Digitální měna Bitcoin

Marek Drábek

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Marek Drábek**
Osobní číslo:	**A12676**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Digitální měna Bitcoin**
Téma anglicky:	**The Bitcoin Payment System**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na téma digitálních měnových systémů.**
2. **Zaměřte se na digitální měnu Bitcoin – možnosti jejího získání, bezpečnost apod.**
3. **Popište možnosti využití digitální měny Bitcoin.**
4. **Proveďte testování výše zmíněných možností získání digitální měny.**
5. **Vyzkoušejte a popište obchodování na burze pomocí digitální měny.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **PAGLIERY, J. Bitcoin and the future of money. Chicago, Illinois : Triumph Books. ISBN: 978-1629370361**
2. **KELLY, B. The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World. Wiley. ISBN: 978-1118963661.**
3. **FRANCO, P. Understanding Bitcoin: Cryptography, Engineering and Economics. Wiley. ISBN: 978-1-119-01916-9**
4. **GET STARTED WITH BITCOIN. [online]. [2015] [cit. 2015-02-06]. Dostupné z: http://www.bitcoin.com/**
5. **BITCOINMAN. Co je Bitcoin? – vše o digitální měně Bitcoin [online]. [2015] [cit. 2015-02-06]. Dostupné z: http://www.bezpecne-online.cz/**

Vedoucí bakalářské práce: **Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **6. února 2015**

Termín odevzdání bakalářské práce: **21. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen na elektronickém nosiči v příruční knihovně Fakulty managementu a ekonomiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

1. že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
2. že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 19. 5. 2014

.....
podpis diplomanta

ABSTRAKT

Cílem bakalářské práce je popsat co je digitální měna Bitcoin, na jakém principu funguje, jak a kde se používá, jaké má výhody/nevýhody oproti klasickým měnám. Zhodnocena je její bezpečnost a možný budoucí potenciál. Praktická část se zaměří na popis možností jak měnu získat, jaké vybavení je k tomu potřeba i se zhodnocením aktuální návratnosti. Na závěr práce popisuje kde a jak měnu uchovávat a jak s ní obchodovat na burze.

Klíčová slova: Bitcoin, těžba, těžař, miner, blockchain, uzel, blok, target, inflace, deflace, hazard, kurz, ASIC jednotka, FPGA čip, antminer, Paypal, dvojí utrácení, burza

ABSTRACT

The main purpose of this bachelor thesis is to explain what the digital currency Bitcoin is, how it works, how and where to use it and what are the advantages and disadvantages in comparison to standard currencies. Hereafter it deals with safety and future potential. The practical part describes the possibilities of getting this currency and the required facilities. Eventually, it discusses the profitability and the issues of storage of the currency and trading on the stock exchange.

Keywords: Bitcoin, mining, miner, blockchain, node, block, target, inflation, deflation, gambling, exchange rate, ASIC unit, FPGA chip, antminer, Paypal, double spending, stock exchange

„Každá lidská činnost se nakonec musí nějak projevit v číslech.“

Tomáš Baťa

OBSAH

ÚVOD

Každý z nás, nejen pro potřeby svého života manipuluje s materiálními hodnotami, které jsou reprezentovány penězi. O všechny státem vydané peníze se stará centrální měnový systém, na čele s centrální bankou, který funguje v každém státě jako monopol. Před několika málo lety se objevily tzv. digitální měnové systémy. Jednalo se o malé finanční systémy, kde hodnotu reprezentoval určitý typ nefalšovatelných souborů. Dlouho byly používány jen v úzkých kruzích počítačových nadšenců, kteří jej akceptovali. Myšlenka, že by se z malé digitální měny mohl časem stát reálný konkurent centrální měny, nebyla příliš reálná. Digitální systémy se pomalu rozšiřovaly, postupně si získaly pozornost finančních institucí, následně se o ně začala zajímat média a asi před 4 roky, jakoby se strhla lavina, začaly být stále více používány veřejností. Díky velké poptávce se začlenily dokonce mezi obchodovatelné komodity. Dnes umožňují především vykonávat platby ve virtuálním prostředí, jakým může být třeba hraní her, sociální sítě, nebo výměna online kreditu za zboží a služby. Prvenství mezi digitálními měnami si jednoznačně drží měna Bitcoin. Ve svých začátcích se příliš nelišil od svých konkurentů a jeho hodnota byla zanedbatelná, jednalo se o centy dolarů. Postupně se stával čím dál populárnějším, především pro svou jednoduchou manipulovatelnost. V další fázi následoval raketový start jeho hodnoty, až do výšek stovek dolarů za jeden kus. Známé jsou historky o tom, jak jistí lidé trávili dny na smetišti, ve snaze najít svůj starý pevný disk z počítače, který kdysi vyhodili do smetí a měli na něm několik, v tu dobu bezcenných Bitcoinů. Kdyby se jim to podařilo, někteří by se stali třeba milionáři.

Dnes je Bitcoin rozšířen po celém světě a akceptuje ho čím dál více subjektů. Hodnota všech „kusů“ Bitcoinů se pohybuje v řádech milionů dolarů. Celá jeho síť představuje dnes složitý finanční systém. Jako široce akceptovaný, globální, platební konkurent a pravidelně se konají ekonomické konference, kde se rozebírají jeho stále se rozvíjející možnosti. Jeho hlavním triumfem je fakt, že nespadá pod stát, ale pod vlastní komunitu lidí, která ho zpravuje, což přitahuje množství lidí, kteří nechtějí nechávat všechny své peníze ve spárech vlády.

I. TEORETICKÁ ČÁST

1 DIGITÁLNÍ MĚNOVÉ SYSTÉMY

Dnešní, technologicky se rozvíjející svět umožnil vznik internetových měn. Jedná se o nehmotný druh platidla, který je vytvářen pomocí počítačů, za použití složitých matematických výpočtů. Nejprve vznikaly v úzkém kruhu lidí a měly hodnotu jen pro samotné tvůrce daných měn. Některé se postupem času velmi rozšířily do celého světa a byla jim „přiřazena“ skutečná hodnota vyjádřena globální měnou (většinou americký dolar), nebo třeba zlatem. [9]

Digitální měny mají mnoho výhod oproti běžným tzv. fiat měnám (měny vydávané státem, které jsme povinni akceptovat pro platby v běžném životě), jimiž jsou například rychlá manipulovatelnost (díky internetu je většina převodů téměř okamžitých), či možnosti izolovat toky finančních prostředků od legislativy státu, tím pádem na ně stát nemůže uvalovat regulace, jako je DPH apod.

Mezi hlavní nevýhody digitálních měn spadá především nestálá hodnota, například umělé ovlivnění kurzu je tady jednodušší než u fiat měn. S tím souvisí skutečnost, že digitální měny dnes nejsou vůbec kryty zlatem. Běžní obchodníci ve většině případů nepřijímají digitální měny (až na Bitcoin), a protože potřeba svoje prostředky nejprve převést na běžně používané fiat měny. Svoje digitální peníze máme uloženy na internetových peněženkách, které vlastní soukromé osoby a nemáme žádnou garanci, že o peníze nepřijdeme, jak z důvodu možného podvodu ze strany vlastníka peněženky, tak ze situace, že činnost peněženky ukončí státní orgán (třeba s podezřením na podvodné konání), u kterého následně může být problém s dokazováním vlastnictví prostředků.

Neotřesitelné prvenství v oblasti digitálních měnových systému drží měna Bitcoin. Ta je nejrozšířenější na světě a dnes už patří do oblasti obchodovatelných komodit, po boku ropy a zlata. Nicméně existuje řada dalších, avšak ne tak slavných alternativ.

E-Gold

Tato měna byla založena roku 1996, je to neformální předchůdce všech dnešních digitálních měn. Hodnota peněz na vlastním účtu byla převedena na zlato, nebo na jiný vzácný kov a byly tady okamžité převody mezi účty. Tajná služba USA ukončila činnost této služby kvůli praním špinavých peněz ze strany majitelů. Majitelé bývalých účtů mohou stále podat požadavek na vrácení peněz. Tato měna byla populární mezi falšovateli dokladů, podvodníky a překupníky dětského porna. Obrázek 1 znázorňuje logo E-Gold. [8]

Obr. 1. Logo měny E-gold [37]

Liberty Reserve

Než byla uzavřena tahle služba, byly vykonány transakce ve výši cca 6 miliard dolarů. Měna byla opět využívána při podvodech s kreditními kartami, při investičních krádežích, počítačovém hackerství, pašování drog a u obchodu s dětskou pornografií. Na obrázku 2 je znázorněno logo Liberty Reserve. [8]

Obr. 2. Logo Liberty Reserve [38]

Litecoin

Peer to peer měna, v základech je podobná Bitcoinu. Těžit tuto měnu je ale možné o dost efektivněji, zatím stačí běžný domácí počítač. Podle některých dohadů by se mohla stát hodnotnější, pokud by se používala současně s Bitcoinem. Obrázek 3 znázorňuje logo Litecoinu. [8]

Obr. 3. logo Litecoinu [39]

Peercoin

Má 3. největší trhovou kapitalizaci (po Bitcoinu a Litecoinu). Je to do jisté míry spekulativní měna, jejímž hlavním cílem je, aby její získávání bylo co možná nejmíň náročné na spotřebu energie. Obrázek 4 znázorňuje logo Peercoinu. [8]

Obr. 4. Logo Peeercoinu [40]

Ripple

Jedná se o další měnu na báze matematiky. Zatím se moc nerozšířila, ale její transakce mají být zanedlouho rychlejší než u Bitcoinu. Obrázek 5 znázorňuje logo služby Ripple. [8]

Obr. 5. Logo Ripple [41]

OpenCoin

Měna vytvořená skupinou nadšenců z Německa a Velké Británie. Převzala myšlenku elektronické měny z 80. let zvané E-cash, transakce jsou bez poplatku, nicméně měna zatím není příliš známá. Na obrázku 6 je znázorněno logo OpenCoinu.[8]

Obr. 6. Logo OpenCoin [42]

2 DIGITÁLNÍ MĚNA BITCOIN

Bitcoin (zkratka BTC) je internetová digitální měna, která byla vytvořena s cílem zefektivnit digitální platby v globálním měřítku. Slouží jako alternativa k nynějším měnovým systémům, která je nehmotná a nehmatatelná. Doslovně se jedná jen o řetězec přiřazený určité bitcoin adrese. Hlavním rysem Bitcoinu jako měny je jeho kompletní decentralizace, z čehož vyplývá, že samotnou „výrobu“ měny i potvrzování transakcí mají na starost samotní uživatelé sítě Bitcoin, neexistuje tady žádná centrální banka udělující regulace, jako u jiných měn. [10]

Neméně důležitá je skutečnost, že hodnota Bitcoinu není závislá od důvěry v samotného vydavatele, ale prakticky od poptávky po měně a v důvěru v budoucnost měny jako takové. Její kurz vůči jiným měnám je (proto) velmi nestabilní. Nejmenší část Bitcoinu, se kterou můžeme samostatně manipulovat, je tzv. „Satoshi“ a jedná se o jednu stomiliontinu Bitcoinu (0,00000001 BTC). [2]

Měna je poměrně anonymní, při založení virtuálního účtu pro práci s Bitcoiny není nutné žádné ověření identity, veřejnost si ani nemůže zjistit, kdo má na účtu kolik Bitcoinů. Na druhou stranu, vlastnictví měny je kontrolovatelné ze strany komunity, která spravuje síť Bitcoin a je jen na nás, nakolik jí důvěřujeme. Nicméně nikdy nebyl zaznamenán případ, že by někdo přišel o Bitcoiny kvůli podvodnému jednání ze strany komunity, která spravuje celou síť. [10]

Pojem Bitcoin dále označuje platební síť pro obchod s Bitcoiny a software pro práci s měnou. Obrázky 7 a 8 znázorňují alternativy loga Bitcoinu. [31]

Obr. 7. Logo Bitcoinu [43]

Obr. 8. Alternativní logo Bitcoinu [44]

3 VZNIK MĚNY BITCOIN

Měna Bitcoin byla vytvořena v roce 2009 osobou, nebo skupinou osob, pod pseudonymem Satoshi Nakamoto. To jsou jediné oficiální informace o vzniku, „samotný“ Satoshi Nakamoto jen nějakou dobu přispíval na fórech o Bitcoinu, ale odmítal jakkoliv komentovat jeho roli ve vzniku měny. Proto není jisté, zda se jedná o jednu osobu nebo o skupinu lidí. Na světlo se ale dostává otázka, zda by byl jeden člověk schopný vytvořit digitální měnu s celou sítí určenou pro obchodování s měnou a dále i příslušný software. Nicméně o síť i o software se dnes starají vybrané skupiny lidí, ale ti jen do určité míry zdokonalují dobře fungující základ, který byl vytvořen dříve.(Kelly, 2014, s. 37-45)

Jedna z teorií o „vynálezci“ říká, že se jedná o jednoho muže jménem Dorian Satoshi Nakamoto, 64 – letý modelář žijící v Los Angeles, který v minulosti dělal tajnou práci na elektronice a v komunikacích pro americké ozbrojené síly a různé korporace. Při dotazu novináře to ale tento člověk popřel. Ať už na tom je něco pravdy nebo ne, jeho bývalá práce na utajovaných projektech pro vojensko-průmyslový sektor zahaluje Bitcoin spekulacemi, k jakým účelům byl vlastně původně vynalezen. Na obrázku 9 je znázorněn modelář Satoshi Nakamoto. [3], [4]

Obr. 9. Satoshi Nakamoto, možný tvůrce měny Bitcoin [45]

4 HODNOTA BITCOINU

Jak už bylo řečeno, Bitcoiny nejsou kryty žádnou hmotnou věcí, která by jim alespoň z části propůjčovala hodnotu. Ta vychází, volně řečeno, z důležitosti samotné měny, kterou určuje člověk. Jeho hodnota proto velmi kolísá, v rámci obchodovatelných komodit se jedná o tu s největšími výkyvy. (Pagliery, 2014, s. 60-80)

4.1 Inflace, deflace

Měnu nekontrolují žádné banky ani vlády a maximální počet Bitcoinů v oběhu je předem daný a proto není možné, aby vznikla inflace, která by byla způsobena vydáním většího množství jednotek platidla. Tím pádem žádné banky nemohou touto cestou manipulovat s hodnotou Bitcoinů, tak je to u jiných měn. Maximální možný počet vytěžených Bitcoinů je cca 21 milionů. Nicméně v některých kruzích se objevuje názor, že uvedený počet jednotek měny není dostatečný pro veškerou potřebu. Na druhou stranu je možno obchodovat s každou stomiliontinou Bitcoinu zvlášť (0,00000001 BTC = 1 Satoshi) a tím pádem teoreticky existuje více jednotek této měny, než třeba amerických dolarů. V případě Bitcoinu je ale velmi pravděpodobná deflace – což je jev opačný k inflaci, jedná se o „zvyšování“ hodnoty měny vzhledem k jiným měnám (za stejný počet jednotek nějaké měny dostaneme čím dál míň Bitcoinů.) Souvisí to se zmíněným horním maximem vytěžených Bitcoinů, čím větší bude poptávka, tím vyšší bude deflace. [2]

4.2 Měnový kurz

Bitcoin je mladá měna s vysokou volatilitou, jinak řečeno, má vysoké nárůsty ceny a následně nečekané propady. Díky těmto skutečnostem se dá na měně vydělat nebo prodělat ve velmi krátkých časových intervalech. Otázka, co všechno vlastně vytváří hodnotu této virtuální měny, kromě důvěry v zachovávající si hodnotu, je do jisté míry stále předmětem spekulací. [6]

Na stránce forexsrovnavac.cz se píše: *„Jeden z častých omylů je to, že hodnota měny Bitcoin je přímo určena počtem uživatelů, kteří Bitcoin těží. Podle teorie by to tedy mělo znamenat, že čím více uživatelů Bitcoin těží, tím se zvyšuje jeho hodnota. Nicméně je to právě naopak, stoupající cena Bitcoinu zvyšuje počet minerů, z toho vyplývá, že uživatelé, kteří se podílejí na těžbě této měny, nemohou určovat skutečnou hodnotu. Proto se dnes zastává názor, že hodnota této měny vychází pouze z poptávky a nabídky na trhu a je tak kryta pouze důvěrou, že s ní bude možno v budoucnu zaplatit stejně jako dnes.“* [6]

Existuje mnoho stránek na obchodování s Bitcoiny, směnné kurzy na jednotlivých stránkách logicky nejsou úplně stejné. Největší burzou pro obchod s Bitcoiny byla burza „MtGox“, která dnes už ale nefunguje. Oblíbené jsou dnes burzy „Bitflix“ nebo „Bitcoin.de“. Obchodování s Bitcoiny je možné i na obchodní platformě „Plus500“, ale na rozdíl od burzy, vklady a výběry jsou možné jen ve fiat měně (eura, dolary…), to znamená, že všechny Bitcoiny (a jiné komodity) musíme před výběrem „směnit“ na danou měnu. Na obrázku 10 je znázorněn kurz Bitcoinu k americkému dolaru ze dne 5.9. 2015.

