VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE

Fakulta informatiky a statistiky

Katedra systémové analýzy

BAKALÁŘSKÁ PRÁCE

2015 Jiří Herzán

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE

Fakulta informatiky a statistiky

Katedra systémové analýzy

Studijní program: Aplikovaná informatika

Obor: Informatika

Bitcoin

BAKALÁŘSKÁ PRÁCE

Student : **Jiří Herzán**

Vedoucí : **Ing. Tomáš Klíma**

Oponent : **Ing. Jaromír Veber, Ph.D.**

2015

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze které jsem čerpal.

V Praze dne 20. dubna 2015 Podpis: .....

Poděkování:

Rád bych poděkoval touto cestou Ing. Tomáši Klímovi za odborné vedení mé bakalářské práce. Zejména potom za trpělivost, doporučení, korekturu, čas a cenné rady, které mi pomohly při jejím tvoření. Dále bych chtěl poděkovat svým rodičům a přítelkyni za podporu během dosavadního studia.

Abstrakt

Tato bakalářská práce se zabývá virtuální měnou bitcoin. Práce je dělena do tří částí. První kapitola se zaměřuje na kryptografii, která je využita k zabezpečení bitcoinu. V další kapitole jsou popsány principy základního fungování této kryptoměny a samotný bitcoin mining. Poslední kapitola je částí praktickou a jsou v ní otestovány dvě metody bitcoin miningu.

Práce podává ucelený přehled dané problematiky se zaměřením na bitcoin mining. Hlavní cíl práce spočívá v porovnání bitcoin miningu pomocí testu ASIC mineru a metody Cloud mining. Výsledkem je potom zhodnocení výnosnosti těchto metod.

Klíčová slova

Bitcoin, miner, kryptografie, peer-to-peer, virtuální měna, ASIC, cloud mining, proof-of-work, pool, blockchain

Abstract

Bachelor's thesis is focused on crypto currency bitcoin. The thesis is divided into three parts. First chapter is focused on cryptography, which is used for bitcoin security. Next chapter describes basic bitcoin principles and bitcoin mining. In last chapter there are practically described two methods of bitcoin mining.

The aim of this thesis is to bring coherent view on given themes, especially bitcoin mining. The main goal of this thesis is trying bitcoin mining using ASIC miner and Cloud mining method. The result is a statement about mining profitability.

Keywords

Bitcoin, miner, cryptography, peer-to-peer, virtual currency, ASIC, cloud mining, proof-of-work, pool, blockchain

Obsah

1 Úvod

Bitcoin je síť umožňující nový platební systém pomocí kompletně digitálních peněz. Jedná se o první peer-to-peer platební síť, která je poháněna jejími samotnými uživateli bez zásahu centrální autority nebo prostředníka [1].

1.1 Důvody výběru tématu

Žijeme v době, kdy lidé již téměř nedokáží žít bez počítačů, mobilních zařízení a internetu. Tato zařízení nám každý den slouží pro komunikaci po celém světě, usnadňují práci, pomáhají získávat informace, navigovat nás a dokonce nás baví. Tyto technologie se neustále mění, zlepšují a vyvíjí. Oproti tomu peníze, jakožto prostředek obchodu, jsou stále stejné a mění se pouze možnosti k jejich přístupu a zabezpečení právě pomocí těchto zařízení a technologií. Téma mé bakalářské práce jsem proto zvolil hlavně z důvodu současné popularity, zajímavosti a revolučnosti virtuálních měn. Zejména potom absolvovaný předmět Bezpečnosti informačních systémů – 4SA313 mě bavil a proto jsem se rozhodl, že bych své znalosti z oblasti kryptoměn rád prohloubil.

1.2 Cíle a způsoby dosažení těchto cílů v práci

S pojmem bitcoin jsem se poprvé setkal v roce 2011. V té době hodnota bitcoinu oscilovala v rozmezí 1 – 20 USD [2]. Se svojí nedostatečnou znalostí angličtiny jsem byl vázán pouze na české zdroje, které byly a stále jsou minimální. Dlouhou dobu jsem tedy o této virtuální měně měl pouze základní informace, ale nikdy jsem zcela nezkoumal konkrétní principy.

Mým hlavním cílem v této práci je zhodnocení dvou metod bitcoin miningu na základě praktického testu. Chtěl bych porovnat mining pomocí ASIC zařízení od společnosti Butterfly Labs a cloud mining pomocí služby CEX.IO. ASIC je speciální mikročip vytvoření speciálně pro určité účely [3]. V případě bitcoinu byl navržen speciálně pro potřeby miningu. Cloud mining je oproti tomu v podstatě pronájem mining služeb od některého z poskytovatelů. V mém případě společnost CEX.IO LTD se sídlem v Londýně.

Dále za pomoci zahraniční literatury bych rád vytvořil materiál, který umožní i laikovi pochopení této problematiky. Jelikož se bitcoin neuvěřitelnou rychlostí vyvíjí, chtěl bych také aktualizovat stávající informace. Ze získaných dat vyvodím závěr, zda těžení v domácích podmínkách má v současné době nějaký smysl. K tomuto účelu bude využita hypotéza.

Hypotéza: Bitcoin mining v domácích podmínkách není výnosný.

Rentabilita neboli výnosnost je definována jako schopnost dosažení zisku na základě vložených prostředků [4]. Pro dosažení hlavního cíle práce, tedy pro potvrzení či vyvrácení mé hypotézy, osobně otestuji obě uvedené metody miningu.

1.3 Předpoklady a omezení práce

Jak jsem již zmiňoval, na toto téma bylo v českém jazyce vydáno minimum publikací a odborných článků, proto budou téměř všechny využité zdroje překládány z angličtiny. Z tohoto důvodu také většinu termínů ponechám v originále, tak, aby nedošlo k záměně jejich významu. U těchto termínů jejich význam vždy vysvětlím.

Dalším omezením mé práce jsou finanční prostředky. Jelikož je má hypotéza vedena na domácí podmínky, nechtěl bych přesáhnout investicí do této virtuální měny částku 5000 CZK.

1.4 Struktura práce

Tato bakalářská práce je členěna do kapitol a podkapitol. Kapitoly Kryptografie a Bitcoin jsou částmi teoretickými, které vychází zejména z rešerše odborné literatury.

Kapitola Kryptografie popisuje základy z této vědní disciplíny, které jsou nezbytné pro pochopení problematiky bitcoinu. V této kapitole jsou popsány cíle kryptografie a zejména potom jednotlivé elementy a různé možnosti využití kryptografie.

Další kapitola popisuje fungování a principy bitcoinu. Je zde popsáno, co to bitcoin je, kdo jej vytvořil a kdy, jak bitcoin funguje, na čem staví, jeho vývoj a další informace, které je dobré o této krypto měně znát, abychom si dokázali vytvořit ucelený pohled.

Kapitola věnována bitcoin mimingu je částí praktickou. V jejích podkapitolách je popsán postup vytvoření bitcoin peněženky, dále potom postup zprovoznění ASIC čipu a jeho propojení s českým serverem pro společný mining, který se nazývá Slush's pool. V další kapitole je potom popsán proces nákupu bitcoinů na mezinárodní burze Kraken.com a transfer těchto prostředků na již zmíněný cloud miningový server CEX.IO, kde budou prostředky dále směněny za výpočetní sílu potřebnou pro bitcoin mining.

1.5 Určení práce a očekávané přínosy

Bakalářská práce je psána takovou formou, aby i úplný laik bez jakýchkoliv znalostí z prostředí virtuálních kryptoměn byl schopen porozumět tématu, kterému se tato práce věnuje. Nicméně pro porozumění textu jsou třeba alespoň základní informatické znalosti. Práce tedy cílí na potenciální zájemce o investici do bitcoinu a potom samozřejmě na kohokoliv dalšího, kdo by si chtěl třeba jen rozšířit obzory nebo vyzkoušet něco nového.

Přínosem by mělo být důkladné porovnání různých metod miningu, které by mělo případnému zájemci o mining pomoci v jeho rozhodování. Dalším přínosem je ucelený pohled na bitcoin jako takový, doplnění současných stavů vývoje a upozornění na rizika plynoucí pro běžného uživatele.

Práce v tomto rozsahu si neklade za cíl kompletní zmapování všech metod získávání bitcoinů. Má přinést čtenáři komplexní pohled na tuto problematiku a propojení světa informačních technologií, kryptografie a plateb.

1.6 Doporučení pro správné čtení této práce

Práce je hodně specifického charakteru a spousta termínů vznikla zcela nově, nebo jsou běžně používány v úplně jiném smyslu. Proto před začátkem čtení doporučuji

nalistovat terminologický slovník, který se nachází na konci práce. V tomto slovníku jsou definovány nejčastěji používané termíny v práci, které jsou pro pochopení textů nezbytné.

1.7 Rešerše

Téma bitcoinu je relativně mladé ,a proto je problém zvláště v českém jazyce najít nějakou odbornou literaturu týkající se této problematiky. Druhým problémem je, že se bitcoin velmi rychle vyvíjí, proto bylo také třeba najít zdroje, které jsou aktuální.

Stěžejní knihou této práce je *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* od Andrease M. Antonopoulouse [5]. Kniha je rozdělena do 10 kapitol, ve kterých je popsána historie bitcoinu, jeho principy, dále se v ní píše o jednotlivých klientech, o způsobu tvorby transakcí, blocích a blockchainu, těžbě, zabezpečení a dokonce jsou v ní zmíněny další kryptoměny vycházející z konceptu bitcoinu.

Kniha *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu* [6] se zaměřuje, jak již její název napovídá, zejména na infrastrukturu veřejných klíčů, která je využívána v bitcoinové síti. V knize jsou ve 27 kapitolách velmi dobře popsány základy kryptografie a metody autentizace. Dále pak hesla, biometrika, čipové karty, principy digitálního podpisu, certifikáty a výdej a ověřování jejich platnosti, budování infrastruktury PKI, zabezpečení webové komunikace a mnoho dalšího.

Poslední kniha Understanding Bitcoin: Cryptography, Engineering and Economics [7] je velmi podobného charakteru, jako ta od pana Antonopoulouse. Zaměřuje se také na základní principy fungování bitcoinu. Dívá se na něj však více z ekonomického hlediska a snaží se vyvracet klišé, která o bitcoinu panují.

2 Kryptografie

Tato disciplína vychází z vědního oboru kryptologie. Kryptologie se potom dále dělí právě na kryptografii a kryptoanalýzu. Kryptografie je disciplína, která umožňuje zabezpečenou komunikaci v šifrách mezi dvěma stranami. Kdežto kryptoanalýza se naopak snaží o hledání slabin šifer a jejich luštění. Ve světě vládne neustálý boj mezi kryptografií a kryptoanalýzou. Historicky se dá říci, že vždy vedla kryptografie a díky tomu se daří zabezpečovat komunikaci a přenos dokumentů [8].

Kryptografie má čtyři základní cíle:

- **Důvěrnost** – má za úkol udržet obsah zprávy v tajnosti.
- **Integrita** – stará se o znemožnění neoprávněných úprav zpráv a případné odhalení těchto modifikací.
- **Autentizace** – slouží k ověřování totožnosti. Tedy zda ten s kým komunikujeme je skutečně tím, za koho se vydává. Pro tyto účely může posloužit např. domluvené heslo, klíče od bytu, čipová karta, otisky prstu, atd.
- **Nepopiratelnost** – zajišťuje, že autor nemůže popřít své autorství [8].

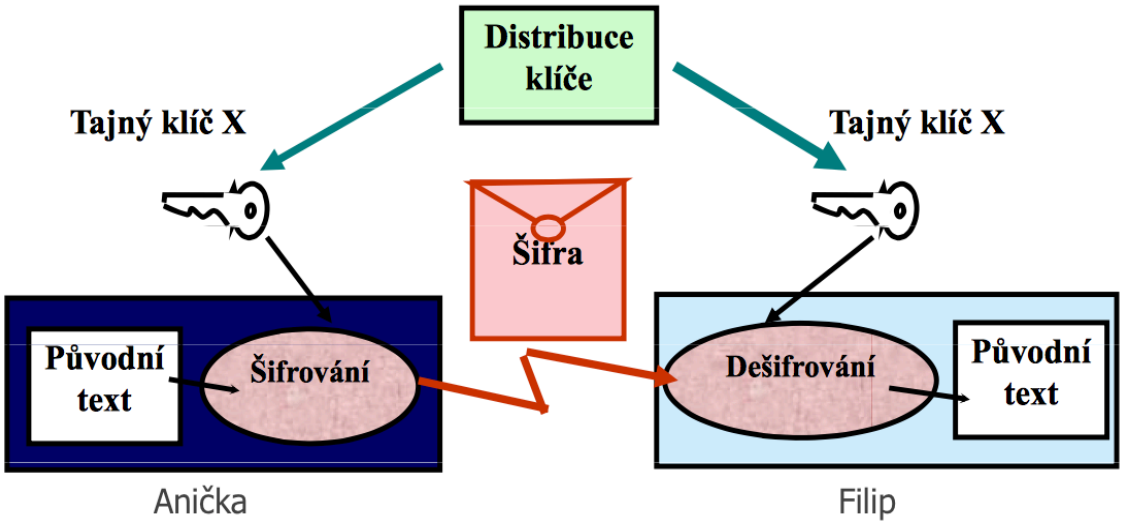
Bitcoin využívá tři základní kryptografické elementy:

- Šifrování a dešifrování
- Hashovací funkce
- Digitální podpis

2.1 Šifrování

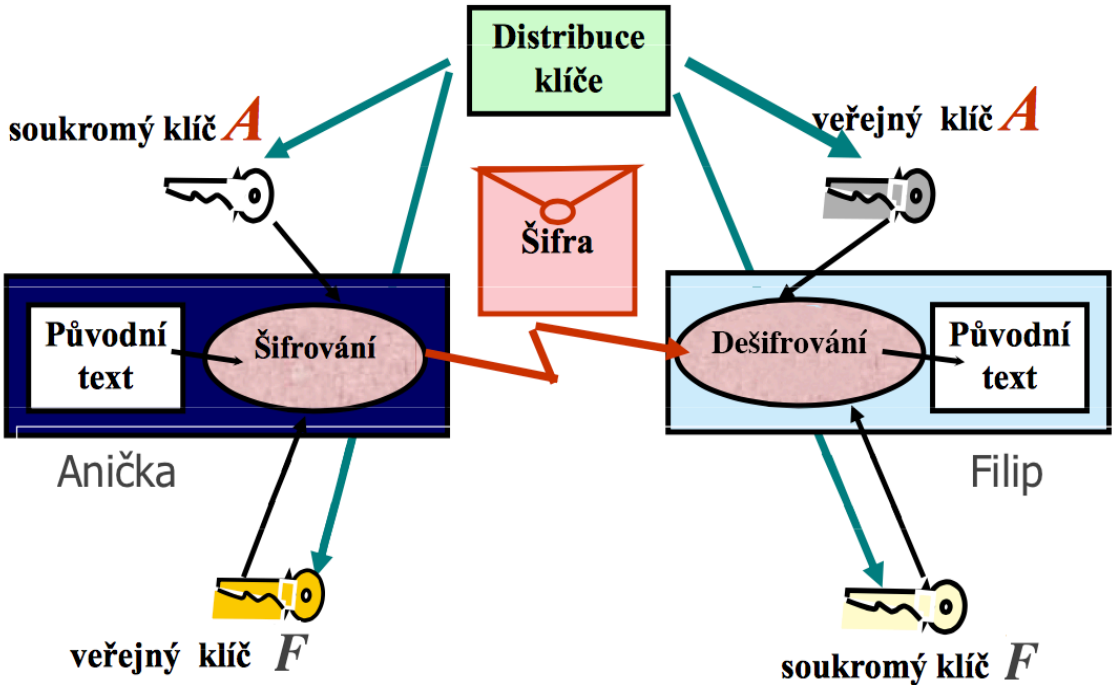
Samotné šifrování slouží pro převádění běžného textu na text zabezpečený. Stará se tedy o důvěrnost zpráv. Na světě existují spousty různých metod a algoritmů pro šifrování textu. Nejznámějším mechanickým strojem je Enigma, kterou používalo Německo během 2. světové války k utajování zpráv. Dáje jsou známy substituční metody, kdy každé písmeno je nahrazeno určitým znakem, či Caesarova šifra, ve které je každé písmeno posunuto o určitý počet znaků v abecedě.

