitcoin měnou, když nesplňuje veškeré znaky měny, které jsou u zavedených měn samozřejmostí? Stačí fakt, že je bitcoin přijímán jako prostředek směny, aniž by byl něčím kryt, nebo alespoň aniž by se za něj někdo nebo něco zaručilo? Zkusíme na něj na okamžik nahlédnout spíše jako na komoditu než na měnu.

Budeme-li nahlížet na bitcoin jako na komoditu, potom by se investice do něj řídila klasickým investičním pravidlem, nakup levně a prodej draze. Zde by investor hned ze začátku počítal s prudce se měnící hodnotou bitcoinu v čase a snažil se dosáhnout největšího výnosu jeho prodejem v okamžiku nárůstu jeho hodnoty. Jako komodita je bezpochyby i určitým lákadlem pro spekulativní investory.[50] Dle mého názoru je vhodnější nahlížet na něj spíše z tohoto úhlu pohledu nežli jako na měnu, jelikož měna oplývá jistou důvěrou v ní vloženou těmi, kteří ji denně užívají. Důvěrou v její hodnotu, která sice kolísá, avšak je udržována v jistých mezích centrálními bankami, jejichž hlavním cílem je udržení cenové stability. A je tak možné realizovat krátkodobé i dlouhodobé investice či spoření, za více stabilních a předvídatelných podmínek.

[50] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 150–151.

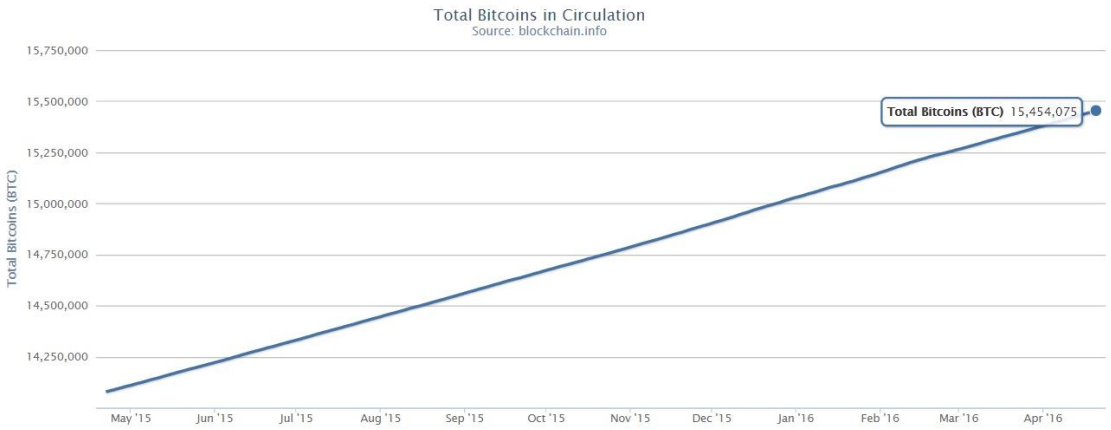
3. Vývoj kurzu bitcoinu

V této kapitole si přiblížíme roli Satoshiho Nakamota v Bitcoin systému a jeho moc nad kurzem bitcoinu. A dále se podíváme na vývoj kurzu bitcoinu, a to od samotného jeho počátku, tedy od roku 2009, až do roku 2016.

Zajímavostí je, že jde o decentralizovanou měnu, která má volně pohyblivý kurz. Její hodnota má být ovlivňována pouze poptávkou a nabídkou na trhu a má být zcela neregulovatelná. Je to však skutečně pravda?

V úvodní kapitole jsme zmínili zakladatele celého Bitcoin systému, Satoshiho Nakamota, po kterém nejrůznější deníky a lidí stále pátrají. Jemu nebo skupině lidí, která stojí za tímto pseudonymem, se však stále daří se skrývat a zůstávat neodhalen. Jediné, co se od roku 2009 podařilo o něm vypátrat je fakt, že si na počátku celého systému, kdy výnosnost dolování byla 50 BTC za zařazený *block* do *block chainu*[51], nashromáždil přibližně 1 milion BTC. A během let z tohoto bohatství utratil zatím přibližně jen 500 BTC[52]. Částka 500 BTC představuje testovací transakce, které Nakamoto zrealizoval v prvních deseti dnech po vydolování základního tzv. Genesis blocku[53]. Tímto činem Nakamoto rozjel celý systém, a následně už jen čekal, kdo se do něj zapojí a jak se bude dále vyvíjet. Fakt, že je Nakamoto majitelem přibližně 1 milionu BTC z něj činí majitele velkého podílu všech doposud vydolovaných bitcoinů. Z následujícího grafu vidíme, že k měsíci dubnu roku 2016 je v oběhu 15 454 075 BTC.