Obr. 10. Kurz Bitcoinu k americkému dolaru [54]

Na pohyby kurzů měny Bitcoin mají, stejně jako i v případě jiných světových měn, vliv finanční události ve světě. Nejdůležitější milníky pro Bitcoin, které ve většině případů přímo ovlivňovaly jeho hodnotu:

5. října 2009*:* poprvé oficiálně stanoven kurz Bitcoinu - 1,309,03 BTC za 1$ (tenhle kurz byl čistě formální, v praxi platilo: 1 BTC = cca 0.003$)

18. srpen 2008: vznik stránky bitcoin.org

3. leden 2009: vytěžen první blok (50 Bitcoinů)

9. leden 2009: vyšla první verze softwaru pro práci s Bitcoinem – Bitcoin 0,1

12. leden 2009: první transakce v Bitcoinech (mezi Satoshim Nakamotem a vývojářem Halem Finneym)

16. prosince 2009: vydán software Bitcoin 0,2

7. červenec 2010: vydán software Bitcoin 0,3 (1 BTC =0.008$)

12. červenec 2010: kurz 1 BTC = 0,08$ (hodnota Bitcoinu vzrostla na desetinásobek za 5 dnů, díky rozmachu aplikace Bitcoin 0,3)

6. únor 2010: vznik první burza pro Bitcoin - Bitcoin Market

Březen 2010: první reálná transakce, programátor Laszlo Hanyecz koupil dvě pizzy za 10 000 Bitcoinů

17. července 2010: vznik burzy MtGox. (Magic the Gathering online Exchange – burza na výměnu hracích karet hry Magic the Gathering)

Srpen 2010: objevení zatím jediné chyby v systému, která umožňovala provést transakci dvakrát. Chyba byla opravena

15. srpen 2010: Při jedné transakci se objevilo 184 miliard Bitcoinů. Transakce byla odhalena a vymazána, a tak trochu smetena pod stůl.

6. listopad 2010: hodnota všech Bitcoinů překročila 1 milion dolarů (aktuální kurz 1 BTC = 0.5$)

Leden 2011: vytěžen blok 105000, což znamená, že bylo vytěženo již 5,25 milionů Bitcoinů, co je 1/4 z maximálního objemu 21 milionů Bitcoinů.

9. únor 2011: dosažena parita s americkým dolarem (1 BTC = 1$)

Březen 2011: otevřeny burzy, poprvé nabízející výměnu Bitcoinů za Britskou libru, Polský zlotý, nebo Brazilský real.

Duben 2011: dosažena parita s Eurem a následně s Britskou librou.

Červen 2011: historicky nejvyšší kurz - 1 BTC = 31.9$. Následně byly na burze MtGox (nejpoužívanější pro obchod s Bitcoiny) zcizeny účty mnoha lidem, kteří přišli o své Bitcoiny, díky čemu klesl kurz na hodnotu 1 BTC = 001$.

Leden 2012: stále panovala nedůvěra v měnu po nedávných útocích, kurz 1 BTC = 5,27$

Březen 2012: největší krádež Bitcoinů v historii – odcizeno bylo dohromady 46 000 BTC

Květen 2012: burza Bitcoinica po hackerském útoku přišla o 18 000 BTC.

Září 2012: burza Bitfloor taktéž po hackerském útoku přišla o 24 000 BTC

Listopad 2012: vytěžen blok 210000, polovina maximálního počtu Bitcoinů

6. prosinec 2012: burza Bitcoin Central dostala jako první na světe bankovní licenci, postupně čím dál více společností začalo akceptovat platby v Bitcoinech.

Březen 2013: hodnota všech Bitcoinů na světě dosáhla hodnoty jedné miliardy amerických dolarů

1. duben 2013: kurz Bitcoinu překonal hranici 100$

8. duben 2013: kurz Bitcoinu překonal hranici 200$

20. duben 2013: kurz se propadl na hodnotu 100$ za 1 BTC díky hackerskému útoku na burzu Bitcoin Central

Srpen 2014: Německo uznalo Bitcoin jako měnu, ostatní státy ani centrální banky to ale v plánu nemají

Říjen 2013: v kanadském Vancouveru vznikl první automat na Bitcoiny

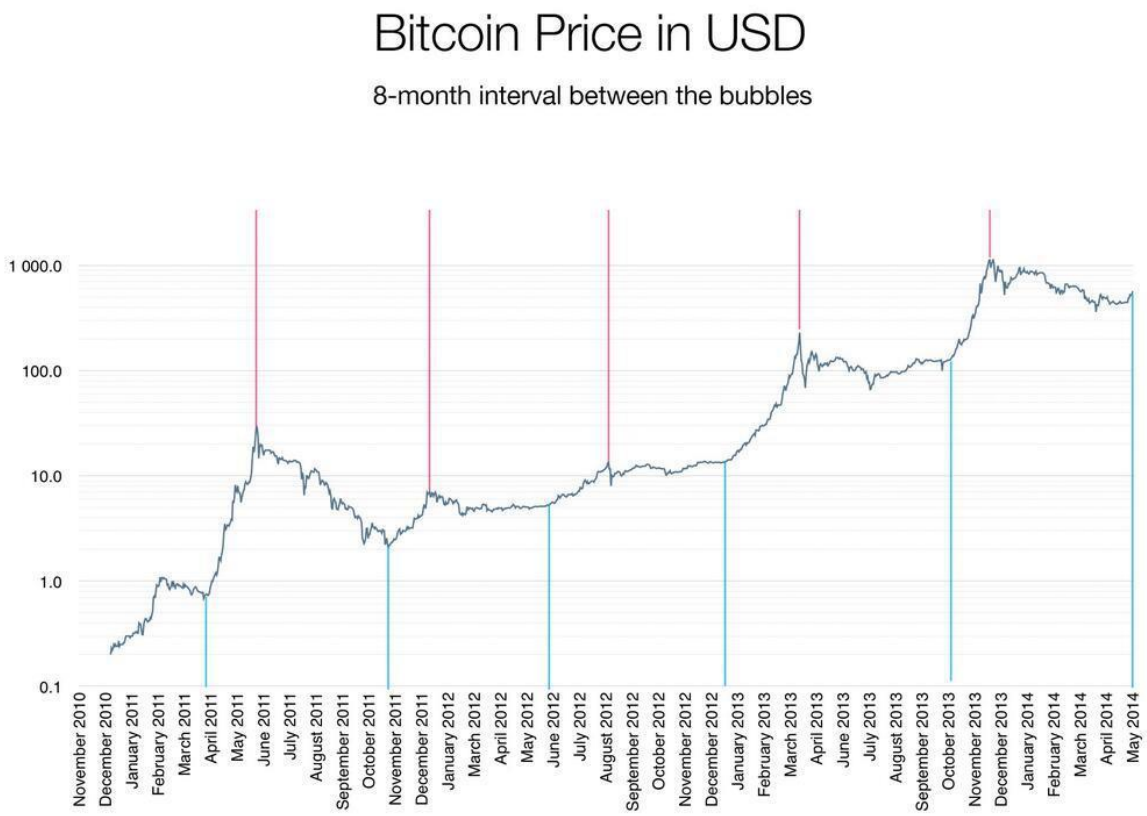
Listopad 2013: Bitcoin dosáhl dodnes nepřekonané hranice 1240$, na chvíli se 1 Bitcoin stal hodnotnější než unce zlata

Únor 2014: burza MtGOx kvůli ztrátám ze softwarové chyby ukončila svou činnost (spekuluje se o škodách v hodnotách 700 000 BTC) [7]

Leden 2015:v Rusku bylo zablokováno mnoho stránek s Bitcoiny, s cílem minimalizovat vliv Bitcoinu na ekonomiku. [74]

Květen 2015: ohlášena nová kryptoměna HayekCoin, má se jednat o 1. kryptoměnu na světě, která je zcela kryta zlatem. Kolují rozsáhle spekulace, co to bude znamenat pro Bitcoin. [31]

Na obrázku 11 je znázorněn vývoj hodnoty kurzu Bitcoinu v letech 2010-2014.



Obr. 11. Vývoj kurzu Bitcoinu k americkému dolaru v letech 2010-2014 [55]

5 SLOŽKY SÍTĚ BITCOIN

Jak už bylo zmíněno, tak síť Bitcoin nepodléhá žádné autoritě, a proto musí být udělána tak, aby se postarala „sama o sebe“.

5.1 Uživatelé

Činnost účastníků sítě se primárně skládá z nákupu a prodeje Bitcoinů. Pokud uživatel Bitcoiny také vytváří, jinak řečeno těží, je označován pojmem „těžař“.

5.1.1 Bitcoin adresa

Každý účastník pro manipulaci s Bitcoiny potřebuje svoje konto. To je reprezentováno bitcoin adresou, která vznikla z veřejného klíče. [16]

Postup vytvoření adresy: [16], [18], [27], [28], [30]

1. Pomocí ECDSA algoritmu je vygenerován 256-bitový soukromý klíč. ECDSA je zatím nefalšovatelný algoritmus pro vytváření šifrovaných zpráv a digitálních klíčů.
2. Ze soukromého klíče je vygenerován 520-bitový, nekomprimovaný, veřejný klíč, označme jej „PubK“ (public key)
3. Nad veřejným klíčem se spočítá SHA256 hash, obsah výstupu:

   číslo S (256 bitů) = SHA256(PubK)
4. Nad „číslem S“ je spočítána hashovací funkce RIPEMD-160. Jedná se o zatím neprolomenou hashovací funkci se 160-bitovým číslem na výstupu. Obsah výstupu:

   číslo R (160 bitů) = RIPEMD160(číslo S)
5. Před „číslo R“ je přidán prefix „0x00“, výstup:

   číslo E (168 bitů) = "0x00" + R
6. Nad číslem E se spočítá SHA256 hash, nad výsledkem znovu SHA256 hash, výstup: číslo D (256 bitů) = SHA256(SHA256(číslo E))
7. Z čísla D se použije prvních 32 bitů, které představují kontrolní součet výsledné adresy - „číslo C“
8. Bitcoin adresa (200 bitů) = číslo E + číslo C

9. Pro lepší čitelnost je číslo převedeno do formátu „base58“. Jedná se o systém zobrazování binárních dat pomocí ASCII tabulky, který neobsahuje znaky l,I,O,0“, které si jsou na pohled dost podobné. Z prefixu „0x00“ vznikne po konverzi vždy „1“, proto každá bitcoin adresa začíná tímto číslem.

5.1.2 Bitcoin peněženka

Bitcoin peněženka je nepostradatelný nástroj na příjem a manipulaci s Bitcoiny. Je schopna nám vytvořit bitcoin adresu. Existuji 2 druhy peněženek pro příjem Bitcoinů: [18], [19]

1. Online peněženky, které poskytují rychlou a snadnou obsluhu, ke svému kontu se můžeme připojit z jakéhokoliv počítače připojeného k internetu, protože soubor se soukromým klíčem je na serveru. S tím souvisí možná hrozba, majitel služby má přístup ke klíčům všech klientů, které by mohl teoreticky zneužít.
2. Offline peněženky, ke kterým je potřeba klient v počítači, na pevný disk je uložen soubor se soukromým klíčem, takže se uživatel připojí jen z konkrétního počítače. Offffline peněženky si při prvním spuštění stahují celou, nebo část blockchain (aktuální velikost (9.5.2015) činí 33,247 GB).

5.2 Uzly

Uzly udržují konzistentní strukturu Bitcoin sítě. Každý uzel obsahuje aktuální verzi blockchain, pomocí které rozhoduje, zda příchozí transakci schválí nebo ne (ověří hashe a digitální klíče). Z platných transakcí uzly vytvářejí bloky a informace o nich rozesílají uzlům v jiných částech Bitcoin sítě. Na činnost uzlů se ve velké míře zaměřují případní podvodníci, se snahou vytvořit falešnou transakci, která by prošla procesem schválení. [11]

5.3 Bloky

Bloky jsou stavební kameny celé Bitcoin sítě. Jsou to unikátní soubory dat, které se seskupují se v rozsáhlém řetězci bloků, tzv. blockchain. Tento řetězec tvoří historii všech transakcí v Bitcoin síti a každý uzel v síti obsahuje jeho aktuální verzi. (Franco, 2014, s. 15)

Formát bloku: [11]

- *identifikátor začátku bloku, vždy 0xD9B4BEF9*

- *velikost bloku v bytech*
- *hlavička:*
  - *verze bloku*
  - *hash předcházejícího bloku*
  - *hash všech transakcí v bloku*
  - *časové razítko (počet sekund od 1.1.1970)*
  - *target (256-bitové číslo označující složitost)*
  - *nonce (32-bitové číslo)*
- *počet transakcí v bloku*
- *samotný seznam transakcí*

5.4 Transakce

Transakční systém je založen na tzv. asymetrické kryptografii. Jedná se o typ šifrování, kde figuruje dvojice klíčů. Prvním je veřejný klíč, který slouží na šifrování zpráv a může ho vlastnit kdokoliv. Naproti tomu soukromý klíč dešifruje poslané zprávy a patří jen jeho vlastníkovi. [29]

Transakce je v principu zpráva pro Bitcoin síť. Tvořena je vstupní a výstupní částí. Vstupní část transakce obsahuje hash z předchozí transakce, který je podepsán soukromým klíčem aktuálního odesilatele transakce, a veřejný klíč toho samého odesilatele pro následné ověření platby. Výstupní část obsahuje samotný počet Bitcoinů ve formě jednotek Satoshi, časové razítko a bitcoin adresu příjemce. Díky faktu, že výstup z předchozí transakce se stává vstupem do následující transakce, jsou všechny transakce vystopovatelné a není možné přidat do bloku uměle vytvořené, jinak řečeno zfalšované transakce. [29]

Celé ověření transakcí vykonává speciálně pro Bitcoin síť vytvořený skript, který je obsažen v každé transakci. Při odeslání transakce je na vstupu veřejný klíč odesílatele a digitálně podepsaný hash transakce od odesílatele. Následně se digitální podpis odesílatele ověří s jeho veřejným klíčem. Výstupní část obsahuje samotný postup, kterým se ověří transakce. Na straně adresáta má skript k dispozici jeho podpis transakce (soukromý klíč) a jeho veřejný klíč. Skript zahashuje veřejný klíč (vznikne adresa), veřejným klíčem se ověří digitální podpis, čím se potvrdí, že transakce je skutečně určena jemu. [29]

Zůstatek na účtu není uložen ve formě jedné společné množiny tvořenou všemi vlastněnými Bitcoiny, ale zůstává rozdělen v hodnotách jednotlivých transakcí, které jsme přijali. Kvůli tomu transakce můžou obsahovat více vstupů i výstupů. Patrné je to na následujícím příkladu: Na prázdný účet obdržíme transakci ve výši 10 BTC. Následně chceme odeslat 5 BTC. Naše transakce bude mít 2 výstupy: V 1. výstupu se odešle 5 BTC adresátovi a ve 2. výstupu se odešle 5 BTC zase zpět na náš účet. Platí to samozřejmě i obráceně, pokud zůstatek na našem účtu tvoří menší částky a chceme poslat větší částku, tak nutný počet menších částek bude tvořit jednotlivé vstupy do naší transakce. [29]

Transakce, jinak řečeno „toky peněz“, nejsou nijak šifrovány, všechny jsou dohledatelné v blockchain. Anonymní jsou sice samotné bitcoin adresy, ale na základě námi zveřejněné bitcoin adresy by bylo možné dohledat naše transakce a tím pádem i naše zůstatky. Anonymita celé Bitcoin sítě tkví v tom, že systém dovoluje uživateli vytvořit si velký počet vlastních bitcoin adres a všechny můžou být svázány jen třeba s jedním kontem. Tyto adresy si můžeme vytvořit ve své bitcoin peněžence. Doporučuje se použít novou adresu pro každou větší transakci. Maximální možný počet adres v síti je 2^{160} (hodnota je daná rozsahem hashovací funkcí RIPEMD-160, která je použita při tvorbě adresy). [16], [29]

6 TĚŽBA BITCOINŮ

Těžba, anglicky řečeno „mining“, je proces získávání Bitcoinů využitím výpočetní jednotky, kterou nejdříve býval procesor nebo grafická karta počítače, nicméně dnes se nepoužívá nic jiného než specializované čipy, vytvořené primárně pro tento účel. Těžba je výpočetně velmi náročný proces, nicméně vzrůstající hodnota Bitcoinů způsobila nárůst těžařské sítě do globálních rozměrů. Těžba je jediný způsob, kterým vznikají nové Bitcoiny. [5]

