Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra informačních technologií

Studijní program : Aplikovaná informatika

Obor: Informační systémy a technologie

Analýza těžby alternativních kryptoměn

DIPLOMOVÁ PRÁCE

Student : Bc. Miroslav BALLEK

Vedoucí : Ing. Tomáš Bruckner, Ph.D.

Oponent : Ing. Michal Šebesta

2014

Prohlášení:

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

V Praze dne 15.12.2014 . . . . . .

Miroslav Ballek

Poděkování

Rád bych tímto způsobem poděkoval především mému vedoucímu práce, panu doktoru Brucknerovi zato, že se mnou měl ohromnou trpělivost.

Abstrakt

Bitcoin se v průběhu několika posledních let stal globálně úspěšným a velmi sledovaným projektem. Jedná se o druh decentralizované digitální měny, jejíž fungování je založeno na matematicko-kryptografických principech a vzniká pomocí výpočetně náročného procesu, který se nazývá těžba. Existuje také tisíce dalších alternativních kryptoměn, které i přes fakt, že bitcoin v mnoha ohledech překonávají, zůstávají mediálně téměř neznámé.

Ústředním tématem této práce je rozsáhlý ekosystém alternativních kryptoměn a analýza jejich těžby. Cílem je na praktickém příkladu ukázat, jak těžba alternativních kryptoměn probíhá a zjistit, jestli lze konkrétním typem grafické karty profitabilně těžit.

Před úspěšným dosažením cíle jsem musel nejprve ekosystém kryptoměn zanalyzovat. Dále potom různé kryptoměny vzájemně porovnat a na závěr zrealizovat těžební operaci a vyhodnotit její výsledky.

Hlavní přínos práce je ve zmapování rozsáhlého ekosystému kryptoměn a nalezení odpovědi na otázku, proč jsou některé kryptoměny úspěšnější než jiné. Za dílčí přínos považuji praktickou ukázku realizace těžby alternativních kryptoměn a zjištění, za jakých podmínek se dají alternativní ktyptoměny profitabilně těžit pomocí grafické karty.

Struktura práce je rozdělena na tři hlavní části. První část je věnována podrobnému vysvětlení pojmu kryptoměna, z čeho se skládá a na jakých principech funguje. Obsahem druhé části je kromě analýzy ekosystému, také vzájemné porovnání určitého vzorku alternativních kryptoměn. Třetí část je část praktická, ve které jsem uskutečnil reálnou těžební operaci.

Klíčová slova

Kryptoměna, těžba, altcoin, bitcoin

Abstract

Over the past few years, bitcoin has become a globally successful and much followed project. It is a kind of decentralized digital currency, which functions based on mathematical-cryptographical principles and is created using a computationally intensive process called mining. Thousands of other alternative crypto currencies exist, which have so far stayed unnoticed by the media, even though they outperform bitcoin in many aspects.

The central topic of this paper is the extensive ecosystem of alternative crypto currencies and an analysis of their mining process. The goal is to demonstrate, by means of a practical example, how alternative crypto currencies are mined and also to find out, if it's possible to mine crypto currencies profitably with specific type of a graphic card.

To successfully reach this goal I had to first analyse the ecosystem of crypto currencies. Subsequently I compared different crypto currencies to one another and eventually successfully implemented the mining operation and evaluated its results.

The main contribution of this paper is to answer the question of whether and how alternative crypto currencies can be profitably mined. I believe the particular benefit of this work rests not only in the practical demonstration of how alternative crypto currencies are mined but also in the summary description of the crypto currency ecosystem's composition and the factors that influence the price of these crypto currencies.

Structurally, this paper is divided in three main parts. The first part is dedicated to the explanation of the term *crypto currency*, what it comprises and according to which principles it functions. The second part contains an analysis of the ecosystem as well as a comparison of a fixed sample of alternative crypto currencies. The third part is the practical part, during which I undertook a real mining operation.

Keywords

Cryptocurrency, mining, altcoin, bitcoin

Obsah

1 Úvod…… 4

2 Rešerše zdrojů 5

3 Kryptoměna 6
3.1 Problematika definice bitcoinu a dalších kryptoměn....6
3.2 Původ kryptoměn....7
3.3 Kryptografie, základ kryptoměn 9
3.3.1 Asymetrická kryptografie 10
3.3.2 Kryptografické funkce 10
3.3.2.1 Kryptografická Hashovací funkce 10
3.3.2.2 Kryptografická funkce pro odvození klíče 11
3.4 Využití kryptografie v kryptoměnách 11
3.4.1 Princip kryptoměn a z čeho se skládájí 11
3.4.1.1 Privátní a veřejný klíč 12
3.4.1.2 Adresa....12
3.4.1.3 Klient a peněženka....13
3.4.1.4 Transakce 13
3.4.2 Metody konfirmace transakcí a zajištění bezpečnosti 14
3.4.2.1 Proof of Work 14
3.4.2.2 Proof of Stake....15
3.4.3 Blok 16
3.4.4 Blockchain....17

4 Analýza ekosystému alternativních kryptoměn....18
4.1 Rozdělení projektů....19
4.2 Referenční kryptoměna Bitcoin (BTC) 20
4.2.1 Využití bitcoinu v reálné ekonomice 22
4.2.1.1 Trh s nelegálními produkty a službami....23
4.2.1.2 Obcházení legislativních a regulatorních bariér 23
4.2.2 Hodnota Bitcoinu 24
4.3 Alternativní kryptoměny a řetězce....24
4.3.1 Jak nová alternativní kryptoměna vzniká....25
4.3.2 Účastníci trhu 26

5 Rozdělení projektů podle jejich významu 28
5.1.1 Tržní cena 28
5.1.2 Tržní kapitalizace 29
5.1.3 Směnárny....31
5.1.3.1 Na jakém principu směnárny fungují 32

5.1.3.2 Rizika směnáren a příklady jejich selhání....32
5.1.4 Představení nejvýznamějších alternativních kryptoměn....34
5.1.4.1 Litecoin (LTC)....34
5.1.4.2 Dogecoin (DOGE)....34
5.1.4.3 DarkCoin (DRK)....35
5.1.4.4 PeerCoin (PPC)....36
5.1.4.5 BitcoinDark (BTCD)....36
5.1.4.6 Monero (XMR)....37
5.1.4.7 YbCoin (YBC)....37
5.1.4.8 FeatherCoin (FTC)....38
5.1.4.9 ByteCoin (BTE)....38
5.1.4.10 PrimeCoin (XPM)....38
5.1.4.11 Quark (QRK)....39
5.1.4.12 ReddCoin (RDD)....39
5.1.4.13 VertCoin (VTC)....40
5.1.5 Příklady dalších alternativních kryptoměn....40
5.1.6 Několik příkladů alternativních řetězců....41
5.1.6.1 Ripple (XRP)....41
5.1.6.2 MaidSafeCoin (MAID)....42
5.1.6.3 CounterParty (XCP)....42
5.2 Porovnání alternativních kryptoměn....43
5.2.1 Typické rozdíly v technickém zpracování....43
5.2.1.1 Různé nastavení parametrů PoW a PoS....44
5.2.1.2 Měnová báze....44
5.2.1.3 Podle typu využitého těžebního algoritmu....45
5.2.1.4 Anonymita....45
5.2.1.5 Další funkcionality....45
5.2.2 Typické brandingové rozdíly....45
5.2.2.1 Název a logo....46
5.2.2.2 Zaměřením na učitý segment uživatelů....46
5.2.2.3 Způsob, rozsah a kvalita prezentace....46
5.2.2.4 Možnosti směny mincí a jejich využití....47
5.2.3 Faktory určující úspěšnost a popularitu altcoinů....47
5.2.3.1 Různé pohledy na faktory úspěchu....48
5.2.3.2 Stanovení faktorů úspěšnosti nových altcoinů....49
6 Těžba kryptoměn....50
6.1 Úvod do analýzy těžby....50
6.1.1 Těžba obecně....50
6.1.1.1 Podrobné vysvětlení procesu těžby na příkladu....51
6.1.2 Náročnost těžby....52

6.1.2.1 Různé způsoby stanovení náročnosti těžby 53
6.1.2.2 Faktory ovlivňující výši náročnosti 54
6.1.3 Těžební hardware a software 55
6.1.3.1 CPU – Těžba procesorem 55
6.1.3.2 GPU – Těžba grafickou kartou 55
6.1.3.3 FPGA – Těžba programovatelným hradlovým polem 56
6.1.3.4 ASIC – Těžba čipy, navrženými pro specifické užití 56
6.1.3.5 Výkonnost jednotlivých typů těžebního hardwaru 57
6.1.3.6 Těžební software 58
6.2 Způsoby realizace těžby 58
6.2.1 Solo těžba 58
6.2.2 Těžba v poolu 58
6.2.3 Težba v multipoolu 59
6.2.4 Cloudová těžba 59
6.3 Výnosnost těžby a těžební strategie 60
6.4 Realizace reálné těžební operace 61
6.4.1 Cíl těžební operace 61
6.4.1.1 Metoda dosažení cíle 61
6.4.2 Těžební hardware 61
6.4.3 Výběr způsobu těžby 62
6.4.3.1 Cloudová těžba NiceHash 62
6.4.3.2 Založení bitcoinové peněženky na blockchain.info 64
6.4.4 Výběr a zprovoznění těžebního softwaru 65
6.4.4.1 Instalace těžebního software SGminer 5.1 65
6.4.4.2 První nastavení těžebního software SGminer 5.1 66
6.4.4.3 Správné nastavení softwaru SGminer k těžbě 68
6.4.4.4 Měření spotřeby elektrické energie 70
6.4.5 Měření výkonnosti těžby 71
6.4.6 Výsledky měření a jejich vyhodnocení 72

7 Závěr……. 73

Seznam použitých zdrojů 74

Seznam obrázků a tabulek 83
Seznam obrázků 83
Seznam tabulek 83

Přílohy……..... 84

1 Úvod

V roce 2009 byl vynalezen Bitcoin. Jednalo se o zlomový okamžik v historii platebních systémů a měn všeobecně. Během posledních pěti let se slovo bitcoin stalo pojmem již téměř všeobecně známým, bylo napsáno mnoho článků, natočena řada dokumentů. Faktem je, že se pojem bitcoin zapsal do historie.

Většina mediální pozornosti se zaměřuje na bitcoin jako na experiment, který dal zbohatnout celé řadě lidí, ale také spoustu lidí o peníze připravil. Mnohem méně pozornosti je však věnováno alternativním kryptoměnám, které jsou bitcoinu blízké, ale v mnoha zásadních parametrech odlišné a snaží se původní koncept, funkcionalitu bitcoinu různými způsoby vylepšit.

Oblast alternativních kryptoměn je zajímavá nejenom díky svému dynamickému rozvoji, ale především je to oblast rozsáhlá a téměř neprozkoumaná. Kromě desítek populárních kryptoměn, existují stovky až tisíce dalších různě úspěšných projektů.

Stěžejním tématem této diplomové práce není Bitcoin, kterému bylo věnováno mnoho pozornosti nejenom v různých akademických pracích, ale kryptoměny alternativní a jejich těžba. Toto téma mě zaujalo především z hlediska technického a investičního. Podle mého názoru se koncept kryptoměn stále nachází ve své rané a velmi experimentální fázi vývoje, z čehož plyne potenciál pro zajímavé investiční a podnikatelské příležitosti.

Těžba kryptoměn je proces, při němž dochází k tvorbě virtuálních mincí, které můžeme směnit za peníze reálné. Tento proces se vyplatí provozovat do chvíle, než náklady na těžbu převýší zisk z prodeje mincí.

Hlavním cílem této práce je zanalyzovat ekosystém alternativních kryptoměn a na praktické realizaci těžební operace ukázat, zda s pomocí grafické karty lze alternativní kryptoměny profitabilně těžit. K dosažení cíle je potřeba nejprve pojem kryptoměna objasnit a dále pak porozumět tomu, z čeho se alternativní kryptoměny skládají, jak fungují, k čemu slouží a jakým způsobem se těží.

Každá z kryptoměn, kterou zkoumám, má různé parametry, těží se odlišným způsobem a může fungovat na různých principech. Prvním dílčím cílem je v teoretické části práce nejenom popsat jejich fungování, ale zároveň určit, v čem se jednotlivé kryptoměny vzájemně liší. Tyto poznatky nám pak mohou pomoci porozumět tomu, proč jsou některé alternativní kryptoměny úspěšnější.

Dalším dílčím cílem je zrealizování těžební operace v rámci několika druhů kryptoměn, díky které zjistím, jestli je možné s konkrétním typem grafické karty tyto měny profitabilně těžit.

Hlavní přínos práce je ve zmapování rozsáhlého ekosystému kryptoměn a nalezení odpovědi na otázku, proč jsou některé kryptoměny úspěšnější než jiné. Za dílčí přínos považuji praktickou ukázku realizace těžby alternativních kryptoměn a zjištění, za jakých podmínek se dají alternativní ktyptoměny profitabilně těžit pomocí grafické karty.

Práce je určena nejenom kryptografickým nadšencům, ale prakticky každému, kdo se zajímá o nové technologie.

2 Rešerše zdrojů

Alternativní kryptoměny jsou téma, které zatím nebylo podrobně popsáno v žádné akademické práci, či knize. Bitcoin je středem zájmu celé řady prací, ale další alternativní kryptoměny již nikoliv. Proto jsem musel při vypracování této práce vycházet především z internetových zdrojů, různých diskusních fór a specializovaných zpravodajských webů, které o novinkách v ekosystému alternativních kryptoměn píší.

Za zmínku stojí diplomová práce Dominika Škody s názvem „*Bitcoin jako forma digitálních peněz*“, ve které autor popisuje hlavně obecné fungování bitcoinu a jeho využití. Dalším dílem, které musím zmínit je bakalářská práce „Analýza virtuální měny Bitcoin“, kde autor Petr Huťťák rovněž popisuje fungování bitcoinu, ale i z více technického hlediska.

Ovšem nejzajímavější práce vznikají v zahraničí. Andreas M. Antonopoulos ve své knize „*Mastering Bitcoin*“, dokázal celou kryptoměnu popsat v zatím největším rozsahu a i velmi technicky. Tato kniha se v budoucnu stane určit základním zdrojem informací nejen o bitcoinu, ale také dalších kryptoměnách, které v ní autor zmiňuje. Autor se ve své knize snaží také o určitou klasifikaci různých alternativních kryptoměn, avšak ne vždy se mu to s přesností daří, což zmíním v další části této práce.