[51] FORRESTER, Daniel & SOLOMON, Mark (2014). *Bitcoin Explained: Today´s Complete Guide to Tomorrow´s Currency.* CreateSpace Independent Publishing Platform. S. 58.
[52] GUTTMANN, Benjamin (2013). *The Bitcoin Bible.* Books on Demand. S. 241.
[53] BRADBURY, Danny (2014). Coin desk. [online]. Cit. 18. 4. 2016. Dostupné z: http://www.coindesk.com/dangerous-satoshi-nakamoto/.



Obr. 4 Množství bitcoinů v oběhu k dubnu 2016
Zdroj: *Blockchain info.* [online]. Cit. 18. 4. 2016. Dostupné z: https://blockchain.info/charts/total-bitcoins.

Jako majitel nezměrného podílu bitcoinů na trhu, má Nakamoto jistou moc nad vývojem kurzu bitcoinu. Existují tři scénáře, jak může Nakamoto naložit se svým 1 milionem BTC včetně dopadů na Bitcoin systém.

Prvním a zároveň nejhorším scénářem, který by mohl nastat je, že se Nakamoto rozhodne uvolnit velkou část bitcoinů naráz do oběhu. Podobně jako 6. října 2014, kdy bylo uvolněno do oběhu 26 000 BTC na směnném portálu BitStamp, a následně došlo k poklesu tržní ceny bitcoinu o 10%, by Nakamoto uvolněním velkého objemu bitcoinů způsobil pokles jeho tržní ceny. To však není vše. Jako zakladatel celého systému, kdyby se Nakamoto rozhodl směnit bitcoiny za jinou měnu, vyjádřil by tak nedůvěru ve svůj vlastní projekt a tím by ho s velkou pravděpodobností odsoudil k zániku.[54]

Druhým scénářem, dle Sergia Demiana Lernera, by byl akt směny jeho jmění zodpovědně a po malých částech. Na začátku by mohl směnit zlomky bitcoinu a provést transakce z účtů, o kterých víme, že jsou pod jeho kontrolou. Následně by mohl ohlásit všem uživatelům sítě, že se chystá směnit své jmění po částech. To by zřejmě vedlo k prudkému poklesu hodnoty bitcoinu, avšak pozdější reakce by mohla být pozitivní. Vzhledem k tomu, že by proces uvolňováni bitcoinů byl řádně popsán

[54] BRADBURY, Danny (2014). Coin desk. [online]. Cit. 18. 4. 2016. Dostupné z: http://www.coindesk.com/dangerous-satoshi-nakamoto/.

a dodržován. Třeba by takový akt mohl navrátit důvěru v bitcoin a jeho hodnota by opět vzrostla.[55]

Třetí možností je, dle Sergia Lernera, jejich eliminace. Nakamoto by mohl odeslat svůj milion bitcoinů na finální bitcoinovou adresu, odkud by nebylo možné je odeslat dál. Tím by zcela zmizely z oběhu a celkový počet bitcoinů, který je v současnosti stanoven na 21 milionů, by klesl na zhruba 20 milionů. Navíc by vzrostla poptávka po těch, které již v oběhu jsou a bitcoin by v konečném důsledku posílil.[56]

Poslední možností by podle Gavina Andresena, současného předního správce Bitcoin systému, jemuž ho sám Satoshi Nakamoto předal, byla kombinace nákupu a eliminace bitcoinů. Nákupem bitocinů a následnou eliminací těch, které vlastní, by mohlo dojít k posílení bitcoinu a Nakamoto by jejich prodejem dosáhl kýženého zisku.[57]

Bohužel toto jsou jen dohady, a jelikož o Satoshim Nakamotovi není známo nic, bude si muset celý Bitcoin systém počkat na kroky, které jeho tvůrce v budoucnu podnikne, a jaké budou mít reálné dopady, to se teprve uvidí.

[55] BRADBURY, Danny (2014). Coin desk. [online]. Cit. 18. 4. 2016. Dostupné z: http://www.coindesk.com/dangerous-satoshi-nakamoto/.
[56] BRADBURY, Danny (2014). Coin desk. [online]. Cit. 18. 4. 2016. Dostupné z: http://www.coindesk.com/dangerous-satoshi-nakamoto/.
[57] BRADBURY, Danny (2014). *Coin desk.* [online]. Cit. 18. 4. 2016. Dostupné z: http://www.coindesk.com/dangerous-satoshi-nakamoto/.