Šifrování se dále dělí na symetrické a asymetrické. Symetrické šifry využívají pouze jednoho klíče, který umožňuje šifrování i dešifrování. Tedy autor i příjemce používají stejný klíč, který drží v tajnosti. Uvažujme tedy příklad, kdy Anička chce poslat zprávu Filipovi. Anička použije tajný klíč a zprávu zašifruje. Filip šifru přijme a pomocí stejného tajného klíče šifru převede na původní zprávu [8]. Tento proces je ilustrován na obrázku číslo 2.1.



Obrázek 2.1 : Schéma symetrické šifry (Zdroj: [9])

U asymetrických šifer vlastní každá ze zúčastněných osob soukromý a veřejný klíč. Pokud by Anička chtěla Filipovi poslat asymetricky šifrovanou zprávu, použije pro zašifrování zprávy Filipův veřejný klíč, který umožňuje pouze šifrování zpráv. Filip pomocí svého soukromého klíče dešifruje zprávu od Aničku. V případě, že bude chtít Filip Aničce odpovědět, použije pro zašifrování odpovědi Aniččin veřejný klíč. A Anička pomocí svého soukromého klíče zprávu dešifruje. Tento příklad je ilustrován na obrázku číslo 2.2.



Obrázek 2.2 : Schéma asymetrické šifry (Zdroj: [9])

Tímto je zajištěna důvěrnost dat, nikoliv však integrita, autentizace a nepopiratelnost. Uvažujme tedy, že mezi Filipem a Aničkou stojí ještě Michal, který zachytil Aniččin veřejný klíč adresován Filipovi. Ten nahradí za svůj vlastní veřejný klíč a doručí jej Filipovi. Stejně tak Michal zachytí Filipův veřejný klíč určený pro Aničku a znovu jej nahradí. V tomto momentě je schopen komunikaci kontrolovat a nezjistitelně modifikovat. Proto je třeba zabezpečení komunikace ještě posílit [8].

2.2 Hashovací funkce

Hashování je matematická funkce převádějící vstupní data na většinou kratší číslo o fixní délce, kterému se říká otisk [6].

Hashování má tři základní vlastnosti, pro jejíž demonstraci využijeme algoritmus SHA-256 (Secure Hash Algorithm). Tento algoritmus převádí vstupní text na 256-bitový (32 byte) otisk. Pro získání otisku bylo využito online překladu volně dostupného na serveru www.xorbin.com Tato funkce se využívá i pro bitcoin mining.

- **Velikost vstupních dat neovlivňuje velikost výsledného otisku, jehož délka je vždy stejná.**

Vstup:
Jirka
Výstup:
46bd7035b256d24318002441a67910d056468c34b6520b7564fbf0c0a178be60

Vstup:
„Dobře, že jsi mi dal tu bedýnku, v noci to bude jeho domeček...“
„Ovšem. A budeš-li hodný, dám ti také provázek, abys ho mohl ve dne přivázat. A kolík.“
Zdálo se, že tento návrh malého prince zarazil.
„Přivázat? To je ale podivný nápad!“
„Víš, když ho neuvážeš, půjde, kam mu napadne, a ztratí se.“
Můj přítel se znovu zasmál: „A kampak by šel?“ „Kamkoli. Stále rovně...“
Tu malý princ vážně poznamenal: „To nevadí, u mne je to velice malé!“
A tak trochu smutně dodal: „Když jde člověk stále rovně, daleko nedojde...“
Výstup:
d8d15249c601401e83faecd94f414f1d582a6bef420e55d60c53a92c8a70eb8f

V tomto případě můžeme vidět, že slovo o pěti znacích má stejně dlouhý otisk jako úryvek z knihy Malý princ [10] o 511 znacích. Otisk obou vstupů má 64 znaků.

- **Malá změna ve vstupních datech povede k rozdílnému otisku.**

Vstup:
Jmenuji se Jirka Herzán
Výstup:
79a1489ff73f9ae846269ec3de8d8fdbae08d292f7fe9023c2b49842f0d26ccd

Vstup:
Jmenuji se Jirka Herzán.
Výstup:
7e92073ca3921a623a21a0b60536cce6c6545e24048cfb931495fc60bfb11726

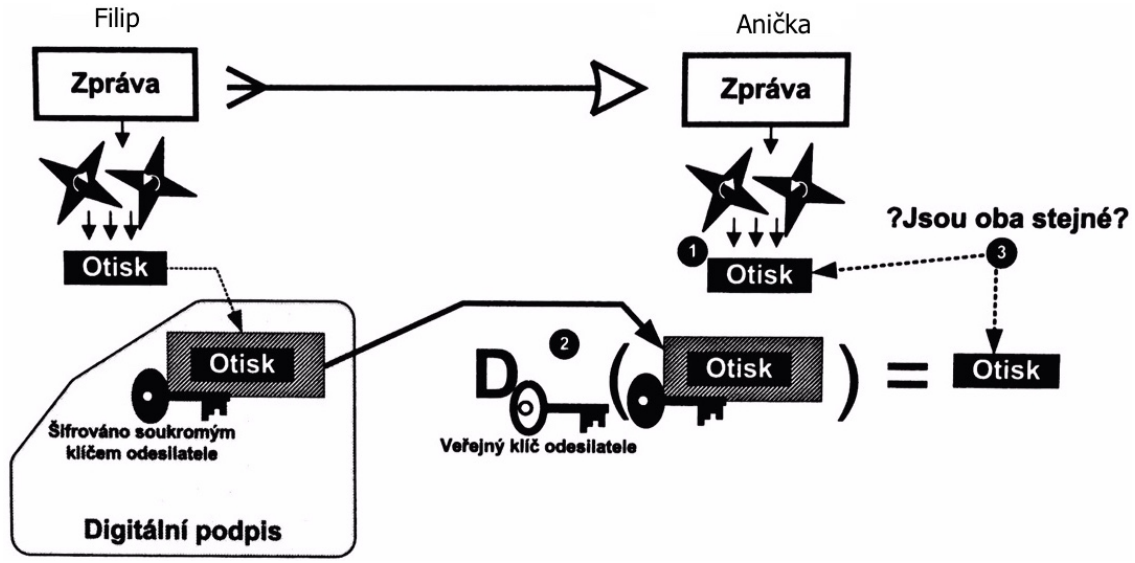
Z tohoto příkladu je patrné, že i minimálním rozdílem, jakým je znaménko na konci věty, vznikne diametrálně odlišný otisk.

- **Hashovací funkce jsou založeny na principu jednosměrnosti.** Z vstupních dat je snadné získat otisk, avšak vypočítat hodnotu vstupních dat z otisku je výpočetně velmi náročné [6].

2.3 Digitální podpis

Šifrování zajišťuje důvěrnost obsahu, hashování integritu. Speciální schémata s kombinací těchto algoritmů nám přidávají nepopiratelnost. Digitální podpis se dá proto přirovnat k běžnému, rukou psanému podpisu. Jeho výroba probíhá ve dvou krocích. Zaprvé je třeba vytvořit otisk např. pomocí již zmíněného SHA 256. Ve druhém kroku je tento otisk dále šifrován soukromým klíčem a tímto vznikne digitální podpis.

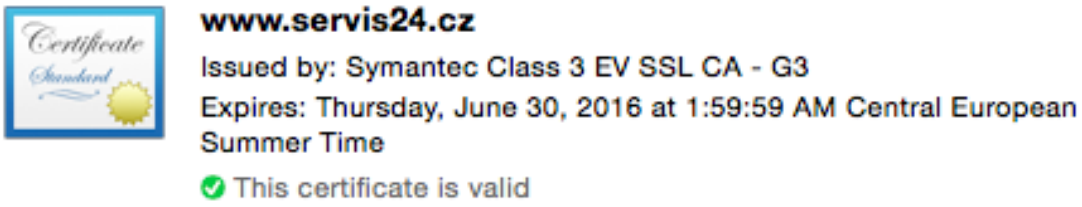
Filip napíše zprávu pro Aničku. Z této zprávy vytvoří otisk, který následně zašifruje pomocí svého soukromého klíče. Tento zašifrovaný otisk slouží jako digitální podpis. Dále Filip zprávu zašifruje pomocí Aniččina veřejného klíče a obě tyto šifry doručí Aničce. Anička použije svůj soukromý klíč pro dešifrování zprávy a Filipův veřejný klíč pro dešifrování podpisu. Následně vytvoří nový otisk zprávy, který porovná s otiskem získaným dešifrováním podpisu. Pokud jsou tyto otisky totožné, je zprávě přidána také nepopiratelnost [8] [6].



Obrázek 2.3 : Schéma digitálního podpisu (Zdroj: [6])

V kryptografii bývá dále využíváno třetího nezávislého subjektu, který může naši identitu potvrdit například oproti občanskému průkazu a vydává certifikáty, které je možno následně připojit ke zprávě. Subjektu, který vydává tyto certifikáty, se říká certifikační autorita. Tohoto systému se využívá například v elektronickém

bankovnictví a internetový prohlížeč platnost certifikátu kontroluje při každém přístupu. Příkladem může být internetové bankovnictví České spořitelny, které běží na serveru servis24.cz. Vydavatel tohoto certifikátu je americká společnost Symantec Corporation [11]. Dále třeba při komunikaci s úřady na dálku je v České republice možno využití osobního kvalifikovaného certifikátu.



Obrázek 2.4 : Certifikát České spořitelny (Zdroj: Autor)

Při uzavírání smluv na dálku bývá často využíváno časových razítek, které stejně jako certifikáty vyžadují nezávislou autoritu. Časové razítko je struktura obsahující čas, otisk dokumentu, vydavatele certifikátu a pořadové číslo. Toto je dále stvrzeno autoritou. V případě, že by Filip boural a chtěl po bouračce s bankou na dálku sjednat havarijní pojištění pro možnost podvodu, bude pro pojišťovnu jednoduché podle časového razítka určit, že ke sjednání pojištění došlo až po havárii [6].

Tyto dvě poslední zmíněné metody zabezpečení komunikace jsou hojně využívány po celém světě pro běžné úkony, jako je právě elektronické bankovnictví, komunikace s úřady atd. Ve světě bitcoinu toto však vůbec nefunguje a žádných certifikačních ani jiných autorit není třeba.

3 Bitcoin

3.1 Co je to Bitcoin

Bitcoin je plně decentralizovaná virtuální kryptoměna, která není závislá na žádné centrální autoritě, jež by se starala o tvorbu nebo tok peněz. Tato virtuální měna je chráněna proti zneužití kryptografickým algoritmem. Každý uživatel vlastní soukromý a veřejný klíč. Veřejný klíč se dá přirovnat k běžnému číslu účtu v bance a soukromý klíč zase slouží pro tvorbu transakcí. Každá tato transakce je zaznamenávána a odkazuje na transakce předešlé.

Podstatou bitcoinu je tedy velký dokument (účetní kniha), odkazující na všechny transakce v historii bitcoinu. Kopie tohoto dokumentu je uložena na každém počítači v bitcoinové síti. Je třeba si uvědomit, že veškerá čísla v tomto dokumentu mají jen takovou hodnotu, jakou uživatelé věří, že mají a jsou ochotni za ni měnit reálné statky a služby. Stejný princip funguje i u každé ničím nekryté měny. [12]

Příkladem kryté bankovky je dvaceti pěti koruna československá emitovaná v roce 1953. V pravém spodním rohu zadní strany bankovky (obrázek. 3.1) je vytištěno: **„Bankovky jsou kryty zlatem a ostatními aktivy státní banky československé.“**

Obrázek 3.1 : Bankovka v hodnotě 25 korun československých (Zdroj: [13])

Dotaz na názor ohledně problematiky bitcoinu jsem ze zvědavosti poslal i do kanceláře českého matematika, doktora Karla Janečka. Odpovědi se mi dostalo od jeho tajemníka doktora Tomáše Marady. Osobně mi nezbývá, než s panem doktorem souhlasit.

> „Dobrý den, pane Herzáne,
>
> odpovím Vám za sebe, ale názor Karla Janečka je velmi podobný. Asi sám víte, že Bitcoin není jen alternativní měna, ale mnohem důležitější je samotná technologie Blockchain, která je za Bitcoinem a možnosti, které tato technologie otevírá. Považuji vynález Blockchainu za jeden z nejdůležitějších objevů 21. století a jsem přesvědčen, že naprosto transformuje celou společnost a umožní ji posunout se dále.“

Zdroj:[14]

3.2 Vznik Bitcoinu

Podle legend Satoshi Nakamoto začal na konceptu bitcoinu pracovat již v roce 2007. Dodnes však není známo, zda se jedná o jednu osobu či skupinou osob. Název Satoshi Nakamoto je japonského původu a proto se spousta lidí domnívá, že Bitcoin vznikl právě v Japonsku. Japonština však nikdy v komentářích zdrojového kódu či ve fórech pod tímto pseudonymem použita nebyla. Satoshi je běžné mužské japonské jméno nesoucí význam moudrý či bystrý. Švýcarský programátor Thomas Stefan zkoumal Satoshiho příspěvky a zjistil, že téměř žádné příspěvky nebyly sdíleny v čase mezi pátou až jedenáctou hodinou ranní GMT (Greenwich Mean Time). Toto časové rozpětí odpovídá někomu, kdo v této době spí na území východního pobřeží Severní či Jižní Ameriky [15]. Po zakladateli měny byla také pojmenována jeho nejmenší část Satoshi. Tato část se už nedá dále nijak dělit.