6.1 Proces těžby

Při těžbě se těžař snaží vytvořit nový jedinečný blok. Základem pro vytvoření bloku je vytvoření hashe předchozího bloku, a to pomocí transakce hashovací funkce.[11]

Definice hashovací funkce: *„Hashovací funkce je transformace, která jako vstup přijímá řetězec znaků o libovolné délce. Výsledkem je pak řetězec znaků s pevnou délkou, tzv. otisk.“* [12]

Hashování bloku transakcí probíhá pomocí hashovací funkce SHA256, která z řetězce vstupních dat vytvoří hash o délce 256 bitů (64 znaků v hexadecimální soustavě). Navíc se jedná o dvojité hashování, to znamená, že na výstupu z první hashovací funkce proběhne transformace ještě jednou.[13]

Samotné vytvoření hashe je analogický, výpočetně nepříliš náročný proces. Kdyby jen toto stačilo k vytvoření nového bloku, všechny Bitcoiny by byly za velmi krátký čas vytěženy a pravděpodobně by neměly žádnou hodnotu. Bitcoin síť má proto implementován systém tzv. „Proof of work“ (volně přeloženo jako „důkaz o vykonané práci“), který je vlastně zodpovědný za skutečnost, že těžení Bitcoinů je výpočetně náročný proces. Jedná se o vytvoření specifického řetězce, který je výpočetně náročné vytvořit, ale jeho pravost je jednoduché ověřit. [11]

Těžící zařízení hledá náhodné 32 - bitové číslo (v bloku označeného jako „nonce“), které se spolu s časovým razítkem přidá do transakce, nad kterou vykoná dvojité hashování. Na výstupu je číslo (hash), jehož velikost musí být menší, než je hodnota udávaná v kolonce „target“ (tato hodnota není stálá, proč to tak je, je vysvětleno v další části). Na úspěšné vytvoření zmíněného hashe není žádný algoritmus, jediný známý způsob je použití „hrubé síly“, jinak řečeno testování všech možných kombinací, jednu po druhé. Při vytěžení nového bloku těžící zařízení předá svůj objevený blok spolu s jeho otiskem uzlu, který z něj

spočítá dvojitý SHA256 hash, následně oba hashe porovná a pokud se shodují, blok je schválen. Následně se do něj připíše transakce s adresou, na kterou je poslána odměna pro těžaře. Nakonec uzel rozešle tuto informaci dalším uzlům. [11]

Nicméně transakce je označena za „potvrzenou“ až poté, co je do blockchain přidáno dalších 100 bloků. Do té doby je odměna evidována na účtu jako „nepotvrzená“. [33]

Odměna se každé 4 roky snižuje o polovinu, od spuštění sítě v roce 2009 až do prosince 2012 činila 50 BTC, aktuálně (duben 2015) je to 25 BTC. Těžař dostává kromě odměny i tzv. „transakční poplatek“, kterého výše není závislá od stanovené hodnoty bloku. Výše transakčního poplatku se liší od každého nalezeného bloku, konkrétní hodnota se pohybuje v rozmezí asi 0,01-0,3 BTC.[11], [29]

6.2 Obtížnost

Síť Bitcoin má zvláštní princip, který zaručuje uvolňování stejného množství Bitcoinů za konstantní časovou jednotku i za předpokladu, že se do těžení zapojuje stále více těžařů s čím dál lepším technickým vybavením. Každých 10 minut se uvolní do oběhu 1 blok Bitcoinů (aktuálně 25 jednotlivých Bitcoinů). [5]

Aby Bitcoin síť udržela uvedené „konstanty“, tak obsahuje protokol, který každých 14 dnů upravuje náročnost objevení nového bloku, vzhledem k celkovému výpočetnímu výkonu zařízení všech těžařů. Jde o upravení hodnoty „target“, kterou obsahuje každý blok. Hodnotu reprezentuje 256 bitové číslo, které udává maximální velikost hashe, který může obsahovat nově vytěžený Bitcoin. Čím je hodnota menší, tím je výpočetně náročnější objevení nového bloku. Target se aktualizuje na hodnotu, které odpovídá uvolnění jednoho bloku za 10 minut vzhledem k aktuální světové výpočetní síle, vždy po 2016 blocích, co představuje přibližně 2 týdny.[14], [70]

Mezi těžaři je hodně rozšířen pojem „obtížnost“, který představuje číslo, kolikrát je v tuhle chvíli těžší nalézt blok, v porovnání s nejlehčím případem (v případě, že hodnota target je maximální). Aktuální hodnotu obtížnosti získáme vydělením maximální hodnoty target s aktuální hodnotou target.[15]

Maximální hodnota target (tato hodnota byla aktuální na samotném začátku těžby Bitcoinů, je to největší možné 256-bitové číslo):

- Hexadecimální zápis:
  0x00000000ffff0000000000000000000000000000000000000000000000000000

- Dekadický zápis (zaokrouhleno): 26 959 946 667 $x10^{57}$

Aktuální hodnota target (4.5.2015):

- Hexadecimální zápis:
  0x00000000000001713DD0000000000000000000000000000000000000000000
- Dekadický zápis (zaokrouhleno): 56 586 088 341 x 10^{46}

Aktuální obtížnost (dekadický zápis): 47643398017,803 [15], [19]

V praxi pak nastává situace, že se zařízením se stálým výpočetním výkonem vytěžíme za každý měsíc méně, než za předchozí měsíc (momentálně zhruba asi o 2,5% / měsíc). Naopak může nastat situace, že klesne zájem o těžbu a těžařů ubude, síť Bitcoin to následně zaznamená a sníží náročnost nalezení nového bloku, podle aktuálního výpočetního výkonu všech těžařů.[14], [15]

Konkrétní příklad na grafické kartě Radeon HD7870 (s rychlostí 400MH/s): [5]

08.04.2013 vytěžila cca 0,026 BTC denně.

02.09.2013 vytěžila cca 0,0031 BTC denně.

12.11.2013 vytěžila cca 0,0004 BTC denně .

30.06.2014 vytěžila cca 0,000011 BTC denně.

6.3 Těžící hardware

Bitcoiny se těží s pomocí zařízení s funkcí výpočetní jednotky, které obsahují 1 nebo více procesorů a hlavním úkolem je zpracování vstupních dat na výstupní. Zásadním atributem je výkonnost, anglicky „hash rate“, která se udává v počtu hashů, které je schopno zařízení vyzkoušet za 1 sekundu. Například dříve zmíněná grafická karta Radeon 7870 má rychlost 400 MH/s, to znamená, že karta vyzkouší 400 000 000 hash kombinací za 1 sekundu. Dalšími důležitými atributy jsou pořizovací cena a množství spotřebované elektrické energie.[5]

6.3.1 Počítačové procesory

V začátcích se k těžbě využíval zásadně jen procesor počítače. Výkon se pohyboval v rozmezí 1 – 120 MH/s. Dnes už je tento způsob maximálně neefektivní, výdělek by byl prakticky nulový. Tabulka 1 obsahuje porovnání výkonu procesorů Intel, v tabulce 2 je porovnání výkonu procesorů AMD. [16]

Tab. 1. Porovnání výkonu procesorů Intel [16]

Model	Výkon (MH/s)
Atom Z520	1,2
Core 2 Extreme X9000	7,2
Core 2 Duo E8400	7,0
Core 2 Duo T9400	4,2
Core 2 Quad Q8200	10,9
Core i7 980X	19,2
Core i5 650	5,1
Core i5 2400	14,0
4x Xeon E7450	60

Tab. 2. Porovnání výkonu procesorů AMD [16]

Model	Výkon MH/s
Turion X2 RM-70	1,9
Athlon64 X2 6000+	2,8
Phenom II X4 810	11,0
Phenom II X6 1150	15,8
2x Opteron 6128	32,4
4x Opteron 6174	115

6.3.2 Grafické karty

V další fázi se těžily Bitcoiny pomocí grafických karet. Ty představovaly několikanásobný nárůst výkonu oproti procesorům. Efektivní byly grafické karty od výrobce ATI Radeon, model HD 7990 dosahoval rychlost až 1200 MH/s. Naproti tomu grafické karty vyrobené společností nVidia kvůli odlišné architektuře nedosahovaly vhodných výsledků, výkon

nejvýkonnějších modelů se pohyboval v rozmezí 100-340 MH/s. Dnes je tento způsob rovněž prakticky nepoužitelný, náklady na elektřinu by byly mnohem vyšší než samotné minimální výdělky za Bitcoiny. V tabulce 3 jsou porovnány výkony grafických karet nVidia a v tabulce 4 je porovnání výkonů grafický karet AMD. [16]

Tab. 3. Porovnání výkonu grafických karet nVidia [16]

Model	**Výkon (MH/s)**
8800GT	25
9800GTX	32
GTX 285	53
GTS 450	45
GTX 480	100
GTX 560 Ti	67
GTX 570	98
GTX 580	156
GTX 590	193
GTX 670	112
GTX 680	120
GTX Titan	340

Tab. 4. Porovnání výkonu grafických karem AMD [16]

Model	**Výkon (MH/s)**
HD 4850	75
HD 4870	90
HD 5570	73
HD 5750	116
HD 5770	156

HD 5850	250
HD 5870	340
HD 6750	170
HD 6850	250
HD 6870	300
HD 6970	385
HD 6990	740
HD 7770	190
HD 7850	300
HD 7870	400
HD 7950	500
HD 7970	650
HD 7990	1200

6.3.3 Specializované čipy

V následujícím období přišla na trh zařízení se specializovanými obvody, určenými výhradně jen na těžbu kryptoměn. Těžaři je označují pojmem „miner“. [16]

Tzv. programovatelná hradlová pole (FPGA) byla sice výkonově porovnatelná s grafickými kartami, ale spotřebovaly podstatně méně elektrické energie. Nicméně v dnešní konkurenci těžařů je uvedený způsob také ekonomicky nerentabilní. Tabulka 5 obsahuje porovnání výkonu FPGA čipů. [16]

Tab. 5. Porovnání výkonu FPGA čipů [16]

Model	**Výkon (MH/s)**	**Spotřeba (W)**
Icarus	380	19
ModMiner Quad	800	40
X6500 FPGA Miner	400	17

ZTEX USB-FPGA Module 1,15b	90	neuvedeno
ZTEX USB-FPGA Module 1,15x	215	neuvedeno
ZTEX USB-FPGA Module 1,15y	860	neuvedeno

Dnes se už Bitcoiny těží jen se zařízením zvaným „ASIC jednotka“. ASIC jednotky jsou nejvýkonnější těžící zařízení na trhu a mají příznivou spotřebou energie. Nejstarší modely mají výkon 1-50 GH/s, aktuální jednotky disponují výkonem 180 – 3000 GH/s a ve vývoji jsou stále výkonnější modely. Jeho výroba je náročná (porovnatelná s procesory), ale díky jeho využití je po něm pochopitelně velký zájem. [16]

ASIC jednotky se vyskytují ve 2 provedeních: [16]

1. USB ASIC jednotky, které se připojují přes USB rozhraní, jsou fyzicky malá zařízení s výkonem 0.5-3 GH/s. Mají velmi nízkou spotřebu energie, ale díky nízkému výkonu jsou vhodné spíš pro rekreační těžaře. Obrázek 12 zachycuje 3 kusy zařízení zvaného „ASICMinerBlockErupter“.

Obr. 12. USB Asic jednotky [47]

2. „Standalone“ jednotky, které mají vestavěný síťový adaptér, takže nepotřebují být připojeny k počítači. K internetu se připojí pomocí vestavěné wi-fi antény nebo ethernetovým kabelem a pracují samostatně. Jsou to fyzicky větší zařízení s váhou 3-15 kg, osazeny kvalitním ventilátorem. V provedení Standalone se vyrábí drtivá

většina zařízení, která se podílejí na výkonu celé Bitcoin sítě. Obrázek 13 znázorňuje miner „Rockminer Prisma“ s výkonem 1.4 TH/s od firmy Minereu.

Obr. 13. Miner „Rockminer Prisma“ [48]

Nejoblíbenější modely

Na výrobu ASIC jednotek se specializují konkrétní firmy jako Bitman, Butterflylabs, Minereu a další. Asi nejznámější ASIC jednotky pocházejí z rodiny „Antminer“, od zmíněného výrobce Bitman.

Antminer S1

První „miner“ z rodiny, dnes se už pro svůj nedostačující výkon nevyrábí. Na jaře roku 2014 patřil mezi nejvýkonnější minery na trhu a určitou dobu ho kvůli své nedostupnosti vlastnil jen úzký okruh těžařů. Na obrázku 14 je zachycen Antminer S1.[17], [22]

Obr. 14. Antminer S1 [49]

Antminer S2

Výkonný miner, který je vhodný především kvůli své stále nízké efektivitě (1 W/GH/s) do míst s levnější elektrickou energií. Na obrázku 15 je zachycen Antminer S2. [21]

Obr. 15. Antminer S2 [50]

Antminer S3

Další Antminer měl sice menší výkon i spotřebu, ale na tu dobu nejlepší efektivitu. Dnes se už nevyrábí, ale poskytuje dostačující výkon pro konkurenceschopnou těžbu. Na obrázku 16 je zachycen Antminer S3. [20]

Obr. 16. Antminer S3 [51]

Antminer S4

Patří mezi nejvýkonnější minery současnosti, disponuje slušnou efektivitou, ale výkonu také odpovídá cena. Na obrázku 17 je zachycen Antminer S4.[36]

Obr. 17. Antminer S4 [52]

Antminer S5

Nejmodernější miner z rodiny, poskytuje vysoký výkon s nejlepší efektivitou ze všech minerů. Na obrázku 18 je zachycen Antminer S5. [22]

Obr. 18. Antminer S5 [53]

Detailní parametry těžících zařízení z rodiny Antminer obsahuje tabulka 6.

Tab. 6. Technické specifikace *Antminerů [17], [20], [21], [22], [36]*

Model	**Výkon (GH/s)**	**Spotřeba (W)**	**Efektivita (W/GH/s)**	**Orientační cena (Kč)**
Antminer S1	180-200	360	2	800 (bazar)
Antminer S2	1000	1100	1,1	39200(nový) 10000 (bazar)
Antminer S3	440	366	0,83	4500 (bazar)
Antminer S4	2000	1380	0,69	28250 (nový)
Antminer S5	1155	590	0,51	8350 (nový)

6.4 Sdružené těžení

Z hlediska stále se zvyšující náročnosti nalezení Bitcoinu těžaři nepracují po jednom ve stylu „sami za sebe“, ale ve skupinách zvaných „pool“. Když člen skupiny nalezne nový blok, tak odměna za něj je rozdělena všem členům skupiny podle toho, kolik vytěžil dílčích kousků. 1. pool na světě vznikl v Česku, jmenuje se „Slush“. [5]

6.5 Spotřeba energie

Čím více se Bitcoin dostal do popředí, globálně se začala řešit otázka spotřeby zdrojů na výrobu Bitcoinů. Na jednu stranu se můžeme trochu filozoficky zamyslet nad celým systémem, protože nastala situace, kdy v procesu těžení jen řešíme problém, který jsme si uměle vytvořili, abychom získali Bitcoin, kterému jsme uměle přiřadili hodnotu. To stojí energii, která ne vždy pochází z obnovitelných zdrojů.

Podle magazínu Forbes se denně spotřebuje elektřina v hodnotě 15 milionů dolarů (300 milionů Kč), s odvoláním na oficiální statistiky serveru Blockchain.com. Do diskuze se dostali odborníci ze stránky Bitcoined.cz, kterým vyšla hodnota 7 149 730 Kč. Nicméně největší roli ve všech výpočtech hrála výpočetní síla celé Bitcoin sítě, a proto můžeme jen hádat, kde je pravda, protože není znám přesný počet jednotlivých typů zařízení v oběhu, které se liší svou efektivitou. Jednoznačné je jenom to, že těžba bude probíhat, dokud bude mít ekonomický potenciál.[23], [24]

7 BEZPEČNOST

Globálně rostoucí obliba Bitcoinu časem přitáhla pozornost různých podvodníků. Ti se zaměřili na jedné straně na možnosti jak zcizit Bitcoiny, které jsou už v oběhu a obchoduje se s nimi, tak i na možné slabiny celé Bitcoin sítě, která by jim dovolila dostat do oběhu Bitcoiny falešné.