Co se týče technického zpracování těžby, tak nejlepší práce co jsem četl, byla „*Bitcoin and The Age of Bespoke Silicon*“ od autora Michaela Bedforda. V práci velmi dobře popisuje historický vývoj těžebních zařízení, od standardních procesorů po specializované čipy ASIC. Bohužel i tato práce je spíše zaměřena na bitcoin.

Největším problémem ekosystému kryptoměn, je obrovská roztříštěnost informací. Například když jsem se snažil najít konkrétní specifika jedné ze zajímavých alternativních kryptoměn, tak to byl téměř nepřekonatelný problém. Najít zdroj informací, který by byl seriózní a vysvětloval danou problematiku dopodrobna, bývá téměř nemožné. Proto jsem musel jednotlivé informace hledat po střípkách na různých sociálních sítích, anebo internetových fórech.

3 Kryptoměna

3.1 Problematika definice bitcoinu a dalších kryptoměn

První kryptoměnou vůbec se stal Bitcoin. Ve spojení s bitcoinem se setkáme s celou řadou pojmů, které se snaží bitcoin definovat a charakterizovat. Mnoho z nich není jednoznačných, avšak ve výsledku je nejčastěji používán pojem „kryptoměna“ („Crypto currency“).

V případě oficiální Bitcoin wikipedie jsou bitcoiny hlavně definovány jako digitální měna („Digital currency“). Podle tohoto zdroje jsou bitcoiny také známy pod pojmy jako cyber měna, digitální hotovost, digitální peníze, e-peníze, elektronické peníze a celou řadou dalších pojmů.(1)

Údajný tvůrce bitcoinu Satoshi Nakamoto ve své práci představuje elektronickou verzi hotovosti, založenou na bázi „peer to peer“, kde jsou veškeré transakce realizovány bez pomoci centrální protistrany. Tento systém nazývá bitcoinem a v případě konkrétních jednotek pojednává o bitcoinu jakožto o elektronické minci.(2)

Definice jednotlivých pojmů ať už se jedná o kryptoměnu, digitální měnu nebo kupříkladu elektronické peníze, se do určité míry vzájemně nahrazují.

Neexistuje jednotná oficiálně stanovená definice co konkrétně kryptoměna, či digitální měna je. Oficiální bitcoin wikipedie definuje digitální měny jako peníze, které se dají elektronicky směnit. Tato definice je velice široká a podle mého názoru nepraktická.(3)

Lepší a přesnější definici nabízí kupříkladu investopedia, kde je kryptoměna definována jako „*Digitální neboli virtuální měna, která využívá metody kryptografie v rámci svého zabezpečení. Kryptoměna je těžko padělatelná, právě díky této metodě. Definující vlastností kryptoměn je fakt, že nejsou vydávány žádnou centrální autoritou, díky čemuž jsou teoreticky imunní vůči vládním intervencím a manipulacím.*“ (4)

Problémem této definice je fakt, že zmiňují absenci centrální autority, což nemusí být pravdou v případě všech dostupných kryptoměn.

Stručnější a podle mého názoru nejlepší definici nabízí techopedia, kde je kryptoměna jednoduše specifikovaná jako „*Kryptoměna je typ digitální měny, která využívá kryptografii v rámci bezpečnostních opatření a opatření proti padělání*.“ (5)

Bitcoin je první vytvořenou kryptoměnou, zdaleka však ne jedinou kryptoměnou veřejnosti dostupnou a známou. Existuje celá řada dalších kryptoměn, které se svými vlastnostmi od bitcoinu velmi odlišují a zároveň tak boří některé definice.

Pro účely této práce jsou proto kryptoměny definovány velice jednoduše a všeobsáhle, kryptoměny jsou „*Digitální měny, které využívají metody kryptografie*.“.

3.2 Původ kryptoměn

V osmdesátých a devadesátých letech dvacátého století společně s rozvojem kryptografie, vzniklo hnutí takzvaných „Cypherpunks“. V rámci tohoto hnutí se volně sdružili kryptografičtí výzkumníci a entusiasté, kteří dále rozvinuli celou řadu inovativních myšlenek, nápadů a přístupů ke komunikaci, ekonomice a politice za využití kryptografie. Paradigma tohoto hnutí se dá definovat jako snaha o „*Nahrazení centralizovaných systémů, které interakce prosazují nátlakem, za decentralizované systémy dobrovolných interakcí, jejichž pravidla jsou vynucovány principy postavené na matematice a ekonomii.*“ (6)

Nosnou myšlenkou daného hnutí je strach z přílišné centralizace a možnosti jejího komerčního nebo politického zneužití. Jako příklad mohu zmínit dvouleté zablokování možnosti lidem zasílat dotace organizaci WikiLeaks prostřednictvím systémů společností Visa, Paypal a MasterCard. Další ukázkou síly monopolu a centralizace mezinárodního bankovního systému je zavedení sankcí západními státy vůči Iránu. (7)

Jedním z úspěchů hnutí bylo vytvoření serveru pro anonymní přeposílání emailů, díky čemuž se podařilo zabránit zavedení exportních restrikcí v USA na kryptografické technologie a zařízení. (6)

V případě úspěšného zavedení restrikcí by nejenom došlo k omezení možností občanů ve vzájemné anonymní komunikaci, ale také by hrozila situace, která nastala v Jižní Koreji. Nastavené restrikce vytvořily v Jižní Koreji faktický monopol aplikace Internet Explorer, protože veškerá šifrovaná online komunikace musí využívat prvků Active X od společnosti Microsoft. V praxi tak uživatelé se zařízením od společnosti Apple, nebo jiných prohlížečů než Microsoft Explorer, nemohou využívat v Jižní Koreji například služeb internetového bankovnictví, online nákupů a internetových stránek e-governmentu. (8)

Jeden ze členu hnutí Timothy C. May, inženýr, politický spisovatel a vědec, v roce 1994 podotkl, že společností akceptovaná digitální měna vznikne v rámci několika následujících let. Tento optimistický odhad se naplnil se vznikem bitcoinu až o 14 let později. (6)

Rozvoj internetu v poslední dekádě postupně zvýraznil potřebu rychlých, jednoduchých a uživatelsky přístupných platebních systémů. Jako příklad mohu uvést Paypal, Moneybookers a prakticky veškeré další elektronické platební systémy.

Tyto systémy jsou stále ve větší míře využívány k rychlému internetovému nákupu zboží a služeb, sponzoringu, darům a mezinárodnímu převodu financí mezi jednotlivými uživateli. Společně s rozvojem těchto systémů se rozvíjela i myšlenka měny virtuální, neboli elektronické. Rostoucí popularita sociálních sítí (Např. Facebook,Twitter, Reddit,…) a internetových počítačových her pro více hráčů (Např. World of Warcraft, World of Tanks, League of Legends,…) dala vzniknout celé řadě komunitních/herních virtuálních měn.

Mnohdy se jedná o uzavřené systémy spravované vývojáři daných her/sociálních sítí, kde uživatelé mohou tyto virtuální peníze získat buďto prostřednictvím splnění různých úkolů/činností, nebo směnou/nákupem peněz virtuálních za peníze reálné podle určitého kurzu a pravidel. (Směnný kurz je většinou stanoven vývojáři/správci daného systému.) Těchto virtuálních peněz mohou následně uživatelé využít k nákupu zboží/služeb v rámci daného systému. Tyto virtuální peníze mají většinou podobu bodů nebo tzv. „zlatých mincí“ („Gold coins“).

Evropská centrální banka definuje virtuální peníze jako „Neregulované, digitální peníze, které jsou emitované a obvykle kontrolované jejich tvůrci. Tyto peníze jsou akceptovány v rámci určitých internetových komunit.“ (9)

Je nutné podotknout, že koncept alternativních neregulovaných měn se neobjevuje až s příchodem bitcoinů. V historii je se dá najít cela řada příkladů alternativních lokálních měn, či měn založených na různých principech. Jako příklad se dají uvést různé měny vydávané organizacemi, korporacemi nebo lokálními vládami.

Virtuální peníze se dají zároveň dále klasifikovat podle jejich vztahu k penězům běžně využívaných v reálné ekonomice:

1, Uzavřené systémy virtuálních měn – Jedná se o systém, ve kterém uživatelé získávají veškeré virtuální peníze pouze určitými činnostmi uvnitř hry, nebo komunity a tyto peníze se nedají využít k nákupu reálných statků ani ke směně za reálné peníze. Tento druh uzavřeného systému virtuálních peněz bývá často nazýván jako „pouze herní“. Tento systém je charakteristický pro počítačovou hru World of Wacraft a měnou „Zlato“ („Gold“). (9)

2, Systém virtuálních peněz s jednosměrným tokem – V rámci tohoto systému dochází k jednosměrné směně reálných peněz za peníze virtuální. Takto směněné prostředky se nedají zpětně převést do formy reálné měny. Kurz, za kterého tato směna probíhá, je nastaven správcem daného systému. Některé systémy umožňují směnu opačného směru, kde za virtuální „body“ lze zakoupit/získat reálné statky, slevu, nikoliv však přímo reálné peníze. Zástupcem tohoto systému je například Facebook se svými Facebook kredity. (9)

3, Systém virtuálních měn s obousměrným tokem – Uživatelé těchto systémů mohou volně směňovat peníze virtuální za peníze či statky reálné a to na základě jasně daného kurzu, který se může měnit. Příkladem je virtuální měna dolar Linden („Linden Dollars“.) využita v rámci hry Second Life. Do této kategorie spadá většina obchodovatelných kryptoměn včetně bitcoinu. (9)

Důvody, proč vznikají různé systémy virtuálních měn, jsou například:

- Společnosti jejich prostřednictvím mohou využívat různé marketingové strategie, kdy klient využíváním služeb získává virtuální body, za které následně může získat celou řadu slev, či nakoupit konkrétní produkty, nebo služby.
- Profit provozovatele systému tvořený ze situace, kdy uživatelé přestanou být aktivními členy systému, ale nespotřebují veškeré získané virtuální prostředky.
- Vytvoření alternativy k reálným penězům, která nebude limitována a regulována centrálními bankami.

Až do vynalezení první kryptoměny bitcoinu, měli všechny tyto systémy jeden společný fakt, byly centralizované. Za jejich vývojem a správou vždy stála organizovaná skupina lidí s možností svévolně měnit celé jeho fungování a parametry.

Každý kdo uvažuje o tom, že začne akceptovat jakoukoliv digitální měnu jako platidlo, narazí na dva zásadní problémy.

Jedním z nich je autenticita peněz, která určuje, zda jsou dané peníze autentické a nejedná se tak o falzifikáty. Žádný obchodník nebude prodávat své zboží za peníze, u kterých si není stoprocentně jist, že jsou pravé.

Digitální peníze nemají svou hmotnou formu, díky čemuž může teoreticky kdokoliv nárokovat peníze někoho jiného. Může nastat situace, kdy dostaneme zaplaceno za určité zboží a později se dozvíme, že ve skutečnosti těmito penězi bylo již zaplaceno zboží jiné a tudíž na ně nemáme nárok. Jedná se o problém tzv. dvojího utracení.

S oběma problémy se můžeme setkat i v běžném životě. Bankovky jsou proti padělání chráněny různými ochrannými prvky a není možné jednou bankovkou platit na dvou místech zároveň. Reálné peníze mají i svou digitální formu, například číslo na běžném účtu. V tomto případě zamezuje padělání a dvojímu utracení síť nadnárodních centrálních autorit evidující veškeré finanční transakce.

Bitcoin a další kryptoměny tyto problémy řeší prostřednictvím užití různých kryptografických metod. Využívají čtyř klíčových inovací: (10)

- Decentralizované sítě typu klient-klient. (Protokol)
- Veřejné knihy všech transakcí. (Blockchain)
- Decentralizovaného emitování a distribuce měny založeném na matematicko-deterministických principech. (Těžba)
- Decentralizovaný systém verifikace uskutečněných transakcí. (Transakční skript)

3.3 Kryptografie, základ kryptoměn

Kryptografie, nebo česky také šifrování, je nauka o metodách a technikách zabezpečené komunikace za účasti třetí strany, se kterou ovšem nechceme sdílet obsah komunikace. (11)

Ve své podstatě se jedná o analyzování a vytváření protokolů, které zamezí třetím stranám narušit datovou integritu, autenticitu, nepopiratelnost a zabrání v přečtení obsahu zpráv. (11)

- Integrita – Příjemce zpráv musí mít možnost ověřit, zda zpráva nebyla na cestě od odesílatele třetí stranou zfalšována, nebo jinak změněna.
- Autenticita – Příjemce zpráv musí být schopen prokazatelně určit odesílatele dané zprávy a zároveň další uživatelé nemohou přebírat identitu jiných odesílatelů.
- Nepopiratelnost – Odesílatel zprávy nesmí mít možnost klamavě popřít, že je autorem zprávy.

Laicky se dá říci, že základním cílem kryptografie je zašifrovat určitou čitelnou zprávu do nečitelné podoby, textu, který se dá následně rozšifrovat prostřednictvím určitého klíče. Klíč je informace určující, jak má být zpráva transformována do výsledného zašifrovaného textu.

Kryptoměny využívají metodu asymetrické kryptografie a různých tzv. kryptografických funkcí.

3.3.1 Asymetrická kryptografie

Asymetrická kryptografie používá dva různé, ale zčásti matematicky propojené klíče, soukromý a veřejný. Jeden z klíčů je vždy využit v případě dešifrování a druhý v případě šifrování.

V případě této metody je majitelem zveřejněn veřejný šifrovací klíč, který následně může kdokoliv využít k zašifrování zprávy majiteli určené. Majitel rovněž vlastní svůj privátní klíč, jehož prostřednictvím zašifrované zprávy dešifruje a který drží v tajnosti.

Majitelé všech kryptoměn typu bitcoin jsou identifikováni prostřednictvím veřejných klíčů, které jsou spojeny s konkrétními mincemi. Pokud majitel chce své bitcoiny poslat někomu jinému, vytvoří transakci s nadefinovaným počtem mincí, ke které připojí veřejný klíč budoucího vlastníka a svůj privátní klíč. Odesláním této transakce do zbytku bitcoinové sítě jsou všichni ostatní účastníci seznámeni s tím, že novým majitelem definovaného počtu mincí se stává vlastník nového veřejného klíče. Přiložením privátního klíč původní vlastník potvrzuje, že transakce je autentická. Veškerá historie všech transakcí je veřejně všemi účastníky uchovávána, každý tak může zjistit, která adresa je aktuálním vlastníkem konkrétní skupiny bitcoinů. (12)

3.3.2 Kryptografické funkce

Jako příklad kryptografických funkcí zmíním hashovací funkce, nebo také funkce pro odvození klíče („Key derivation function“). Konkrétní kryptografické funkce využívané ve dvou nejznámějších měnách, bitcoinu a litecoinu, jsou SHA256 a Scrypt. Velké množství alternativních kryptoměn využívá různé modifikace zmíněných kryptografických funkcí.