> **Platí:**
>
> 1 Satoshi = 0.00000001BTC nebo-li 100,000,000 Satoshi = 1 BTC

Doména Bitcoin.org byla poprvé registrována 18. srpna 2008. Dále potom 31. října téhož roku byly pomocí mailing listu webu www.metzdowd.com zveřejněny první informace, návrhy a popisy bitcoinu v dokumentu Bitcoin: A Peer-to-Peer Electronic Cash. 3.1.2009 byl vytěžen první blok „0“ a tím vzniklo 50 bitcoinů (zkráceně BTC). Tento blok bývá také často označován jako Genesis. O několik dní

později byl nahrán první software Bitcoin-QT, který umožnil užívání bitcoin sítě. Zhruba do poloviny roku 2010 se Nakamoto podílel na dalším vývoji software a potom přestal úplně komunikovat s vývojářským světem. V této době předal kontrolu nad úložištěm zdrojového kódu a přístup ke klíčům, které umožňují odesílat altert messages(výstražná zpráva) napříč bitcoin sítí Gavinu Andersenovi. Výstražné zprávy nesou informaci o kritických chybách v síti a jsou zobrazovány všem uživatelům. V této době jsou známí pouze tři majitelé soukromých klíčů, které umožňují odesílání výstražných zpráv. Jsou jimi právě Satoshi Nakamoto, Gavin Andersen a uživatel theymos. Existují však další lidé, kteří můžou posílat výstražné zprávy v případě neschopnosti zmíněných [16].

3.3 Vývoj hodnoty bitcoinu

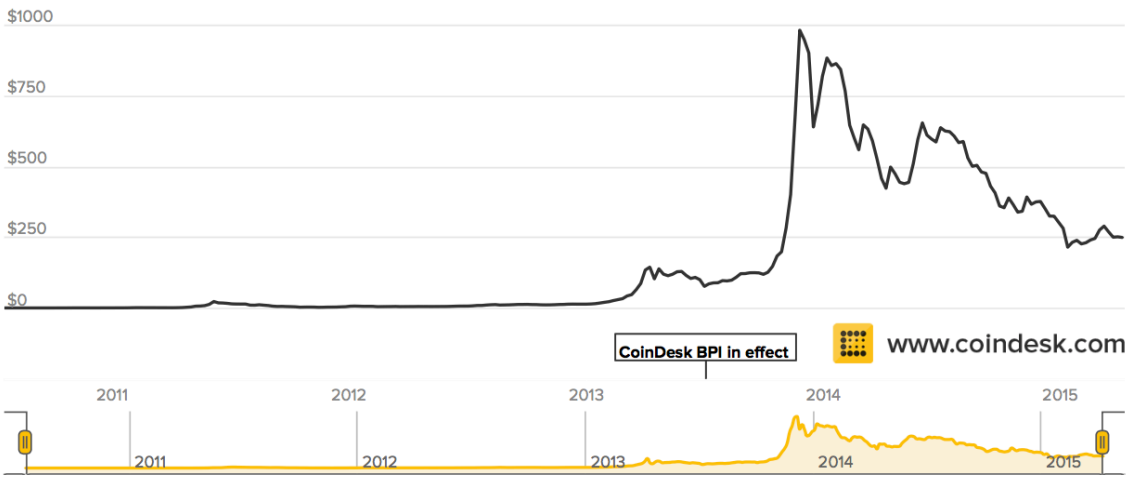
Bitcoin jakožto mladá měna se vyznačuje vysokou volatilitou. Jeho hodnota tedy značně kolísá a stejně jako další měny je bitcoin ovlivněn různými ekonomickými vlivy. V polovině roku 2010 byla hodnota jednoho bitcoinu zhruba 0.06 USD. Do konce dubna 2011 jeho hodnota pomalým tempem vrostla na cenu přibližně 3USD/BTC. V této době začal první boom, kdy se 11.6.2011 obchodoval 1BTC za 29.60 USD. Dále následovalo znovu klesání až k hodnotě 2.3USD/BTC, kterého bylo dosaženo v listopadu téhož roku. Potom až do konce roku 2013 hodnota Bitcoinu pomalým tempem rostla k 13USD/BTC. Dále v prvním čtvrtletí vzrostla hodnota téměř osmnáctkrát, kdy se 9.4.2013 rovnala 230USD/BTC. Do začátku listopadu 2013 bitcoin silně osciloval a jeho hodnota se rychle měnila v řádech desítek USD. V listopadu 2013 začala hodnota bitcoinu raketovou rychlostí růst a dne 4.12.2013 se 1BTC obchodoval za rekordních 1147.25 USD [2]. Na konci února 2014 následovalo ohlášení krachu první vzniklé BTC burzy Mt. Gox. Po tomto krachu zůstaly obrovské dluhy jak v BTC tak v běžných měnách, které investoři nikdy nezískali. Několik dnů na to následoval čínský zákaz nákupu krypto měn za jüany.

Mt. Gox původně vznikl v roce 2007 za účelem výměny populárních Magic kartiček. Nicméně v roce 2010 byl účel serveru změněn na bitcoinovou směnárnu. Tato společnost byla příkladem zanedbanosti, nezkušenosti a slabého managementu. V době krachu společnost oznámila ztrátu 750000 BTC uživatelů a 100000 BTC

vlastních. Zhruba o půl roku později bylo oznámeno nalezení 200000 BTC na starém pevném disku z roku 2011. Dnes je tomu již více než rok od vyhlášení krachu Mt. Gox a stále se nepodařilo zjistit, kde se nachází chybějících 650000 BTC. Vedení Mt. Gox tvrdí, že bitcoiny byly ukradeny a že útočníci nepozorovaně čerpali peníze ze směnárny dlouhá léta [17].

Velké popularitě se dostalo bitcoinu v Číně, jelikož umožňoval snadnou směnu jüanu za další měny jako je euro nebo dolar. Tato směna je jinak v Číně přísně kontrolována a k jejímu provedení je třeba speciální povolení. Vláda takto ztrácela přehled nad tím, kolik eur a dolarů se mezi lidmi nachází a proto následoval zákaz. Čína na trhu bitcoinu značně dominuje a toto byl opravdu velký zásah [18].

Výše zmíněné události by měly být velkým varováním značící snadnou ovlivnitelnost bitcoinu. Dalším ovlivňujícím faktorem v druhé polovině roku 2014 byl rozprodej bitcoinů zabavených vládou USA z nelegální činnosti serveru Silk Road. Tento rozprodej proběhl zatím ve třech aukcích. První proběhla v červu roku 2014, druhá potom v prosinci. Zatím poslední aukce je datována k 5.3.2014. Celkem už tedy vláda USA tímto způsobem prodala na 120 000 BTC a stala se tak největším překupníkem bitcoinu v historii [19]. Z těchto a mnoha dalších důvodů má hodnota bitcoinu od jejího maxima ze 4.12.2013 až do současnosti spíše klesající tendenci a jeho hodnota se v prvním čtvrtletí 2015 držela mezi 200-300USD/BTC.



Obrázek 3.2 : Vývoj hodnoty bitcoinu (Zdroj: [20])

3.4 Bitcoinoví klienti

Pro připojení k bitcoinové síti je třeba si stáhnout počítačovou aplikaci, anebo použít nějakou webovou. Dnes je těchto aplikací nespočetné množství a dělí se na tři základní druhy.

3.4.1 Tlustý klient

Mezi tlusté klienty patří i mnou používaný Bitcoin-Qt. Je to v podstatě jediný klient svého druhu, který u uživatele na disku uchovává veškerou historii transakcí. Z důvodu, že zabírá mnoho paměti, není pro koncového uživatele vhodný. V dnešní době bitcoin není ještě zcela rozšířen, a proto se počet jeho transakcí ani nepřibližuje společnostem jako je VISA nebo MasterCard. Kdyby však počet transakcí vzrostl, nebylo by možné, aby běžní uživatelé skladovali celou transakční historii.

3.4.2 Tenký klient

Pro koncové uživatele je mnohem vhodnější volbou tenký klient. Tento druh klienta drží v uživatelově počítači soukromé klíče a pro ověření transakcí se přistupuje k důvěryhodnému serveru třetí strany. V poslední době se tento druh klienta rozšiřuje hodně do mobilních zařízení. Při platbě v kavárně Paralelního Polisu v Praze mi byla doporučena aplikace Blockhain – Bitcoin Wallet, která je dostupná jak pro systémy iOS tak i Android. Při provádění plateb se využívají QR kódy, takže nemůže nastat špatné zapsání adres. Oficiální webové stránky Bitcoin.org zase doporučují pro začínající uživatele klienta Multibid, který je dostupný pro počítače běžící pod Windows, OS X i Linux.

3.4.3 Web klient

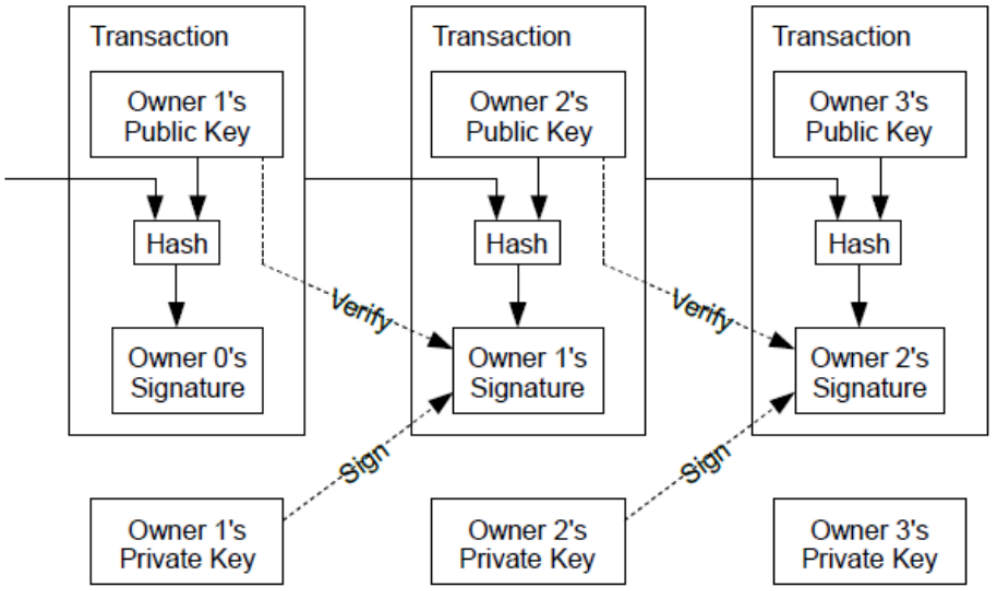
K naší peněžence se u webových klientů dostaneme pomocí internetového prohlížeče. Tento typ klienta drží veškeré informace na serverech třetí strany. Proto je vhodné, aby poskytovatel této služby byl dobře prověřen a jeho servery zabezpečeny.

Každý ze zmíněných druhů klientů má své výhody i nevýhody a proto je na konkrétních uživatelích aby se sami rozhodli, který druh je pro jejich potřeby nejvhodnější. Myslím si, že výběr správného bitcoin klienta je stejně důležitý jako

výběr banky, ve které máme uloženy naše peníze. Nejenom směnárny typu Mt. Gox mohou zkrachovat, může se stát, že zkrachují i banky, jako tomu bylo např. v roce 2008 u banky Lehman Brothers v USA [21] [5].

3.5 Transakce

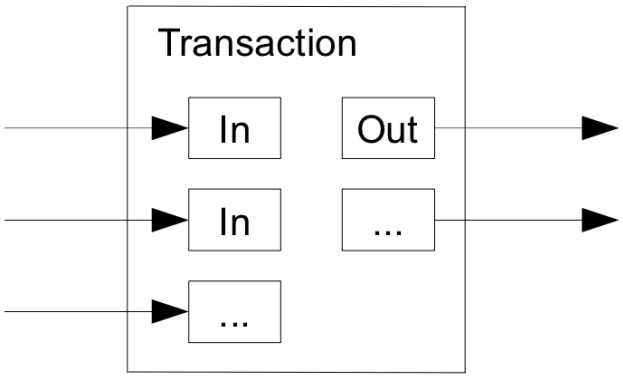
Jednotlivé transakce jsou vysílány do sítě a říkají, že např. 1 BTC bude z účtu Aničky stržen a naopak 1 BTC přibude na účtu Filipa. Každý počítač si potom tuto transakci uloží do své kopie dokumentu - tzv. blockchain. To znamená, že všichni vidí transakce všech ostatních uživatelů, což je základní rozdíl oproti běžným bankovním účtům, kde můžeme vidět pouze vlastní transakce. Aby byla zajištěna nepopiratelnost transakce, je třeba pro každou transakci vygenerovat digitální podpis pomocí soukromého klíče. Tím zároveň prokážeme, že jsme právoplatnými majiteli bitcoinů, které patří k určitému veřejnému klíči. Díky tomu může každý uživatel sítě zkontrolovat, že odesílatel vlastnil soukromý klíč bez toho, aniž by jej viděli. V podstatě transakce říká, že Anička je právoplatným majitelem a může přesunout některé bitcoiny Filipovi [5].



Obrázek 3.3 : Zabezpečení transakce (Zdroj: [22])

Nyní je třeba dodat, že v bitcoinové síti nejsou uchovávány zůstatky na účtech uživatelů. Pokud tedy Anička chce Filipovi poslat 1 BTC, musí ke zprávě přidat odkazy na předchozí transakce, které dokazují, že její inputy (vstupy) jsou rovny nebo větší než 1 BTC. Pokud odesílaná částka neodpovídá přesně jednomu

z inputů, bude přebytek poslán zpět na náš účet. Abychom si však byli jisti, že tyto transakce jsou pravé, musíme ověřit všechny transakce, které kdy proběhly [22]. Tato kontrola je provedena po prvním spuštění tlustého klienta bitcoinové peněženky a v mém případě zabrala více než 26 hodin času. Při každém dalším spuštění peněženky jsou již jen kontrolovány nové transakce. Tato kontrola probíhá v řádech minut. Momentálně mi peněženka Bitcoin-Qt zabírá 39.7 GB místa na mém disku. Jelikož mé flashové úložiště v počítači má kapacitu 256 GB, jedná se o jeho značnou část. Z tohoto důvodu budu muset brzy přejít na jinou formu klienta.



Obrázek 3.4 : Schéma vstupů a výstupů z transakce (Zdroj: [22])

Jakmile je transakce provedena, považujeme ji za použitou a není ji možné použít znovu. Proto všechny uzly sítě dále kontrolují, zda inputy v transakci už nebyly někdy dříve použity jako output. Outputem se rozumí odchozí transakce. Chceme-li zkontrolovat náš aktuální zůstatek, musíme zkontrolovat všechny provedené transakce v historii a přičíst neutracené inputy.