7.1 Malware

Největším nebezpečím pro běžné uživatele Bitcoin sítě je škodlivý kód, který se může dostat do počítače skrze jeho slabé, nebo neaktuální zabezpečení. Podle studie firmy Dell-Secure Works, která se zaobírá internetovými útoky, existuje přes 100 rodin různých malwarů, které jsou použitelné ke krádežím digitální měny. [9]

V principu není nutné vyvíjet škodlivý kód speciálně pro krádeže digitálních měn. Stačí běžný malware, který odchytává přihlašovací údaje třeba do internetového bankovnictví a s malou modifikací je schopen ukrást přihlašovací údaje k bitcoin peněženkám nebo směnárnám. Malware v sobě obsahuje jejich databázi a spustí sledování stisknutých kláves třeba jen tehdy, když uživatel přistupuje na dané stránky. Program odchytne přihlašovací údaje, které odešle svému tvůrci, který následně může disponovat s celým kontem. Většina bitcoin peněženek se přizpůsobila a obsahuje ověření ve více krocích (kromě přihlašovacích údajů třeba ověření přes sms). Další častý druh malwaru se zaměřuje na offline internetové peněženky. Jeho prací je hledání souborů na pevném disku počítače, které mohou být soukromým klíčem (často se jedná o „wallet.dat"). Po jeho následném nalezení jej malware bez vědomí uživatele nahraje na vzdálený server a útočník opět získá moc nad celým kontem. [9]

Nicméně pokud se věnujeme obchodování s virtuální měnou, měli bychom věnovat zvláštní pozornost zabezpečení svého počítače. [9]

7.2 Falešné Bitcoiny

Určité riziko představují podvodníci, kteří se snaží do sítě „propašovat“ své zfalšované bloky, které by reprezentovaly jejich vlastní Bitcoiny. Síť je proti tomu v principu zabezpečená, protože samotné vytvoření bloku je velmi náročná operace a pokud ho někdo vytvoří, vynaložil velkou práci. Na změnu již existující bloku je potřebné porovnatelné množství práce. Pokud by se někdo usiloval o změnu bloku, který je hlouběji v blockchain,

musel by změnit taky všechny bloky, které jsou nad ním. K tomu by bylo třeba velké množství výpočetní síly, prakticky nadpoloviční část výpočetní síly celé Bitcoin sítě. To je zásadní pravidlo, díky kterému platí, že dokud je síť tvořena poctivými uživateli, nebude v tomhle ohledu zneužita. [34]

7.2.1 Dvojí utrácení

Na principu falešných bloků pracuje také metoda zvaná „dvojí utrácení“ (anglicky „double spending“). Jedná se o situaci, kdy po zrealizování transakce uživatel ještě jednou zahashuje původní blok, podepíše a pošle opět jako platnou transakci. Jinak řečeno, snaží se o odeslání hodnoty, kterou už jednou někomu poslal. Kvůli tomu síť neuzná transakci za platnou do doby, než za transakci vznikne 6 dalších transakcí (proběhne 6 ověření). Tento princip způsobuje, že platby v Bitcoinech nejsou realizované okamžitě, ale až potom, co proběhnou zmíněná ověření. [35]

8 VYUŽITÍ BITCOINU

Bitcoin nepatří mezi fiat měny, proto pro žádného prodejce neplyne povinnost ho akceptovat. V praxi se hlavně jedná především o technické možnosti obchodu a cílovou skupinu zákazníků. Nejuniverzálnější způsob uplatnění Bitcoinů pro online platby je jeho prvotní „směna“ na všude akceptované fiat měny. K tomu nám postačí jakákoliv burza Bitcoinů. Na druhou stranu, stále roste počet institucí, které Bitcoin přijímají jako konkurenceschopné platidlo a v neposlední řadě je to pro ně i známka prestiže.

8.1 Internetové obchody

V počátcích akceptovalo Bitcoin jen pár internetových obchodů, převážně s elektronikou. Doba šla dopředu a dnes už si za Bitcoiny můžeme pořídit cokoliv od jídla, služeb přes letenky, k parfémům a nejrůznějšímu oblečení. Při internetové platbě pomocí Bitcoinů aplikace obchodníka, po vytvoření objednávky zákazníkem, kontaktuje platební server, který vrátí obchodníkovi bitcoin adresu, kterou obchodník zobrazí uživateli spolu s částkou k úhradě. Po úhradě zákazníkem server informuje obchodníka o provedení platby.[71], [72]

Dnes už ale akceptuje Bitcoin i hodně kamenných institucí jako jsou masážní salóny, trafiky, kadeřnictví, restaurace, nebo třeba pobočky občerstvení Subway. V praxi se platba na pokladně převede na Bitcoiny a zákazník zaplatí pomocí aplikace v mobilním telefonu. Ta načte prodejcův QR kód a odešle platbu na adresu, v něm obsaženou. Na účtence jsou platby vedeny v Kč, protože na oficiální příjem Bitcoinů, jako platidla zatím neexistuje v České republice legislativa. [72]

8.2 Propojení s platební bránou Paypal

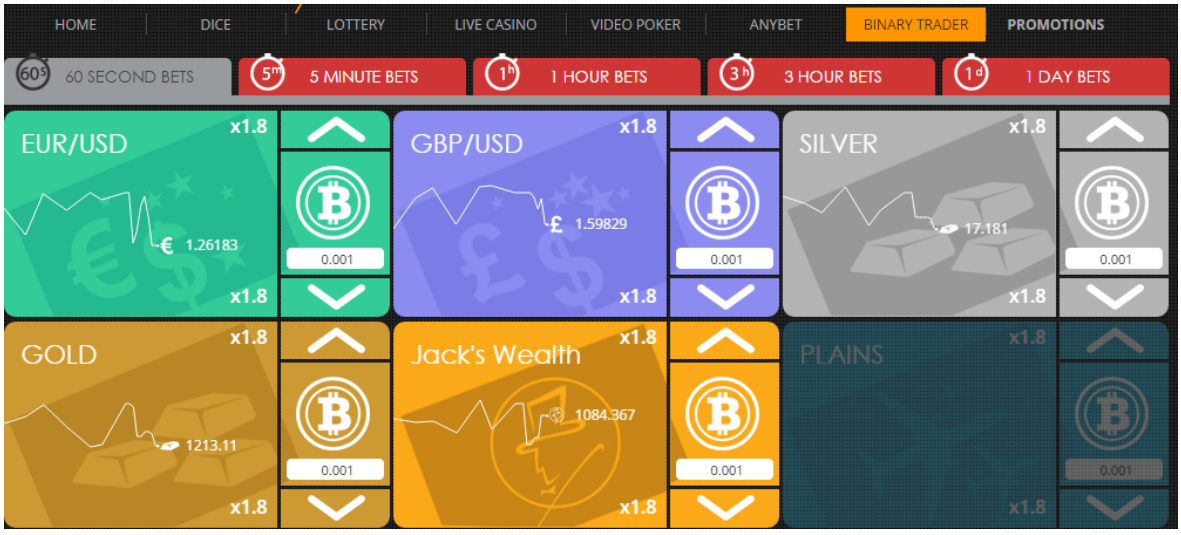
Platební brána Paypal, nejvíce využívána kvůli svému propojení s největší aukční síní světa eBay-em, ale také akceptována množstvím obchodníků po celém světě, ohlásila v září minulého roku začlenění tří virtuálních měn - Bitcoinu, Litecoinu a Dogecoinu do svého systému. Po vyhlášení zprávy stoupl kurz Bitcoinu v průběhu pár hodin o víc než 10% a další 2 měny také nepatrně posilnily. Partnerem Paypalu jsou platební brány BitPay, GoCoin a bitcoin peněženka Coinbase. V současnosti běží testovací provoz, možnosti virtuálních měn v Paypalu mohou zatím využívat jen obchodníci v Severní Americe, kteří používají nástro „Paypal Hub“. Nejedná se ale o přímé integrování kryptoměn do platebního systému, ale Paypal hraje jen roli prostředníka, přes kterého probíhají platby ve virtuálních

měnách. Nyní Paypal čeká, jak se k podpoře virtuálních měn postaví zákazníci a jednotlivé státy. [65]

Největším problémem se zatím jeví fakt, že Paypal nepodporuje možnost vrácení peněz za zboží (anglicky „refund“), pokud bylo koupeno za virtuální měnu. Je to logické, protože virtuální měny jsou ze své podstaty anonymní a případné vrácení platby by nemusel být spolehlivý důkaz, že hodnotu obdržel konkrétní člověk. Dále je tady fakt, že Paypal zde figuruje jen jako prostředník a nemá přímý přístup k virtuálním penězům. Nicméně tento fakt odrazuje hodně lidí od používání Paypalu pro platby v digitálních měnách, protože zde neposkytuje ochranu kupujícího, pro kterou je jinak ve světě tak oblíbený.

8.3 Hazard

Digitální měny se kromě investičních a obchodních příležitostí používají i ve světě online hazardu. Za zmínku stojí stránka FortuneJack.com, což je plnohodnotné kasíno (poskytující bingo, keno, ruletu, automaty, pokr…), ve kterém se sází jen za Bitcoiny a jiné digitální měny. Další službou stránky je sázení na tzv. binární opce. Jde o finanční operaci, kde si můžeme vsadit na jeden ze dvou (proto název „binární“) možných stavů, jak se bude vyvíjet určitá věc finanční sféry (hodnota akcie, měny atd.). Kurzová hladina je 1,8 x 1,8, což je porovnatelné s kurzovou hladinou ve většině stávkových kanceláří. Vkladové možnosti nejsou omezeny jen na Bitcoiny, vložit sem je možno i Litecoiny, Darkcoiny, Dogecoiny, Peercoiny, Namecoiny, Redds a Novacoiny. Podobné služby dále nabízí stránky: BTCOracle.com, Secondstrade.com, Binarybase.com, Updown.bt, Updownbot.bz. Na obrázku 10 je uvítací stránka služby FortuneJack. [73]



Obr. 19. Ukázka sázení binárních opcí na stránce Fortunajack.com [46]

8.4 Automaty na Bitcoiny

Celosvětově první bankomat na Bitcoiny se objevil v říjnu 2013 v kanadském Vancouveru. V květnu 2014 vybudovala firma Marlyle bankomat na Bitcoiny i v České republice. Nachází se v Praze na Arbesově náměstí. Další bankomaty firma provozuje v Bratislavě a v Berlíně. Celkově je na světě asi 20 bankomatů na Bitcoiny. Do bankomatu se zadá cílová adresa bitcoin peněženky a následně se vloží hotovost. Ta je podle aktuálního kurzu burzy Bitstamp převedena na Bitcoiny a odeslána na adresu. Místo ručního zadání adresy můžeme použít i vestavěnou čtečku QR kódů. Ten nám vygeneruje bitcoin peněženka a jeho otisk můžeme mít uložen v mobilním telefonu, nebo jen na papíře (pokud možno v nepoškozeném stavu). Za využití automatu se platí poplatek 1-5% ze směněné částky. Bankomat je dále schopen podle přání zákazníka uskutečňovat nákup a prodej Bitcoinů na významných burzách. U automatu bylo také otevřeno poradenské centrum, a to za účelem přitáhnout nové uživatele k digitálním měnám. Postupem času firma plánuje poskytovat pojištění proti krádeži Bitcoinů a vybudovat bezpečné úložiště pro Bitcoiny. Pražský bankomat na Bitcoiny je zachycen na obrázku 20. [60], [61], [62]

Obr. 20. Bankomat na Bitcoiny v Praze [63]

8.5 EasyCoin

„EasyCoin“ je služba na nakupování Bitcoinů s využitím poboček České pošty a terminálů Sazky. Služba byla spuštěna v lednu 2015. Zákazník si nejprve na stránce https://easycoin.wbtcb.com zadal hodnotu v korunách, za kterou chtěl Bitcoiny koupit, adresu své bitcoin peněženky a obdržel identifikační číslo platby. Následně se s číslem prokázal na pobočce České pošty, kde zaplatil danou částku a Bitcoiny se mu převedly na bitcoin peněženku. Obdobný postup byl pro využití terminálů Sazky, zákazník si doma vytiskl objednávku s čárovým kódem, kterou následně zaplatil na terminálu Sazky, a transakce byla zrealizována. Služba se dala použít jen pro nákup Bitcoinů. Nicméně nepřešly ani dva měsíce, a služba byla pozastavena. Není ani jasné, zda se její provoz obnoví. [64]

II. PRAKTICKÁ ČÁST

9 VLASTNÍ TĚŽBA BITCOINŮ

Jediný způsob získání Bitcoinů, kromě koupě od jiného uživatele, je jejich těžba. Celý její proces, od nastavení zařízení až po příjem vytěžených Bitcoinů, je popsán v následující kapitole.

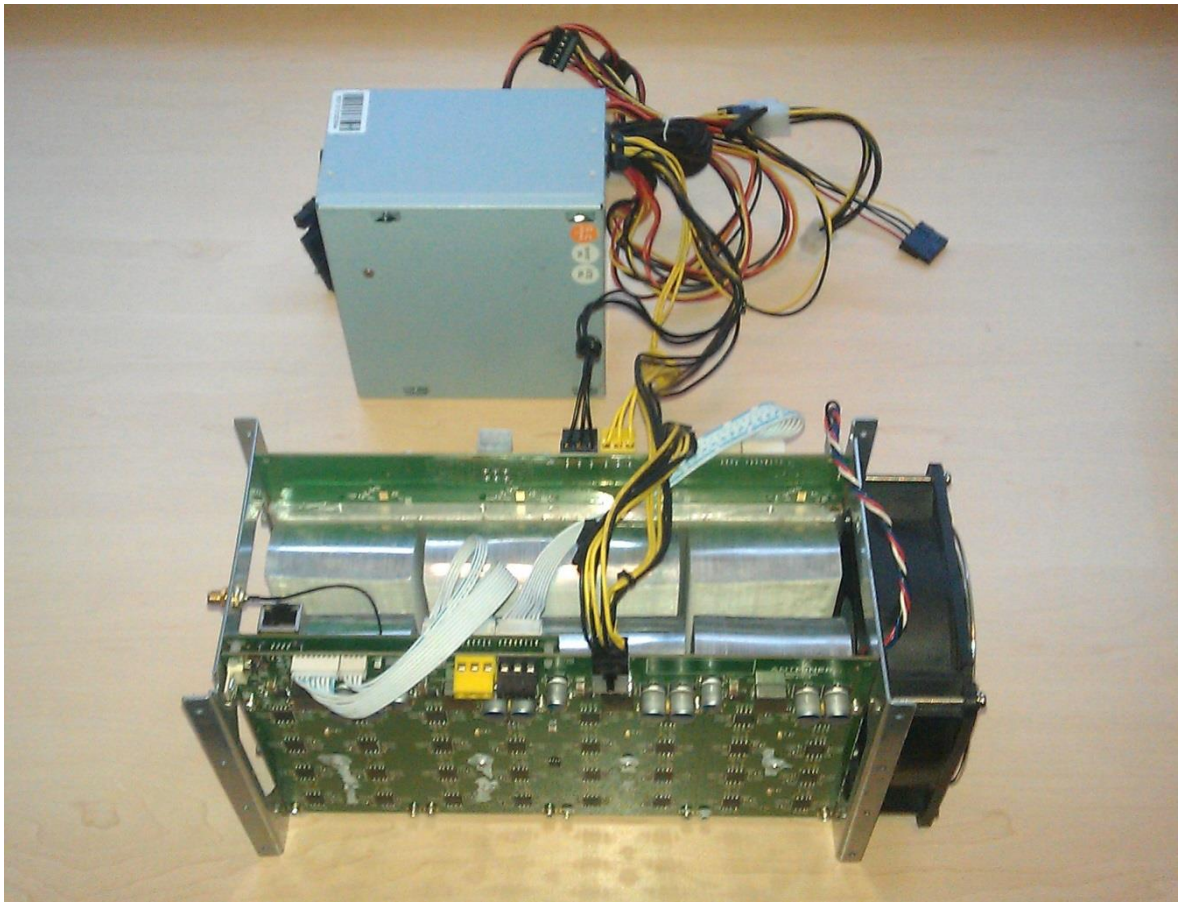
9.1 Příprava

Pro těžbu virtuálních měn potřebujeme kromě samotného těžícího zařízení, konto na některém z poolů, které poskytují „jistotu“ v průběžném získávání malých, ale cenných částí Bitcoinů.

9.1.1 Popis těžícího zařízení

Rozhodl jsem se těžit s ASIC jednotou od firmy Bitman, nazvanou Antminer S1. Jak už název napovídá, miner pochází ze slavné rodiny Antminerů. Jedná se o jejich první počin, který se v době svého vydání (jaro 2014) těšil nevídané popularitě, zejména kvůli svému, na tu dobu vysokému výkonu. Miner disponuje výkonem 180 – 200 GH/s, spotřeba je na hranici 360 W a z toho vychází efektivita kolem 2 W/GH/s. [17]

Zařízení je typu „standalone“, takže se zapojí do elektrické sítě, připojí k internetu pomocí ethernetového kabelu, nebo wi-fi anténou a následně samo těží. Miner má vestavěný silný ventilátor s 3900 otáčkami, který vydává hlučnost asi 40 decibelů, což je asi jako malý vysavač, kvůli tomu je ho vhodné umístit na místo, kde nás nebude případný hluk obtěžovat. Zařízení spolu s externím napájecím zdrojem je zachyceno na obrázku 21.