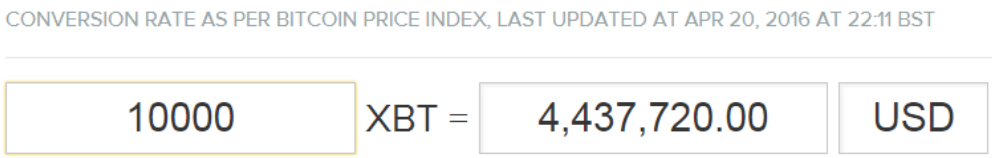
Nyní se podíváme na vývoj kurzu bitcoinu od roku 2009 do roku 2016.

Obr. 5 Graf vývoje kurzu BTC/USD
Zdroj: *Blockchain info.* [online]. Cit. 18. 4. 2016. Dostupné z: https://blockchain.info/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.

Z grafu je možné vidět, že Bitcoin systém poměrně dlouho zůstával bez povšimnutí. Prvním příjemcem bitcoinu, tedy kromě samotného Satoshiho Nakamota, se stal Hal Finney. Ten kontaktoval Nakamota v raných začátcích projektu a pomáhal mu s jeho rozjetím. Dne 12. ledna 2009 přijal transakci v hodnotě 10 BTC. Šlo o transakci zkušební, přesto však platnou a Finney se tak stal historicky prvním příjemcem bitcoinů.[58]

První platbou v kamenném obchodě byl nákup dvou pizz. Zakoupil je Laszlo Hanyecz dne 22. května 2010 v Pappa John´s pizzas. Dohromady jej dvě pizzy přisly na 10 000 BTC. V roce 2010 by ho pizzy vyšly v přepočtu na 25 USD, avšak ke dni 20. 4. 2016 by hodnota 10 000 BTC, kterou za ně zaplatil, odpovídala v přepočtu na americký dolar přibližně 4 437 720 USD.[59]

[58] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 20–21.
[59] CAFFYN, Grace (2014). *CoinDesk.* [online]. Cit. 18. 4. 2016. Dostupné z: http://www.coindesk.com/bitcoin-pizza-day-celebrating-pizza-bought-10000-btc/.



Obr. 6 Převod XBT/USD
Zdroj: *Bitcoin calculator.*[online]. Cit. 20. 4. 2016. Dostupné z: http://www.coindesk.com/calculator/.

O rok později, v únoru 2011, dosáhl bitcoin parity s americkým dolarem, tedy 1 BTC = 1 USD. Což přilákalo pozornost deníku *Time*, který o průlomovém Bitcoin systému publikoval článek.[60]

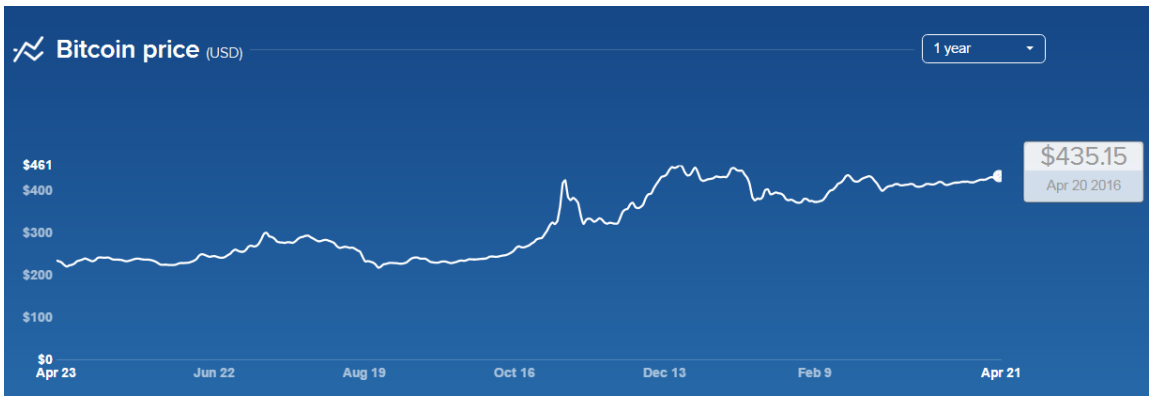
Zlomovým rokem se stal až rok 2013, kdy vzrostl počet uživatelů zapojených do Bitcoin systému, a s nimi začal růst i objem realizovaných transakcí. Rostoucí poptávka po bitcoinu zapříčinila růst jeho ceny. Největší nárůst ceny byl zaznamenán konce roku 2013. Růst byl tak rychlý, že 18. listopadu ráno byla hodnota 1 BTC rovna 478 USD a o půlnoci ten samý den byl 1 BTC roven již neuvěřitelným 744 USD[61]. Hodnotu 1000 USD potom bitcoin dočasně překročil dne 27. listopadu 2013, a to na nejstarší burze pro obchody s touto kybernetickou měnou – Mt.Gox. K jeho růstu patrně přispělo jednání o virtuální měně v americkém Senátu.[62] Na vrcholu své hodnoty byl bitcoin dne 29. listopadu 2013, kdy byl dosahoval hodnoty 1242 USD.[63]