Podstatu kryptografických funkcí vysvětlím na následujících dvou příkladech.

3.3.2.1 Kryptografická Hashovací funkce

Hashovací funkce je matematickou funkcí, která převádí vstupní data různé délky na výstupní tzv. Hash hodnotu, která má vždy fixní počet znaků. Mezi tyto funkce patří i Hashovací funkce SHA256 s rozsahem výstupních hodnot 256 bitů. (13)

Kryptografická hashovaní funkce je funkcí jednosměrnou. V případě jednosměrných funkcí je výpočetně jednoduché transformovat data do Hash hodnoty, ale zpětný převod této hodnoty do vstupních dat je velice výpočetně náročné. (13)

Charakteristické vlastnosti této funkce jsou:

- Výsledný Hash má vždy stejnou délku, bez ohledu na délku vstupních dat.
- I s malou změnou vstupních dat se výsledná Hash hodnota zásadně změní.
- Z Hash hodnoty je téměř nemožné zrekonstruovat původní data.
- Díky unikátnosti Hash hodnoty, jí lze v praxi využít pro identifikaci unikátních dat.
- Vypočtení Hash hodnoty je jednoduché bez ohledu na rozsah vstupních dat.

V praxi se tato funkce nejčastěji využívá při ověření integrity dat, hesel, souborů a pseudonáhodném generování dat. Také je možné funkci využít při derivaci nových klíčů a hesel od hesla nebo klíče původního. (13)

Příklad transformace dat do Hashe při využití SHA256:
Vstup: Kryptologie
Výstup: 5a4bd7ecaf80f153689a5460caf9392d65515af83f047e0edaa1fe3f4273a8ef

Vstup: Kryptografie
Výstup: 47655e07f8ff1f905dc1759e8594488c0789c69425aeabeecfe9ab735411828a

Vstup: Kryptografie a kryptologie
Výstup: d9b56481bad27183d808a2efa60c11db1cd4f46873d94093886cc5dfd07ff88f

3.3.2.2 Kryptografická funkce pro odvození klíče

Jedná se o funkci, která vytvoří jeden nebo více klíčů z dat, obvykle hesla, za použití hashovací funkce. Hlavním důvodem pro vytvoření takto derivovaného klíče mohou být nevyhovující vlastnosti původního hesla (Délka, složitost,…), bránící v jeho potenciálním využití v roli kryptografického klíče. Další využití tato funkce má v podobě obrany proti útokům hrubou silou, kdy se útočník snaží prolomit bezpečnost systematickým mnohočetným zkoušením různých hesel. Řešení dané funkce je výpočetně náročné a proto systematické zkoušení statisíců různých hesel se stává mnohonásobně obtížnější.

Na zjednodušeném typu této funkce je postaven algoritmus Scrypt, který je hojně využíván v rámci těžby alternativních kryptoměn. (14)

3.4 Využití kryptografie v kryptoměnách

Prostřednictvím kryptografie je u kryptoměn zabráněno snahám o podvodné narušení integrity systému, kterým je například realizace fiktivních transakcí, či dvojité platby stejnými prostředky. Tento problém se vyskytuje především u digitálních měn, kde si můžeme peníze představit jako soubor dat, který můžeme zkopírovat a odeslat dvěma lidem zároveň. Určení pravosti takové transakce je zodpovědností provozovatele systému digitální měny, který musí určit, zda je soubor originál nebo kopie. Revolučním přínosem kryptoměn je řešení tohoto problému bez nutnosti třetí strany. (20)

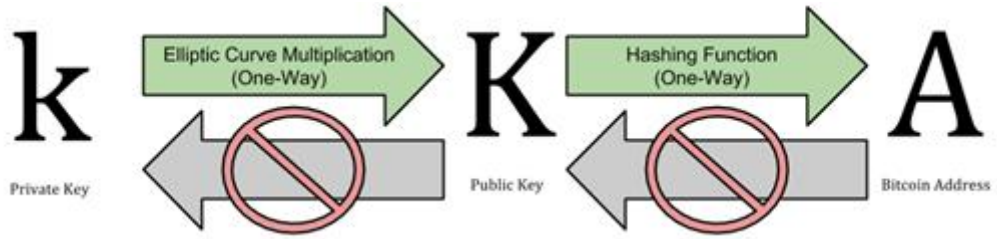
3.4.1 Princip kryptoměn a z čeho se skládají

Mnoho kryptoměn využívá principy a kryptografické funkce stejné nebo odvozené od bitcoinu. Tato část je proto věnována stručnému popisu bitcoinu, z čeho se skládá a jaké principy využívá.

3.4.1.1 Privátní a veřejný klíč

Privátní klíč je náhodně vybrané číslo rozsahu 128-512 bitů. Z privátního klíče je, za pomoci jednosměrné kryptografické funkce multiplikace eliptických křivek, vygenerován klíč veřejný. Z takto vytvořeného veřejného klíče můžeme prostřednictvím jednosměrné hash funkce vygenerovat Bitcoin Adresu.

Privátní klíč se využívá k podepsání převodu bitcoinů z jedné adresy na další. Privátní klíče jsou matematicky svázány s konkrétními adresami. Prostřednictvím tohoto klíče můžeme ovládat veškeré mince, které jsou tímto klíčem zabezpečené. Bezpečná úschova privátního klíče je základním parametrem zabezpečení všech kryptoměn. Ztráta privátního klíče se rovná ztrátě veškerých bitcoinů.



Obrázek č. 1 Tvorba Bitcoinové adresy z veřejného klíče a klíče privátního. Zdroj: (32)

Klíč lze zobrazit několika způsoby, hexadecimálně, pomocí formátu Base58, nebo ve formě tzv. Mini klíče. Formát mini klíče je nejčastěji využit v případě použití QR kódů a fyzických bitcoinů a to z důvodu nejmenší velikosti. (16)

Příklad privátního klíče ve formátu 256 bitového čísla:

E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D A6 1F 20 BD 67 FC 23 3A A3 32 62

Příklad privátního klíče ve formátu Mini klíče:

SzavMBLoXU6kDrqtUVmffv

3.4.1.2 Adresa

Adresa je identifikátor cílového účtu, na který můžeme bitcoiny převést. Skládá z 26 až 34 alfanumerických znaků a vždy začíná číslicí 1 nebo 3. Adresa nesmí obsahovat znaky nuly „0“, velkého „O“, malého „i“ a velkého „I“. Toto omezení bylo zavedeno z rizika snadné zaměnitelnosti různých adres s podobnými znaky. Technicky je adresa tvořena 160-bitovým hashem veřejného klíče vytvořeného algoritmem ECDSA. Adresy dalších kryptoměn jsou odlišné. (18)

Příklad bitcoin adresy:

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

Informace obsažené uvnitř každé adresy jsou:

- Informace pro jakou síť je adresa určena.
- Kontrolní součet pro zajištění integrity dat.
- Hash veřejného klíče vlastněného uživatelem.

Nové adresy jsou generovány za pomoci bitcoin klienta, vyřešením algoritmu ECDSA a několika dalších matematických operací.

3.4.1.3 Klient a peněženka

Klient je v zásadě program, který slouží jako hlavní komunikační nástroj se zbytkem bitcoin sítě. Obsahuje funkcionalitu peněženky a databázi uskutečněných transakcí společně s nástrojem pro jejich ověření. Dále umožňuje realizaci nových transakcí a plní roli uzlu.

Můžeme je z hlediska funkcionality dělit na soubory a programy. Programy slouží především k vytvoření veřejných a privátních klíčů, prostřednictvím kterých můžeme bitcoiny přijímat a odesílat. V souborech jsou ukládány privátní klíče a další informace vztahující se k realizovaným transakcím v rámci celé peněženky. Většina dostupných řešení obsahuje obě funkcionality. (18)

Základní tři formy bitcoin klienta jsou plný klient, tenký klient a web klient. Hlavní rozdíl mezi těmito typy je v tom, do jaké míry chceme sami odpovídat za bezpečné uschování bitcoinů. (17)

Plný klient plní funkci uzlu, neboli „Node“. Což znamená, že obsahuje a stahuje veškeré realizované transakce v síti. Tyto transakce jsou v uzlu ověřeny a dále synchronizovány se zbytkem sítě. Provozování node je však náročné nejenom na množství odesílaných a přijímaných dat, ale také na paměť, protože program musí uchovávat celou historii transakcí. Jedná se o několik gigabitů dat, a tato velikost neustále roste. Plný klient je naprosto samostatný a k jeho fungování není potřeba využívat dalších služeb.(18)

Hlavní rozdíl mezi tenkým a plným klientem je v rozsahu ukládané historie transakcí. Přístup k historii transakcí je umožněn skrze servery třetích stran, a proto tyto transakce tenký klient neukládá. Slouží především jako peněženka pro uchování kryptoměny.

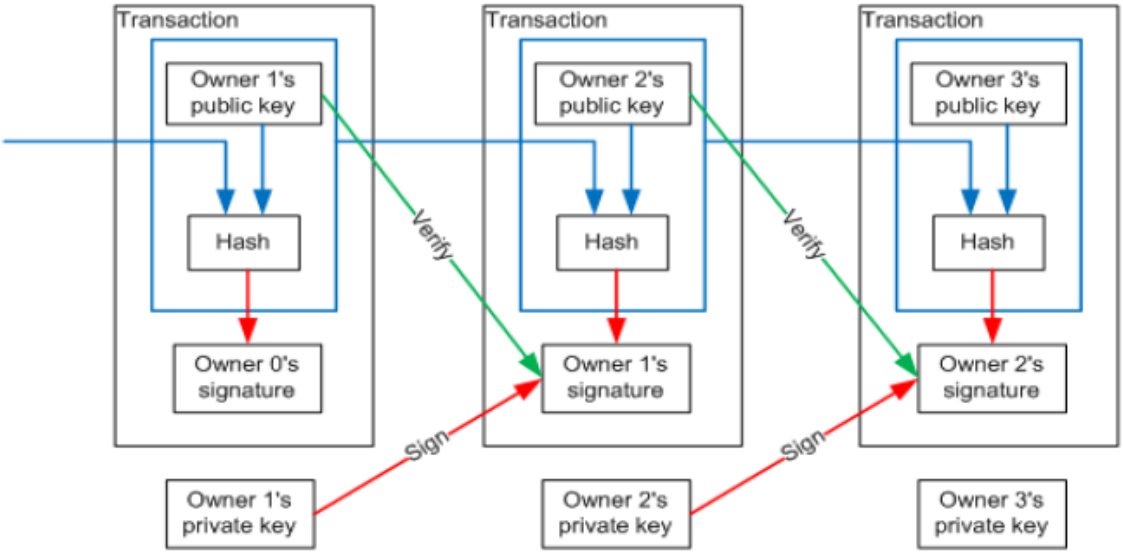
Klient a peněženka může být založena online na různých webových serverech tuto službu poskytující. Většina peněženek obsahuje klíčové páry pro každou z vygenerovaných adres, seznam uskutečněných transakcí z a na naše adresy, uživatelské nastavení, reservní klíče, základní klíč a před-generované klíče. V tomto případě běží klient plně na serverech třetích stran a uživatel k němu jen vzdáleně přistupuje.(19)

3.4.1.4 Transakce

Jako transakce se označuje převod bitcoinů z jedné adresy na další. Ve chvíli kdy nový majitel obdrží bitcoiny na svojí adrese, obdrží ve své podstatě řetězec digitálních podpisů, který obsahuje informaci o předešlých transakcích a počtu převedených bitcoinů. Když dané mince chce převést dále, přiloží k danému řetězci veřejný klíč příjemce a klíč vlastní. Tento

řetězec je následně odeslán do zbytku bitcoinové sítě, kde je metodou Peer-to-Peer distribuován mezi veškeré další uživatele a zařazen do nově vytvořeného bloku.

Při využití Peer-to-Peer způsobu distribuce dané transakce mezi uživateli systému, vzniká problém jak ověřit transakci bez jedné centrální protistrany za účelem zamezení potenciální dvojí transakce. Jediná možnost jak určit, která transakce byla první a tudíž pravá, je v evidenci veškerých transakcí. Bez jedné centrální protistrany lze toho dosáhnout tím, že veškeré transakce budou veřejné a účastníci budou moci konfirmovat jednotnou historii transakcí v pořadí, ve kterém byly transakce vytvořeny. Tento problém je vyřešen využitím například kryptografické metody Proof of work, pomocí které se určuje, které transakce jsou platné a které ne. (20)



Obrázek č. 2 Princip tvorby transakcí. Zdroj: (str.6, 23)

3.4.2 Metody konfirmace transakcí a zajištění bezpečnosti

Tyto metody ve své podstatě nahrazují centrální server, který poznamenává čas vytvoření jednotlivých transakcí a tuto informaci rozesílá dále mezi ostatní uživatele.

Kromě zajištění bezpečnosti a integrity sítě definují také způsob, jakým jsou nové mince vytvářeny a distribuovány mezi uživatele. (21)

3.4.2.1 Proof of Work

Proof of work byl prvotně vytvořen jako opatření proti emailovému spamu. PoW je založeno na principu hledání tzv. „Částečné hash kolize. Pro celou řadu kryptografických hash funkcí se dá náročnost tohoto hledání odhadnout, protože nejefektivnější způsob je využití tzv. Brute force metody, při které dochází k postupnému zkoušení hodnot, dokud není výsledek úspěšně nalezen. Princip PoW je nejlépe vysvětlen na následujícím příkladu:

Máme základní textový řetězec „Hello, world!“ a naším cílem je při zachování tohoto řetězce nalézt konkrétní variantu hashe SHA-256, která bude začínat podřetězcem „0000“. Požadovaného cíle postupně dosáhneme přidáváním na konec původního řetězce číslo, které se bude s každým dalším pokusem, vytvořením nového hashe, zvětšovat o jednotku. V tomto případě cílovou hodnotu hash začínající na řetězec „0000“ nalezneme po 4251 pokusech.