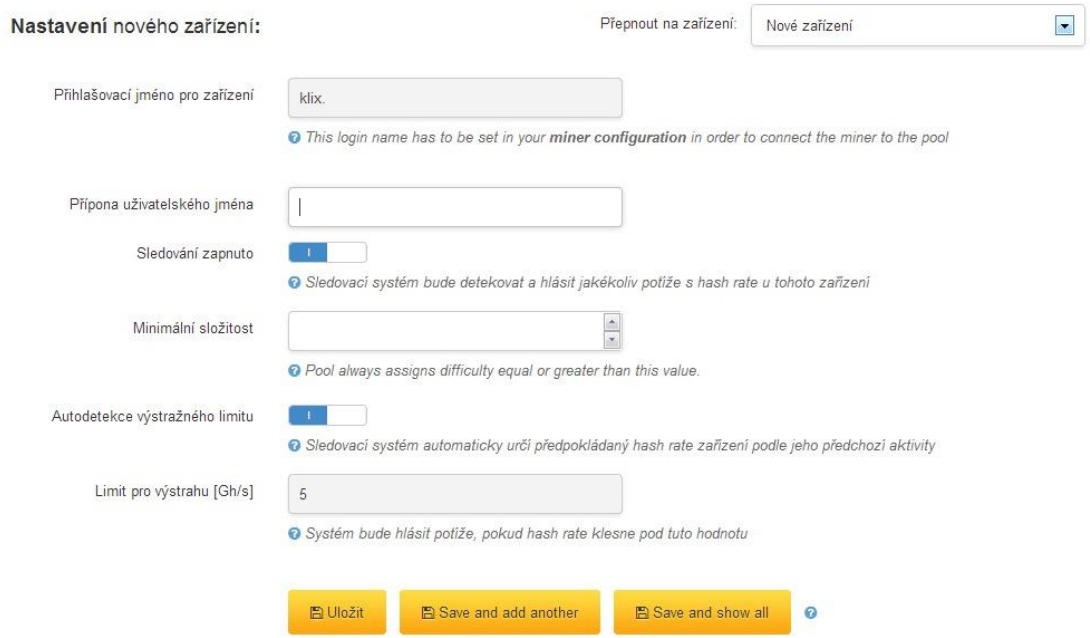
Obr. 21. Vlastní Antminer S1 s napájecím zdrojem

9.1.2 Výběr poolu

Seskupení, v kterých těžaři pracují, se nazývají Pool. Na světě je jich množství, liší se především svým celkovým výkonem a poplatky. Čím je vyšší celkový výkon poolu, tím těžař dostává více menších odměn a naopak, při méně výkonných poolech dostává těžař menší množství hodnotově větších odměn. Celkový výsledek je stejný, vše se odvíjí od výkonu zařízení.

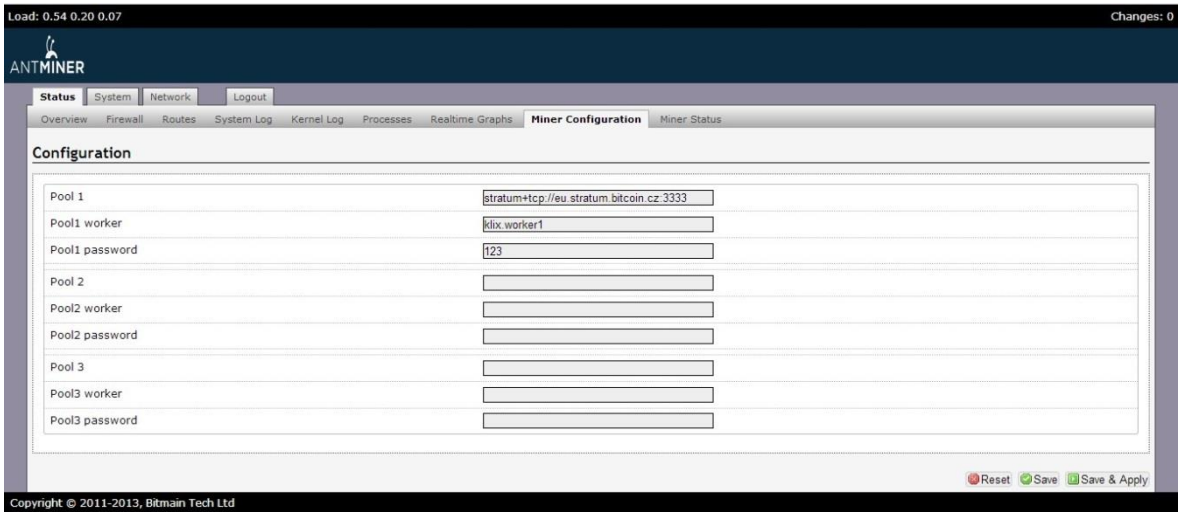
Rozhodl jsem se těžit v asi nejznámějším poolu v České republice, nazvaným „Slush“, který je dostupný na adrese: https://mining.bitcoin.cz/. Průměrný výkon se pohybuje na hranici 16 PH/s a pool si bere 2% z každého vytěženého bloku.

Po samotné registraci si musíme přidat ke kontu svůj miner. Přejdeme na „Můj účet“ → „Zařízení“ → „Přidat zařízení“. K zařízení stačí napsat jen jeho přezdívku a zařízení se nám přiřadí k účtu. Formulář pro zaregistrování nového mineru na účet je zobrazen na obrázku 22.



Obr. 22. Registrace nového těžícího zařízení na svůj účet

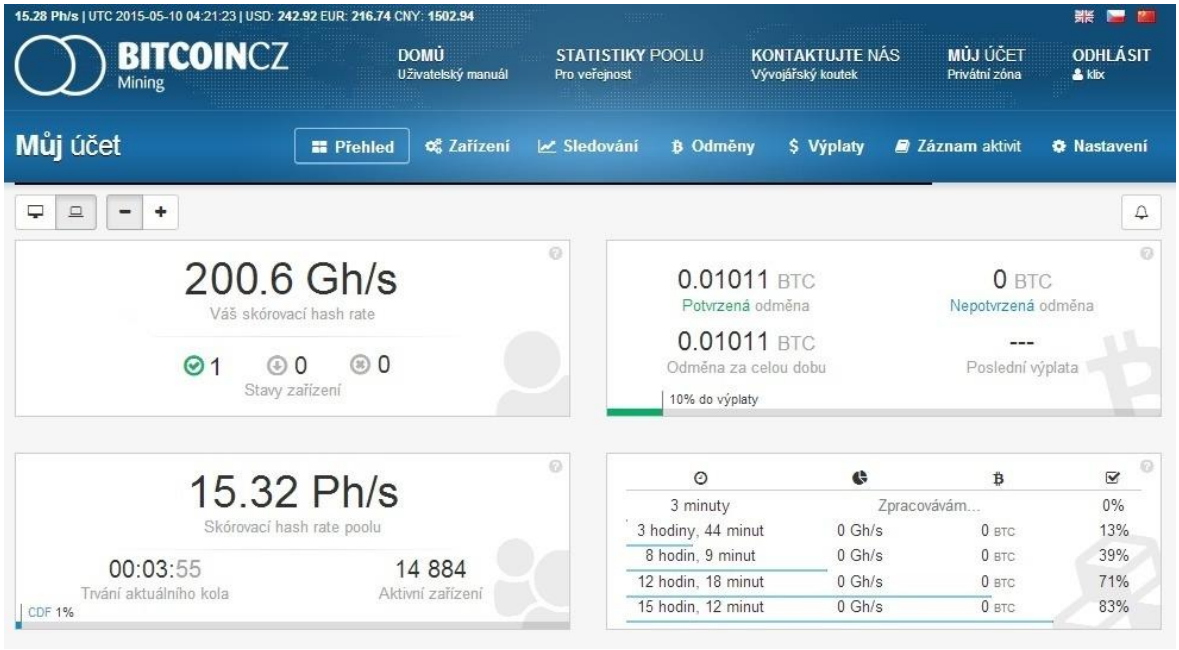
Data z poolu je nyní nutné vložit do těžícího zařízení. Přes IP adresu se dostaneme do konfigurace mineru, kde zadáme těžební adresu, kterou najdeme na poolu (ta je unikátní pro každý pool), dále identifikátor zařízení ve tvaru „uživatelské jméno.jméno zařízení“ a nakonec si zvolíme heslo, nutné k těžení na vlastním účtu (bez vyplnění kterého by se teoreticky mohl cizí těžař připojit na náš účet a těžit v náš prospěch, jenže tahle situace není v praxi možná, protože pokud heslo není vyplněno, pool nepovolí těžbu). Nastavení přihlašovacích údajů do mineru je znázorněno na obrázku 23.



Obr. 23. Nastavení poolu v mineru

9.2 Těžba

Když máme všechno nastaveno, zapneme miner, který sám začne těžit. Po přihlášení na stránce poolu můžeme vidět aktuální rychlost svého zařízení. Mineru trvá asi 1-2 hodiny, než dosáhne úroveň standardního výkonu. Ten si za ideálních podmínek dlouhodobě udržuje. Obrázek 24 zachycuje titulní stránku poolu při vlastním těžení.



Obr. 24. Těžení na poolu

Na kartě „Moje zařízení“ můžeme sledovat detaily vlastního zařízení, můžeme mu třeba nastavit hodnotu pro „Výstražný limit“, v tomto případě nám přijde na email upozornění, pokud průměrný výkon zařízení klesne pod tuto hodnotu.

Možné výkonnostní výkyvy jsou většinou způsobené buď nestabilním připojením k internetu (miner neobdrží všechna data potřebná na hashování), nebo přehříváním (průměrná pracovní teplota mého zařízení je 38ºC, což neznačí žádný problém). [25]

9.2.1 Odměna

Při nalezení nového bloku členem poolu je odměna rozdělena mezi všechny, v ten okamžik aktivní členy, podle vzorce:

$$\text{Odměna} = \text{hodnota bloku} * (1 - \text{poplatek poolu}) * \frac{\text{vlastní hash rate}}{\text{hash rate poolu}} \qquad (1)$$

Hodnota bloku je tvořena aktuálním základem 25 BTC + transakční poplatky z daného bloku. Obě hodnoty hash rate ve vzorci jsou z přesného okamžiku nalezení bloku, průměr-

né hash rate poolu bývá v rozmezí 15 – 16,5 PH/s, v závislosti od výkonu připojených zařízení.

Pokud například hash rate poolu v okamžiku nalezení bloku byl 14,6 PH/s, vlastní hash rate 178 GH/s a hodnota bloku 25,16907748 BTC, po dosazení do předešlého vzorce dostaneme odměnu 0,00030071 BTC.

$$25{,}16907748 * (1 - 0{,}02) * \frac{178}{14600000} = 0{,}00030071 \quad (2)$$

Hodnoty ve vzorci se v průběhu těžení mění s malou odchylkou, proto ve výsledku vždy dostáváme odměny za každý nalezený blok, v přibližné hodnotě 0,0003 BTC.

Při běžném hash rate (zmíněných 15-16,5 PH/s) trvá poolu nalezení nového bloku v průměru 3 až 5 hodin. Z mých dosavadních zkušeností s těžbou, nejrychleji byl blok nalezen za 3 minuty a 40 sekund a naopak nejdelší proces nalezení trval 21 hodin, 30 minut a 34 sekund. Na obrázku 25 vidíme záznam těžby, která probíhala necelé 2 dny.

ID bloku	Blok nalezen v	Trvání	Skórovací hash rate poolu	Váš skórovací hash rate	Vaše odměna	Hodnota bloku	Zbývá potvrzení
23891	2015-04-20 01:52:32	03:29:50	14.62 Ph/s	176.7 Gh/s	0.00029632 BTC	25.01057470 BTC	Potvrzený
23890	2015-04-19 22:22:42	01:11:21	14.97 Ph/s	182.6 Gh/s	0.00030080 BTC	25.15649049 BTC	Potvrzený
23889	2015-04-19 21:11:21	00:34:23	14.33 Ph/s	169.2 Gh/s	0.00029165 BTC	25.20539411 BTC	Potvrzený
23888	2015-04-19 20:36:58	00:03:40	14.41 Ph/s	176.8 Gh/s	0.00030061 BTC	25.01017084 BTC	Potvrzený
23887	2015-04-19 20:33:18	20:03:48	14.60 Ph/s	178.0 Gh/s	0.00030071 BTC	25.16907748 BTC	Potvrzený
23886	2015-04-19 00:29:30	00:32:42	15.51 Ph/s	168.5 Gh/s	0.00026664 BTC	25.05090899 BTC	Potvrzený
23885	2015-04-18 23:56:48	01:49:52	15.84 Ph/s	185.1 Gh/s	0.00028699 BTC	25.07315927 BTC	Potvrzený
23884	2015-04-18 22:06:56	00:14:41	15.54 Ph/s	188.9 Gh/s	0.00029827 BTC	25.04921324 BTC	Potvrzený
23883	2015-04-18 21:52:15	02:43:50	15.64 Ph/s	187.4 Gh/s	0.00029393 BTC	25.04168622 BTC	Potvrzený
23882	2015-04-18 19:08:25	00:31:55	15.11 Ph/s	161.0 Gh/s	0.00026148 BTC	25.04544550 BTC	Potvrzený
23881	2015-04-18 18:36:30	04:40:25	15.30 Ph/s	173.5 Gh/s	0.00027943 BTC	25.15355122 BTC	Potvrzený
23880	2015-04-18 13:56:05	01:20:58	15.72 Ph/s	172.8 Gh/s	0.00027053 BTC	25.11911034 BTC	Potvrzený
23879	2015-04-18 12:35:07	02:18:19	16.40 Ph/s	181.3 Gh/s	0.00027153 BTC	25.06461644 BTC	Potvrzený
23878	2015-04-18 10:16:48	04:17:15	16.18 Ph/s	166.7 Gh/s	0.00025422 BTC	25.16947633 BTC	Potvrzený
23877	2015-04-18 05:59:33	03:53:19	15.34 Ph/s	174.7 Gh/s	0.00027943 BTC	25.03892629 BTC	Potvrzený

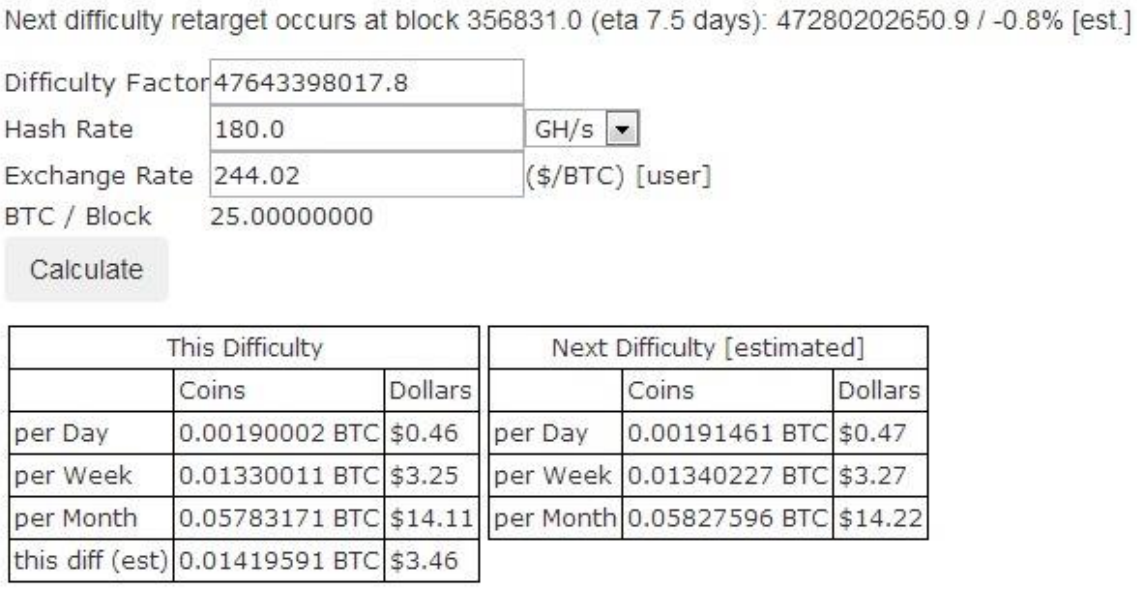
Obr. 25. Záznam těžení

Online kalkulačka

Na výpočet (i možných budoucích) výdělků můžeme použít online kalkulačku na adrese: https://alloscomp.com/bitcoin/calculator.