Je třeba velmi pečlivě kontrolovat, jaké klíče-adresy do transakcí zadáváme. I nepatrná změna ve veřejném klíči, na který adresujeme bitcoiny povede k odeslání platby, ale tato platba nikdy nebude doručena. Díky tomu nepřijde o bitcoiny pouze naše peněženka, nýbrž celá síť. Dalším příkladem může být ztráta soukromého klíče k naší peněžence z důvodu poruchy pevného disku, na kterém je peněženka uložena. Jsou známy případy, kdy uživatelé z těchto důvodů přišli o tisíce BTC [5].

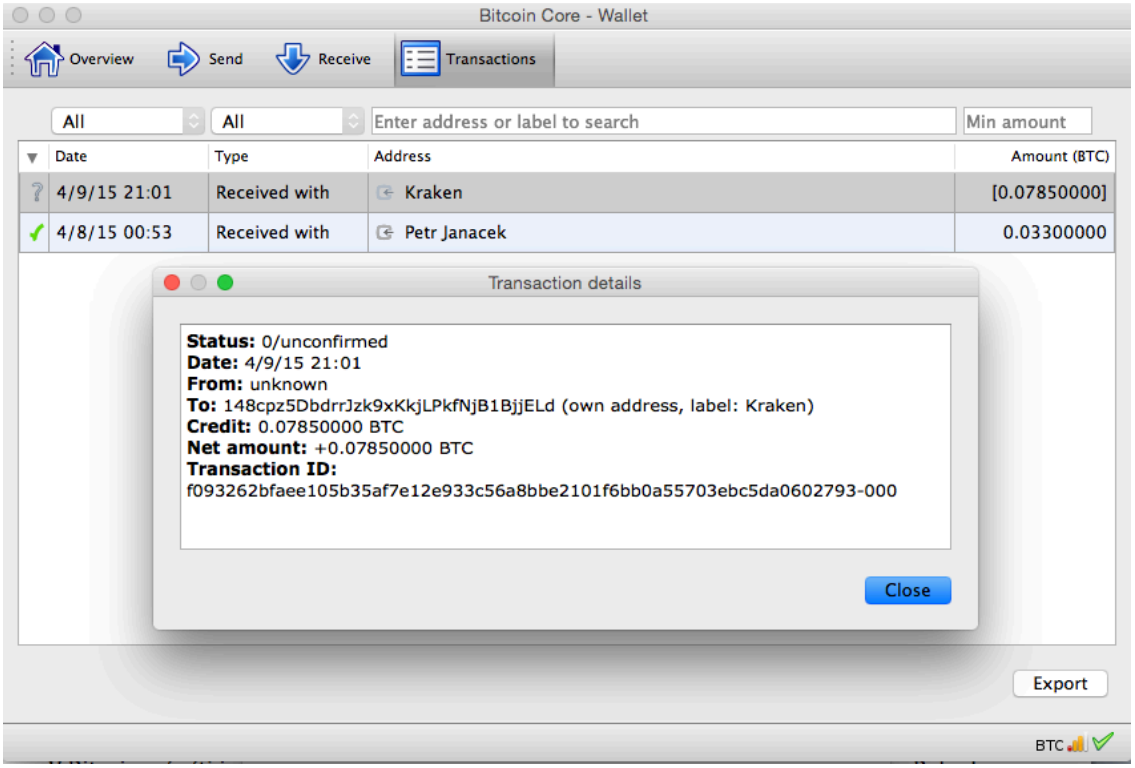
3.6 Double spending (dvojité utrácení)

Je třeba si uvědomit, že veškeré transakce jsou posílány sítí od uzlu k uzlu a pořadí, ve kterém tyto transakce obdržíme, neodpovídají pořadí, ve kterém tyto transakce byly vytvořeny. Jak jsem již zmínil v části kryptografie, bitcoin využívá jiného druhu časového razítka. U tohoto typu není autorita, která by čas opravdu potvrdila a proto časové razítko v případě bitcoinu není dostatečným důkazem.

Představme si tedy, že Anička zaplatí Filipovi 1 BTC a počká na potvrzení o odeslání produktu. Hned po potvrzení by mohla Anička použít stejné inputy pro novou transakci, kterou adresuje sama sobě. V tomto momentě by některé uzly v síti obdržely tuto transakci dříve než tu pro Filipa. A po obdržení transakce pro Filipa by ji vyhodnotily jako neplatnou. Filip by byl bez peněz i bez produktu. V tomto případě by nebylo možno prokázat, která transakce ve skutečnosti vznikla dříve. U běžných platebních systémů je toto řešeno centrální autoritou, které všichni věří. U bitcoinu je řešením tohoto problému blockchain a block mining [5] [12].

3.7 Blockchain (řetězec bloků)

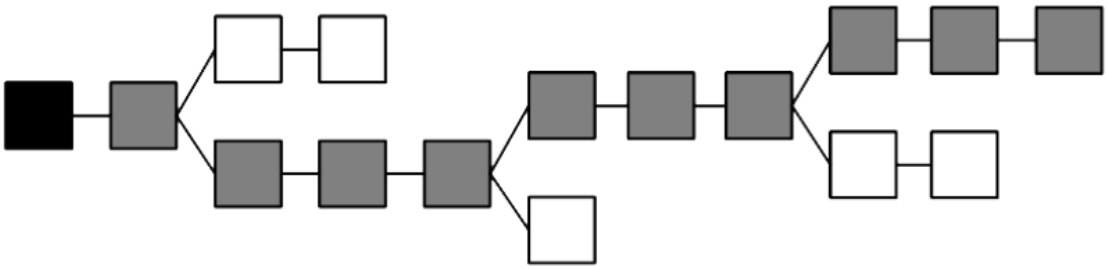
V bitcoinové síti jsou jednotlivé transakce řazeny do skupin, které se nazývají bloky. Každý blok obsahuje odkaz na blok předchozí. Spojením těchto bloků vzniká tzv. blockchain. Díky tomu je možno se vrátit k prvnímu bloku, který kdy byl vytvořen – Genesis bloku. Transakce ve stejném bloku jsou považovány za transakce, které vznikly ve stejném čase. Naopak transakce, které v bloku ještě nejsou, považujeme za nepotvrzené. Příklad nepotvrzené transakce je možno vidět na obrázku číslo 3.5.



Obrázek 3.5 : Příklad neověřené transakce (Zdroj: Autor)

Bloky v sobě dále nesou řešení matematického problému. Správnost tohoto řešení je jednoduše ověřitelná. Řešení úkolu je pro každý blok odlišné. Jakýkoliv uzel může vzít sesbírané nepotvrzené transakce, přidat k nim řešení matematického úkolu a vytvořit nový blok. Tomuto procesu se říká block mining (těžba bloků). Uživateli, který se těžbou zabývá miner (těžař) a slovem miner je také označováno zařízení, pomocí kterého jsou prováděny výpočty matematických úkolů. Pro proces těžby bloků a označení uživatele zabývajícího se těžbou bude využíván český překlad. V této práci ponechám zařízení pro těžbu originální název miner. Výkonnost minerů bývá nejčastěji uváděna v GH/s. To znamená, že miner poskytující výpočetní sílu 1 GH/s je schopný generovat 1,000,000 otisků za sekundu [5].

Blockchain je řetězec bloků, který je občas větven. Větvení nastane, pokud dva těžaři ve stejnou dobu vytvoří blok. Následně jsou bloky přidávány k těžařově nejbližší větvi. Jakmile je jedna z větví prodloužena, je považována za platnou a další bloky budou již přidávány na její konec. Všechny transakce z bloků v neplatné větvi zaniknou a je třeba je zařadit do nového bloku.



Obrázek 3.6 : Příklad větvení blockchainu (Zdroj: [23])

Zánikem větve ztratí transakce potvrzení. Proto je velmi důležité sledovat, kolikrát byla transakce potvrzena. Pokud je transakce v hlavní větvi řetězce, má potvrzení 1. Za každý následující blok získává + 1 potvrzení. Pro použití bitcoinů získaných jako odměnu za těžbu je třeba mít okolo 100 potvrzení. Obecně platí, že přijaté transakce, které mají více než 6 potvrzení, je možno považovat za velmi bezpečné, a proto bývá vyžadováno u větších transakcí. Když víme, že je generován 1 blok každých 10 minut, ověření jedné transakce potom trvá asi hodinu. Naopak u platby za drobnost jako je káva, bývají platby považovány za bezpečné již po 10 minutách. Na obrázku číslo 3.7 je stejná transakce jako na obrázku 3.5, ale v tomto momentě má již 406 potvrzení [5].

Status: 406 confirmations
Date: 4/9/15 21:01
From: unknown
To: 148cpz5DbdrrJzk9xKkjLPkfNjB1BjjELd (own address, label: Kraken)
Credit: 0.07850000 BTC
Net amount: +0.07850000 BTC
Transaction ID:
f093262bfaee105b35af7e12e933c56a8bbe2101f6bb0a55703ebc5da0602793-000

Obrázek 3.7 : *Informace o transakci (Zdroj: Autor)*

Zde je dobré si uvědomit, že potvrzení transakce je mnohonásobně delší než předání hotovosti prodavači nebo přiložení debetní karty k platebnímu terminálu. Na druhou stranu příjem platby kreditní kartou bez ověření totožnosti je srovnatelným riskem jako vydání zboží oproti nepotvrzené transakci [5].

3.8 Block Mining (těžba bloků)

Těžba bloků je proces emitace nových bitcoinů a zároveň se stará o zabezpečení celé sítě proti podvodným zásahům a utrácení stejných prostředků více než

jednou. U bitcoinu se předpokládá, že většinu výpočetní síly vlastní slušní uživatelé a případný útočník nemá šanci získat více než polovinu výpočetní síly sítě [7].

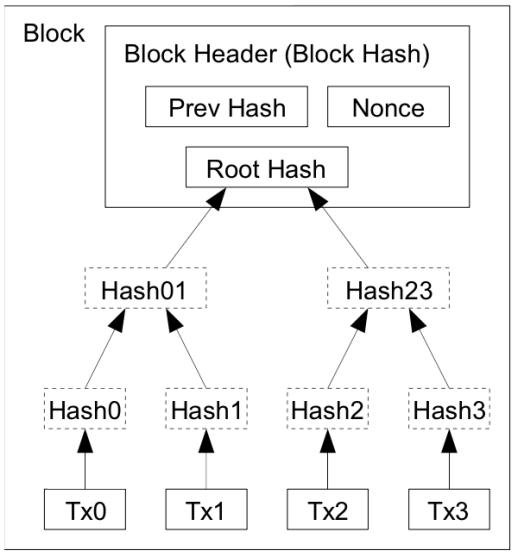
Těžaři jsou motivování k těžbě odměnou za potvrzený blok. Tato odměna začínala na 50 BTC. Nyní je rovna 25 BTC za potvrzený blok a nadále bude každé 4 roky, nebo přesněji každých 210000 bloků, snížena na polovinu. Tímto způsobem bude do roku 2140 vytěženo skoro 21000000 BTC. Toto je hodně zásadní rozdíl oproti běžným měnám. U měny jako je euro toto celkové množství není ničím dáno a v případě potřeby, centrální banky, jakožto věřitelé v poslední instanci, peníze prostě vytvoří. Podobně není možno Bitcoin srovnávat s komoditami jako je zlato, u kteréhož se předpokládá, že jednou bude vytěženo. U zlata platí, že čím více jej budeme těžit, tím více jej vznikne [21]. U bitcoinu v případě zvýšení těžby bude upravena složitost úkolů tak, aby vzniklo přesně stanovených 25 BTC za potvrzený blok. Další odměnou, kterou těžaři získávají, jsou transakční poplatky. Těžaři proto upřednostňují transakce, u kterých odesílatel nastavil vyšší transakční poplatek. Jakmile budou všechny bitcoiny vytěženy, budou motivováni k těžbě pouze těmito transakčními poplatky.

První transakce přidaná do bloku je vždy generation transakce nebo také coinbase transakce. Zde je uvedena částka, kterou miner za provedenou práci obdrží. Množství nově emitovaných bitcoinů, které v tento moment vzniknou z ničeho, je vypočítáno podle čísla aktuálního bloku. Jestliže je vyplacená částka redukována každých 210000 bloků a tzv. Height (Počet bloků předcházející současný blok. Height genesis bloku je 0. [24]) posledního vytěženého bloku byla 352387, algoritmus sám pozná, že má vytvořit 25 nových BTC.

Obtížnost úkolů, které musí minery řešit se aktualizuje tak, aby byl vytvořen přibližně jeden blok za 10 minut. Náročnost je většinou zvyšována s rostoucí výpočetní silou celé sítě. Občas se však stane, že je náročnost snížena. Tento jev byl zaznamenán např. několikrát v posledních měsících [25].

Jelikož jsou těžaři motivováni ziskem, zaměřuje se v prvé řadě na transakce s nejvyšším poplatkem. Z každé takové transakce vytvoří pomocí hashování otisk.

Dále vezme dva otisky a znovu je zahashuje. Toto se opakuje tak dlouho, dokud nezbude pouze jeden otisk, kterému se říká Merkle Root (Merkleho kořen). Tento systém byl pojmenován po americkém vědci Ralfu Merklovi, který si jej v roce 1979 nechal patentovat jako Merkle tree (Merklův strom) [26].



Obrázek 3.8 : Schéma vzniku Merkle Root (Root Hash) (Zdroj: [22])

Při generování bloků se opakovaně vytváří otisk bloku. Tento otisk je následně kontrolován, zda je menší než target (cíl). Target je počítán jednou za 2015 bloků, což by při časovém intervalu 10 minut/blok mělo odpovídat 1209600 sekundám. Target je tady počítán jako časový rozdíl 1. a 2015. bloku. Tento údaj se dále vynásobí současným targetem a porovná s časovým údajem 1209600 sekund. Je-li výsledek menší, musí se snížit i hodnota targetu a tím dojde ke zvýšení náročnosti. Toto je přímo úměrné celkové velikosti výpočetní síly a je-li generováno 2015 bloků za méně než 14 dnů, znamená to, že se zvýšila výpočetní síla celé sítě. Target je uchováván v hlavičce bloku pomocí proměnné Bits.

Vzorec výpočtu targetu:

$$Nový\ target = \frac{(časové\ razítko\ 2015.\ bloku - časové\ razítko\ 1.\ bloku)\ x\ Aktuální\ target}{1209600}$$

Target ale neoznačuje obtížnost úkolů, nýbrž je to měřítko pro určování obtížnosti [27]. Obtížnost jako taková je v bitcoinové síti označována jako bdiff.

Vzorec pro výpočet obtížnosti:

$$Obtížnost\ (bdiff) = \frac{target\ bloku\ 0}{současný\ target}$$

Aktuální obtížnost je 49,446,390,688 a toto číslo znamená, že nalezení správného otisku je nyní 49,446,390,688 krát náročnější, než bylo nalezení tohoto otisku u bloku 0 [28].