"Hello, world!0" = 1312af178c253f84028d480a6adc1e25e81caa44c749ec81…
"Hello, world!1" = e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139b…
"Hello, world!2" = ae37343a357a8297591625e7134cbea22f5928be8ca2a32a…
…
"Hello, world!4248" = 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55e…
"Hello, world!4249" = c004190b822f1669cac8dc37e761cb73652e7832fb814565…

"Hello, world!4250" = 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc…

Náročnost hledání s délkou požadovaného řetězce exponenciálně stoupá. Vypočtený hash zároveň v sobě obsahuje předchozí hash a náhodné číslo před ním. Každý hash si tedy nese informaci o předchozím generovaném řetězci, což znamená, že každá starší transakce je konfirmovaná dalšími výpočty. Důsledkem toho je skutečnost, že pokud by potenciální útočník chtěl změnit transakci, která se stala v minulosti, musel by zároveň přepočítat veškeré transakce, které po ní následovaly. Prostřednictvím této metody jsou uživatelé odměňováni v závislosti na množství obětovaného výkonu. Čím více výpočetního výkonu bylo investováno do nálezu řešení, tím větší je průměrná odměna v podobě nově vytvořených mincí. (21)

3.4.2.2 Proof of Stake

Obdobně jako v případě Proof of Work tato metoda slouží k potvrzení uskutečněných transakcí a vlastnictví kryptoměny.

Metoda využívá konceptu stáří mincí („Coin age“). Stáří mincí je definováno jako množství mincí násobené dobou, po kterou zůstaly uschované na jedné adrese. Ve chvíli kdy obdržíme 100 mincí a po dobu 10 dní je nebudeme nikam převádět, je stáří mincí v desátém dnu rovno 1000 dnům. Při odeslání mincí na jinou adresu, je tato hodnota následně vynulována. (10)

PoS čas od času náhodně vybere jednoho uživatele, který provozuje plného klienta, a speciální transakcí spotřebuje jeho stáří mincí. Dojde tak k pokusu o vytvoření nového bloku a případnému získání určité odměny v podobě nových mincí. Tento proces se opakuje napříč celou sítí, dokud nedojde k úspěšnému vytvoření nového bloku, který je zařazen do blockchainu a vznikl spotřebováním největšího stáří mincí. Pravděpodobnost získání odměny za vytvořený blok se odvíjí od množství spotřebovávaného stáří mincí, a tedy je přímo závislá na množství uložených mincí na dané adrese. Výsledkem procesu jsou nové bloky potvrzující realizované transakce a vznik nových mincí. Tento proces se nazývá ražba („Minting“). (10)

Cílem této metody je zajistit větší obranyschopnost systému vůči různým druhům útoků. Často je využita u alternativních kryptoměn s malou tržní kapitalizací.

Oproti PoW je tato metoda mnohem méně náročná na spotřebu výpočetního výkonu a tím i elektrické energie. (10)

Varianty Proof of Stake

Cunicula – kombinace Proof of Work a Proof of Stake

Tato nejčastější varianta kombinuje obě metody. Skládá se ze dvou fází, distribuční a udržovací. V první distribuční fázi, je využito PoW, jehož prostřednictvím uživatelé těží nové mince až do určitého maximálního množství. Tento proces trvá relativně krátkou dobu, často se jedná pouze o pár měsíců a slouží k rozdělení základního množství mincí mezi uživatele. Na konci první fáze dochází k přechodu na metodu PoS, která přebírá úlohu vytváření nových mincí a zajištění bezpečnosti systému. (24)

Systém by nebyl funkční bez dostatečného množství uživatelů provozující plné klienty, které sdílejí informace napříč sítí. K provozování plného klienta jsou uživatelé motivováni především úročením stávajících mincí. (12)

Maximální množství mincí, není v případě užití této metody přesně stanoveno. Udává se většinou očekávaný roční procentuální nárůst.

Tuto variantu využívá kryptoměna Peercoin. (10)

Proof of stake – Velocity

Varianta byla poprvé představena v kryptoměně Reddcoin. (25)

Hlavním rozdílem oproti PoS je snaha o řešení problému hromadění mincí. Při metodě PoS jsou uživatelé primárně motivováni k hromadění co největšího počtu mincí, protože pouze tak se zvyšuje jejich šance na případnou odměnu v podobě mincí nových. Uživatelé z toho důvodu nemají motivaci mince utrácet a tím pádem kryptoměna přestává plnit účel prostředku směny. (25)

Problém je řešen přidáním parametru aktivity („Velocity“), který mění výpočet stáří mince. Nově získané mince generují hodnotu stáří mince rychleji, než mince dlouhodobě uskladněné na jedné adrese. (25)

3.4.3 Blok

Záznamy o transakcích jsou permanentně ukládány do souborů nazývané bloky. Blok obsahuje záznam nejposlednějších transakcí v rámci Bitcoin sítě, které ještě nebyly zaznamenány v bloku předešlém. Všechny bloky jsou uspořádány do řetězce bloků („Blockchain“) a nové bloky jsou vytvořeny a zařazeny vždy na konec tohoto řetězce.

Bloky obsahují mimo záznamů transakcí také referenční odkaz na blok předešlý a řešení náročného matematického problému. Toto řešení je pro každý blok unikátní, ale jednotlivé bloky jich mohou mít několik. Poté co je jedno z řešení nalezeno, zbytek sítě velmi jednoduše potvrdí, že je daný výsledek správný a blok s novými transakcemi je zaevidován do blockchainu.(22)

Hledání řešení tohoto problému se nazývá těžba, neboli „mining“. Uživatel, který vyřešil problém daného bloku jako první, získává odměnu ve formě určitého počtu nově vygenerovaných bitcoinů. Tento počet byl v době vzniku bitcoinu stanoven na 50 bitcoinů a zmenšuje se na polovinu pokaždé, když se nalezne řešení problémů ve 210 000 blocích. Aktuálně je odměna stanovena na 25 bitcoinů za nový blok. (22)

Problematice těžby se budu věnovat podrobněji v následující kapitole.

3.4.4 Blockchain

Systém Bitcoinu dvojí útratě zabraňuje vytvořením veřejně přístupné databáze tzv. „Blockchain“, do které jsou veškeré transakce registrovány v předem daném pořádku a s časovou známkou. Řetězec se skládá z bloků a každý nový blok je zařazen na konec tohoto řetězce. Ve chvíli kdy je generován nový blok uživateli systému, dochází k „hlasování“ o tom, který blok bude zařazen na konec řetězce a tím veškeré transakce, které blok obsahuje ověřeny a permanentně uloženy. V jeden okamžik tak může být v rámci sítě generováno několik bloků. Výběr bloku, který nakonec bude zařazen na konec řetězce, závisí na množství investovaného výpočetního výkonu. Zbylé bloky, nebo dokonce i řetězce bloků zaniknou. Vzniku těchto zaniklých řetězců bloků se říká větvení („Forking“). To vede k tomu, že jsou akceptovány pouze ty bloky s transakcemi, se kterými souhlasilo nejvíce uživatelů, a na jejíž akceptaci bylo vynaloženo nejvíce výpočetního výkonu. Tato databáze je distribuovaná napříč sítí prostřednictvím plných klientů, nodů. (22)

Nahlédnout do databáze uskutečněných transakcí můžeme například prostřednictvím webu blockchain.info.

První blok v řetězci je blok genesis a je definován jako část bitcoin protokolu.

4 Analýza ekosystému alternativních kryptoměn

Od konce roku 2008, kdy jako první kryptoměna v historii vznikl bitcoin, se trh rozrostl na několik tisíc různých alternativních kryptoměn. Celá řada z těchto nově vzniklých projektů, již dnes prakticky neexistuje, nebo jsou téměř neaktivní. Jednak je to dáno nízkou přidanou hodnotou, kterou tyto projekty nabídly, ale také faktem, že celá řada z nich byla koncipována jako projekty podvodné.

Kryptoměny, které vznikly po bitcoinu, se označují jako měny alternativní, neboli „Altcoins“. Těchto měn je několik set, přesný počet je velmi těžké stanovit, protože každým dnem vznikají nové a mrtvé projekty jsou ze seznamů vyřazovány. Web cryptocoincharts.info eviduje k dnešnímu datu (9.11.2014) 1117 kryptoměn, oproti tomu web coinmarketcap.com pouze 538. Celkový počet kryptoměn, včetně těch již neaktivních, je odhadován na více než 5000. Reálné číslo ovšem bude ještě několikanásobně větší. (26,27 ,28,29)

Rychlost s jakou se celý ekosystém alternativních kryptoměn vyvíjí je nevídaná. Za poslední rok postupně zaniklo a realizovalo se nespočet projektů, proto je možné a vysoce pravděpodobné, že v již krátké době bude tato práce v mnoha ohledech zastaralá.

Z důvodu ohromujícího množství není možné v rámci této práce podrobně obsáhnout, nebo alespoň zmínit, všechny alternativní kryptoměny. Většina se ovšem dá rozdělit do určitých kategorií, podle charakteristik, které mají společné. Některé měny se od bitcoinu liší pouze nepatrně, zatímco jiné pracují na zcela odlišných principech. Celá řada takových projektů nemá za cíl vytvořit další měnu, ale například platformu pro ověření pravosti kontraktů nebo registraci jmen.

Mnoho nových projektů vzdalo pokusy o vytvoření nové digitální měny využitelné v klasickém platebním styku a namísto toho přináší nové funkcionality. Jádro však zůstává ve většině případů stejné, je založeno na principech decentralizace a využívá kryptografii.

4.1 Rozdělení projektů

S novými trendy v ekosystému kryptoměn začíná být viditelný problém správných definicí a názvů, které jednotlivé projekty charakterizují. Schválně jsem použil termín projekt, protože jak záhy bude patrné, použití termínu alternativní kryptoměna je mnoha konkrétních případech zavádějící.

Ekosystém se skládá z více jak stovek různých projektů, které vznikají nejenom odvozením od bitcoinu, či litecoinu ale také jako projekty zcela nové. V tomto ohledu narazíme na pojmy typu alternativní kryptoměna, kryptoměna 2.0, Meta-Coin, Alt-coin, Alt-Chain a mnoho dalších. Většina zmíněných pojmů se snaží o kategorizaci projektů z hlediska společných parametrů, či funkčnosti.

Bitcoin je definován jako kryptoměna. Pro veškeré projekty vzniklé po bitcoinu se ustálil termín alternativní kryptoměna, zkráceně „AltCoin“. Je však otázkou, zda není tento termín zavádějící, protože řada nových projektů nemá s měnami jako prostředkem směny nic společného. (30)

V této souvislosti se začal objevovat termín Kryptoměna 2.0, která oproti kryptoměnám alternativním plní nejenom funkci platforem pro vývoj aplikací, ale poskytují například také decentralizovaná řešení volebního procesu, validaci chytrých kontraktů, bankovnictví, směnáren a komunitního fundování projektů. (31)

Nazývat proto všechny projekty alternativními kryptoměnami není zcela šťastné, avšak stále se jedná o běžnou praxi v rámci internetových komunit, informačních webů a dokonce i některých akademických prací.

Výše zmíněné příklady termínů ukazují snahu ekosystému o určitou kategorizaci na základě funkčnosti jednotlivých projektů. V rámci rešerše jsem narazil pouze na jedinou práci, ve které by se její autor pokusil o taxonomii podrobnější.

Andreas Antonopoulos ve své práci „Mastering Bitcoin“ podle účelu rozděluje projekty na alternativní kryptoměny a alternativní řetězce („Alt-Chains“). Primárním účelem Altcoinů je nahrazení měny, zatímco účel řetězců je stejný jako v případě Kryptoměn 2.0. (32)

Ačkoliv se jedná o celkem jednoznačné a jednoduché rozdělení, můžeme narazit na projekty, které nebudeme schopni s určitostí zařadit. Příkladem je NXT, který obsahuje funkcionality typické pro kryptoměny v. 2.0, ale zároveň je snaha ho prosadit jako standardní platidlo a prostředek směny. Dokonce i autor Andreas Antonopulos řadí projekt NXT nejprve mezi alternativní řetězce a posléze jej detailněji zmiňuje společně s ostatními Altcoiny. (32,33)

Dále trochu nejasně definuje další kategorii tzv. meta mincí („Meta-Coins“) a meta řetězců („Meta-Chains“), které účelem spadají do kategorie alternativních řetězců a odlišují se pouze technologickou implementací. (32)

Autor se zároveň odmítá blíže věnovat skupině alternativních měn, které charakterizuje jako centralizované nebo nevyužívající metody Proof of Work. Jako příklad takového systému se zmiňuje Ripple, sloužící k rychlým platbám a směně různých forem peněz. (32)

Na základě výše uvedených poznatků dělím jednotlivé projekty na nejvyšší úrovni podle funkcionality na alternativní kryptoměny a alternativní řetězce.

Nejprve ale musím podrobněji zmínit bitcoin, ze kterého mnohé další projekty vycházejí a který je stále projektem nejznámějším a nejúspěšnějším. Dále pak krátce zmíním další významné projekty, které jsou v určitých ohledech inovativní, nebo aktuálně populární. Pokusím se také identifikovat, proč jsou některé měny oblíbenější než druhé a co je toho příčinou. Z pohledu těžební problematiky se budu jednotlivým projektům věnovat podrobněji v následující kapitole.

4.2 Referenční kryptoměna Bitcoin (BTC)

Bitcoin je kryptoměna. Ve své podstatě se jedná o „*Soubor konceptů a technologií, které dohromady tvoří základ ekosystému digitálních peněz.*“ (32)

První ucelený koncept bitcoinu byl publikován v říjnu 2008, jehož autorem byl Satoshi Nakamoto. I přes velkou snahu investigativních novinářů se zatím nepodařilo s určitostí identifikovat, kdo se za daným pseudonymem skrývá. Spekuluje se o několika jedincích, nebo dokonce skupinách osob. (34)

Začátkem ledna 2009 byl vytěžen první blok, blok genesis, společně se kterým byly vytvořeny první bitcoiny. První transakce byla uskutečněna nedlouho poté. Koncem roku 2010 Satoshi projekt opouští a jeho vývoj je předán do rukou skupiny nadšenců a programátorů, kteří se spojili do uskupení nazvaného Bitcoin Foundation. Od té doby zodpovídají za další vývoj, propagaci a legální ochranu projektu. (35)

Můžeme namítnout, že bitcoin vlastně není decentralizovaný, protože se o jeho další vývoj stará skupina vývojářů, která může parametry systému de facto změnit. Ano je pravda, že vývojáři můžou například vydat novou verzi klienta, který bude pracovat odlišněji. Uživatelé však nemusí tohoto klienta začít využívat a mohou setrvat u verze původní. Ti, kteří na nového klienta přestoupí, nebudou pak schopni komunikovat se většinovým zbytkem sítě a systém nebude funkční. (36)

Lidé mohou kryptoměnu získat dvěma způsoby. Převodem od ostatních uživatelů, nebo vytvořením bitcoinů zcela nových. Před získáním samotné měny musíme mít vytvořené místo, na které měnu přijmeme, peněženku.