Do kolonky „Hash rate “ zadáme výkon zařízení a kalkulačka nám na základě aktuální složitosti, kurzu Bitcoinu k americkému dolaru a aktuálního výpočetního výkonu celé Bit-

coin sítě vypočítá přibližnou ziskovost v jednotkách amerických dolarů. Kalkulačka také odhadne změnu ziskovosti v následujícím období, kdy bude upravená obtížnost nalezení nového bloku. Na obrázku 26 vidíme analýzu výdělků z těžby na základě zadaných dat do online kalkulačky.


Next difficulty retarget occurs at block 356831.0 (eta 7.5 days): 47280202650.9 / -0.8% [est.]

Difficulty Factor 47643398017.8
Hash Rate 180.0 GH/s
Exchange Rate 244.02 ($/BTC) [user]
BTC / Block 25.00000000
Calculate

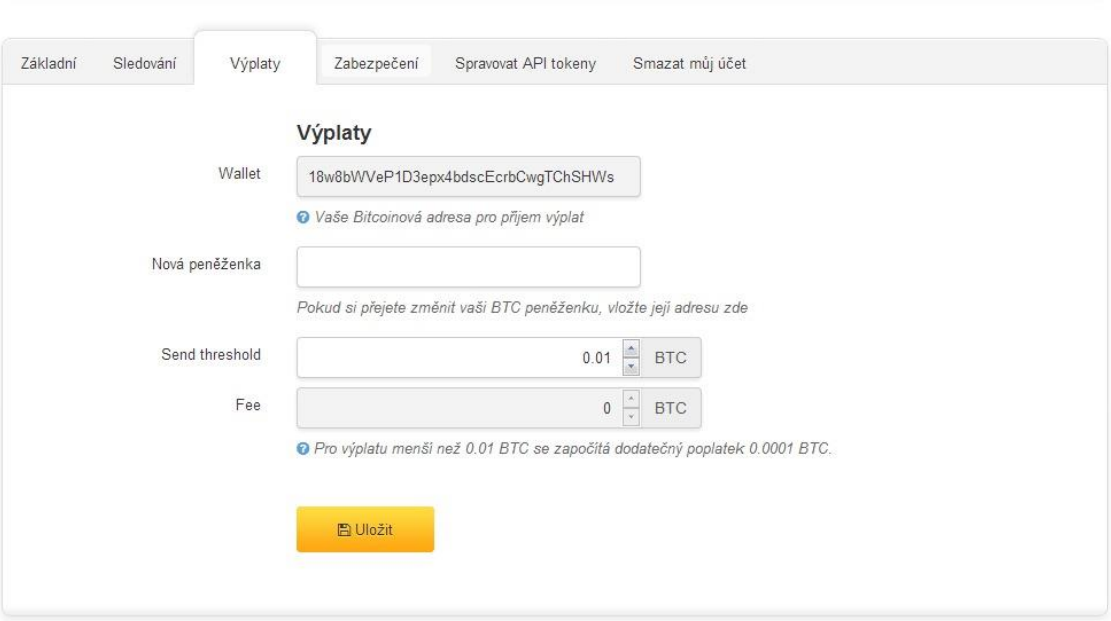
This Difficulty		
	Coins	Dollars
per Day	0.00190002 BTC	$0.46
per Week	0.01330011 BTC	$3.25
per Month	0.05783171 BTC	$14.11
this diff (est)	0.01419591 BTC	$3.46

Next Difficulty [estimated]		
	Coins	Dollars
per Day	0.00191461 BTC	$0.47
per Week	0.01340227 BTC	$3.27
per Month	0.05827596 BTC	$14.22

Obr. 26. Ukázka práce online kalkulačky [56]

9.2.2 Výplata vytěžených Bitcoinů

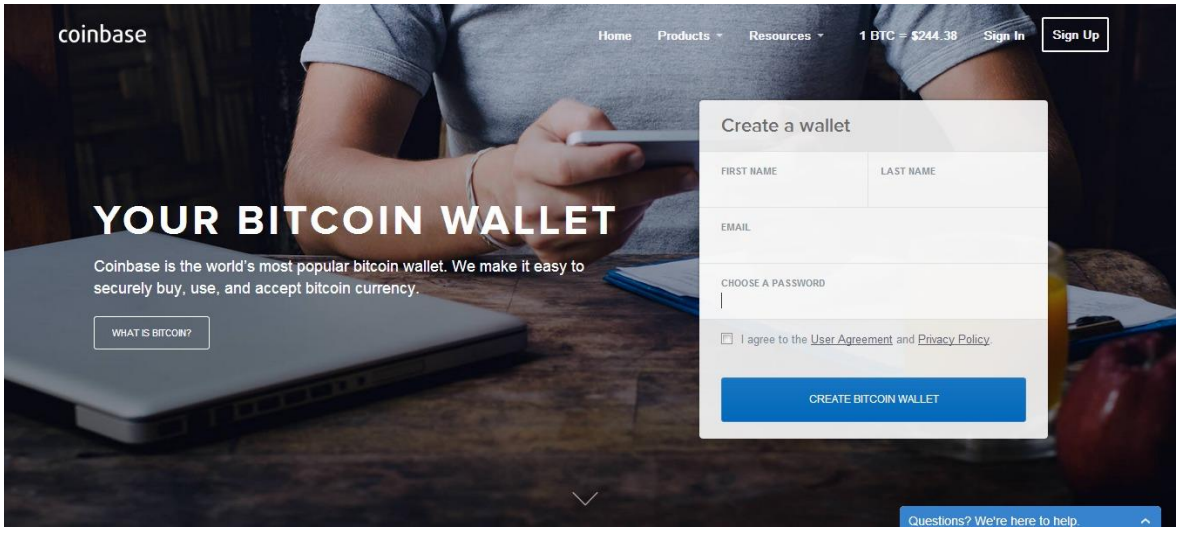
Pokud si chceme své vytěžené Bitcoiny nechat vyplatit na bitcoin peněženku, tak na stránce poolu klikneme na položku „Nastavení“, přejdeme na kartu „Vyplatit“, kde vyplníme svou bitcoin adresu a do kolonky „Send Treshold“ napíšeme sumu, kterou chceme vyplatit. Proces završíme kliknutím na tlačítko „Uložit“. Tím je požadavek na výplatu evidován v systému a zhruba do hodiny je nám platba odečtena z účtu a poslána na zadanou bitcoin adresu. Na obrázku 27 je znázorněn výběr Bitcoinů z poolu na bitcoin peněženku.



Obr. 27. Vyplnění požadavku na výplatu

9.2.3 Alokování měny na bitcoin peněžence

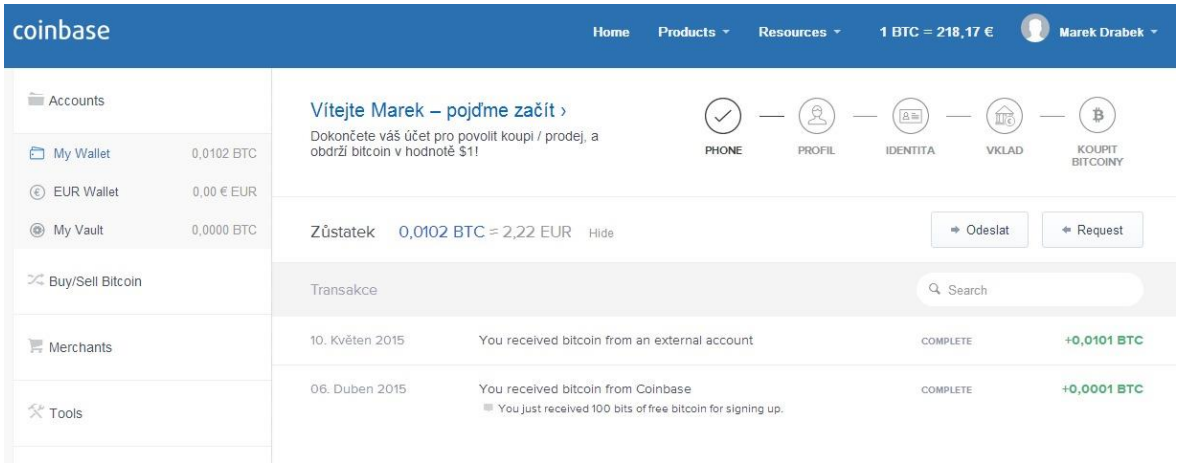
Pro příjem plateb v Bitcoinech slouží bitcoin peněženka. Zvolil jsem online peněženku „Coinbase“, dostupnou na adrese: https://www.coinbase.com/. Titulní stránka peněženky je zachycena na obrázku 28.



Obr. 28. Titulní stránka peněženky Coinbase [57]

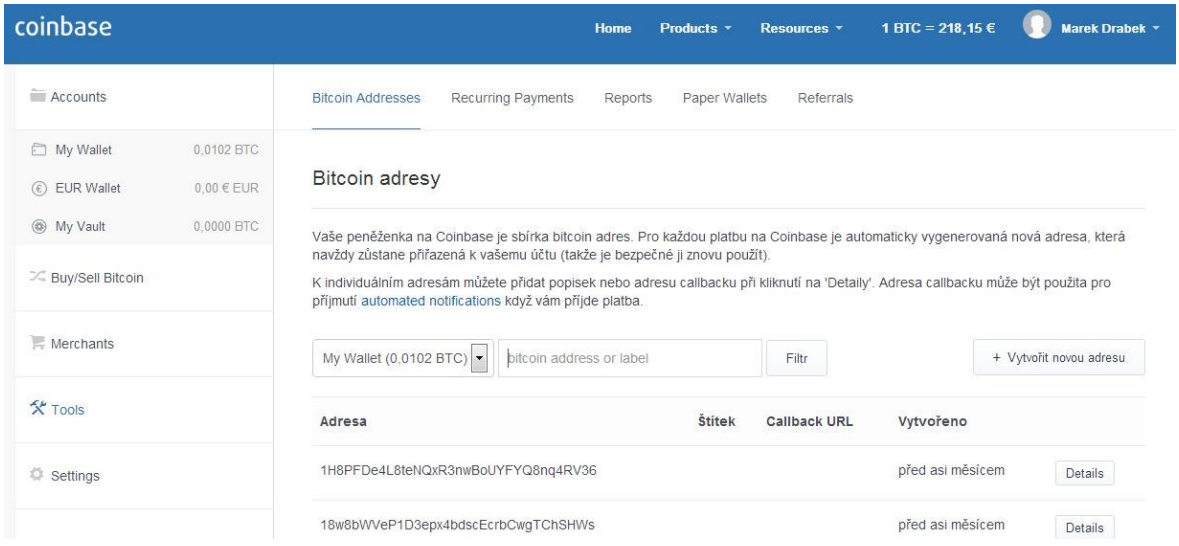
Používání peněženky není složité, po přihlášení do konta vidíme v hlavním okně svůj zůstatek a seznam nedávných plateb. Na obrázku 29vidíme stav konta, konkrétně dvě obdržené platby, první je v hodnotě 0,001 BTC, tuhle platbu dává peněženka každému za regis-

traci. Druhá platba, v hodnotě 0,0101 BTC je z poolu Slush, kterou jsme si nechali poslat v předcházející kapitole.



Obr. 29. Stav konta na peněžence Coinbase

V peněžence si můžeme generovat vlastní bitcoin adresy pro příjem budoucích plateb a propagaci na internetu. V sekci „Tools“ přejdeme na kartu „Bitcoin Addresses“ a klikneme na tlačítko „Vytvořit novou adresu“. Ukázku generování nových bitcoin adres vidíme na obrázku 30.



Obr. 30. Generování bitcoin adres na peněžence Coinbase

9.2.4 Spotřeba energie a náklady

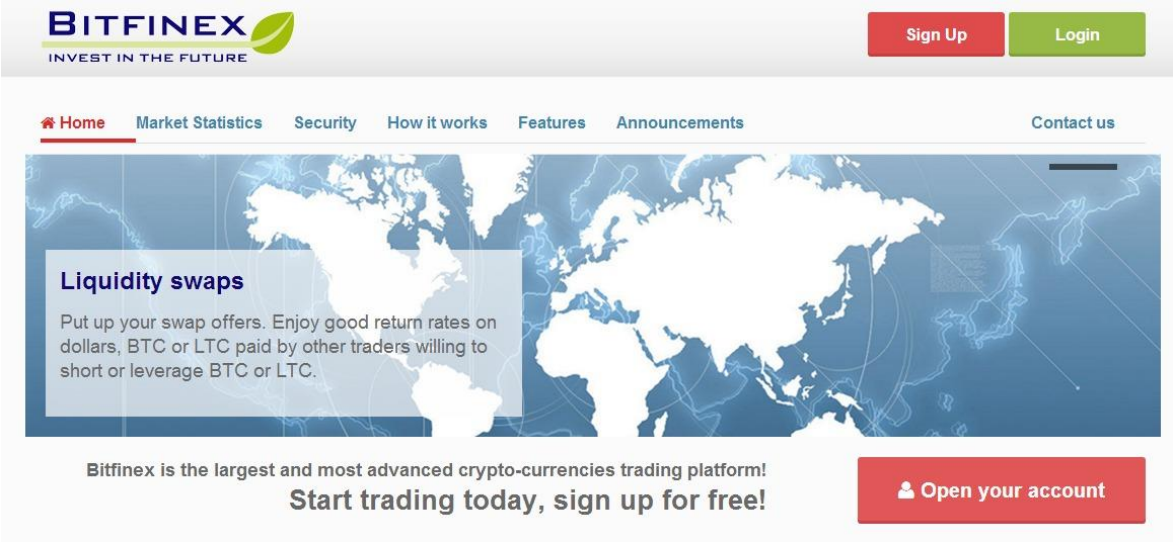
V podmínkách panelového domu není těžba na Antmineru S1 dnes už rentabilní. Vzhledem ke svému příkonu 360 W, za jeden měsíc nepřetržitého provozu, miner spotřebuje

elektrickou energii za cca 715,4 Kč. Na druhou stranu, při průměrném výkonu 180 GH/s vytvoří, podle výše zmíněné kalkulačky, Bitcoiny v hodnotě asi 346,5 Kč (14,06 $).

Z toho je patrné, že zařízení si nevydělá ani samo na svůj chod, konkrétně vyprodukuje 48,4% prostředků, které jsou potřeba, pro jeho činnost. Pro domácí použití je dnes potřeba těžící zařízení, které je minimálně ekvivalentem Antmineru S3 (výkon 440GH/s, spotřeba 366 W), který za měsíc po odečtení nákladů vydělá cca 87 Kč.

10 OBCHODOVÁNÍ NA BURZE

Na obchodování s Bitcoiny jsem si vybral burzu Bitfinex, která je dostupná na adrese: https://www.bitfinex.com/.Na obrázku 31 vidíme náhled uvítací stránky.



Obr. 31. Uvítací stránka burzy Bitfinex [58]

10.1 Vklad na účet

Po otevření účtu jsem provedl vklad v Bitcoinech. Připsání trvalo asi jednu hodinu od zadání transakce. Burza podporuje vklady v amerických dolarech, Bicoinech a Litlecoinech. Americké dolary přijímá ve formě mezinárodního bankovního převodu a poplatek za vložení činí 0,1% z vkladu (minimum však 20$), vklady přes Bitcoiny a Litecoiny jsou zdarma. Burza poskytuje možnost mít samostatný účet na každou z vložených měn. Na obrázku 32 vidíme rozdělení účtu pro americké dolary a Bitcoiny.