Jak jsem již zmínil, minery neustále vytvářejí otisky bloků. K tomu aby dosáhly hodnoty nižší, než je target je využíváno nonce. Nonce je v Bitcoinu 32 bitové číslo, které je přidáváno na konci otisku bloku a znovu hashováno. Velmi dobrý příklad je uveden na Bitcoinové wiki. Budeme pracovat s textem „Hello world!“. Naším targetem je nalezení otisku začínajícím třemi nulami. K základnímu textu „Hello world!“ přidám první nonce „0“ a provedu hashování pomocí SHA-256. Vznikne otisk:

1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

Tento otisk však nezačíná „000“ a proto musím nonce nahradit za „1“ a proces se opakuje, až získáme otisk začínající „000“. Průběh řešení bude:

"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => **000**0c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

V tento moment můžu veřejně oznámit, že nonce pro tento příklad je „4250“ a každý další uživatel může jednoduše ověřit, že po hashování "Hello, world!4250" získá otisk:

0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9 [29]

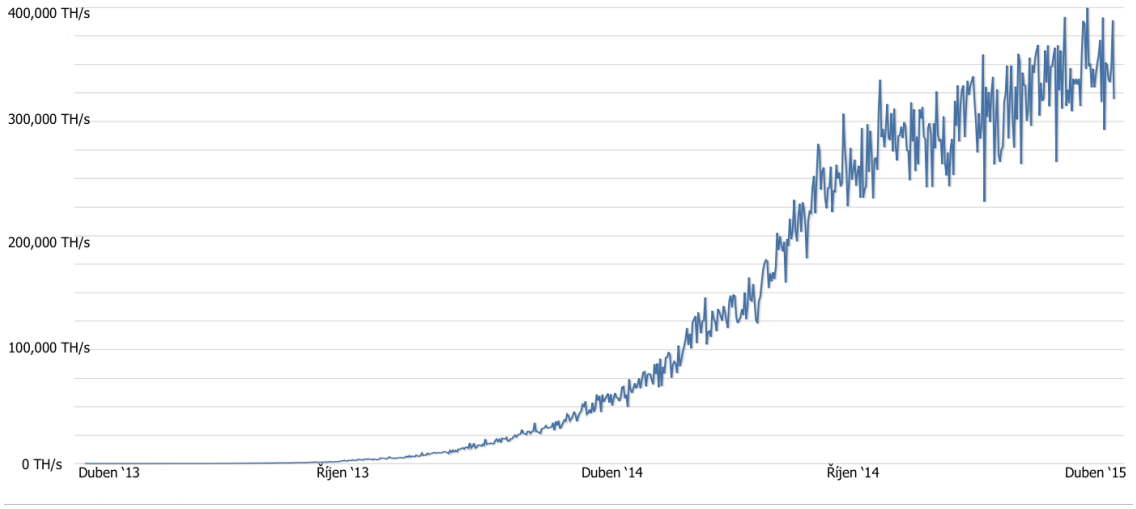
Pro správné řešení tohoto příkladu je nutné vytvořit 4251 otisků. Mnou vlastněný miner zvládá tvořit přes 5 milionů otisků za sekundu. Tuto úlohu by vyřešil za méně než 0.00085 sekundy.

Nově generovaný blok obsahuje:

- Verzi protokolu
- Otisk hlavičky předchozího bloku
- Merkle root
- Časové razítko – není potvrzeno autoritou
- Bits
- Nonce

Náročnost úkolu je postupně přizpůsobována celkové výpočetní síle sítě. Proto nalezení správné nonce v dnešní době je velmi náročný úkol. Tím, že naleznu správnou nonce dokazuji, že jsem vykonal určitou práci. Tomuto konceptu se říká Proof-of-work (dokázání práce). A tímto způsobem je tvořen celý blockchain. Jelikož jednotlivé bloky obsahují otisk předchozí hlavičky, není možné změnit blok, který je už v blockchainu, protože i malá změna by ovlivnila výsledný otisk a tím celý blockchain [5].

Na následujícím grafu je možno vidět rostoucí tendenci veškeré výpočetní síly Bitcoin sítě. Na grafu je také vidět zvětšující se volatilita sítě, kdy v průběhu března 2015 dosáhla výpočetní síla sítě téměř 400 000 TH/s a ještě v tom stejném měsíci byl zaznamenán propad pod 300 000 TH/s, což je rozdíl více než 25%. Proč však dochází k takovýmto výkyvům nedokáži vysvětlit. Předpokládám, že těžaři odpojují své minery, aby nedocházelo k zvýšení náročnosti úkolů. Tento předpoklad však nemám ničím podložen.



Obrázek 3.9 : Graf vývoje výpočetní síly od dubna 2013 do současnosti (Zdroj: [30])

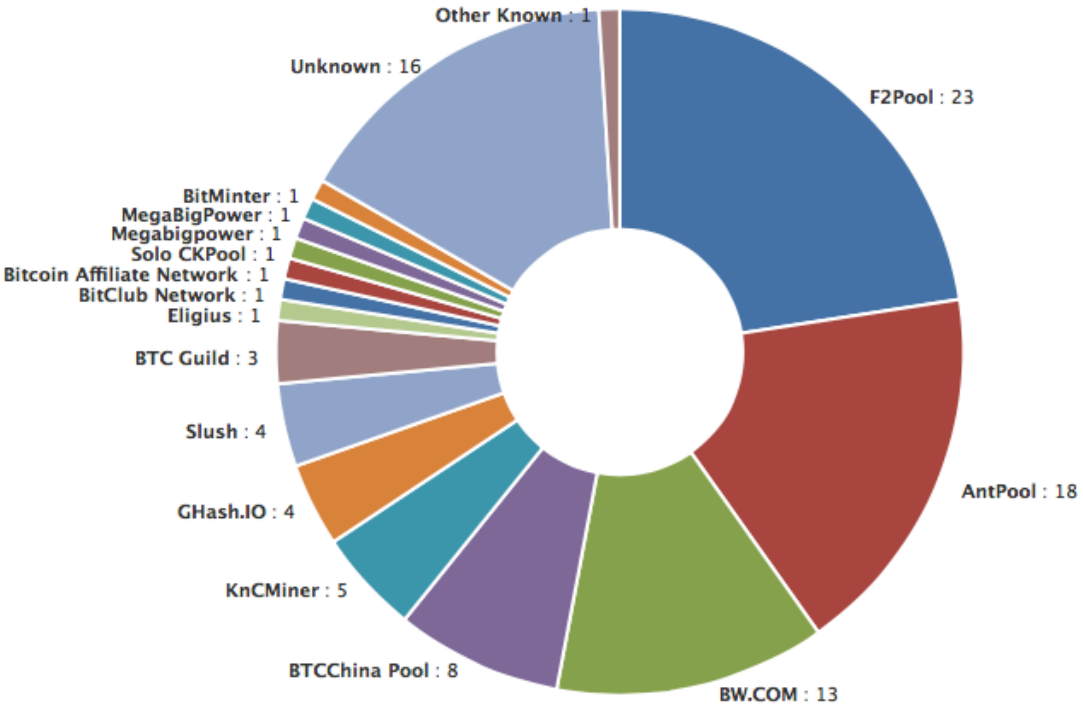
Abych to zrekapituloval, těžba bitcoinů probíhá následujícím způsobem:

1. Miner vezme transakce a postupně z nich vytváří otisky. Dále vždy spojí dva otisky a vytvoří z nich pouze jeden otisk. Tímto způsobem pokračuje, až zůstane pouze jeden otisk – Merkle root.
2. Nyní miner vezme celkový text bloku, přidá náhodnou nonce hodnotu a vytvoří otisk. Výsledný otisk porovná se současným targetem. Tento proces je opakován do té doby, než je hodnota výsledného otisku menší než Target. Jinými slovy řečeno, že je na začátku dostatečný počet nul.
3. Tento blok je zařazen do blockchainu a každý uživatel může jednoduše ověřit, že miner vykonal práci tím, že ověří správnost použité nonce.
4. Po sto ověřeních je těžaři připsána odměna 25 BTC.

Nejdůležitější funkcí těžby není emitace nových bitcoinů a odměňování těžařů, jak by se mohlo na první pohled zdát. Jejím hlavním úkolem je zabezpečit bitcoin jako takový pomocí minerů a tím podává základ pro decentralizovaný systém digitálních peer-to-peer peněz. Díky tomu je bitcoin tak geniálním vynálezem.

3.9 Pool Mining

Složitost jednotlivých úkolů je dnes natolik vysoká, že i kdybych vlastnil výpočetní sílu v řádech TH/s, nalezení správné nonce hodnoty by bylo jako výhra v loterii. Z tohoto důvodu se těžaři spojují do uskupení, kterému se říká pool. V poolech těžaři spojují svou výpočetní sílu a následnou odměnu si mezi sebou rovnoměrně dělí. Tímto způsobem si každý těžař zajistí alespoň nějaký pravidelný přísun bitcoinů [7].



Obrázek 3.10 : Graf výpočetní síly jednotlivých poolů za poslední 4 dny.(15.4.2015) (Zdroj: [31])

Aktuálně největším poolem je čínský F2Pool, který vznikl 5. května 2013. Patří mu téměř 25% celkové výpočetní síly [32]. Následován je AntPoolem, který je vlastněn společností Bitmain Technologies Ltd. Tato společnost dále nabízí služby cloud miningu, o kterém bude řečeno více v praktické části práce, a potom samotné minery prodává [33]. Třetím největším současným poolem je BW.com. Z jeho webových stránek bylo zatím přeloženo do angličtiny jen minimum, takže nelze zjistit žádné další informace. Jelikož je drtivá většina textu v čínských znacích, usuzuji, že pool bude mít čínský původ. Tyto informace by naznačovaly, že více než 50% dnešní výpočetní síly dnes pochází z Číny.

Historicky se procentuální poměr hodně rychle měnil. Pooly jako GHASH.IO, BTC Guild a nebo Slush's pool patřily mezi největší a vlastnily přes 30% veškeré výpočetní síly. Avšak i dnes patří mezi 10 největších [31].

3.10 Budoucnost bitcoinu

Lidé bitcoin vnímají pouze jako platební systém, ale ve skutečnosti je bitcoin technologií, pro kterou peníze jsou pouze jednou z možností využití. Podstatou je, že uživatelé si můžou sami rozhodnou, jakou hodnotu pro ně bitcoin představuje. V podkapitole 3.1 bylo zmíněno, že se bitcoin dělí na 100 milionů dílů nazývaných Satoshi. Každý tento dílek může být programován a můžou mu být přiděleny různé vlastnosti. 1 Satoshi potom může představovat m^3 plynu, prokazovat vlastnictví majetku, tanker ropy či třeba hlas ve volbách. Pokud představuje jeden bitcoin hodnotu třeba 500 euro, potom je možné tuto jednotku naprogramovat tak, aby byla použitelná pouze pro nákup jídla u certifikovaných obchodníku. Z tohoto důvodu už není třeba kontrolovat pravidla zpětně, peníze jsou takto přímo naprogramovány a kontrolovány při nákupu [7] [34].

Velice pravděpodobné ovšem je, že budoucností bitcoinu nebude bitcoin samotný. Bude to něco, co využívá technologie blockchain. Nicméně spoluzakladatel serveru Blocksteram.com Austin Hill v rozhovoru pro Institutional investor tvrdí, že výpočetní síla, která potvrzuje transakce v současném blockchainu je tak velká, že by bylo třeba investice 800 milionů až 1 miliardy dolarů s obrovským přístupem k polovodičům, aby mohl být současný blockchain narušen [35]. Příští generace programátorů přinesou stovky možností využití bitcoinu. Jenom je třeba si uvědomit, že peníze jsou pouze informace a bitcoin, potažmo blockchain přináší možnost, jak tyto informace bezpečně přenášet [36].

3.11 Jak získat bitcoiny anonymně?

Bitcoin není anonymní platební systém, tak jak se mnozí lidé domnívají. Kdykoliv používáme bitcoinového klienta zveřejňujeme tím naši IP adresu. Ať už bitcoiny získáváme miningem nebo je jednoduše nakupujeme, je třeba se registrovat v poolech či směnárnách. Pro nákup virtuálních měn na mezinárodních burzách je

vyžadováno ověření pomocí platného osobního identifikačního průkazu. Nákup bitcoinů musí být proveden platební kartou, která byla vystavena na stejné jméno na který je veden účet ve směnárně. I když si pro každou platbu vygenerujeme novou dvojici klíčů, při odesílání větší platby přiznáváme, že jsme právoplatní majitelé těchto transakcí. Tyto a další jsou příklady, kdy po sobě zanecháváme stopu a transakce mohou být jednoduše přiřazeny k naší identitě [21].

Jsou však postupy, jakými lze anonymní používání bitcoinu zařídit, anebo se mu alespoň přiblížit. Pro anonymní pohyb po internetu dobře poslouží TOR (The Onion Software), který funguje na principu klient-server. Veškerý klientův datový tok prochází nejprve sítí Tor a až potom je doručen cílovému počítači [37]. Díky tomu můžeme používat bitcoiny s tím, že se světem sdílíme pouze náš veřejný klíč. Tento veřejný klíč může být generován nový, pro každou příchozí transakci [5].

Pro anonymní nákup bitcoinů je třeba zřídit anonymní platební kartu. Pro tyto účely se dá velmi dobře použít například Blesk Peněženka [38]. Tato peněženka se nijak neliší od běžné platební karty a je vydávána ve spolupráci se společností MasterCard. Kartu lze získat ve větších trafikách po celé ČR. Pro úplné zajištění anonymního nákupu lze využít tzv. bílého koně. Přímo v trafice je potom možno na kartu bez prokázání totožnosti nahrát až 15000,- CZK. Kartu je však nutno zaktivovat pomocí SMS. Tuto SMS pošleme s anonymně koupenou SIM kartou. Český server simplecoin.cz umožňuje nákup bitcoinů pouze na základě emailové adresy, kterou je také možno založit anonymně. Na tuto emailovou adresu jsou potom zaslány platební údaje. Platbu provedeme pomocí anonymní karty. Ihned po připsání platby posílá Simplecoin.cz bitcoiny na uvedený veřejný klíč naší peněženky [39]. V tuto chvíli můžeme platit zcela anonymně získanými bitcoiny.

4 Bitcoin Mining – praktická část

Systém jakým jsou bitcoiny emitovány je již popsán v předchozí kapitole. V této části práce bych se rád na samotnou těžbu podíval z praktické stránky. Proto tato kapitola bude věnována těžbě bitcoinů jednak pomocí ASIC mineru z dílen Butterfly Labs a dále potom pomocí tzv. Cloud miningu. Pro tyto účely jsem využil služeb směnárny CEX.IO, která vlastní pool CHASH.IO

Server CEX.IO obchoduje s vlastní výpočetní silou podobně jako s jakoukoliv měnou či komoditou. Tuto výpočetní sílu, na serveru označovanou jako GHS, je možno směnit za USD nebo BTC [40]. Jakožto občanovi žijícím v Evropské Unii je pro mne mnohem výhodnější nákup GHS za Eura. Pro nákup BTC jsem se rozhodl využít směnárnu Kraken.com, která má dlouhodobě lepší kurzy.