Po roce 2013 následuje prudký pokles hodnoty bitcoinu. V únoru 2014 došlo ke krachu dosavadní největší burzy pro obchodování s bitcoiny, Mt.Gox, a došlo tak ke ztrátě přibližně 400 milionů USD.[64] Vyšetřování vedlo k závěrům, že se na krachu burzy podílel tehdejší šéf burzy Mark Kerpelès, který byl následně obviněn ze zpronevěry bitcoinů.[65]

[60] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 23.
[61] FREEPUB (2013). *Freepub.cz.* [online]. Cit. 19. 4. 2016. Dostupné z: http://www.freepub.cz/2013/cena-bitcoinu-poprve-dosahla-1000-dolaru/.
[62] REDAKCE (2013). *Investiční web.* [online]. Cit. 19. 4. 2016. Dostupné z: http://www.investicniweb.cz/zpravy-z-trhu/2013/11/27/bitcoin-je-jako-bublina-jiznich-mori/.
[63] ROONEY, Ben (2013). *CNN Money*. [online]. Cit. 19. 4. 2016. Dostupné z: http://money.cnn.com/2013/11/29/investing/bitcoin-gold/index.html.
[64] PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. S. 156.
[65] ČTK (2015). *E15.cz.* [online]. Cit. 19. 4. 2016. Dostupné z: http://e-svet.e15.cz/internet/japonsko-obvinilo-nekdejsiho-sefa-bitcoinove-burzy-ze-zpronevery-1226582.

Po prudkých výkyvech kurzu bitcoinu v roce 2013 a 2014, se vývoj jeho hodnoty v roce 2015 v porovnání s předchozími roky ustálil. V srpnu 2015 klesl bitcoin v důsledku devalvace čínského jüanu pod 200 USD. Avšak už koncem roku 2015 docházelo opětovně k posilování bitcoinu. V listopadu 2015 se přiblížil kurz bitcoinu hranici 500 USD za jednotku. Příčinou posilování bitcoinu byla podle expertů zvýšená poptávka z Číny.[66]

Aktuální kurz bitcoinu, ke dni 20. 4. 2016, je 1 BTC = 435.15 USD.



Obr. 7 Aktuální kurz BTC/USD
Zdroj: *Coinbase.* [online]. Cit. 20. 4. 2016. Dostupné z: https://www.coinbase.com/charts.

[66] TÝM FXSTREET.CZ (2015). *FXstret.cz*. [online]. Cit. 19. 4. 2016. Dostupné z: http://www.fxstreet.cz/kurz-bitcoinu-se-dostal-nad-500-dolaru.html.

4. Budoucnost fenoménu

Vzhledem k tomu, že je prozatím vydolováno pouze 15 454 075 BTC z celkového finálního objemu 21 milionů BTC, je celý Bitcoin systém stále atraktivním pro jeho uživatele. Odměnou za jejich účast na spravování celého systému, je každému uživateli stanovené množství bitcoinů za každý zařazený *block* do *block chainu*. Nyní je tato odměna rovna 25 BTC za každý *block*.

Avšak bude celý systém představovat výnos i v okamžiku, kdy bude všech 21 milionů BTC v oběhu?