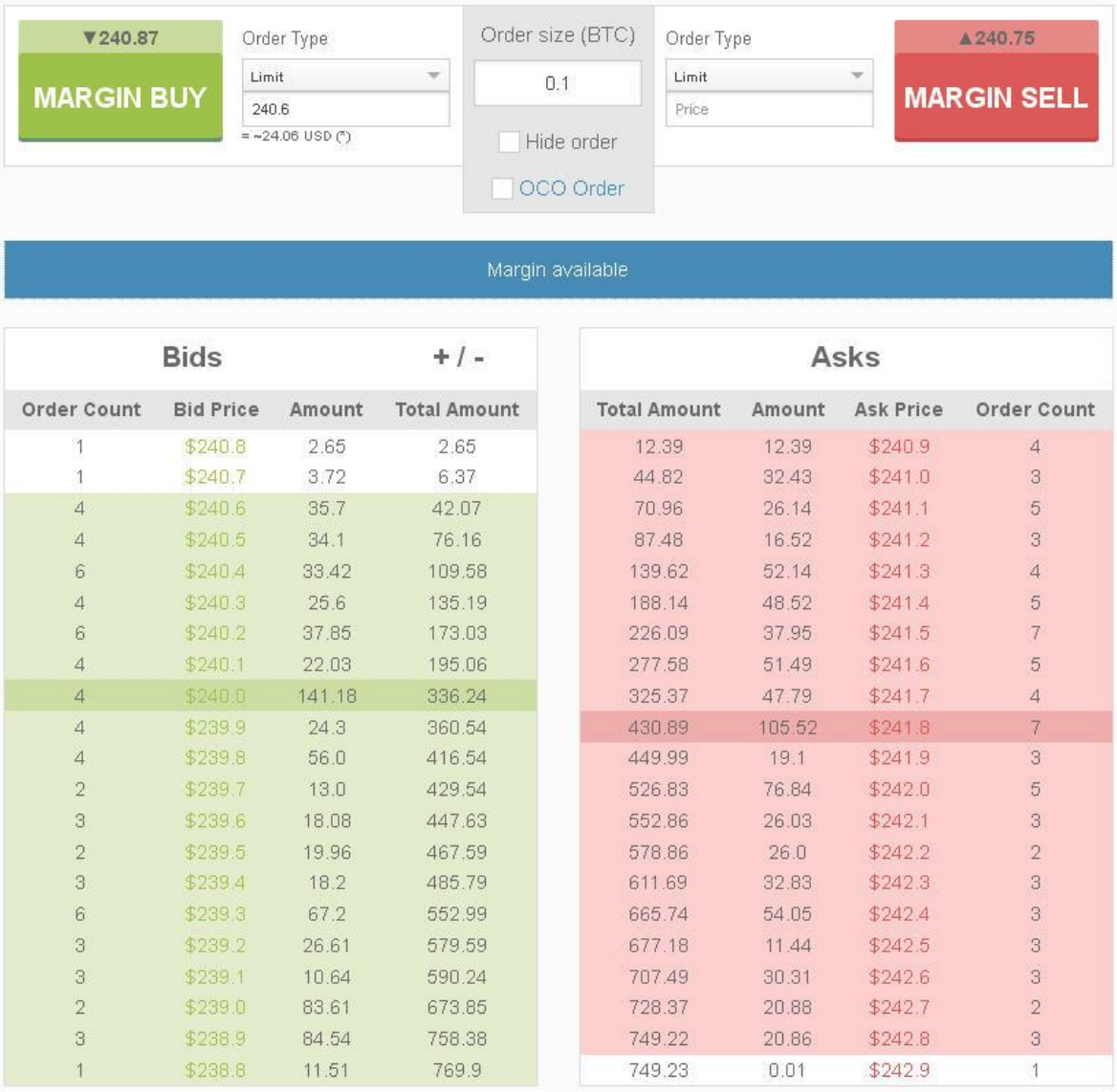
YOUR BALANCE		$651.82	
trading	deposit	exchange	Total
596.83 USD	0.00 USD	1.00 USD	**597.82 USD**
0.17 BTC	0.00 BTC	0.05 BTC	**0.22 BTC**

Obr. 32. Stav účtu

10.2 Operace s poptávkou a nabídkou

Principem každé burzy je obchodování dvou stran, prodejce a kupujícího. Prodejce nabízí množství nějaké hodnoty za určitou cenu a kupující hledá nejpříznivější cenu pro svůj hledaný produkt. Na burze se člověk stává jak prodejcem, tak kupujícím.

Aktuální poptávku a nabídku po Bitcoinech najdeme v sekci „Margin available“ a zvolíme „BTC“. Řádky, které jsou zvýrazněné, představují operace s větším počtem Bitcoinů. Na obrázku 33 vidíme cenovou nabídku a poptávku po Bitcoinech v amerických dolarech, ze dne 10.5.2015.



Obr. 33. Poptávka a nabídka po Bitcoinech

Obrázku 33obsahuje zelený sloupec s názvem „Bids“ pro poptávku a červený „Asks“ pro nabídku. Význam jednotlivých položek:

Sloupec Bids

Order count: počet příkazů lidí, kterých poptávka je v jedné cenové kategorii

Bid price: poptávaná cena za 1 jednotku artiklu

Amount: množství BTC poptávaného za danou cenu

Total Amount: vyjadřuje kolik BTC je v příkazech před tímhle celkem

Sloupec Asks

Total Amount: vyjadřuje kolik BTC je v příkazech před tímhle celkem

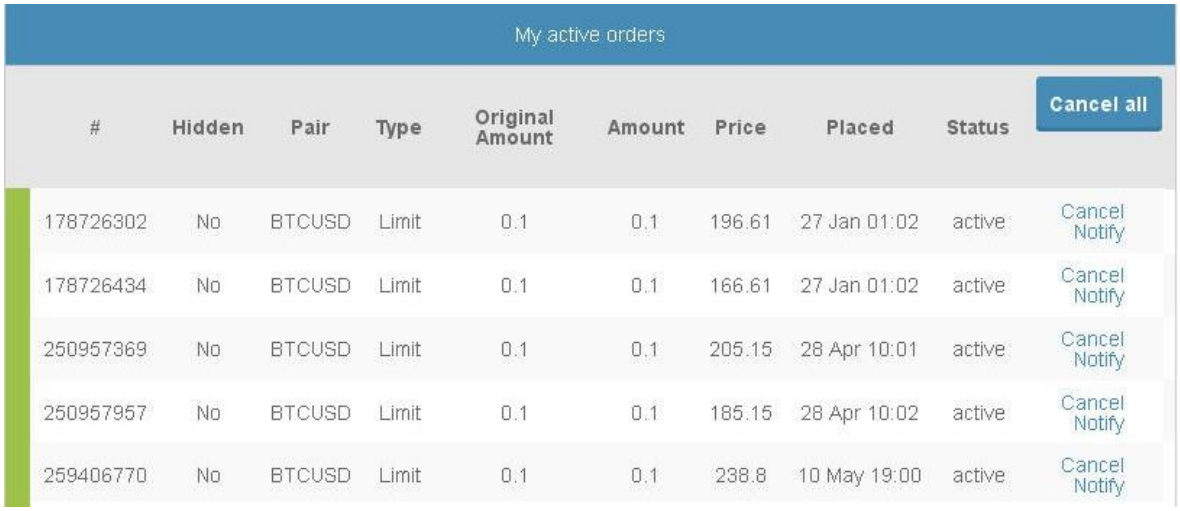
Amount: množství BTC nabízeného za danou cenu

Ask price: požadovaná cena za 1 BTC

Order count: počet příkazů lidí, kterých poptávka je v jedné cenové kategorii

10.3 Vytvoření vlastní nabídky a poptávky

Poptávku vytvoříme napsáním poptávané hodnoty do „Margin Buy“ a v „Order size“ zadáme počet jednotek. Vznikne nám poptávka, kterou vidí všichni účastníci burzy. Pokud jiný účastník souhlasí s cenou a koupí od nás artikl, suma na účtu se nám hned aktualizuje v závislosti od vzniklého obchodu. Na obrázku 34 je znázorněna vytvořená poptávka po Bitcoinech v hodnotě amerických dolarů, například v posledním řádku poptávám 0,1 BTC za 23,88$ (238,8$ je hodnota za 1 kus).

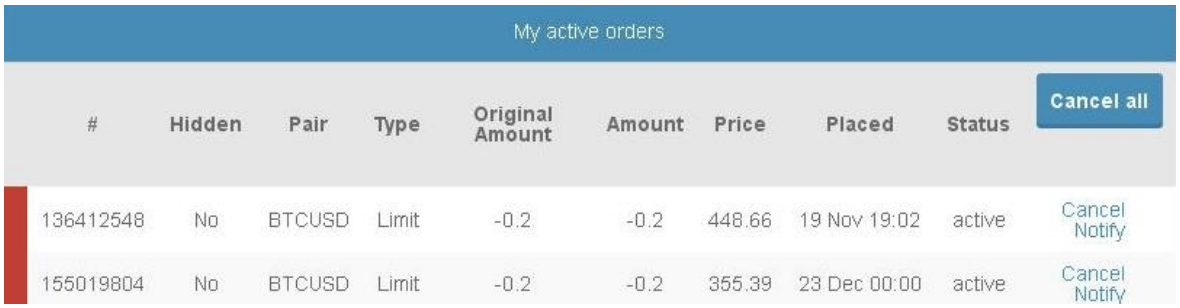


My active orders

#	Hidden	Pair	Type	Original Amount	Amount	Price	Placed	Status	Cancel all
178726302	No	BTCUSD	Limit	0.1	0.1	196.61	27 Jan 01:02	active	Cancel Notify
178726434	No	BTCUSD	Limit	0.1	0.1	166.61	27 Jan 01:02	active	Cancel Notify
250957369	No	BTCUSD	Limit	0.1	0.1	205.15	28 Apr 10:01	active	Cancel Notify
250957957	No	BTCUSD	Limit	0.1	0.1	185.15	28 Apr 10:02	active	Cancel Notify
259406770	No	BTCUSD	Limit	0.1	0.1	238.8	10 May 19:00	active	Cancel Notify

Obr. 34. Poptávka po Bitcoinech

Obdobná pravidla platí pro vytvoření nabídky, jen místo do „Margin buy“ se nabízená hodnota zadá do „Margin sell“. Na obrázku 35 je znázorněna vytvořená nabídka po Bitcoinech, opět v hodnotě amerických dolarů, konkrétně v posledním řádku nabízím 0,2 BTC za 71,078$ (hodnota 355,39 platí pro 1 BTC)



My active orders

#	Hidden	Pair	Type	Original Amount	Amount	Price	Placed	Status	Cancel all
136412548	No	BTCUSD	Limit	-0.2	-0.2	448.66	19 Nov 19:02	active	Cancel Notify
155019804	No	BTCUSD	Limit	-0.2	-0.2	355.39	23 Dec 00:00	active	Cancel Notify

Obr. 35. Nabídka Bitcoinů

Z jednotlivých obchodů se strhávají poplatky, které jsou počítány z celého objemu dané platby. Čím uskutečníme více obchodů, tím menší platíme jednotlivé poplatky. Jejich výši vidíme v tabulce7.

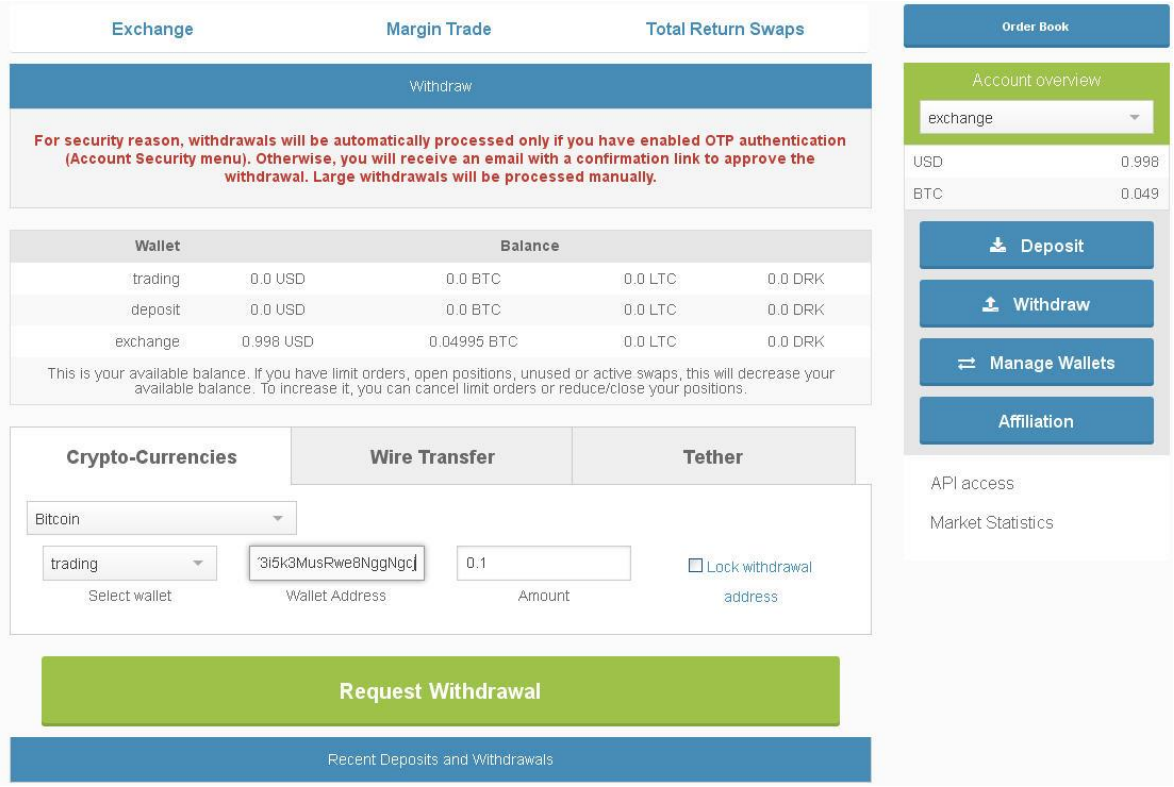
Tab.7. Poplatky za obchody [59]

Executed in the last 30 days (BTC)	Maker fees	Taker fees
0 or more traded	0,01%	0,2%
500 or more traded	0,08%	0,2%
2000 or more traded	0,06%	0,2%
5000 or more traded	0,04%	0,2%

15 000 or more traded	0,02%	0,2%
25 000 or more traded	0,0%	0,2%

10.4 Výběr z účtu

Pro výběry z účtu platí ty samé možnosti a poplatky jako pro vklady, tj. ve formě každé ze tří měn, u amerického dolaru je to s poplatkem. Výběr z účtu na bitcoin peněženku je znázorněn na obrázku 37.



Obr. 36. Požadavek na výběr z účtu

ZÁVĚR

Investice do Bitcoinu se zdají velmi lákavé, jeho raketový nárůst hodnoty učinil z hodně lidí zbohatlíky. Nicméně kurz Bitcoinu je stále velmi vrtkavý, ze ziskového investování na burze se může v krátkém časovém horizontu stát noční můra, ze které se můžou jednotliví investoři dlouho vzpamatovávat. Investice do těžících zařízení se může zdát jako mnohem větší jistota z ohledu návratnosti prostředků, avšak nic v téhle sféře není černobílé. Z porovnání vyplývá, že k ziskovému těžení Bitcoinů potřebujeme na jedné straně hardware za desítky tisíc korun a na straně druhé přijatelnou situaci na burze, která zachová hodnotný kurz Bitcoinu (ideálně ne příliš nižší, než je aktuálně).

Bitcoin můžeme využit i bez účelu zisku, jen třeba jako alternativní formu uložení svých peněz. Oproti zmíněným nevýhodám, které spočívají především v jeho nestálém kurzu a „neověřené“ komunitě, která ho spravuje. Z mnoha ohledů je výhoda, že měnu nevlastní stát a nespadají na ni jeho regulace a daně (až na Německo, kde je uznána jako oficiální virtuální měna). Samozřejmě mince má i druhou stranu a kromě lidí, co chtějí mít své peníze jen „nedotknutelné“ do budoucna, jsou zde i podvodníci a zločinci, využívající anonymity virtuálních měn pro nezákonné činnosti. V jedné skupině jsou ti míň „nebezpeční“, využívající virtuální měny na uchování hodnot svých peněz, se kterými by jinak manipuloval stát (konfiskace majetku, alimenty atd) a další skupinu tvoří obchodníci s drogami, zbraněmi, bílým masem, pedofilové atd, kterým dovolují virtuální měny vysoký stupeň anonymity při svých převodech finančních prostředků.

Jedním z budoucích scénářů je ten, kdy se svět diferencuje na státy, které budou konkrétní virtuální měny akceptovat, a které ne (třeba Rusko má už dnes k Bitcoinu velmi negativní postoj). Celkový potenciál Bitcoinu, jako alternativní měny, stále roste a je jen na lidech samotných, jak jej budou využívat.