4.1 Nákup BTC

Kraken, Payward Ltd. byl založen 28. Července 2011 v San Francisku, ale až po dvou letech vývoje byla oficiálně spuštěna první beta verze jejich systému. Server se těšil velkému úspěchu a postupně přidával možnost směny za další měny jako je euro, Japonský jen a další krypto měny Litecoin, Namecoin či Dogecoin atd. Dle oficiální zprávy zveřejněné na blogu společnosti bylo dne 14.1.2015 obchodováno na burze tohoto dne více než 12 000 BTC [41].

V podmínkách své práce jsem si dal za cíl, že bych nechtěl na investicích přesáhnout částku 5000 CZK. Proto jsem se rozhodl vložit na svůj účet v této směnárně 110 euro. Směnárna nyní přijímá vklady v eurech, Britských librách, Amerických dolarech a Japonských jenech. Zajímavostí je, že vyjma eura, u všech dalších měn je vyžadováno ověření třetího stupně. Tedy nahrání kopie osobního dokladu na server. V případě eura toto ověření u vkladů do 5000 USD měsíčně není vyžadováno. Je ovšem třeba podotknout, že tyto vklady musí být provedeny z účtu vedeného na stejné jméno, jako je uvedeno v registraci uživatele na serveru. Dotaz ohledně ověřování pomocí osobních dokladů jsem podal přímo na zákaznickou podporu serveru, kde mi bylo odpovězeno, že tyto doklady jsou vyžadovány ze

zákona, aby bylo zamezeno užívání ilegálně vydělaných peněz a podpory terorismu [41].

Pro samotný vklad jsem použil metodu SEPA platby, kterou moje banka, ZUNO BANK AG, zprostředkovává zcela zdarma. Po odeslání platby 110 EUR na účet vedený v německé bance Fidor Bank AG se mi z mého osobního účtu strhlo 3 074.83 CZK. K mému překvapení se vklad na mém účtu na serveru objevil zhruba po již 24 hodinách od odeslání platby.

Následoval obchod, kde jsem za 108.52 EUR + 0.37 EUR poplatek získal 0.479 BTC. Pokud počítám s poplatkem, obchodoval jsem za cenu **227.37 EUR/BTC**. Obchod byl rychlý a bez jakýchkoliv problémů. Celý proces trval v řádech sekundy. Po připsání bitcoinů na moji Kraken peněženku jsem část těchto prostředků převedl na peněženku na již zmíněné burze CEX.IO. Znovu transakce proběhla v řádu minut a bez problému. Musel jsem ale čekat tři bloky, tedy zhruba 30 minut, než byla transakce serverem CEX.IO potvrzena. Poplatek za tuto transakci byl 0.0005 BTC tedy asi 3 CZK. Zbytek prostředků jsem poslal na adresu své osobní peněženky Bitcoin-Qt. Při této transakci jsem již musel čekat 6 bloků (asi hodinu) než byla transakce potvrzena. Výpis transakcí z mé peněženky na serveru kraken.com můžete vidět na obrázku č. 4.1

Type	Currency	Amount	Fee	Balance
Withdrawal	Bitcoin (XBT)	-฿0.07850	฿0.00050	฿0.00000
Withdrawal	Bitcoin (XBT)	-฿0.39950	฿0.00050	฿0.07900
Trade	Euro (EUR)	-€108.54	€0.37	€1.07
Trade	Bitcoin (XBT)	฿0.47900	฿0.00000	฿0.47900
Deposit	Euro (EUR)	€110.00	€0.00	€110.00

Obrázek 4.1 : *Výpis transakcí peněženky na serveru kraken.com (Zdroj: Autor)*

4.2 Cloud mining

Vývoj projektu CEX.IO začal na začátku roku 2013, avšak společnost jako taková vznikla až v listopadu téhož roku. A ve stejném měsíci se GHASH.IO stal největším těžařským poolem na světě. GHASH.IO se nezaměřuje pouze na krypto měny

založené na algoritmu SHA256, ale také na Scryptu. Umožňuje tedy i těžbu krypto měn Litecoin a Dogecoin. Jelikož se jedná o pool, je možné jej propojit s vlastním minerem. Dále potom server nabízí i affilate program. Což jsou jeho velké výhody oproti dalším poolům. Díky své velké popularitě pool v lednu a podruhé v únoru 2014 překročil 50% celkové výpočetní síly Bitcoinu. To by samozřejmě mohlo vést k tzv. 51% attack, který by umožnil Double spending Bitcoinů. Z těchto důvodů mnoho těžařů pool opustilo a přidalo se k menším poolům. GHASH.IO následně vydal dobrovolně prohlášení, že nebude překračovat hodnotu 39.99% celkové výpočetní síly a k tomuto kroku vyzval také další pooly [42].

Oproti směnárně kraken.com akceptuje CEX.IO i vklady pomocí platebních karet, pro které není vyžadována žádná verifikace. Je zde ale docela velký transakční poplatek 4.5% a fixní poplatek 0.25 EUR nebo USD. Zde je potom měsíční limit 15 000 USD/EUR podle druhu vkladu. Naopak pro jakýkoliv typ převodu je žádána kopie osobního dokladu, fotografie kde tento doklad držíme a kopie dokumentu dokazující naše bydliště.

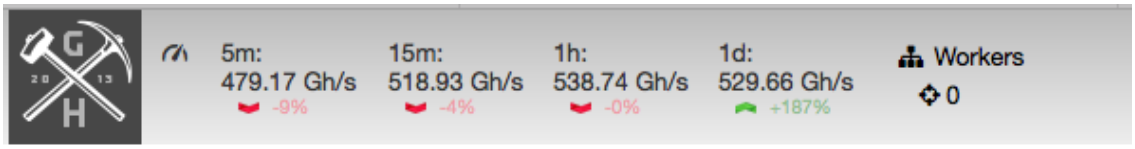
Z obrázku číslo. 4.1 vyplývá, že na moji peněženku na serveru CEX.IO bylo připsáno 0.39950BTC. Na této burze jsem potom nakoupit celkem 543.55098046 GHS za cenu 0.39099999 BTC. Na této peněžence mi posléze zbylo 0.0085001 BTC. Celý proces transakcí je vidět na obrázku č. 4.2.

Částka	Zůstatek	Typ	Poplatek	Popis transakce
-0.39099999 BTC	0.00850001	BUY	-	Buy Order #3277545483
313.03855099 GHS	543.55098046	BUY	฿0.00044953	Bought 313.03855099 GHS at 0.00071801 BTC
2.00000000 GHS	230.51242947	BUY	฿0.00000287	Bought 2.00000000 GHS at 0.000718 BTC
15.00000000 GHS	228.51242947	BUY	฿0.00002153	Bought 15.00000000 GHS at 0.0007179 BTC
2.00000000 GHS	213.51242947	BUY	฿0.00000288	Bought 2.00000000 GHS at 0.00071788 BTC

Obrázek 4.2 : *Nakupování výpočetní síly na burze CEX.IO (Zdroj: Autor)*

V tomto okamžiku jsem konečně mohl začít s virtuálním těžením. Oproti těžbě za pomocí ASIC je spuštění cloudového těžení jednoduché. Nikde se nic nenastavuje, pouze se těžba aktivuje v nastavení uživatele. Pro spuštění je zapotřebí splnit dvě

podmínky. Tou první je vlastnictví nějaké výpočetní síly a druhou kladný zůstatek BTC. Obě podmínky splňuji. Po spuštění těžby téměř okamžitě vidím svou aktivní výpočetní sílu. Po zhruba 24 hodinách zjišťuji, že má reálná výpočetní síla je o necelých 14 Gh/s nižší než ta, kterou vlastním.



Obrázek 4.3 : *Progres práce vlastněné výpočetní síly na serveru GHASH.IO (Zdroj: Autor)*

Jak jsem již zmínil, velkou výhodou tohoto poolu je, že zároveň s bitcoinem jsou těženy i další krypto měny. Konkrétně se jedná o Namecoin (NMC), Ixcoin (IXC) a Devcoin (DVC). Na serveru GHASH.IO jsem virtuálně těžil celkem 46 hodin. Za tuto dobu se mi podařilo natěžit celkem 0.02833260 NMC. Za takto natěžené NMC nejsou strhávány žádné udržovací poplatky a celá částka mi tedy byla připsána do mojí peněženky. Žádnou další ze zmíněných alternativních měn se mi získat nepodařilo.

Úplně odlišná situace nastala v případě těžby bitcoinů, na kterou se server specializuje. Za každý potvrzený blok je emitována částka 25 BTC plus poplatky které uživatelé dávají ke svým transakcím. Tuto částku si mezi sebou těžaři rovnoměrně rozdělí. Abych to zrekapituloval, svou těžbu jsem začal zůstatkem 0.00850001 BTC a 543.55098046 GHS. První potvrzený blok, na kterém jsem se podílel, byl potvrzen přibližně po 12 hodinách. Jednalo se o blok číslo 351317. Nutno podotknout, že jsem se k těžbě přidal přibližně v polovině. To znamená, že celková práce na tomto bloku trvala 24 hodin. Můj podíl se rovnal 0.00104041 BTC. Co mě ale překvapilo, bylo stržení takzvaného poplatku za údržbu, který si server účtuje za každý potvrzený blok. Tento poplatek je na krytí účtů za elektřinu, opravu minerů, správu a další náklady spojené s provozem cloud miningu. Poplatek se rovnal částce 0.00382773 BTC. Takže po prvním potvrzeném bloku se zůstatek v mé peněžence snížil na 0.00571269 BTC.

Původní zůstatek: 0.00850001 BTC
Podíl ze zisku 0.00104041 BTC **<** Náklady na údržbu 0.00382773 BTC
Konečný zůstatek: 0.00571269 BTC
Rozdíl: -0.00278732

Další blok generovaný poolem byl vytěžen asi o 33 minut později. Zde je dobře vidět, že provádění hashovacíh operací závisí hodně na náhodě. V tomto případě byl také podíl na zisku větší než provozní náklady. Zisku se tedy dá docílit, pokud těžba probíhá kratší dobu, než přibližně 4 hodiny. Přesnější odhad se mi nepodařilo získat, z důvodu ukončení těžby po 46 hodinách.

Původní zůstatek: 0.00571269 BTC
Podíl ze zisku 0.00104333 BTC **>** Náklady na údržbu 0.00003284 BTC
Konečný zůstatek: 0.00672318 BTC
Rozdíl: +0.00101049

Tímto způsobem probíhala těžba, bez jakéhokoliv zasahování až do doby, kdy po 46 hodinách začal být můj zůstatek v BTC peněžence záporný. V tomto okamžiku byl cloud mining na mém účtu automaticky zastaven. A mé zůstatky byly následující:

BTC: -0.00037719

NMC: 0.02833260

GHS: 543.55098046

Těžbou se mi tedy podařilo získat malé množství virtuální měny Namecoin, které momentálně nemá téměř žádnou hodnotu. Dále jsem však přišel o svůj počáteční zůstatek BTC a nyní ještě serveru dlužím 0.00037719 BTC. Z toho jasně vyplývá, že cloud mining v době psaní této části bakalářské práce (duben 2015) není výhodný a proto nevyvrací hypotézu uvedenou v úvodu práce.

Provozní náklady jsou samozřejmě hrazeny poskytovatelům v běžných měnách, avšak od těžařů jsou vybírány v BTC. Jelikož je aktuální hodnota 1 BTC rovna

přibližně 230 EUR, jsou poplatky vybírané od těžařů vyšší než provize, které těžbou získají. Pracovníci z podpory serveru CEX.IO mě informovali, že by hodnota musela přesáhnout 305EUR/BTC, aby se cloud mining stal znovu výdělečným.

4.3 ASIC mining

Pro prvotní těžbu bitcoinů byly dostačující běžné procesory v našich počítačích. Postupem času bylo objeveno, že grafické jsou pro tuto činnost mnohem vhodnější a od užívání procesorů se upustilo. Velmi oblíbené se proto staly grafické karty od výrobce ATI Technolgogies, Inc., řady Radeon R9. Dodnes je zejména americký aukční portál Ebay.com těchto karet plný [18]. V dnešní době však už ani tento způsob těžby není efektivní a je využíváno pouze ASIC minerů. Tyto čipy byly vytvořeny k jednomu jedinému účelu a tím je právě těžba bitcoinů. Zřejmě první člověk, které mu byl kdy doručen ASIC miner, byl Jeff Garzik, který 30. Ledna 2013 pomocí twitteru zveřejnil, že mu doručena zásilka z Číny [43]. Tato zásilka obsahovala miner vyrobený společností Avalon, který disponoval výpočetní silou 68 GH/s. V dnešní době společnost na svém webu nabízí miner Avalon 4.1 za cenu 5.95BTC Výpočetní síla tohoto mineru je 4.2 TH/s [44].

Prodejců nabízejících nové minery v České republice je opravdu málo a jejich ceny přes 10,000 CZK by nesplňovaly zadání této práce. Proto jsem se rozhodl pro nákup použitého mineru na některém z aukčních portálů. Nakonec se mi podařilo za částku 521 CZK vydražit na českém serveru Aukro.cz ASIC miner Jalapeno z dílny Butterfly Labs. Jalapeno slibuje výpočetní sílu 5 Gh/s. Musím dodat, že jeho cena se na americkém Ebay.com aktuálně pohybuje v rozmezí 1000 – 3500 CZK.