Jelikož na transakce, které zahrnují velké množství bitcoinů, připadá nutnost platby transakčních polatků, odhaduje se, že by v budoucnu, až budou veškeré bitcoiny vydolovány, mohly být právě tyto poplatky zdrojem příjmů pro uživatele Bitcoin systému. Tím by si mohl celý systém udržet zájem uživatelů. Otázkou zůstává, zda tyto příjmy budou srovnatelné s odměnou za vydolovaný *block*.[67]

Není však pochyb o tom, že se za celým Bitcoin systémem skrývá geniální nápad. To uznala i Evropská centrální banka, která ve svém oficiálním reportu oznámila, že zkoumá potenciál využití *block chainu* jako alternativní prostředek pro spojení centrálních bank v rámci Eurosystému. Důvodem proč se o fungování *block chainu* Evropská centrální banka zajímá je projekt Target2-Securities. Ten byl zaveden v červnu 2015 a má zjednodušit vypořádání obchodů s cennými papíry na celoevropské úrovni. A právě *block chain* by mohl tento projekt uvést do chodu.[68]

Dále je to třeba energetická společnost RWE, která se nechala slyšet, že pracuje na projektu využití digitální technologie za účelem úspory nákladů ve vztahu firma-zákazník. Dle serveru Coindesk spolupracuje se startupem Slock.it na vytvoření systému, který by umožňoval uživatelům elektromobilů, v rámci jejich dobíjení

[67] FAGGART, Evan (2015). *Bitcoin.com*. [online]. Cit. 19. 4. 2016. Dostupné z: https://news.bitcoin.com/what-happens-bitcoin-miners-all-coins-mined/.
[68] BERKA, Jan (2016). *Roklen24*. [online]. Cit. 20. 4. 2016. Dostupné z: http://roklen24.cz/a/wRXvX/fintech-daily-co-ma-spolecneho-blockchain-ecb-a-elektromobily.

u dobíjecích stanic, platit pouze za spotřebovanou energii a ne za celkovou dobu strávenou u této stanice, jak tomu bylo doposud.[69]

V neposlední řadě je to i Bank of England, kdo se zajímá a principy fungování Bitcoin systému. Ve spolupráci s University College of London pracuje na vytvoření vlastního *block chain* systému, avšak s jedním zásadním rozdílem, chce mít v rukou možnost jeho regulace prostřednictvím speciálního šifrovacího klíče. Ten by jí umožňoval korigovat množství RSCoinů v oběhu a zároveň by tak měla dohled nad všemi transakcemi.[70]

Není tedy pochyb, že by Bitcoin systém nebyl zajímavým nápadem, který si získal své příznivce a bude ještě nějaký čas fungovat. Rozhodně však není bezchybný a předvídat jeho další vývoj je k jeho povaze takřka nemožné. S klidem ale můžeme říct, že inspiroval mnoho projektů a obecně se tak stal přínosem.

[69] BERKA, Jan (2016). *Roklen24.cz.*[online]. Cit. 20. 4. 2016. Dostupné z: http://roklen24.cz/a/wRXvX/fintech-daily-co-ma-spolecneho-blockchain-ecb-a-elektromobily.
[70] BERKA, Jan (2016). *Roklen24.cz.*[online]. Cit. 20. 4. 2016. Dostupné z: http://roklen24.cz/a/ibEfM/fintech-daily-znasilni-bitcoin-centralni-banky.

Závěr

Cílem této práce bylo proniknout do principů fungování Bitcoin systému a zhodnotit jeho budoucnost.

Zpočátku byly vymezeny základní pojmy figurující v celém systému. Následně jsme si objasnili, že celý systém je decentralizovaný, tedy bez možnosti regulace vládou, centrální bankou nebo jiným subjektem. I když sám jeho tvůrce, Satoshi Nakamoto, je vlastníkem 1 milionu BTC, což mu dává moc nad vývojem kurzu bitcoinu a i celého Bitcoin systému.

Dále jsme se věnovali otázce, zda bitcoin splňuje definici a znaky, jimiž je vymezen pojem měna. Zároveň byl srovnán se dvěma vybranými měnami, eurem a americkým dolarem. Výsledkem toho srovnání bylo zjištění, že na základě jeho vlastností, je přesnější pohlížet na bitcoin jako na komoditu.

Potom jsme se věnovali vývoji kurzu bitcoinu od doby jeho vzniku až po současnost. Bylo možné na něm pozorovat pomalu rostoucí zájem veřejnosti o systém samotný, až k bodu, kdy bitcoin dosáhl své historicky nejvyšší hodnoty – 1242 USD za jednotku, koncem roku 2013. Pozorovali jsme také nestálost kurzu, která je přímým odrazem poptávky a nabídky na trhu.