SEZNAM POUŽITÉ LITERATURY

[1] Co je Bitcoin a jak funguje?. In: Bitcoinman [online]. [cit. 2014-11-30]. Dostupné z: http://bitcoinman.cz/

[2] Co je to Bitcoin?. Bitcoincz [online]. 2013 [cit. 2014-11-30]. Dostupné z: http://blog.bitcoin.cz/co-je-to-bitcoin/

[3] Satoshi Nakamoto - muž, ktorý vytvoril bitcoin?. Benoow [online]. 2014 [cit. 2014-11-30]. Dostupné z: http://www.benoow.sk/cz/section?id_message=5296&do=changeLang

[4] Údajný zakladatel Bitcoinů dělal tajnou práci pro americké vojáky. Ac24 [online]. 2014 [cit.2014-11-30]. Dostupné z: http://www.ac24.cz/zpravy-ze-sveta/3616-udajny-zakladatel-bitcoinu-delal-tajnou-praci-pro-americke-vojaky

[5] Těžba Bitcoinů / Mining. Bitcoinman [online]. [cit. 2014-11-30]. Dostupné z: http://bitcoinman.cz/index.php?c=tezeni-mining-bitcoinu-jak-vznika

[6] O co jde. Forexsrovnavac [online]. 2014 [cit. 2014-11-30]. Dostupné z: http://www.forexsrovnavac.cz/bitcoin

[7] Bitcoin – od počátků po případ MtGox. Investujeme.cz [online]. 2014 [cit. 2014-11-30]. Dostupné z: http://www.investujeme.cz/bitcoin-undefined-od-pocatku-po-pripad-mtgox/

[8] Kto potrebuje Bitcoin? Čo tak iné virtuálne meny jako alternatívy. Financnytrh.com [online]. 2014 [cit. 2014-11-30]. Dostupné z: http://www.financnytrh.com/kto-potrebuje-bitcoin-co-tak-ine-virtualne-meny-ako-alternativy/a15589

[9] Bitcoin a jiné kryptoměny: Co potřebujete vědět o zabezpečení vaší digitální měny? Euro Zprávy [online]. 2014 [cit. 2015-05-20]. Dostupné z: http://ekonomika.eurozpravy.cz/ceska-republika/89740-bitcoin-a-jine-kryptomeny-co-potrebujete-vedet-o-zabezpeceni-vasi-digitalni-meny/

[10] Bitcoin pod lupou, časť 1/2. PC.sk [online]. 2013 [cit. 2015-05-19]. Dostupné z: http://pc.zoznam.sk/bitcoin-pod-lupou-cast-12

[11] Bitcoin pod lupou, časť 1/2. PC.sk [online]. 2013 [cit. 2015-05-19]. Dostupné z: http://pc.zoznam.sk/bitcoin-pod-lupou-cast-12?page=3

[12] Hashovací funkce. Kryptografie [online]. [cit. 2015-05-19]. Dostupné z: http://www.kryptografie.wz.cz/data/hash2.htm

[13] On theSecure Hash Algorithm family. Staff Science [online]. 2008 [cit. 2015-05-19]. Dostupné z:http://www.staff.science.uu.nl/~werkh108/docs/study/Y5_07_08/infocry/project/Cryp08.pdf

[14] Těžba Bitcoinů / Mining. Bitcoinman [online]. [cit. 2015-05-19]. Dostupné z: http://www.bitcoinman.cz/index.php?c=tezeni-mining-bitcoinu-jak-vznika

[15] Difficulty. Bitcoin wiki [online]. 2014 [cit. 2015-05-19]. Dostupné z: https://en.bitcoin.it/wiki/Difficulty

[16] Bitcoin pod lupou, časť 2/2. PC.sk [online]. 2013 [cit. 2015-05-19]. Dostupné z: http://pc.zoznam.sk/bitcoin-pod-lupou-cast-22?page=1

[17] AntMiner S1 (MOQ: 2 units). Bitmain [online]. [cit. 2015-05-19]. Dostupné z:https://www.bitmaintech.com/productDetail.htm?pid=000201401071627479 92Ce5uBuxW06D6

[18] Bitcoin peňaženka. Bitcoiny.Sk [online]. 2013 [cit. 2015-05-19]. Dostupné z:http://bitcoinysk.wix.com/home#!penazenka/c1nke

[19] Real-timestats. Bitcoin Block Explorer [online]. [cit. 2015-05-19]. Dostupné z: https://blockexplorer.com/q

[20] Review: Antminer S3 450 gh/s Bitcoin ASIC Miner By Bitmain. Cryptocoinsnews [online]. 2014 [cit. 2015-05-19]. Dostupné z: https://www.cryptocoinsnews.com/review-antminer-s3-450-ghs-bitcoin-asic-miner-bitmain/

[21] AntMiner S2 1TH/s Miner (1w/GH/s) Batch 1 - Sold Out. Bitmain [online]. 2013 [cit. 2015-05-19]. Dostupné z:https://bitmaintech.com/productDetail.htm?pid=000201403141354465 10cxXNeYAy06E5

[22] ANTMINER S5 BATCH 5. Bitmain [online]. [cit. 2015-05-19]. Dostupné z: https://www.bitmaintech.com/productDetail.htm?pid=000201503030950187 16e2uWKIA70662

[23] Těžba bitcoinů je spojena s velkou spotřebou elektřiny. Novinky.cz [online]. 2014 [cit. 2015-05-19]. Dostupné z:http://www.novinky.cz/internet-a-pc/324458-tezba-bitcoinu-je-spojena-s-velkou-spotrebou-elektriny.html

[24] Spotřeba elektřiny BTC sítě. Bitcoined [online]. 2014 [cit. 2015-05-20]. Dostupné z: http://www.bitcoined.cz/spotreba-elektriny-btc-site/

[25] Odborná terminologie. Bitcoin.cz [online]. [cit. 2015-05-19]. Dostupné z: https://mining.bitcoin.cz/user-manual/terminology/

[26] Rozdíly mezi symetrickou a asymetrickou šifrou. Fi.muni [online]. [cit. 2015-05-19]. Dostupné z:http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm#_Rozdíly_mezi_symetrickou_a asymetri

[27] Base64. Base64 [online]. [cit. 2015-05-20]. Dostupné z: https://www.base64decode.org/

[28] ECDsa – třída. Microsoft [online]. 2015 [cit. 2015-05-19]. Dostupné z: https://msdn.microsoft.com/cs-cz/library/system.security.cryptography.ecdsa(v=vs.110).aspx

[29] Bitcoin pod lupou, časť 1/2. PC zoznam [online]. 2013 [cit. 2015-05-20]. Dostupné z: http://pc.zoznam.sk/bitcoin-pod-lupou-cast-12?page=2

[30] RIPEMD-160. EHash [online]. 2008 [cit. 2015-05-19]. Dostupné z: http://ehash.iaik.tugraz.at/wiki/RIPEMD-160

[31] There's a new crypto currency coming, and it'sbacked by gold. Business Insider [online]. 2015 [cit. 2015-05-19]. Dostupné z: http://www.businessinsider.com/hayek-cryptocurrency-backed-by-gold-2015-5#ixzz3ZzoABnoD

[32] Bojí se ČR bitcoinu? Apogeo [online]. 2015 [cit. 2015-05-19]. Dostupné z: http://www.apogeo.cz/aktuality/boji-se-cr-bitcoinu-1241/

[33] Mining.bitcoin.cz [online]. 2009 [cit. 2015-05-19]. Dostupné z: https://mining.bitcoin.cz

[34] Podvod, nebo revoluce? Euro [online]. 2013 [cit. 2015-05-19]. Dostupné z: http://euro.e15.cz/archiv/podvod-nebo-revoluce-1028685

[35] Decentralizovaná kryptoměna Bitcoin. ABC Linuxu [online]. 2015 [cit. 2015-05-19]. Dostupné z:http://www.abclinuxu.cz/clanky/decentralizovana-kryptomena-bitcoin#double-spending

[36] ANTMINER S4 -B1 SOLD OUT. Bitmain [online]. [cit. 2015-05-19]. Dostupné z: https://bitmaintech.com/productDetail.htm?pid=00020140916100720380cS1tRWd00684

[37] Mining Bitcoin forFun and (BasicalyNo) Profit: Part 1: Introduction. Famicoman [online]. 2013 [cit. 2015-05-19]. Dostupné z: http://famicoman.com/wp-content/uploads/2013/09/egold-300x193.gif

[38] Liberty Reserve Closed, Owners Get Arrestedfor Money Laundry. Parsherald [online]. 2013 [cit. 2015-05-19]. Dostupné z:http://parsherald.com/wp-content/uploads/2013/05/Liberty-Reserve-Closed-Owners-Get-Arrested-for-Money-Laundry1.jpg

[39] Kto potrebuje Bitcoin? Čo tak iné virtuálne meny ako alternatívy. Finančný trh [online]. 2014 [cit. 2015-05-19]. Dostupné z: http://www.financnytrh.com/ias/profile2_articles/2014_clanky/Kto_potrebuje_Bitcoin_Co_tak_ine_virtualne_meny_ako_alternativy_Litecoin.jpg

[40] Why Peercoin? Peercoin [online]. [cit. 2015-05-19]. Dostupné z: http://peercoin.net/assets/img/logos/logo.png

[41] Crypto Currency. NFC Cash World [online]. 2014 [cit. 2015-05-19]. Dostupné z:http://www.nfccw.com/img/portfolio/ripplecoin.png

[42] Kto potrebuje Bitcoin? Čo tak iné virtuálne meny jako alternatívy. Finančný trh [online]. 2014 [cit. 2015-05-19]. Dostupné z:http://www.financnytrh.com/ias/profile2_articles/2014_clanky/Kto_potrebuje_Bitcoin_Co_tak_ine_virtualne_meny_ako_alternativy_OPenCoin.jpg

[43] Bitcoin Logo Psd. Logo Kid [online]. [cit. 2015-05-19]. Dostupné z: http://logo-kid.com/bitcoin-logo-psd.htm

[44] PayPal considering including Bitcoin. PC Techmag [online]. [cit. 2015-05-19]. Dostupné z:http://pctechmag.com/2013/04/paypal-considering-including-bitcoin/

[45] The Great He-Said, She-Said Game of theTrue Bitcoin Creator. Mashable [online]. 2014 [cit. 2015-05-19]. Dostupné z:http://mashable.com/2014/03/07/dorian-nakamoto-satoshi-nakamoto/

[46] Binary Trader. Gyazo [online]. [cit. 2015-05-19]. Dostupné z: http://gyazo.com/a15927203856052fcf122061054d389d.pngtext

[47] ASIC miner. Samkear [online]. [cit. 2015-05-19]. Dostupné z: http://samkear.com/wp-content/uploads/2013/08/ASICMiner-USB-Block-Erupter.jpg

[48] ROCKMINER PRISMA 1.4T~1.45TH/S WITH 1100W BTC ASIC MINER. Minereu [online]. [cit. 2015-05-19]. Dostupné z:http://cdn.shopify.com/s/files/1/0667/4297/products/P1_large.jpg?v=1415701746

[49] Antminer s1. Cryptolayaway [online]. [cit. 2015-05-19]. Dostupné z: http://cryptolayaway.com/wp/wp-content/uploads/2015/04/minero-bitcoin-bitmain-antminer-s1-180ghs-mineria-on-hand-13524-MLA20078901894_042014-F.jpg

[50] Bitcoin Forum. Bitcointalk [online]. [cit. 2015-05-19]. Dostupné z: https://ip.bitcointalk.org/?u=https%3A%2F%2Ffarm8.staticflickr.com%2F7178%2F13894570891_d58d6d4be0_c.jpg&t=552&c=1yhtNUceAV_TVw

[51] ANTMINER S3 -B5 SOLD OUT. Bitmain [online]. [cit. 2015-05-19]. Dostupné z: https://bitmaintech.com/productDetail.htm?pid=00020140630025130637RV8OhOwt06BC

[52] ANTMINER S4 -B1 SOLD OUT. Bitmain [online]. [cit. 2015-05-19]. Dostupné z:https://bitmaintech.com/userfiles/image/003201409251143517l2BbAXDYnD067F.jpg

[53] Selling. Amazon [online]. 1994 [cit. 2015-05-19]. Dostupné z: http://ecx.images-amazon.com/images/I/81ZKOGHf0aL._SX466_.jpg

[54] Bitcoin kurz. Bitcoin kurz [online]. [cit. 2015-05-19]. Dostupné z: http://www.bitcoin-kurz.cz/

[55] Bitcoin Price. Pando Daily [online]. [cit. 2015-05-19]. Dostupné z: http://pandodaily.files.wordpress.com/2014/05/bitcoin-8-month-cycles.jpg?w=1022&h=770

[56] Bitcoin Mining Calculator. Alloscomp [online]. 2014 [cit. 2015-05-19]. Dostupné z: https://alloscomp.com/bitcoin/calculator

[57] Coinbase [online]. 2012 [cit. 2015-05-19]. Dostupné z: https://www.coinbase.com/

[58] Bitfinex [online]. 2013 [cit. 2015-05-19]. Dostupné z: https://www.bitfinex.com/

[59] Fees schedule. Bitfinex [online]. 2013 [cit. 2015-05-19]. Dostupné z: https://www.bitfinex.com/pages/fees

[60] V Praze začal fungovat první bankomat. E15 [online]. 2014 [cit. 2015-05-19]. Dostupné z: V Praze začal fungovat první bankomat Více na: http://zpravy.e15.cz/byznys/finance-a-bankovnictvi/v-praze-zacal-fungovat-prvni-bankomat-s-bitcoiny-1088698#utm_medium=selfpromo&utm_source=e15&utm_campaign=copylink

[61] V Praze se otevře první bitcoinový bankomat. E-svět [online]. 2014 [cit. 2015-05-19]. Dostupné z: http://e-svet.e15.cz/it-byznys/v-praze-se-otevre-prvni-bitcoinovy-bankomat-1055001

[62] První obousměrný bitcoin bankomat v ČR – ohlédnutí. Btctip [online]. 2014 [cit. 2015-05-19]. Dostupné z:http://btctip.cz/prvni-obousmerny-bitcoin-bankomat-v-cr-male-ohlednuti

[63] S virtuálními měnami lze pohodlně obchodovat už i v České republice!. České Novinky [online]. 2014 [cit. 2015-05-19]. Dostupné z: http://www.ceskenovinky.eu/wp-content/uploads/2014/05/3072457-prvni-bankomat-na-bitcoiny-v-ceske-republice-je-v-prazskych-holesovicich-1-300x400p0.jpeg-222x300.jpg

[64] Virtuální měnu bitcoin je nově možné kupovat na poštách a terminálech Sazky. Hospodářské Noviny [online]. 2015 [cit. 2015-05-19]. Dostupné z: http://byznys.ihned.cz/c1-63416330-virtualni-menu-bitcoin-je-nove-mozne-kupovat-na-postach-a-terminalech-sazky

[65] PayPal vsadil na bitcoin, litecoin a dogecoin. Zatím opatrně. Btctip [online]. 2014 [cit. 2015-05-19]. Dostupné z:http://btctip.cz/paypal-vsadil-na-bitcoin-litecoin-a-dogecoin-zatim-opatrne

[66] FRANCO, P. Understanding Bitcoin: Cryptography, Engineering and Economics. Hoboken: Wiley, 2014. ISBN 978-1-119-01916-9.

[67] KELLY, B. The Bitcoin Big Bang: How Alternative Currencies Are About to Changethe World. Greenwich: Wiley, 2014. ISBN 978-1118963661.

[68] PAGLIERY, J. Bitcoin and the future of money. Chicago, Illinois: Triumph Books, 2014. ISBN 978-1629370361.

[69] Get started with Bitcoin. [online]. [2015] [cit. 2015-02-06]. Dostupné z: http://www.bitcoin.com/

[70] Target. Bitcoin wiki [online]. 2012 [cit. 2015-05-19]. Dostupné z: https://en.bitcoin.it/wiki/Target

[71] Bitcoin platby – platební brána Bitcash.cz. Bitcash.cz [online]. 2013 [cit. 2015-05-19]. Dostupné z:http://bitcash.cz/forum/showthread.php?s=&threadid=1004

[72] Jak se platí bitcoinem v Česku. Živě.cz [online]. 2014 [cit. 2015-05-19]. Dostupné z: http://www.zive.cz/clanky/jak-se-plati-bitcoinem-v-cesku/sc-3-a-172284/

[73] Jak se láká na binární opce aneb Nevěřte všemu Read more: http://www.investujeme.cz/jak-se-laka-na-binarni-opce-aneb-neverte-vsemu/#ixzz3aZCtuDp5. Investujeme.cz [online]. 2014 [cit. 2015-05-19]. Dostupné z: http://www.investujeme.cz/jak-se-laka-na-binarni-opce-aneb-neverte-vsemu/

[74] Kryptoměna Bitcoin se v Rusku stala veřejným Nepřítelem. Ekonomický deník [online]. 2015 [cit. 2015-05-20]. Dostupné z:http://ekonomicky-denik.cz/kryptomena-bitcoin-se-v-rusku-stala-verejnym-nepritelem/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BTC Bitcoin

FPGA tzv. „Field Programmable Gate Array“ - programovatelná hradlová pole

ASIC tzv. „Application Specific Integrated Circuit“ - typ obvodů vyráběných pro konkrétní aplikaci

SEZNAM OBRÁZKŮ

SEZNAM TABULEK