Jednotky měny jsou vytvářeny procesem, který se nazývá těžba. Kdokoliv se může prostřednictvím ať už svého počítače, nebo jiného výpočetního zařízení tohoto procesu bez omezení zúčastnit. Z hlediska systému není primárním účelem procesu těžby tvorba nových bitcoinů, ale ověření a zapsání uskutečněných transakcí do veřejné databáze, blockchainu. Bez dostatečného množství různých těžařů, by systém nebyl schopen zaručit pravost transakcí. Z toho důvodu jsou uživatelé k této činnosti motivováni odměnou v podobě nově vytvořených bitcoinů.

Množství jednoho bitcoinu se označuje jako 1 BTC. Jedná se o jednu minci dané kryptoměny. Stejně jako má česká koruna haléře, můžeme i bitcoin štěpit na menší části. Protokol umožňuje mince rozštěpit až na 8 desetinných míst. Jednotka nejmenšího možného množství bitcoinu je satoshi. (37)

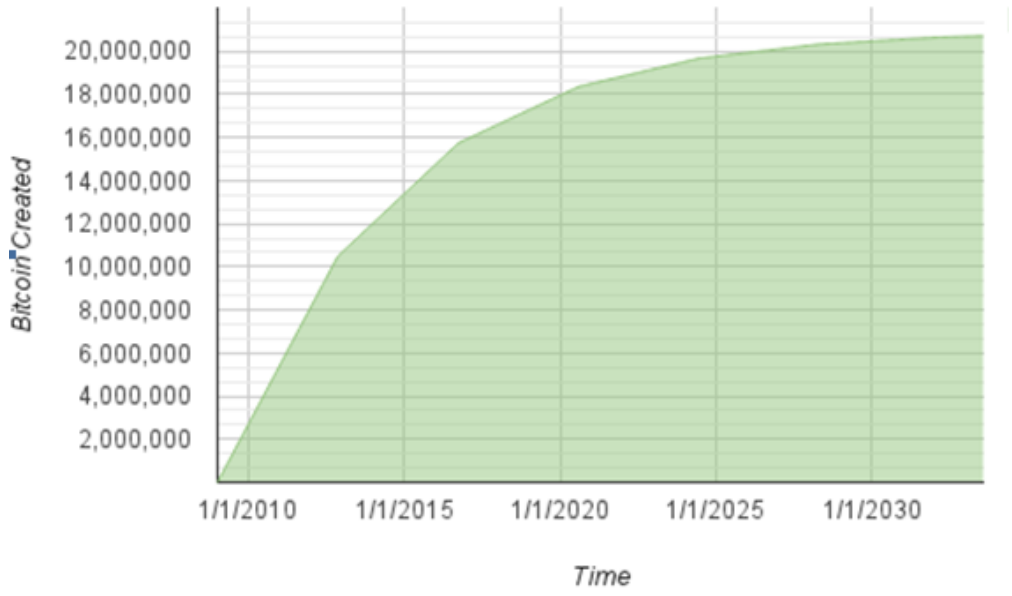
1 BTC	=	1 bitcoin
0.01 BTC	=	1 centibitcoin (1 cBTC)
0.001 BTC	=	1 millibitcoin (1 mBTC)
0.000 001 BTC	=	1 microbitcoin (1 µBTC)
0.000 000 01 BTC	=	1 satoshi

V čem se vlastně liší bitcoin od ostatních alternativních kryptoměn? V úvodu jsem zmínil například funkcionalitu, nebo technické zpracování. Charakter každé měny určuje také to, jak jsou nastavené jeho základní parametry typu celkového množství mincí, výše odměny za těžbu, nebo typ zvoleného těžebního algoritmu.

Základní nastavitelné parametry bitcoinu a dalších projektů jsou:

- **Metoda ověření transakcí** - Nejvýznamnější parametr, jehož volba přímo určuje, na jakém principu bude projekt postaven. Ovlivňuje veškeré další parametry kryptoměny, od délky trvání transakcí po nastavení měnové báze, či způsobu těžby. Nejčastější metody jsou Proof of Work a Proof of Stake, nebo jejich kombinace. PoW je charakteristický pro bitcoin, jehož prostřednictvím jsou těženy nové bloky obsahující realizované transakce. (32)

- **Celkové množství mincí** - Od začátku bylo do prosince 2014 vytěženo více jak 13,5 milionu mincí bitcoinu. Tento počet není konečný, protože maximální počet vytěžitelných mincí je nastaven na 21 milionů. Rychlost jakou jsou nové bitcoiny generovány se i přes nárůst obětovaného výpočetního výkonu neustále snižuje. Odhaduje se, že poslední mince bude vytěžena až v roce 2140. Maximální množství mincí tak určuje, zda se jedná o kryptoměnu deflačního nebo inflačního charakteru. Alternativní kryptoměny nemusí mít maximum stanovené.(22)



Obrázek č. 3 Celkový počet bitcoinových mincí v závislosti na čase. Zdroj: (32)

- **Průměrná doba vytěžení nového bloku** – Tento nastavitelný parametr definuje průměrnou dobu, za jakou je nový blok vytvořen. V případě bitcoinu se jedná o 10 minut, tedy v průměru 6 nových bloků za hodinu. Nově vytvořené bloky obsahují potvrzení uskutečněných transakcí, což znamená, že k potvrzení nové transakce nedojde dříve jak za deset minut. I přes nárůst těžebního výkonu, nedochází k urychlení tvorby nových bloků, protože se mění náročnost těžby, kterou systém stanovuje dynamicky po vytěžení 2016 bloků. (32)

- **Změna obtížnosti** – Určuje, po jaké době proběhne automatický přepočet a nastavení náročnosti těžby. Hodnota se udává nejčastěji v množství vytěžených bloků.(38)

- **Odměna za vytěžený blok** – Těžaři jsou za úspěšné vytěžení bloku odměněni určitým počtem bitcoinů. Tato hodnota se v průběhu času periodicky snižuje na polovinu. Dochází k tomu po úspěšném vytvoření 210 tisíc bloků, tedy v průměru každé 4 roky. Na počátku byla odměna rovna 50 BTC, aktuální výše je 25 BTC za úspěšně vytěžený blok. Někdy v roce 2016 dojde k změně odměny na 12.5 BTC. (37)

- **Změna odměny za vytěžený blok** – Parametr určující po kolika vytěžených blocích, se sníží odměna za nový blok. (37)

- **Zralost mincí** – Doba, po kterou nemůžeme nově vytvořené mince převést na jinou adresu. Aktuální verze bitcoinu má hodnotu nastavenou na 101 bloků, což znamená, že nově vytěžené mince můžeme použít až poté, co dojde k vytěžení 101 následujících bloků. (32)

- **Těžební algoritmus** – V závislosti na volbě určuje především efektivitu, s jakou budeme schopni kryptoměnu těžit za pomoci různých technologií. Bitcoin využívá SHA 256d. (32)

4.2.1 Využití bitcoinu v reálné ekonomice

Způsoby jak se dají bitcoiny získat jsem již zmínil. Otázkou ale je, k čemu nám získaná kryptoměna vlastně bude, jaké má potenciální využití a jaké jsou její výhody, případně nevýhody?

Bitcoin má, stejně jako jiné měny, několik základních funkcí a způsobů využití. Především se jedná o funkci všeobecného prostředku směny a uchovatele hodnoty.

Řada obchodníků, výrobců a poskytovatelů služeb již akceptuje bitcoin jako jednu z platebních metod. Můžeme jej tedy využít v rámci bezhotovostního nákupu zboží a služeb. Výhodou v tomto případě jsou oproti platebním kartám nebo bankovním převodům nízké transakční náklady, které jsou prakticky nulové. Bohužel i přes existenci různých směnáren, není jednoduché bitcoiny získat. Směna reálných peněz za bitcoiny je většinou doprovázena řadou určitých omezení a poplatků, které ve výsledku jeho další využití prodražují.

Bitcoiny akceptují stovky internetových obchodníků a poskytovatelů služeb. Můžeme s nimi nakupovat webové služby typu DNS, počítačové hry, fyzické produkty od potravin po nemovitosti, platit programátory za vývoj aplikací, účetní služby nebo třeba letenky a další ubytování. Typově tedy všechno, co můžeme nakoupit i za peníze reálné. (39)

4.2.1.1 Trh s nelegálními produkty a službami

Existují také produkty a služby, které se za peníze reálné sice dají nakoupit, ale oproti bitcoinu mnohem složitěji. S bitcoinem, vznikl i rozsáhlý internetový černý trh, na kterém můžeme online nakupovat drogy, falešné doklady, pornografii, či dokonce objednávat služby typu nájemných vražd. Důvod využití kryptoměn na černém trhu je jejich anonymita.

Všechny uskutečněné transakce jsou ukládány do blockchainu, do kterého může nahlížet kdokoliv. Z této databáze ale nejsme schopni přesně identifikovat, mezi kterými osobami daná transakce proběhla, dokážeme zjistit pouze adresy, z a na kterou byly mince převedeny. Pokud majitel nezveřejní, že daná adresa patří zrovna jemu, nemáme šanci skutečného majitele adresy určit. V praxi lidé většinou využívají pro úschovu a směnu kryptoměn služby webových směnáren a peněženek. Registrují se zde svými reálnými údaji, jejíž pravost provozovatel služby ověřuje vyžádáním osobních dokumentů, většinou pasu a faktury za energie, prokazující bydliště. (22, str. 83)

Internetová tržiště, kde probíhá obchod s nelegálními službami a látkami, se nazývají trhy temné sítě („Dark net markets“). Většina z nich není dostupná prostřednictvím standardních internetových prohlížečů, je potřeba využít klienta Tor. Software Tor slouží k především k anonymnímu surfování po webech, čehož je dosaženo přesměrováním veškeré internetové komunikace skrze rozsáhlou síť dalších serverů, čímž uživatel skryje svojí IP adresu. (40)

Tato tržiště fungují na stejném principu jako kupříkladu Amazon, tedy pouze jako platforma pro různé prodejce, kteří zde své zboží formou nabídek inzerují. Uživatelé si mohou vybrat z velkého množství nabízeného zboží, největším zástupcem jsou ale drogy. Po zvolení konkrétního produktu a množství, kupující odešle svou nabídku společně se zašifrovanou adresou bydliště prodejci. Zároveň dojde k zablokování určitého množství kryptoměny, které odpovídá cenně vybraného produktu. Tyto prostředky jsou odblokovány ve chvíli, kdy nakupující potvrdí úspěšné převzetí poštovní zásilky obsahující požadovaný produkt. Kupující může posléze zveřejnit hodnocení kvality ať už samotného produktu, tak procesu objednávky. U prodejců s vysokým počtem kladných hodnocení se dá očekávat, že je jejich produkt kvalitní. Kupující tak má vysokou záruku toho, že obdrží bezpečný produkt vysoké jakosti. (6)

Všeobecně nejznámějším příkladem takového tržiště je Silk Road, jehož provoz byl po zásahu amerických tajných služeb ukončen v roce 2013, zanedlouho poté však vznikla řada dalších tržišť. Nejaktivnější tržiště jsou Agora a Evolution, kde je nabízeno více jak 15 tisíc různých položek, většinou drog. Hodnota obchodů zrealizovaných prostřednictvím Silk Road v době největší aktivity, byla odhadovaná na 20 až 30 milionu dolarů ročně. Popularita tržišť roste, což zvyšuje poptávka po kryptoměnách a tím pádem i jejich hodnotu. (41,42,43)

4.2.1.2 Obcházení legislativních a regulatorních bariér

Hlavním charakteristickým rysem bitcoinu je fakt, že se jedná o měnu globální, nerespektující hranice. V případě mezinárodních finančních transakcí se můžeme setkat s množstvím překážek. Od různých legislativních omezení, bankovní kontroly až celou řadu poplatků. Zaslat platbu subjektu, který má sídlo například v některém z asijských států může být spjato s celou řadou kontrol, poplatků a ve výsledku zpracování takovéto platby může trvat i několik dní. Bitcoin je v tomto případě zajímavou alternativou, kdy můžeme převést podstatné

množství finančních prostředků rychle a bez nákladů. Existuje řada lokálních směnáren, které následně umožňují zpětnou směnu bitcoinů do měny reálné.

Zmínil jsem legislativní a regulatorní bariéry, které se vztahují na měny reálné. Klasickým případem je Čína, ve které se bitcoin těší zdaleka největší popularitě. V Číně jsou především investiční možnosti obyvatelstva velmi omezené, to se týká jak cenných papírů, tak nemovitostí. Obchodování s kryptoměnami, které nejsou centrálně regulované státem, se tak stává nejenom zajímavou investiční příležitostí, ale také způsobem jak nabytý kapitál ochránit. O velikost čínského trhu vypovídá fakt, že více jak 70 procent všech transakcí s bitcoiny, je denominováno v Juanech.(44)(45)

Komplikovaný a omezený je také vývoz kapitálu do zahraničí. Tyto restrikce Číňané obcházejí prostřednictvím bitcoinu, který je v zemi dostupný a z podstaty nejde státně regulovat. Princip spočívá v nákupu kryptoměny za regulované čínské Juany a následnou směnu například za dolary americké. Toto se samozřejmě nelíbí čínské vládě, které se tak komplikuje kromě kontroly kapitálu také boj s praním špinavých peněz. (22, str 66)

4.2.2 Hodnota Bitcoinu

John Mauldin správně zmiňuje globální ekonomicko-politickou situaci, na kterou se projekt bitcoinu a dalších kryptoměn snaží reagovat. V roce 2008 a 2009 prožil svět největší ekonomickou krizi od druhé světové války. Jednotlivé státy začaly okamžitě reagovat formou státních zásahů, ať už se jedná o záchranu bank, či tištění nových peněz. Mnohé banky zkrachovaly, s čímž mnoho lidí přišlo o své celoživotní úspory. Důvěra lidí v systém tak byla otřesena a bitcoin začal těžit z vyšší pozornosti médií jakožto peněz, se kterými není téměř možné centrálně manipulovat. (46)

Jako příklad autor uvádí kyperskou krizi, kdy došlo ke zhroucení tamějšího bankovního systému, a lidé tak přišli o vklady vyšší než 100 tisíc eur. Ve stejné době hodnota bitcoinu v krátké době vzrostla o desítky procent. Ke konci roku 2013 došlo v Číně k podobnému růstu zájmu o bitcoin v souvislosti se začínajícím zpomalováním tamější ekonomiky a hrozby prasknutí dluhové bubliny. (46)

Když pomineme ekonomicko-ideologické přínosy typu omezené možností státní regulace a deflační charakter měny, tak zbude anonymního využití v šedočerné ekonomice a jako investiční nástroj. Samozřejmě můžeme namítnout, že tou hlavní výhodou jsou nízké nebo spíše žádné transakční poplatky a rychlost s jakou jsou transakce realizované. Obávám se ale, že v případě každodenního využití, při srovnání s platebními systémy typu PayPal tento argument neobstojí.