V závěru jsme se věnovali otázce, co nastane, až bude veškerých 21 milionů BTC v oběhu. Je možnost, že uživatelé budou přijímat zisk ve formě poplatků za transakce, avšak ty s největší pravděpodobností nebudou výdělečné natolik, aby si systém udržel zájem uživatelů. Avšak dle odhadů poslední bitcoin bude vytěžen až roku 2140 a do té doby se může ještě mnohé změnit. Jedno je však jasné, nápad, který stojí za Bitcoin systémem a způsob zapisování transakcí do *block chainu* inspiroval mnohé ke zdokonalení nebo přizpůsobení tohoto mechanismu. A můžeme říci, že Bitcoin systém nám je určitým přínosem.

Summary

At the very beginning this thesis is introducing Bitcoin system while defining its crucial terms and explaining how it works. It reveals the idea that is behind the entire Bitcoin system and rules that apply in a digital currency world. It of course devotes a subchapter to the mysterious inventor of the Bitcoin system. Later on it focuses on the nature of bitcoin and examines whether it is rather a currency or a commodity. After that it describes bitcoin´s volatile exchange rate. At the end it assesses future of Bitcoin system.

Klíčová slova

Satoshi Nakamoto, Bitcoin systém, bitcoin, *block, block chain, peer-to-peer*, decentralizace, bitcoinová adresa, bitcoinová peněženka, kryptoměna, měna, komodita, kurz bitcoinu.

Seznam pramenů a literatury

Bibliografické zdroje

- ČERNOHORSKÝ, Jan a TEPLÝ, Petr (2011*). Základy financí.* Praha: Grada. ISBN 978-80-247-3669-3.
- FORRESTER, Daniel & SOLOMON, Mark (2014*). Bitcoin Explained: Today´s Complete Guide to Tomorrow´s Currency.* CreateSpace Independent Publishing Platform. ISBN 978-1497311312.
- GUTTMANN, Benjamin (2013). *The Bitcoin Bible.* Books on Demand. ISBN 978-3732284320.
- PAGLIERY, Jose (2014). *Bitcoin: And the Future of Money.* Triumph Books. ISBN 978-1629370361.
- REVENDA, Zbyněk (2011). *Centrální bankovnictví.* Praha: Management Press. ISBN 978-80-7261-7.

Internetové zdroje

- (2013). *Wikisofia.* [online]. Cit. 6. 3. 2016. Dostupné z: https://wikisofia.cz/wiki/Bitcoin.
- BERKA, Jan (2016). *Roklen24.cz.*[online]. Cit. 20. 4. 2016. Dostupné z: http://roklen24.cz/a/wRXvX/fintech-daily-co-ma-spolecneho-blockchain-ecb-a-elektromobily.
- *Bezpecne-online.cz*. [online]. Cit. 10. 3. 2016. Dostupné z: http://www.bezpecne-online.cz/surfuj-bezpecne/sosani-a-sdileni-dat/peer-to-peer-site-jak-funguji-a-kde-je-problem.html.
- *Bitcoin calculator.*[online]. Cit. 20. 4. 2016. Dostupné z: http://www.coindesk.com/calculator/.
- *Bitperia s.r.o. – Spojujeme digitální světy.* [online]. Cit. 15. 3. 2016. Dostupné z: http://bitperia.cz/katalog/.
- *Blockchain info.* [online]. Cit. 18. 4. 2016. Dostupné z: https://blockchain.info/charts/total-bitcoins.
- BRADBURY, Danny (2014). Coin desk. [online]. Cit. 18. 4. 2016. Dostupné z: http://www.coindesk.com/dangerous-satoshi-nakamoto/.
- BRADBURY, Danny (2014). Coin desk. [online]. Cit. 18. 4. 2016. Dostupné z: http://www.coindesk.com/dangerous-satoshi-nakamoto/.
- CAFFYN, Grace (2014). *CoinDesk.* [online]. Cit. 18. 4. 2016. Dostupné z: http://www.coindesk.com/bitcoin-pizza-day-celebrating-pizza-bought-10000-btc/.
- *Coinbase.* [online]. Cit. 20. 4. 2016. Dostupné z: https://www.coinbase.com/charts.
- ČTK (2015). *E15.cz.* [online]. Cit. 19. 4. 2016. Dostupné z: http://e-svet.e15.cz/internet/japonsko-obvinilo-nekdejsiho-sefa-bitcoinove-burzy-ze-zpronevery-1226582.
- FILLNER, Karel (2015). *Btctip.cz.* [online]. Cit. 13. 3. 2016. Dostupné z: http://btctip.cz/jak-vyhodne-koupit-a-prodat-bitcoiny/.