4.3.1 Detailní popis ASIC mineru BFL Jalapeno

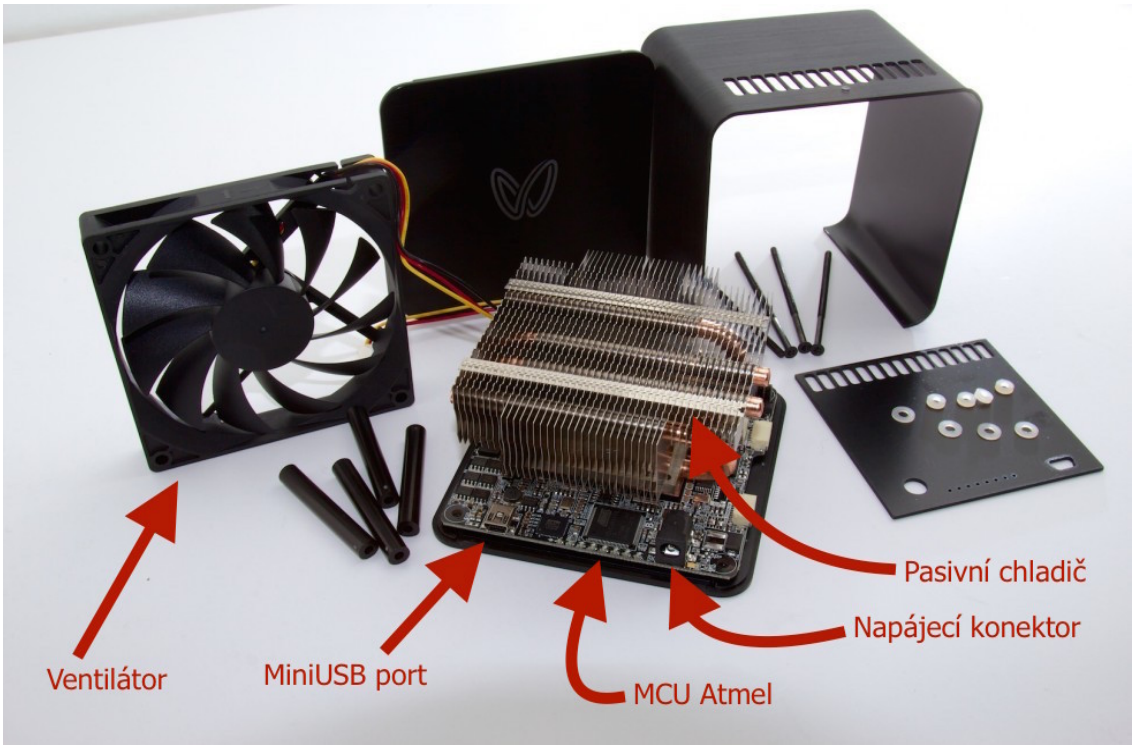
Zhruba v polovině roku 2012 společnost Butterfly Labs Inc. oznámila, že začne vyrábět bitcoinové minery, které využívají ASIC technologie. Později, na konci června, začala přijímat první předobjednávky s cenovkou 274 dolarů za 5 GHs výkonu. Společnost slibovala dodání na podzim téhož, roku avšak první minery byly doručeny až v dubnu roku 2013 [45] [46].

Technické parametry:

- Rozměry: 10 x 10 x 7.6 cm
- Váha: 0.6 kg
- Provozní teplota: 80 °C
- Spotřeba elektřiny: 32 Wh

Miner je díky svému ventilátoru při těžbě poměrně hlučný.

Obrázek 4.4 : Bitcoin miner Butterfly Labs Jalapeno 5 GHs (Zdroj: [46])



Obrázek 4.5 : Komponenty mineru BFL Jalapeno (Zdroj: [45]

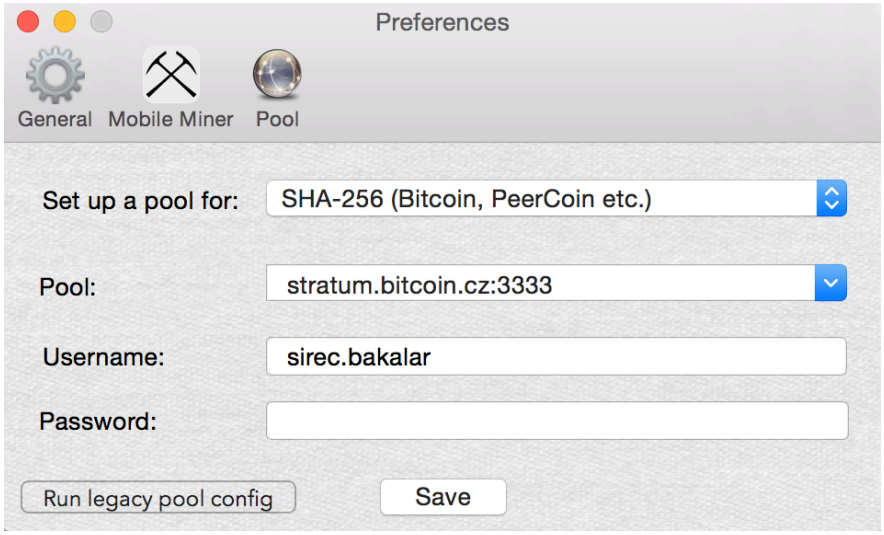
Jelikož jsem Čech, je pro mne snad i povinností připojit svou výpočetní sílu k prvnímu založeném poolu na světe vůbec – Slush's poolu. Tento pool byl založen 27. listopadu 2010 českým programátorem Martinem Palatinusem neboli slushem. Slushovým posledním projektem je Bitcoin trezor. Současná výpočetní síla tohoto poolu je přibližně 15.5 Ph/s [47][48].

Pool běží na serveru https://mining.bitcoin.cz. Registrace je jednoduchá a je vyžadováno pouze ověření pomocí emailu. Pro přidání vlastního mineru je třeba vytvořit tzv. Workera (pracovníka). Jméno každého pracovníka je složeno z přihlašovacího jména a názvu pracovníka ve formátu: prihlasovaci_jmeno.nazev_pracovnika. Přihlašovací jméno mého zařízení je sirec.bakalar. Heslo není třeba vyplňovat, protože v případě krádeže přihlašovacích údajů zařízení, by pouze dotyčná osoba těžila v můj prospěch.

Miner Jalapeno byl pomocí standardního USB kabelu připojen k laptopu MacBook Pro 13“ 2013 Late v konfiguraci Intel Core i5 2.4 Ghz Haswell, 8GB DDR3 1600MHz Ram. Počítač běží pod operačním systémem OS X Yosemite verze 10.10.2. Pro

propojení mineru se serverem Slush's poolu jsem využil aplikaci MacMiner verze 1.5.24. Tato aplikace nabízí jednoduché GUI, podporu tří nejrozšířenějších backendů (bfgminer, cgminer, cpuminer). Není tedy nutné instalovat žádné další dodatky v terminálu.

Po spuštění MacMineru je třeba nastavit, jaký druh virtuální měny budeme těžit, server poolu a přihlašovací údaje zařízení. Mé nastavení je vidět na obrázku číslo 4.6.



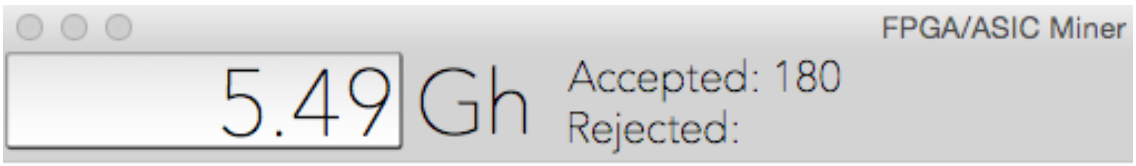
Obrázek 4.6 : Nastavení aplikace MacMiner pro připojení k Slush's poolu (Zdroj: Autor)

V záložce „View" klikneme na „Show ASIC Device Miner". Po otevření okna spustíme těžbu kliknutím na tlačítko „Start". MacMiner automaticky detekuje připojený miner Jalapeno a začíná těžit. Jako první je spuštěn back-end bfgminer verze 5.0.0. Dále je načten konfigurační soubor, který obsahuje informace o serveru, název klienta atd. Následuje připojení k serveru pomocí protokolu stratum. Dále je informace o aktuální složitosti celé sítě 49.4G = 49446390688. Na dalším řádku je popsána detekce nového bloku následována informací o tom, že API běží na portu 4028. Každých 20 sekund MacMiner vypisuje průměrnou rychlost minerů, přijaté (A:), zamítnuté (R:) bloky a hardwarové problémy (HW:). Jelikož byla těžba právě zahájena, logicky nebyly zatím akceptovány žádné bloky, ani se nevyskytnul žádný HW problém. Celý start aplikace je vidět na obrázku číslo 19.

```
[2015-04-11 21:17:13] Started bfgminer 5.0.0-unknown
[2015-04-11 21:17:13] Loaded configuration file /Users/RiVall/Library/Application Support/MacMiner/bfgurls.conf
[2015-04-11 21:17:14] Probing for an alive pool
[2015-04-11 21:17:15] Pool 0 http://stratum.bitcoin.cz:3333 alive
[2015-04-11 21:17:15] Pool 0 is hiding block contents from us
[2015-04-11 21:17:15] Network difficulty changed to 49.4G (354.0P)
[2015-04-11 21:17:15] Stratum from pool 0 detected new block
[2015-04-11 21:17:16] API running in IP access mode on port 4028
20s: 2.08 avg: 5.36 u: 4.51 Gh/s I A:0 R:0+0(none) HW:0/none
20s: 3.35 avg: 5.36 u: 5.26 Gh/s I A:0 R:0+0(none) HW:0/none
20s: 4.21 avg: 5.44 u: 4.86 Gh/s I A:0 R:0+0(none) HW:0/none
[2015-04-11 21:18:25] Accepted 01fea0db BFL 0  Diff 128/10
[2015-04-11 21:18:31] Accepted 1186848f BFL 0  Diff 14/10
[2015-04-11 21:18:35] Accepted 0ee2a9f0 BFL 0  Diff 17/10
```

Obrázek 4.7 : Startování těžby v aplikaci MacMiner (Zdroj: Autor)

Další obrázek č. 4.8 popisuje průběh těžby. V levém horním rohu je vidět současná rychlost těžby. 5.49 GH/s je téměř o 10% více, než je napsáno v popiscích od výrobce. Vedle toho se nachází informace o přijatých a zamítnutých blocích. 0 zamítnutých bloků naznačuje, že je vše v naprostém pořádku. První řádek ukazuje datum a aktuální čas, informaci o přijetí bloku, jeho číslo, druh mineru BFL (Butterfly labs) a obtížnost bloku.




```
[2015-04-10 21:01:19] Accepted 06268d97 BFL 0  Diff 41/8
[2015-04-10 21:01:21] Accepted 1a6e5b17 BFL 0  Diff 9/8

[2015-04-10 21:01:21] Accepted 1a6e5b17 BFL 0  Diff 9/8
20s: 5.46 avg: 5.44 u: 5.57 Gh/s I A:171 R:0+0(none) HW:0/none
[2015-04-10 21:01:27] Accepted 0ec14e41 BFL 0  Diff 17/8

[2015-04-10 21:01:27] Accepted 0ec14e41 BFL 0  Diff 17/8
[2015-04-10 21:01:33] Accepted 121ae12b BFL 0  Diff 14/8

[2015-04-10 21:01:33] Accepted 121ae12b BFL 0  Diff 14/8
[2015-04-10 21:01:40] Accepted 16aee766 BFL 0  Diff 11/8

[2015-04-10 21:01:40] Accepted 16aee766 BFL 0  Diff 11/8
20s: 5.34 avg: 5.43 u: 5.53 Gh/s I A:174 R:0+0(none) HW:0/none
[2015-04-10 21:01:47] Accepted 0167b0ec BFL 0  Diff 182/8
```

Obrázek 4.8 : Průběh těžby v aplikaci MacMiner (Zdroj: Autor)

Oproti cloud miningu na CEX.IO si Slush‘s neúčtuje žádné provozní, ani jiné poplatky. Každopádně můj miner spotřebovává přibližně 32 wattů za hodinu. Tato hodnota byla získána pomocí wattmetru. Náklady spojené s provozem počítače, externího displeje a dalších zařízení počítat nebudu, protože by běžely i v případě nevyužívání mineru. V roce 2015 by cena elektřiny měla být 4.83 CZK/kWh včetně DPH a dalších poplatků [49].

Pomocí ASIC mineru jsem s odchylkou pár minut těžil 10 dnů. Pokud budu uvažovat cenu 0.00483 CZK/Wh, spotřeboval Jalapeno miner za 10 dnů elektřinu v ceně **37.0944 CZK**

Cena elektřiny spotřebovaná minerem za hodinu..... 32 x 0.00483 = 0.15456 CZK
Cena elektřiny spotřebovaná minerem za 240 hodin..... 240 x 0.15456 = 37.0944 CZK

Za těchto 10 dnů jsem se podílel na generování 62 bloků. Zde musím dodat, že podle statistik nebyla moje výpočetní síla vždy přes 5 GH/s. Občas Slush’s pool zobrazoval skórovací Hash rate okolo 3.5 GH/s. Předpokládám, že toto bylo zapříčiněno občasným odpojením počítače od internetu a tím byla ztracena komunikace se serverem. Za tuto práci jsem byl poolem odměněn 0.00048 BTC. Pokud převedu částku na České koruny, dostanu přibližně 2.94 CZK [50].

Zajímavostí je, že minimální výše odměn, kterou je Slush’s pool ochoten poslat do soukromé peněženky je 0.01 BTC. Musel bych těžit více než 209 dnů při současné složitosti, abych na tuto sumu dosáhl.

Po odečtení nákladů a odměn za těžbu je vidět, že jsem skončil ve ztrátě 34.1544 CZK. Ani tento druh těžby tedy nevyvrací hypotézu o nevýnosnosti miningu.

Celkové náklady za elektřinu: 37.0944 CZK
Celkové odměny za těžbu: 2.94 CZK
Rozdíl: **-34.1544**

4.4 Hypotéza: Bitcoin mining v domácích podmínkách není výnosný.

V případě cloud miningu jsem po skončení těžby přišel celkem o 0.0088772 BTC(53.10 CZK), které jsem musel uhradit po převedení výpočetní síly zpět na Bitcoiny. Pokud bych nepočítal cenu ASIC mineru, tak rozdíl mezi odměnami za těžbu a náklady na elektrickou energii je -34.1544 CZK.

Otestováním obou metod Bitcoin miningu jsem nepřišel k žádnému zisku a tím byla hypotéza potvrzena.

5 Závěr

V teoretické části této bakalářské práce jsou popsány základní principy fungování bitcoinu a zejména potom aktualizovány údaje na současné poměry. Přece jen se tato kryptografická měna velmi rychle vyvíjí a dost možná, že za pár měsíců i údaje v této bakalářské práci nebudou aktuální. Během psaní této práce jsem objevil spoustu dalších problémů, jejichž zkoumání a testování by mohly být dobrými náměty pro pokračování na úrovni diplomové práce.

Pozůstatkem po této práci jsou odkazy v blockchain, dokazující vlastnictví mého veřejného klíče okolo 0.5 BTC. Tuto částku převádět zpět na CZK nebudu a kopii peněženky si uložím na externí úložiště. Jako spekulant budu doufat ve zhodnocení a hodnotu přesahující tisíce USD.

Praktickým přínosem pro čtenáře této práce by mělo být faktické ověření nevýnosnosti těžby bitcoinů v domácím prostředí. Zde si troufám poukázat na fakt, že už i v dnešní době jsou třeba investice v řádech desítek tisíc USD, abychom měli alespoň základní předpoklad pro schopnost generování bloků. Faktem je že dnešní hodnota BTC je tak nízká, že ani získání odměny 25 BTC není dostatečné pro pokrytí našich nákladů. Čím budou potom těžaři motivováni v budoucnosti, když celý koncept bitcoinu je závislý na jejich práci?

V této bakalářské práci byly otestovány dvě metody těžby bitcoinů a dále provedena jejich analýza z důvodů určení výnosnosti. Z výsledků jasně vyplývá, že těžba bitcoinů v domácích podmínkách nepřináší vůbec žádný zisk a s největší pravděpodobností skončí těžař ve ztrátě. Aby se cloudová těžba stala znovu výdělečnou, musela by hodnota jednoho bitcoinu vzrůst alespoň na 305 EUR. U těžby pomocí minerů, které připojíme k poolu je situace ještě tragičtější a v podstatě v dnešní době není možné vydělat těžbou ani na počáteční investici do mineru.