4.3 Alternativní kryptoměny a řetězce

Cílem alternativních kryptoměn, zkráceně také altcoinů, je podobně jako v případě bitcoinů, nabídnutí alternativy ke měnám reálným. Většina altcoinů sdílí základní funkčnost s první kryptoměnou bitcoinem, jehož zdrojový kód byl při tvorbě nové měny upraven. Takto vzniklé alternativní kryptoměny jsou de facto bitcoinové odnože („Forks“).

První altcoin, který získal širší popularitu uživatelů, byl vytvořen ke konci roku 2011. Jedná se o litecoin. Není to ale první projekt vzniklý po bitcoinu, tím byl namecoin, který ale z hlediska kategorizace musím zařadit mezi alternativní řetězce a proto ho zmíním později. Alternativní kryptoměny vytvořené před litecoinem, jenž ale nezískaly širší popularitu, byly například ixcoin nebo tenebrix. (47)

Do konce roku 2012 bylo aktivních kolem 20 různých projektů, v porovnání s rokem 2011 tento počet narostl o deset nových kryptoměn. Situace se změnila v roce 2013, kdy došlo k ohromnému rozvoji a nárůstu množství nových projektů na celkový počet přesahující 200. Zrychlující trend se potvrzuje i v roce 2014, aktuálně web MapOfCoins.com eviduje více než 700 různých kryptoměn. (47)

Příčinou tohoto zrychlení rozvoje ekosystému kryptoměn byla, podle mého názoru, cenová exploze bitcoinu. Vrchol nastal ke konci roku 2013, kdy měl 1 BTC hodnotu větší než 1100 USD. Začalo docházet k masivní mediální propagaci bitcoinu, se kterou rostl i počet investorů, uživatelů a vývojářů. Při pohledu na vývoj grafu ceny bitcoinu se mnoho lidí vrhlo do vytváření nových alternativních kryptoměn s přesvědčením, že upravení několika málo parametrů stačí k tomu, aby měna získala všeobecnou popularitu spojenou s prudkým nárůstem její hodnoty. Tento názor přetrvává i dnes. (22)

Mnoho úspěšných projektů můžeme zařadit do kategorie alternativních řetězců. Primárním účelem těchto projektů není vytvoření prostředku směny ve smyslu nových peněz. Mohou ale v rámci svého fungování generovat mince, které slouží ke směně za jiný systémový zdroj nebo kontrakt.

Typickým zástupcem je namecoin, který decentralizovaným způsobem spravuje internetovou doménu s koncovkou .bit. Systém můžeme využít nejen k registraci nové domény, ale také k úschově informací typu otisku prstů, emailu, různých adres a dalších. Veškeré úkony spotřebovávají mince, které můžeme získat buď nákupem, nebo těžbou. (48)

4.3.1 Jak nová alternativní kryptoměna vzniká

Vytvořit novou alternativní kryptoměnu nikdy nebylo jednoduší. Vzhledem k tomu, že zdrojové kódy nejen dvou nejpopulárnějších měn bitcoinu a litecoinu jsou veřejně přístupné ke stažení, vznikla celá řada návodů a dokonce i služeb, které celý proces vzniku výrazně usnadňují. Postup je celkem jednoduchý a téměř každý s alespoň základní znalostí programování v jazyce C++ by měl být schopný novou kryptoměnu vytvořit v rámci několika málo hodin. Zdrojové kódy mnoha měn jsou dostupné na serveru Github.com.

Ve chvíli kdy máme stažené zdrojové kódy jedné z předních kryptoměn, můžeme jednoduše parametry v kódu změnit a při úspěšném zkompilování je nová měna vytvořena. Nejčastěji měněnými parametry jsou: Název měny, průměrná doba vytvoření nového bloku, po kolika vytěžených blocích dojde k zvýšení náročnosti těžby, jaká bude odměna za vytěžené bloky, po jaké době dojde ke snížení odměny za vytěžený blok a jaké porty měna využívat. Rovněž se dají měnit parametry typu náročnost těžby a další. (49)

Existuje dokonce i webová služba, prostřednictvím které můžeme alternativní měnu vytvořit během pár minut. U takto, za určitý poplatek, vytvořené kryptoměny, můžeme určit její jméno, použitý hashovaní algoritmus (SHA256 nebo Scrypt) a další parametry rychlosti těžby a distribuce mincí. (50)

Předešlý postup vzniku je typický pro alternativní kryptoměny odvozené od bitcoinu, nebo litecoinu. Takto vzniklé kryptoměny mají povětšinou velmi malou přidanou hodnotu a liší se pouze příběhem a myšlenkou, která stála za jejich vznikem. Jako příklad mohu uvést měnu amerických indiánských kmenů MazaCoin, nebo českou CzechCrownCoin. Obě zmíněné měny se zaměřují na uživatele určité národnosti. (51)

Mnoho vývojářů a nadšenců se nespokojuje pouze s vytvářením klonů a snaží se posunout funkcionalitu kryptoměn o krok dále. Nejnovější trend na poli nových měn je tvorba tzv. Kryptoměn 2.0, jejichž cíl a funkcionalita je od zbytku výrazně odlišná. Více prostoru této problematice věnuji dále.(31)

Autorem nové měny může být naprosto kdokoliv. Jedná se převážně o jednotlivce nebo v lepším případě organizované skupiny nadšenců. Autoři svou identitu skrývají je ve většině případů za pseudonym, stejně jako tomu je v případě autora bitcoinu, Satoshi Nakamota. (52)

Vznik nových projektů a měn je většinou ohlášen a propagován napříč internetovou komunitou, což je také hlavní způsob jakým se jejich tvůrci snaží nalézt nové následovníky a rozšířit tak bázi uživatelů. Propagace probíhá především na oficiálním internetovém fóru, nejen Bitcoinových nadšenců, Bitcointalk.org a komunitních webech typu Reddit.com. Oblíbená je také síť Twitter. Každá z alternativních kryptoměn mívá také vlastní internetovou stránku a princip fungování významnějších měn, je popsán v dokumentech na těchto webech dostupných. Například prostřednictvím webu altcoincalendar.info, lze sledovat, kdy a které nové měny budou spuštěny.

Serióznější projekty vyvíjené často celými skupinami vývojářů spotřebovávají při své snaze nemalé množství zdrojů, času a peněz. Častý způsob pokrytí těchto nákladů je proces tzv. první nabídky mincí („Initial Coin Offering“), což je pojem převzatý z prostředí kapitálových trhů, konkrétně veřejné nabídky akcií. Podobně jako u akcií se jedná o nabídku určitého množství měny k nákupu investory. K této nabídce dochází zpravidla před samotným představením projektu široké veřejnosti a před umožněním získat mince například těžbou. (53)

Pro vývojáře se jedná o zajímavý způsob jak pokrýt prvotní náklady na vývoj a prezentaci projektu. Investor oproti tomu nemá žádné záruky, že vývojář daný projekt úspěšně dokončí nebo s takto získanými prostředky jednoduše neuteče. Investoři proto stále častěji využívají podmíněných smluv („Escrow“). Jedná se o svěření financí třetí straně, která je předá nabyvateli až po splnění smluvních podmínek. I přes vysoké riziko na straně investora je tento způsob financování projektu stále velmi častý. (17)

4.3.2 Účastníci trhu

V ekosystému alternativních krytoměn můžeme rozlišit čtyry druhy uživatelů. Jedná se o běžné uživatele, kteří altcoiny využívají převážně k nákupu zboží nebo převodu financí. Uživatelé mohou nakupovat zboží od obchodníků, pro které altcoiny představují další způsob platebního styku se zákazníkem.

S kryptoměnami obchodují hlavně další dvě skupiny uživatelů. Těžaři, kteří se podílejí na tvorbě kryptoměn se záměrem takto vytvořené kryptoměny se ziskem prodat. Druhu skupinou jsou spekulanti, kteří kryptoměny nakupují a prodávají. Jejich cílem je vydělat na kurzovém

pohybu. V obou skupinách se dají nalézt individuální amatérští nadšenci, skupiny nadšenců nebo dokonce obchodní společnosti.

5 Rozdělení projektů podle jejich významu

Významnost jednotlivých alternativních kryptoměn a řetězců je možné určit podle jejich aktuální tržní kapitalizace. (Počet vytěžených mincí * tržní cena jedné mince.) Webové servery sledující tržní kapitalizaci jsou například coinmarketcap.com, cryptocoincharts.info, worldcoinindex.com nebo cryptocoinrank.com. (26,56, 56, 57)

Dalším důležitým parametrem jsou možnosti směny, jak a kde můžeme altcoiny směnit za reálné peníze.

Pro výpočet tržní kapitalizace potřebujeme znát tržní cenu kryptoměny, za kterou se obchoduje na směnárnách.

5.1.1 Tržní cena

Alternativní kryptoměny se obchodují nejčastěji ve formě směnitelného kurzu vůči bitcoinu, či jiným měnám. Kotace a styl obchodování připomíná reálný trh měn, Forex. Hlavní tři páry, ve kterých se kryptoměny za reálné peníze obchodují, jsou BTC/USD, BTC/EUR a BTC/CNY. Prostřednictvím některých směnáren se dají krypotměny obchodovat kupříkladu i za britskou libru, ruský rubl nebo japonský jen. Alternativní kryptoměny s malou tržní kapitalizací se zřídkakdy obchodují přímo za měny reálné. Neobchodovanější páry alternativních kryptoměn ve vztahu k Bitcoinu jsou LTC/BTC, DOGE/BTC, DRK/BTC. (58)

Tabulka č. 1 Obchodované kryptoměnové páry Zdroj: (60)

TRH	MĚNA	OBJEM ZA 24 HODIN	KURZ	NEJVYŠŠÍ KURZ ZA POSLEDNICH 24 HODIN	NEJNIŽŠÍ KURZ ZA POSLEDNICH 24 HODIN
DRK/LTC	DarkCoin	21.9 BTC	0.79872459	0.88014930 LTC	0.68023219 LTC
DOGE/LTC	Dogecoin	4.19 BTC	0.00005996	0.00006320 LTC	0.00005900 LTC
FTC/LTC	FeatherCoin	3.75 BTC	0.00677406	0.00683214 LTC	0.00663214 LTC
MOON/LTC	MoonCoin	1.71 BTC	0.00000021	0.00000025 LTC	0.00000021 LTC
RBBT/LTC	RabbitCoin	1.23 BTC	0.00000007	0.00000009 LTC	0.00000007 LTC
XPM/LTC	PrimeCoin	1.10 BTC	0.04130483	0.04130483 LTC	0.03937280 LTC
BC/LTC	BlackCoin	0.668 BTC	0.01014997	0.01076098 LTC	0.00892043 LTC
DIME/LTC	DimeCoin	0.613 BTC	0.00000004	0.00000004 LTC	0.00000003 LTC
TIPS/LTC	FedoraCoin	0.548 BTC	0.00000006	0.00000007 LTC	0.00000006 LTC
VTC/LTC	VertCoin	0.536 BTC	0.01571212	0.01600000 LTC	0.01532405 LTC
NXT/LTC	Nxt	0.476 BTC	0.00553505	0.00562491 LTC	0.00520644 LTC
AUR/LTC	AuroraCoin	0.389 BTC	0.01011901	0.01146330 LTC	0.00977770 LTC
MEOW/LTC	KittehCoin	0.358 BTC	0.00000023	0.00000028 LTC	0.00000022 LTC
HTML5/LTC	Html5Coin	0.351 BTC	0.00000063	0.00000078 LTC	0.00000050 LTC
PPC/LTC	Peercoin	0.275 BTC	0.21695254	0.22589782 LTC	0.20678962 LTC
KARM/LTC	KarmaCoin	0.265 BTC	0.00000048	0.00000050 LTC	0.00000046 LTC
DVC/LTC	DevCoin	0.231 BTC	0.00000863	0.00000875 LTC	0.00000780 LTC
IFC/LTC	InfiniteCoin	0.186 BTC	0.0000014	0.00000152 LTC	0.00000120 LTC
ASC/LTC	AsicCoin	0.181 BTC	0.000007	0.00000795 LTC	0.00000700 LTC

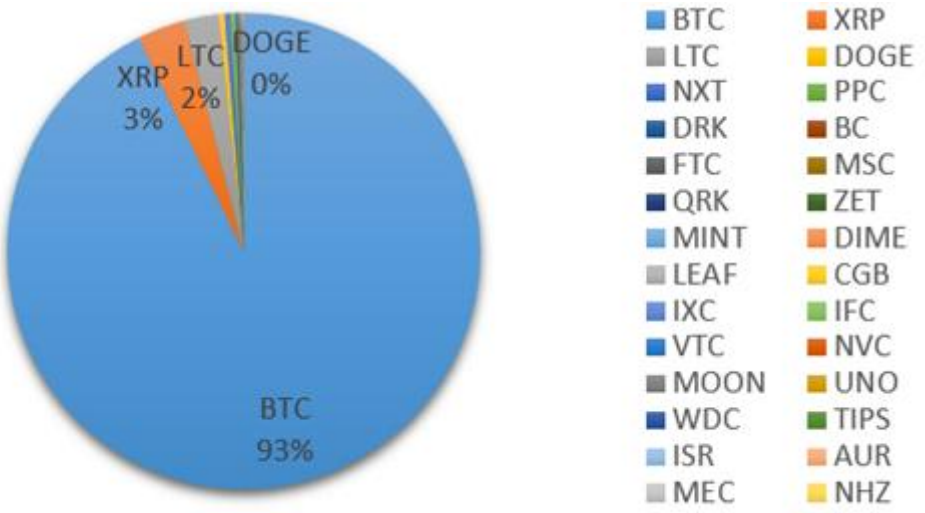
Většina obchodů probíhá prostřednictvím směnáren, kurzy jednotlivých kryptoměn jsou stanovovány na základě aktuální poptávky a nabídky. Kryptoměny jsou na rozdíl od ostatních trhů s finančními nástroji obchodovány 24 hodin denně po dobu 7 dní v týdnu. Aktivních je

více jak 70 různých směnáren a většina z nich se zaměřuje hlavně na směnu bitcoinu za měnu reálnou (Dolar, Jüan, Euro,…).

5.1.2 Tržní kapitalizace

Podle mého názoru nejpřehlednější a nejobsáhlejší žebříček nabízí web coinmarketcap.com.