- FREEPUB (2013). *Freepub.cz.* [online]. Cit. 19. 4. 2016. Dostupné z: http://www.freepub.cz/2013/cena-bitcoinu-poprve-dosahla-1000-dolaru/.
- HRACH, Jan (2011). *ABC Linuxu – Decentralizovaná kryptoměna bitcoin*. [online]. Cit. 11. 3. 2016. Dostupné z: http://www.abclinuxu.cz/clanky/decentralizovana-kryptomena-bitcoin.
- KHALIQ, Azzief (2014). *Hongkiat Technology Design Inspiration*. [online]. Cit. 10. 3. 2016. Dostupné z: http://www.hongkiat.com/blog/bitcoin-wallets/.
- KUBIIN (2013). *Svět Bitcoinu*. [online]. Cit. 15. 3. 2016. Dostupné z: http://bitcoin.kubiin.net.
- REDAKCE (2013). *Investiční web.* [online]. Cit. 19. 4. 2016. Dostupné z: http://www.investicniweb.cz/zpravy-z-trhu/2013/11/27/bitcoin-je-jako-bublina-jiznich-mori/.
- ROONEY, Ben (2013). *CNN Money*. [online]. Cit. 19. 4. 2016. Dostupné z: http://money.cnn.com/2013/11/29/investing/bitcoin-gold/index.html.
- SINGHA. *Bitcoin – česká grafika*. [online]. Cit. 15. 3. 2016. Dostupné z: http://bitcoin.singha.cz/ceska-grafika.
- ŠMACH, Radek. *Kurzy měn ČNB.* [online]. Cit. 25. 3. 2016. Dostupné z: http://www.kurzymencnb.cz/Menovy-kurz.php.
- TÝM FXSTREET.CZ (2015). *FXstret.cz*. [online]. Cit. 19. 4. 2016. Dostupné z: http://www.fxstreet.cz/kurz-bitcoinu-se-dostal-nad-500-dolaru.html.

Příloha č. 1:

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

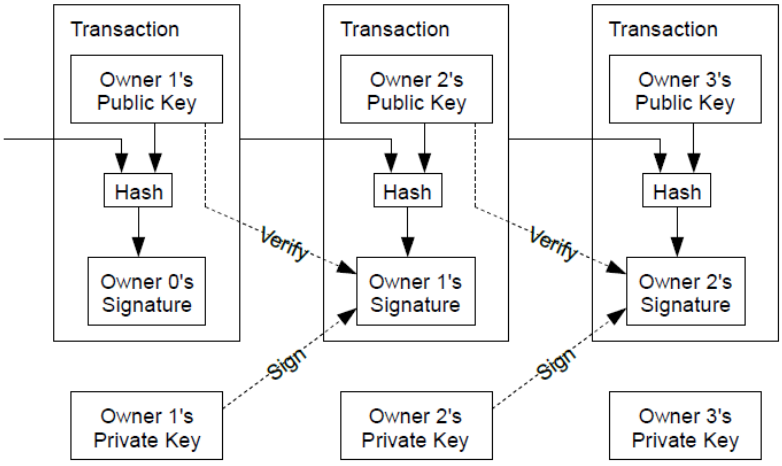
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non- reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double spent.

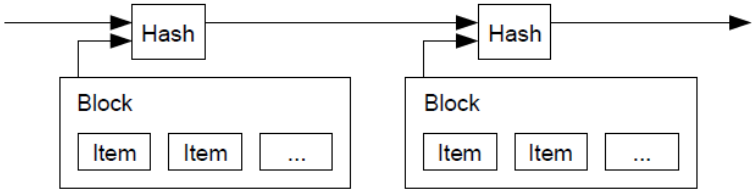
The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in

which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

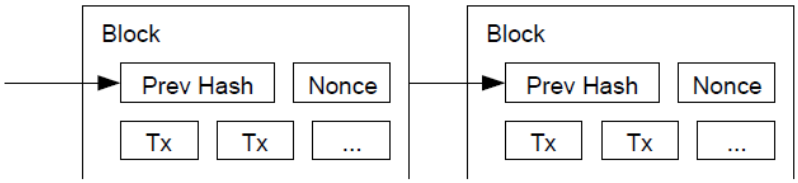
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof- of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the

proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof- of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