Terminologický slovník

Pojem	Význam
Adresa	Identifikační číslo dlouhé 26-35 znaků, které začíná číslem 1 nebo 3. Na tuto adresu se posílají BTC [5].
ASIC	Application Specific Integrated Circuit je obvod vytvořený pro specifickou činnost [3].
Bdiff	Hodnota vypočítaná pomocí target hodnoty určující obtížnost zařazení nového bloku do blockchainu[28].
Bids	Bids je hodnota uložená v hlavičce bloku přenášející informaci o targetu[28].
Bitcoin	Bitcoin je projekt vytvořený pseudonymem Satoshi Nakamoto. Tento projekt umožňuje decentralizované posílání bitcoinů pomocí peer-to-peer sítě. Pojmem bitcoin je také označována jednotka virtuální měny[Vlastní definice autora].
Blok	Bloky obsahují transakce provedené přibližně ve stejné době a odkaz na blok předchozí. Blok je tvořen jednou za 10 minut[Vlastní definice autora].
Blockchain	Účetní kniha bitcoin sítě obsahující veškeré transakce provedená za celou historii. Blockchain je tedy řetězec všech potvrzených bloků[5].
BTC	Zkratka pro bitcoin jako virtuální měnu. 1 BTC = 100,000,000 Satoshi
Cloud mining	Cloud mining je pronájem výpočetní síly umožňující těžbu bitcoinů[Vlastní definice autora].
Coinbase	Transakce emitující nové bitcoiny. Coinbase je vždy uvedena v bloku jako první[5].
Genesis blok	Genesis blok nebo také blok 0 je vůbec první blok, který byl vytvořen 3.1.2009. Je také stanovující hodnotou pro výpočet targetu [7].
Input	Vstupní informace transakce obsahující odkazy na předchozí transakce a dokazující vlastnictví bitcoinů[12].
Krypto-grafie	Vědní disciplína vycházející z kryptologie. Kryptografie zajišťuje utajovanou komunikaci [9].
Merkle root	Merhleho kořen je otisk vzniklý z otisků všech transakcí v bloku. Vždy se vezmou dva otisky transakcí, ze hterých se vytvoří pouze jeden otisk. Tímto systémem se pokračuje, až zůstane pouze jeden poslední otisk - merkleho kořen [26].
Micro-controller	Zkráceně MCU je integrovaný obvod, který obsahuje celý mikropočítač[Vlastní definice autora].
Miner	Označení pro člověka zabývající se těžbou, nebo také pro konkrétní zařízení, které těžbu provádí[Vlastní definice autora]..
Mining	Proces vytváření otisků pro zařazení bloku do blockchainu[Vlastní definice autora]..
Otisk	Výstup hashovací funkce, která převádí data na většinou kratší číslo o fixní délce[8].
Output	Výstupní informace z transakce. Outputy obsahují informace o tom, na jakou adresu budou jednotlivé inputy odeslány[12].
Peer-to-peer	V přímém překladu jako rovný s rovným, je typ sítě, která umožňuje komunikaci přímo mezi jednotlivými uživateli[7].
Peněženka	Peněženka je aplikace, která se stará o správu soukromých klíčů a

	tvorbu transakci[5].
Pool mining	Poolem je označováno sdružení těžařů, kteří spojují svou výpočetní sílu, a když se některému podaří generovat nový blok, následnou odměnu si rovnoměrně rozdělí [48].
Proof-of-work	Jedná se koncept, kdy je třeba prokázání vykonané práce předtím, než je služba obdržena[5].
SHA-256	SHA-256 je druh hashovacího algoritmu, jehož výstupem je 256-bitový otisk[8].
Target	Target je hodnota, se kterou miner srovnává výsledný otisk bloku [28].
TOR	Software umožňující anonymní pohyb na internetu[37].
Transakce	Transakce jsou vysílány do bitcoin sítě za účelem posílání BTC mezi uživateli [7].
Uzel	Účastník peer-to-peer sítě[Vlastní definice autora].

Literatura

[1] What is Bitcoin? *bitcoin.org* [online]. [vid. 2. duben 2015]. Dostupné z: https://bitcoin.org/en/faq#what-is-bitcoin

[2] Bitcoin Market Price (USD). *blockchain.info* [online]. [vid. 11. duben 2015]. Dostupné z: https://blockchain.info/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

[3] Zákaznický integrovaný obvod - ASIC. *Wikipedie - otevřená encyklopedie* [online]. [vid. 2. duben 2015]. Dostupné z: http://cs.wikipedia.org/wiki/Z%C3%A1kaznick%C3%BD_integrovan%C3%BD_obvod

[4] BÁBEK, JIŘÍ. Finanční analýza a vzorce. *INBOOX* [online]. 8. březen 2013 [vid. 23. duben 2015]. Dostupné z: http://www.inboox.cz/news/financni-analyza-a-vzorce-pro-humanitni-typy/

[5] ANTONOPOULOS, ANDREAS M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA: O'Reilly Media, 2014. ISBN 978-1-4493-7403-7.

[6] DOSTÁLEK, LIBOR. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* Brno: Computer Press, 2006. ISBN 80-251-0828-7.

[7] FRANCO, PEDRO. *Understanding Bitcoin: Cryptography, Engineering and Economics*. Hoboken, New Jersey: Wiley, 2014. ISBN 978-1-119-01916-9.

[8] PALOVSKÝ, RADOMÍR. Bezpečnost informačních systému - Přednáška 2. In: . Přednáška. VŠE. 23. únor 2015.

[9] KLIMEŠ, CYRIL. Kryptografie. In: [online]. B.m. [vid. 28. březen 2015]. Dostupné z: http://prf-czv.osu.cz/nabidka/seminar/data/Kryptografie.pdf

[10] ANTOINE DE SAINT-EXUPÉRY. *Malý princ*. Praha: Ottovo nakladatelství, 1998. ISBN 80-7181-244-7.

[11] SSL Certificate by Symantec. *symantec.com* [online]. [vid. 8. duben 2015]. Dostupné z: http://www.symantec.com/ssl-certificates/#

[12] DRISCOLL, SCOTT. How Bitcoin Works Under the Hood. *ImponderableThings (Scott Driscoll's Blog)* [online]. [vid. 24. březen 2015]. Dostupné z: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

[13] Bankovky a štátovky 1953 / 25 Kčs - 1953. *mojasbierka.sk - zberateľský portál* [online]. [vid. 15. duben 2015]. Dostupné z: http://www.mojazbierka.sk/index.php?m=bankovka&id=96

[14] MARADA, TOMÁŠ. *Vás názor na problematiku Bitcoinu a dalších virtuálních kryptoměn*

[15] *Satoshi Nakamoto - Wikipedia, the free encyclopedia* [online]. [vid. 5. duben 2015]. Dostupné z: http://en.wikipedia.org/wiki/Satoshi_Nakamoto

[16] Bitcoin History: The Complete History of Bitcoin [Timeline]. *History of Bitcoin* [online]. [vid. 3. duben 2015]. Dostupné z: http://historyofbitcoin.org/

[17] HORNYAK, TIM. One year later, we're no closer to finding MtGox's missing millions worth of bitcoins. *PCWorld - Work. Life. Productivity.* [online]. [vid. 11. duben 2015]. Dostupné z: http://www.pcworld.com/article/2892892/one-year-later-were-no-closer-to-finding-mtgoxs-missing-millions.html

[18] OBERMAIER, Z. Bitcoin v roce 2015: pád na dno, nebo restart? *pctuning* [online]. 9. březen 2015 [vid. 9. duben 2015]. Dostupné z: http://pctuning.tyden.cz/hardware/site-a-internet/33637-bitcoin-v-roce-2015-pad-na-dno-nebo-restart?start=5

[19] EVERETT, ROSENFELD. Feds auction $13.5M worth of Silk Road bitcoins. *CNBC* [online]. 5. březen 2015 [vid. 16. duben 2015]. Dostupné z: http://www.cnbc.com/id/102480336

[20] Bitcoin Price Index - Real-time Bitcoin Price Charts. *CoinDesk* [online]. [vid. 6. duben 2015]. Dostupné z: http://www.coindesk.com/price/

[21] KRUPA, VLADIMÍR. Minulost, současnost a budoucnost produkce peněz. In: *Bitcoin meetup*. Paralelní Polis, Praha. 14. duben 2015.

[22] NAKAMOTO, SATOSHI. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. 31. říjen 2008 [vid. 12. březen 2015]. Dostupné z: http://bitcoin.org/bitcoin.pdf

[23] HERENCSÁR, ALBERT. *Kryptografická mena bitcoin* [online]. 2012 [vid. 16. duben 2015]. Dostupné z: http://www.dcs.fmph.uniba.sk/bakalarky/registracia/getfile.php/bak.pdf?id=221&fid=430&type=application%2Fpdf

[24] Block Chain Height, Block Height. *Bitcoin Glossary* [online]. [vid. 13. duben 2015]. Dostupné z: https://bitcoin.org/en/glossary/block-height

[25] Bitcoin Difficulty and Hashrate Chart. *BitcoinWisdom* [online]. [vid. 13. duben 2015]. Dostupné z: https://bitcoinwisdom.com/bitcoin/difficulty

[26] Merkle tree. *Wikipedia, the free encyclopedia* [online]. [vid. 7. duben 2015]. Dostupné z: http://en.wikipedia.org/wiki/Merkle_tree

[27] PAVEL, MATEJ. *Problémy virtuální měny Bitcoin*. Prague, 2014. Universit of Economics, Prague.

[28] Difficulty - Bitcoin. *Bitcoin wiki* [online]. [vid. 9. duben 2015]. Dostupné z: https://en.bitcoin.it/wiki/Difficulty

[29] Proof of work - Bitcoin. *Bitcoin wiki* [online]. [vid. 9. duben 2015]. Dostupné z: https://en.bitcoin.it/wiki/Proof_of_work

[30] Bitcoin Hash Rate. *Blockchain.info* [online]. [vid. 13. duben 2015]. Dostupné z: https://blockchain.info/charts/hash-rate

[31] Bitcoin Hashrate Distribution. *Blockchain.info* [online]. [vid. 5. duben 2015]. Dostupné z: https://blockchain.info/pools

[32] HIGGINS, STAN. How Discus Fish Became China's Largest Bitcoin Mining Pool. *CoinDesk* [online]. 19. září 2014 [vid. 8. duben 2015]. Dostupné z: http://www.coindesk.com/chinese-mining-pool-discus-fish-bitcoin/

[33] Bitmain Technologies Ltd. *BITMAIN* [online]. [vid. 10. duben 2015]. Dostupné z: https://www.bitmaintech.com/about.htm

[34] Bitcoin Properly. *The real value of Bitcoin and crypto currency technology* [online]. [vid. 11. duben 2015]. Dostupné z: http://www.bitcoinproperly.org/#sthash.mgNR6vvE.UOj4NvJ4.dpbs

[35] TIMMS, AARON. The Future of Bitcoin Is Not Bitcoin. *Institutional Investor* [online]. 18. prosinec 2014 [vid. 17. duben 2015]. Dostupné z: http://www.institutionalinvestor.com/article/3411499/banking-and-capital-markets-trading-and-technology/the-future-of-bitcoin-is-not-bitcoin.html?ArticleId=3411499&p=2#.VTDTYRemSq5

[36] MAULDIN, JOHN. Is Bitcoin the Future? *Forbes.com* [online]. 1. prosinec 2014 [vid. 17. duben 2015]. Dostupné z: http://www.forbes.com/sites/johnmauldin/2014/12/01/is-bitcoin-the-future/16/

[37] Tor Project: FAQ. *Anonymity Online* [online]. [vid. 26. duben 2015]. Dostupné z: https://www.torproject.org/docs/faq.html.en

[38] Blesk peněženka. *Bleskpenezenka.cz* [online]. [vid. 26. březen 2015]. Dostupné z: http://penezenka.blesk.cz/

[39] SimpleCoin - snadný nákup Bitcoinů. *Nakupujte a prodávejte Bitcoiny jednoduše.* [online]. [vid. 17. březen 2015]. Dostupné z: http://www.simplecoin.cz/

[40] About Us - CEX.IO. *Bitcoin exchange* [online]. [vid. 6. duben 2015]. Dostupné z: https://cex.io/about/

[41] Kraken - About. *Buy, Sell, and Trade Bitcoins* [online]. [vid. 6. duben 2015]. Dostupné z: https://www.kraken.com/en-us/about

[42] RIZZO, PETE. Ghash.io: We Will Never Launch a 51% Attack Against Bitcoin. *CoinDesk* [online]. 16. červen 2014 [vid. 9. duben 2015]. Dostupné z: http://www.coindesk.com/ghash-io-never-launch-51-attack/

[43] Jeff Garzik on Twitter: „My wife informs me that a package from China arrived. Will investigate when I return home. #Bitcoin". *Twitter* [online]. 30. leden 2013 [vid. 5. duben 2015]. Dostupné z: https://twitter.com/jgarzik/status/296709252351926273

[44] Avalon4.1 4.2T Suite. *EHash Avalon* | [online]. [vid. 15. duben 2015]. Dostupné z: https://ehash.com/product/avalon4-3t-suite-2/

[45] HUTCHINSON, LEE. How a total n00b mined $700 in bitcoins. *Ars Technica* [online]. 30. červen 2013 [vid. 17. duben 2015]. Dostupné z: http://arstechnica.com/gadgets/2013/06/how-a-total-n00b-mined-700-in-bitcoins/

[46] BRADBURY, DANNY. Butterfly Labs' Jalapeno aims to spice up bitcoin mining. *CoinDesk* [online]. 24. duben 2013 [vid. 2. duben 2015]. Dostupné z: http://www.coindesk.com/jalapeno-aims-to-spice-up-bitcoin-mining/

[47] Kontakt | Bitcoin.cz. *BITCOINCZ* [online]. [vid. 17. duben 2015]. Dostupné z: http://blog.bitcoin.cz/kontakt/

[48] Bitcoin Pooled Mining - Bitcoin. *Bitcoin wiki* [online]. [vid. 15. duben 2015]. Dostupné z: https://en.bitcoin.it/wiki/Bitcoin_Pooled_Mining

[49] WOLF, PETR. Jaká je aktuální cena kWh a MWh elektřiny? *Ceny energie* [online]. 22. leden 2015 [vid. 4. duben 2015]. Dostupné z: http://www.cenyenergie.cz/jaka-je-aktualni-cena-kwh-a-mwh-elektriny/

[50] Bitcoin kalkulačka a Bitcoin kurz - vše o digitální měně Bitcoin, kurzy, mining, hashrate, novinky (2015). *Bitcoinman* [online]. [vid. 6. duben 2015]. Dostupné z: http://www.bitcoinman.cz/index.php?c=bitcoin-kalkulacka-bitcoin-kurz

Seznam obrázků