Tržní kapitalizace celého trhu přesahuje více než 5 miliard dolarů. Jedná se však pouze o odhad, protože přesná data neexistují. Z celku zhruba 90 procent tvoří bitcoin (Více než 5 miliard USD). Druhým projektem podle tržní kapitalizace je ripple, který tvoří necelá 3% celkové tržní kapitalizace. (26)



Obrázek č. 4 Velikost tržní kapitalizace různých kryptoměn v USD Zdroj: (26)

Tabulka č. 2 Pořadí padesáti kryptoměn podle jejich tržní kapitalizace. Zdroj: (26)

#	Jméno	Tržní kapitalizace	Cena	Celkové množství mincí	#	Jméno	ržní kapitalizac	Cena	Celkové množství mincí
1	Bitcoin	$ 5 095 156 975	$375.12	13,582,775 BTC	26	Bytecoin	$ 1 435 457	$0.00	166,503,781,735 BCN
2	Ripple	$ 454 221 578	$0.01	30,881,360,458 XRP *	27	InstantDEX	$ 1 213 180	$1.21	1,000,000 DEX *
3	Litecoin	$ 128 172 543	$3.72	34,493,094 LTC	28	Quark	$ 1 150 089	$0.00	248,456,311 QRK
4	BitShares	$ 44 943 544	$0.02	2,497,973,773 BTS *	29	Storjcoin X	$ 1 083 278	$0.03	41,464,404 SJCX *
5	MaidSafeCoin	$ 26 154 543	$0.06	452,552,412 MAID *	30	Primecoin	$ 1 065 585	$0.13	8,168,655 XPM
6	Dogecoin	$ 22 322 077	$0.00	96,509,538,133 DOGE	31	ReddCoin	$ 1 028 844	$0.00	27,262,390,911 RDD
7	Nxt	$ 19 256 744	$0.02	999,997,096 NXT *	32	BitUSD	$ 991 796	$1.01	982,765 BITUSD *
8	Peercoin	$ 15 877 753	$0.72	21,923,089 PPC	33	andacoin (PND)	$ 868 464	$0.00	32,320,482,669 PND
9	Counterparty	$ 14 676 121	$5.54	2,646,826 XCP *	34	UltraCoin	$ 735 236	$0.03	23,066,387 UTC
10	Darkcoin	$ 11 713 931	$2.38	4,923,723 DRK	35	Nxttycoin	$ 673 981	$0.00	1,000,000,000 NXTTY *
11	Namecoin	$ 9 362 957	$0.90	10,441,350 NMC	36	jl777hodl	$ 662 640	$0.07	10,000,000 JLH *
12	Stellar	$ 8 321 334	$0.00	3,545,126,825 STR *	37	Jinn	$ 654 712	$6.55	100,000 JINN *
13	FuelCoin	$ 7 076 767	$0.07	100,101,526 FC2 **	38	Ixcoin	$ 648 284	$0.03	20,999,906 IXC
14	NuShares	$ 4 033 534	$0.01	604,881,045 NSR *	39	Ethercoin	$ 633 951	$0.63	1,000,000 ETC *
15	SuperNET	$ 3 320 226	$4.07	816,061 UNITY *	40	BitShares PTS	$ 628 425	$0.36	1,763,152 PTS
16	BanxShares	$ 2 901 473	$1.12	2,586,882 BANX *	41	XCurrency	$ 626 703	$0.11	5,564,016 XC *
17	Mastercoin	$ 2 826 257	$5.02	563,162 MSC *	42	DNotes	$ 601 568	$0.01	94,041,276 NOTE
18	BitcoinDark	$ 2 471 940	$2.07	1,194,826 BTCD	43	Zetacoin	$ 582 505	$0.00	161,322,565 ZET
19	Monero	$ 2 276 530	$0.45	5,050,056 XMR	44	ShadowCash	$ 563 999	$0.09	6,448,804 SDC *
20	NuBits	$ 2 253 581	$1.00	2,245,631 NBT *	45	Qora	$ 562 679	$0.00	10,000,000,000 QORA *
21	YbCoin	$ 2 039 031	$0.68	3,000,000 YBC	46	sharkfund0	$ 552 392	$416.08	1,328 SF0 *
22	BlackCoin	$ 2 021 493	$0.03	74,726,178 BC *	47	Vertcoin	$ 530 716	$0.05	10,257,000 VTC
23	NXTventure	$ 1 925 680	$1.93	1,000,000 NXTV *	48	BitBay	$ 525 771	$0.00	1,000,063,149 BAY *
24	Swarm	$ 1 741 300	$0.02	100,000,000 SWARM *	49	Viacoin	$ 522 581	$0.04	12,479,700 VIA
25	Feathercoin	$ 1 570 438	$0.03	62,485,090 FTC	50	Infinitecoin	$ 510 870	$0.00	90,595,875,241 IFC

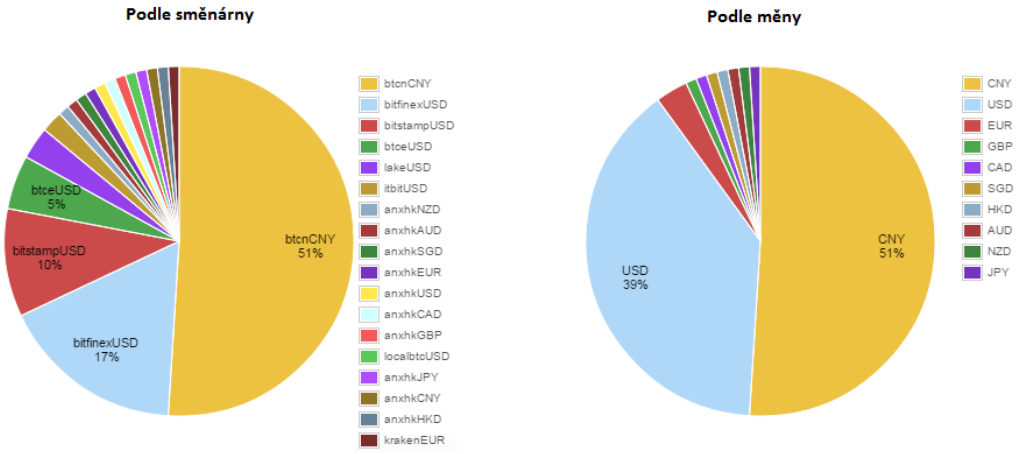
Tabulka č. 3 Pořadí kryptoměn v rozlišení na těžitelné a netěžitelné. Zdroj: (26)

#	Jméno	Tržní kapitalizace	Cena	Celkové množství mincí	#	Jméno	ržní kapitalizac	Cena	Celkové množství mincí
1	Ripple	$ 454 221 578	$0.01	30,881,360,458 XRP *	1	Bitcoin	5 095 156 975	$375.12	13,582,775 BTC
2	BitShares	$ 44 943 544	$0.02	2,497,973,773 BTS *	2	Litecoin	$ 128 172 543	$3.72	34,493,094 LTC
3	MaidSafeCoin	$ 26 154 543	$0.06	452,552,412 MAID *	3	Dogecoin	$ 22 322 077	$0.00	96,509,538,133 DOGE
4	Nxt	$ 19 256 744	$0.02	999,997,096 NXT *	4	Peercoin	$ 15 877 753	$0.72	21,923,089 PPC
5	Counterparty	$ 14 676 121	$5.54	2,646,826 XCP *	5	Darkcoin	$ 11 713 931	$2.38	4,923,723 DRK
6	Stellar	$ 8 321 334	$0.00	3,545,126,825 STR *	6	Namecoin	$ 9 362 957	$0.90	10,441,350 NMC
7	NuShares	$ 4 033 534	$0.01	604,881,045 NSR *	7	BitcoinDark	$ 2 471 940	$2.07	1,194,826 BTCD
8	SuperNET	$ 3 320 226	$4.07	816,061 UNITY *	8	Monero	$ 2 276 530	$0.45	5,050,056 XMR
9	BanxShares	$ 2 901 473	$1.12	2,586,882 BANX *	9	YbCoin	$ 2 039 031	$0.68	3,000,000 YBC
10	Mastercoin	$ 2 826 257	$5.02	563,162 MSC *	10	Feathercoin	$ 1 570 438	$0.03	62,485,090 FTC
11	NuBits	$ 2 253 581	$1.00	2,245,631 NBT *	11	Bytecoin	$ 1 435 457	$0.00	166,503,781,735 BCN
12	BlackCoin	$ 2 021 493	$0.03	74,726,178 BC *	12	Quark	$ 1 150 089	$0.00	248,456,311 QRK
13	NXTventure	$ 1 925 680	$1.93	1,000,000 NXTV *	13	Primecoin	$ 1 065 585	$0.13	8,168,655 XPM
14	Swarm	$ 1 741 300	$0.02	100,000,000 SWARM *	14	ReddCoin	$ 1 028 844	$0.00	27,262,390,911 RDD
15	InstantDEX	$ 1 213 180	$1.21	1,000,000 DEX *	15	andacoin (PND)	$ 868 464	$0.00	32,320,482,669 PND
16	Storjcoin X	$ 1 083 278	$0.03	41,464,404 SJCX *	16	UltraCoin	$ 735 236	$0.03	23,066,387 UTC
17	BitUSD	$ 991 796	$1.01	982,765 BITUSD *	17	Ixcoin	$ 648 284	$0.03	20,999,906 IXC
18	Nxttycoin	$ 673 981	$0.00	1,000,000,000 NXTTY *	18	BitShares PTS	$ 628 425	$0.36	1,763,152 PTS
19	jl777hodl	$ 662 640	$0.07	10,000,000 JLH *	19	DNotes	$ 601 568	$0.01	94,041,276 NOTE
20	Jinn	$ 654 712	$6.55	100,000 JINN *	20	Zetacoin	$ 582 505	$0.00	161,322,565 ZET
21	Ethercoin	$ 633 951	$0.63	1,000,000 ETC *	21	Vertcoin	$ 530 716	$0.05	10,257,000 VTC
22	XCurrency	$ 626 703	$0.11	5,564,016 XC *	22	Viacoin	$ 522 581	$0.04	12,479,700 VIA
23	ShadowCash	$ 563 999	$0.09	6,448,804 SDC *	23	Infinitecoin	$ 510 870	$0.00	90,595,875,241 IFC

Na serveru CoinMarketCap (15.12.2014) je možné jednotlivé projekty filtrovat podle toho, zda je možná těžba nových mincí. Těžba nových mincí není možná u alternativních řetězců s pevně stanoveným počtem mincí. U alternativních kryptoměn nelze nové mince těžit v případě, že již došlo k jejich naprostému vytěžení.(26)

5.1.3 Směnárny

Největší tři směnárny co do denního objemu zobchodovaných bitcoinů jsou BTC China, BitFinex a Bitstamp. Bitcoiny jsou nejčastěji směňovány za Čínský jüan a USD. Stát s největším počtem směnáren je Čína, kde jich má sídlo 11. Následuje USA s 8 směnárnami, Hongkong se 6 je na stejné příčce jako Brasilie, v Kanadě jich je 5 a v Anglii 3. Zbytek 41 směnáren je roztroušen napříč dalšími evropskými a asijskými státy. (23)(60)



Obrázek č. 5 Poměr množství zobchodovaných bitcoinů. Zdroj: (22)

Poměr množství zobchodovaných bitcoinů podle směnárny a podle měny, ve které směna proběhla. Data za posledních 30 dní. (15.12.2014)

Tabulka č. 4 Nejaktivnější směnárny za posledních 30 dní. Zdroj: (59)

Název směnárny	Země	Zobchodovaných bitcoinů	Hlavní obchodní pár	Transakční poplatek	Počet měn	Nejvýznamější obchodní páry
BTC China	Čína	+- 2 008 000 BTC	BTC/CNY	0, bid ask spread	3	BTC/CNY, LTC/CNY, LTC/BTC
Bitfinex	Hong Kong	+- 700 000 BTC	BTC/USD	0 - 0,20 %	6	BTC/USD, DRK/BTC, LTC/USD
Bitstamp	Anglie	+- 400 000 BTC	BTC/USD	0 % - 0,50 %	1	BTC/USD
BTC-E	Bulharsko	+- 200 000 BTC	BTC/USD, BTC/RUB	0,2 %	20	BTC/USD,LTC/BTC,LTC/USD
Cryptsy	USA	+- 40 000 BTC	BTC/USD	0,25 %	421	DRK/BTC, DOGE/BTC, LTC/BTC
Bter.com	China	+- 30 000 BTC	BTC/CNY, BTC/USD	0,0 % - 0,2 %	155	BTC/CNY, BTC/DOGE, DRK/BTC

Do této krátké tabulky jsem vybral jako příklad 4 největší směnárny podle počtu zobchodovaného počtu bitcoinů za posledních 30 dní. Jak je vidět, největší směnárny se soustřeďují pouze na jeden až tři kryptoměny, obchodují hlavně s bitcoiny, litecoiny a vyjímečně s darkcoiny. Nevelké množství směnáren se soustřeďuje na široký výběr alternativních kryptoměn, jako příklad můžeme uvést Cryptsy, kde je možno obchodovat s více jak 400 páry. Zdroj: Zpracováno autorem (60)

Z předešlých grafů a statistik je patrné, že zdaleka nejvíce likvidní je hlavní kryptoměna bitcoin a možnosti směny alternativních kryptoměn jsou z důvodu malého množství směnáren velmi omezené.

5.1.3.1 Na jakém principu směnárny fungují

Směnárny si za samotný proces směny účtují poplatky, výše poplatků se může významně lišit. Některé směnárny žádné poplatky za směnu neúčtuji a namísto toho zpoplatňují výběr vložených financí, nebo nakoupených kryptoměn. Většina směnáren pouze shromažďuje nabídky a poptávky uživatelů, které následně páruje, v tomto případě vystupuje v roli prostředníka. Naproti tomu existují směnárny, kde naší protistranou v obchodu je přímo směnárna, nikoliv jiný účastník. V případě, kdy je směnárna naší přímou protistranou, transakce bez poplatku nejsou. Při bližším zkoumání je patrné, že využívají stejného obchodního modelu jako směnárny reálných měn. Uživatel při samotné směně měny za kryptoměnu poplatek neplatí, ale nakupuje nebo prodává měnu za aktuální tržní cenu, která je pro nákup a prodej mírně odlišná, určená směnárnou. Uživatel tak platí ve své podstatě za rozdíl („Spread“) mezi nákupní a prodejní cenou, směnárny tak vydělávají na daném kurzovém rozdílu. Tento princip platí rovněž v případě směnáren, které za směnu vyžadují navíc procentuální poplatek. (60)

Jednotlivé směnárny se od sebe neodlišují pouze množstvím obchodovaných instrumentů, nebo výši poplatků. Mnoho z nich přichází s řadou dalších technických vylepšení. Některé platformy kupříkladu umožňují obchodování na Margin, zadávání příkazů typu Stop nebo podporují připojení prostřednictvím profesionálního obchodního software typu Metatrader. Dalším důležitým parametrem je typ a množství platebních metod, které jsou dostupné v případě vložení a výběru finančních prostředků. (60)

Neexistuje jeden centrální obchodní kurz, za který jsou například bitcoiny směňovány s dolary. Každá ze směnáren může mít tento kurz nastaven jinak, vzniklé rozdíly jsou příležitostí pro spekulanty, kteří těchto rozdílů využívají v rámci arbitráží, kdy nakupují měnu na jedné burze levněji a na druhé ji se ziskem ve stejný moment prodávají.