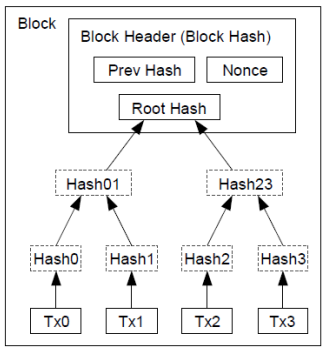
The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is

added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

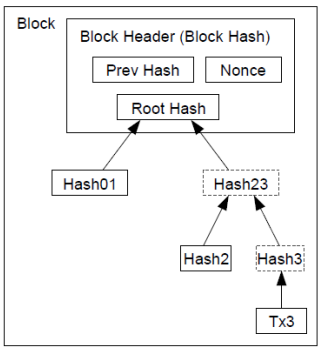
The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



Transactions Hashed in a Merkle Tree

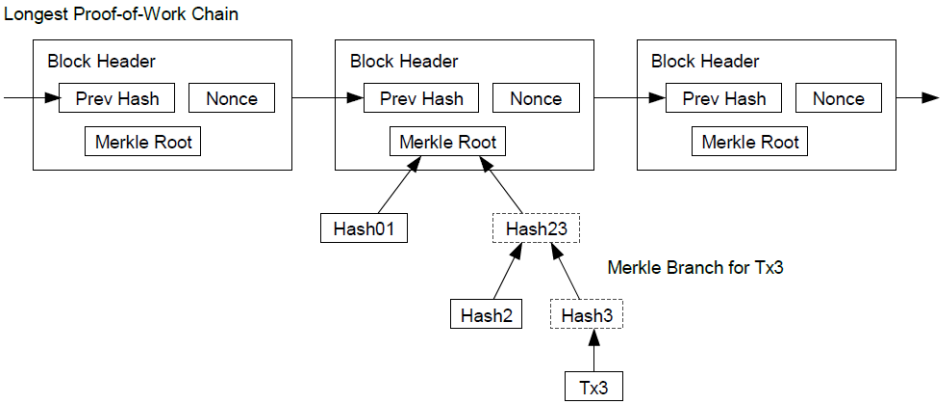


After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

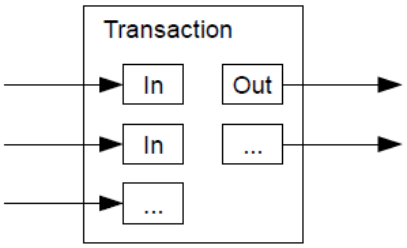
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

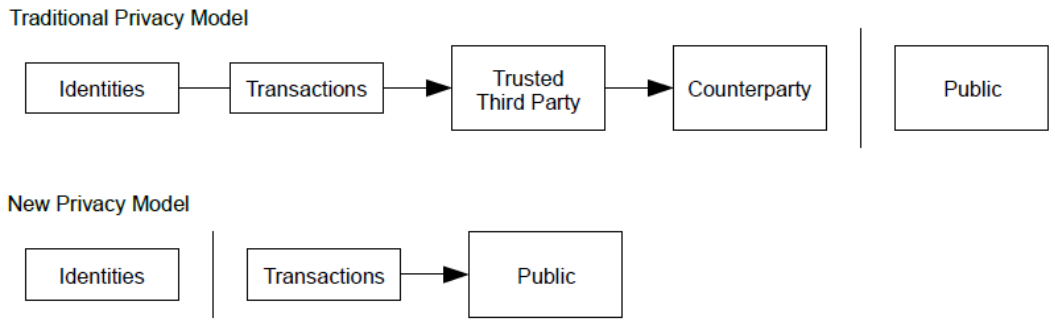
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
qz = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & if\ p \leq q \\ (q/p)^z & if\ p > q \end{cases}$$

Given our assumption that *p* > *q*, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and *z* blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \leq z \\ 1 & if\ k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1-\sum_{k=0}^{z}\frac{\lambda^{k}e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-
        lambda); for (i = 1; i <= k;
        i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9
        P=0.000
0046  z=10
        P=0.000
0012

q=0.3
z=0     P=1.0000000
z=5
P=0.1773523
z=10
P=0.0416605
z=15
P=0.0101008
z=20
P=0.0024804
z=25
P=0.0006132
z=30
P=0.0001522
z=35
P=0.0000379
z=40
P=0.0000095
z=45
```

```
P=0.0000024
z=50
P=0.0000006
```

Solving for P less than 0.1%...

```
P <
0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.