5.1.3.2 Rizika směnáren a příklady jejich selhání

Vzhledem k tomu, že nejsou kryptoměny regulovány, vzniká tak prostor pro různé podvody a krádeže. V případě krádeží se ve většině případů jedná o krádež buď z online peněženky, nebo směnárny. Výjimečně byly evidovány případy ukradení kryptoměny přímo z programové peněženky uložené na pevném disku. V případě směnáren nejednou jejich tvůrci a správci jednoduše veškeré prostředky v držení, kryptoměny a reálné měny na účtech uživatelů, jednoduše zpronevěřili a celý projekt směnárny ukončili. Je nutné podotknout, že

odpovědnost byla vždy přesunuta na neznámého útočníka, který se do systému naboural a prostředky ukradl, nikoliv na správce směnárny. V posledních letech byla takto vykradena a následně zanikla nejedna směnárna. V takovýchto případech obyčejně uživatelé přichází o všechny na platformě uložené prostředky, bez možnosti jakékoliv náhrady. Určení viníka daného podvodu je také velmi obtížné a většina vyšetřování končí konstatováním, že viník nebyl nalezen.

Jako příklad mohu uvést hongkongskou obchodní platformu GBL, ze které se během května až října ztratil majetek více jak 1000 uživatelů za 4,1 milionu dolarů. Směnárna oficiálně ukončila činnost 26. Října a následné šetření police z podvodu nedospělo k žádnému výsledku. (62)

Také v České republice došlo ke krádeži kryptoměn z účtů lidí na směnárně Bitcash.cz. Dne 11. listopadu se neznámý útočník proboural na více jak 4000 účtů a ukradl bitcoiny v hodnotě okolo 2 milionu českých korun. I v tomto případě nebyl skutečný útočník nikdy dopaden a zároveň není jisté, zda to nebyl zinscenovaný podvod jednoho ze správců platformy. (63)

Ovšem největší selhání zabezpečené směnárny vyšlo najevo 28. února 2014, kdy do té doby největší směnárna světa MT.Gox požádala Tokijský soud o ochranu před věřiteli a vyhlásila bankrot. Z platformy a uživatelských účtů zmizelo více než 850 tisíc bitcoinů. Hodnota těchto bitcoinů odpovídala přibližně 474 milionům dolarů. Kromě bitcoinů zmizelo také z účtů 27,3 milionu dolarů. Vina za toto zmizení a krádež byla svalena na chybu v zabezpečení platformy, která dovolovala v některých případech falešný výběr bitcoinů a peněz. Ačkoliv došlo k vyšetřování podvodu, viník nikdy nebyl určen. Jako v případě každého podvodu v rámci bitcoin systému, lidé začali shazovat vinu především na vývojáře platformy. Nejenom, že vývojáři špatně napsaným kódem směnárny útok umožnili, ale také je vysoce pravděpodobné, že se na útoku také podíleli. (65)

5.1.4 Představení nejvýznamějších alternativních kryptoměn

Hlavní oblasti rozdílů mezi jednotlivými alternativními kryptoměnami jsou technické zpracování a marketing. Konkrétní příklady nejen různého technického zpracování, ukážu na reálných příkladech. Nejprve se zaměřím na deset altcoinů s největší tržní kapitalizací, kterým se budu věnovat podrobněji. Poté krátce uvedu řadu projektů, které nejsou tak úspěšné, ale přesto jsou v něčem inovativní.

5.1.4.1 Litecoin (LTC)

Datum spuštění: 7. října 2011
Množství mincí: 84 milionů
Metoda ověření transakcí: Proof of work
Těžební algoritmus: Scrypt
Průměrná doba vytvoření nového bloku: 2.5 minuty

Z hlediska tržní kapitalizace se jedná o největší alternativní kryptoměnu. Od bitcoinu se odlišuje především využitím jiného těžebního algoritmu. Těžba litecoinu nevyžaduje tolik výpočetního výkonu, ale je při ní využito větší množství operační paměti. Nové bloky jsou vytvářeny v průměru každých 2.5 minuty, což má za následek rychlejší konfirmace uskutečněných transakcí. V praxi tak obchodník získá mnohem rychleji potvrzení o uskutečnění platby, než v případě bitcoinu. Pokud bitcoin přirovnáme ke zlatu, tak litecoin bývá označován za stříbro. (65)

Litecoin akceptuje oproti bitcoinu pouze necelá desetina obchodníků, jeho praktické využití je tedy v reálné ekonomice poměrně malé. (66)

5.1.4.2 Dogecoin (DOGE)

Datum spuštění: 8. prosince 2013
Množství mincí: 100 bilionů
Metoda ověření transakcí: Proof of work
Těžební algoritmus: Scrypt s AuxPoW
Průměrná doba vytvoření nového bloku: 1 minuta

Dogecoin vznikl jako vtipná reakce upozorňující na množství nově vznikajících altcoinů bez přidané hodnoty. Maskotem je roztomilý pes rasy Shiba-Inu. Záhy po svém vzniku získal ohromnou podporu internetové komunity na serveru reddit.com, která ho začala masivně propagovat a využívat jako spropitné darované autorům zajímavých příspěvků. Prostřednictvím dogecoinu došlo k veřejné sbírce, která ve výsledku umožnila Jamajskému bobovému týmu zúčastnit se zimní olympiády v Soči. Dogecoin je typickým příkladem toho, jak významnou roli hraje v popularitě měny marketing. (67)

Vrchol popularity dogecoinu nastal v první polovině roku 2014, kdy přišla na trh těžební zařízení ASIC, schopná těžit alternativní kryptoměny s algoritmem Scrypt. Do té doby byla

těžba především výsadou nadšenců, kteří těžili prostřednictvím svých grafických karet. Rázem se tak tento způsob stal neefektivní a část komunity přestala věnovat dogecoinu pozornost.

Jako reakci na upadající zájem, vývojáři změnili protokol a umožnili tak spojení těžby dogecoinu s dalšími altcoiny využívající algoritmu Scrypt.

Dalším specifikem je způsob distribuce, neboli nastavení odměny za těžbu. Oproti litecoinu a bitcoinu, u kterých je odměna za nově vytěžený blok snížena lineárně vždy po určitém množství vytěžených bloků, je v případě dogecoinu odměna snižována nepravidelně podle předem určeného rozvrhu. Způsob distribuce nezůstal od počátku stejný, v průběhu vývoje došlo ze strany vývojářů k jeho změně. Dogecoin nám jasně ukazuje, že dlouhodobé plánování těžby může být velmi riskantní. (67)

5.1.4.3 DarkCoin (DRK)

Datum spuštění: 18. ledna 2014
Množství mincí: 22 milionů
Metoda ověření transakcí: Proof of Work / Proof of Service
Těžební algoritmus: X11
Průměrná doba vytvoření nového bloku: 2.5 minut

Darkcoin je typický řadou inovací. Využívá těžebního algoritmu označovaného jako X11. Jedná se o postupný průběh jedenácti hashovacích funkcí v celkem jedenácti kolech. Jedná se o hashovaní funkce označované jako Blake, Bmw, Groestl, Jh, Keccak, Skein, Luffa, Cubehash, Davite, Simd a Echo. V praxi má využití daného algoritmu dopady na efektivnost těžby za pomoci CPU a GPU, dále pak na spotřebu elektřiny a hlavně zamezuje možnosti těžby prostřednictvím ASIC zařízení. Ve výsledku dochází k situaci, kdy nejefektivnějším způsobem těžby darkcoinu je využití CPU, GPU a to jak z hlediska výkonu tak nákladů na elektrický proud. Tento stav ale nebude trvat navždy. Do několika let se dá očekávat, že dojde k vývoji nového druhu ASIC, který bude schopen algoritmus X11 těžit. (68, 69)

Darksend je název implementace služby umožňující zamlžení původu transakcí, čímž je dosaženo většího množství anonymity. Princip tkví v automatickém zasílání mincí napříč sítí tzv. master uzlům („Master Nodes“), které přijaté množství „zamíchají“ a vrátí zpět na nově vytvořené adresy uživatelům. Princip „zamíchání“ tkví ve skombinování určitého množství přijatých mincí od uživatelů a následném vytvoření jedné transakce s několika výstupy. Velikost přijatého množství mincí od všech uživatelů musí být stejná, protože pouze pak nelze transakce zpětně vysledovat. (69)

Darksend využívá master uzlů, speciálních serverů, které jsou spravované uživateli. Uživatelé jsou motivováni k provozu těchto serverů tím, že s každým nově vytěženým blokem vzniká šance na získání 20% z počtu nových mincí. Tuto mechaniku označují vývojáři darkcoinu termínem důkaz o službě (Proof of Service). (69)

Za pomoci master uzlů lze také téměř okamžitě ověřit pravost transakce. Tato technologie se nazývá InstantX. (69)

DarkCoin se stal poměrně rychle jednou z nejvíce obchodovatelných alternativních kryptoměn. Dokonce i některá ilegální tržiště na temné síti, začínají využívat darkcoin jako hlavní prostředek směny. (70)

5.1.4.4 PeerCoin (PPC)

Datum spuštění: 12. srpna 2012
Množství mincí: Neomezené
Metoda ověření transakcí: Proof of work + Proof of stake
Těžební algoritmus: SHA-256
Průměrná doba vytvoření nového bloku: 10 minut

Peercoin je první alternativní kryptoměna , která začala využívat kombinace metod Proof of work a Proof of stake. Nemá stanovený maximální počet vytvořených mincí, namísto toho je systém nastaven tak, aby docházelo zhruba k jednoprocentní roční inflaci. (71)
Každá transakce je zatížena poplatkem, který je aktuálně stanoven na 0.01 PPC. Namísto toho aby mince z poplatku získal těžař, jsou dané mince zničené. Tento mechanismus působí deflačně. Odměna za těžbu je přímo svázána s aktuální náročností těžby. V principu tak s větším počtem těžařů dochází, získáme menší množství mincí za vytěžený blok. Kromě těžby, lze nové mince získat úročením mincí stávajících. (72)
Metoda Proof of Stake byla použita proto, že nabízí vyšší ochranu proti možnému ovládnutí sítě. Jedná se o útok 51% ("51% Attack"), kdy organizovaná skupina těžařů dosáhne nadpolovičního těžebního výkonu celé sítě, což jim umožní dvojí utrácení mincí. (73)

5.1.4.5 BitcoinDark (BTCD)

Datum spuštění: 9. července 2014
Množství mincí: 1.6 milionu pomocí PoW, 22 milionů celkem
Metoda ověření transakcí: Proof of Work + Proof of Stake
Těžební algoritmus: SHA-256
Průměrná doba vytvoření nového bloku: 1 minuta

Bitcoindark se profiluje jako komunitní projekt, jehož cílem je vytvoření alternativní kryptoměny, která bude podporovat přímé obchodování na bázi klient-klient, směnu aktiv, sportovního sázení a řadu dalších. V jádru vývojáři využili prvky z kryptoměny NXT, což umožnilo přidání zmíněných funkcionalit. Dalším vylepšením je také technologie Teleport, díky které je zaručena vyšší anonymita transakcí. (74)

Před uvedením projektu pro veřejnost vývojáři vytěžili 24 tisíc mincí, jejichž prodejem má dojít k získání dostatečného kapitálu k dalšímu rozvoji. Následuje fáze těžby, v rámci které dojde k vytěžení dalších 1.6 milionu mincí. Poté systém přejde na metodu Proof of Stake a bude docházet k 5% roční inflaci. (74)

5.1.4.6 Monero (XMR)

Datum spuštění: 18. dubna 2014
Množství mincí: 18.4 milionu
Metoda ověření transakcí: Proof of Work
Těžební algoritmus: CryptoNight
Průměrná doba vytvoření nového bloku: 1 minuta

Základem je technologie cryptoNote, která umožňuje vytvářet kryptoměny, jejichž transakce budou zcela anonymní. Technologie cryptoNote není kompatibilní s bitcoinovým protokolem a proto altcoiny vytvořené na tomto základě nemůžeme označovat za větve bitcoinu. (75)

CryptoNote využívá řada alternativních kryptoměn, mezi které patří například bytecoin nebo aeon. Proto nás nemůže překvapit, že monero z části přebírá design od bytecoinu. (75)

Specifické charakteristiky monera jsou nevysledovatelné platby, zcela anonymní transakce a resistence blockchainu proti analýzám historie transakcí. (75)

Použitý těžební algoritmus je cryptoNight, který byl speciálně navržen tak, aby bylo dosaženo nejefektivnější způsobu těžby prostřednictvím CPU. (76)

Z hlediska marketingu si můžeme povšimnout celkem nekvalitního zpracování webových stránek, které obsahují pouze strohé informace o měně a jako hlavní údaj prezentují specifikace těžby. (77)

5.1.4.7 YbCoin (YBC)

Datum spuštění: 29. června 2013
Množství mincí: 3 miliony
Metoda ověření transakcí: Proof of Stake
Těžební algoritmus:
Průměrná doba vytvoření nového bloku: 2 minuty

YbCoin je typickým příkladem alternativní kryptoměny, jejíž inovace je založena pouze na marketingu. Podle oficiálních stránek se jedná o revoluční altcoin cílící na čínské uživatele. Dále se můžeme dočíst, že se jedná o „*měnu založenou na bázi bitcoinu a dalších digitálních měn, které mají výborné atributy.*“ (78)

V podstatě z oficiálních stránek, které jsou z poloviny v čínštině, nemáme šanci zjistit bližší informace o případných technických inovacích. (79)

Pokud se pokusíme o vyhledání dalších zdrojů informací o ybcoinu, narazíme na řadu informačních kanálů, kde je funkcionalita tohoto altcoinu popsána s výraznými rozdíly. Jakoby se jednalo o několik různých projektů sdílející pouze název a logo. (80)

5.1.4.8 FeatherCoin (FTC)

Datum spuštění: 16. dubna 2013
Množství mincí: 336 milionů
Metoda ověření transakcí: Proof of Work
Těžební algoritmus: NeoScrypt
Průměrná doba vytvoření nového bloku: 1 minuta

Tento altcoin vznikl naklonováním litecoinu. Jednou z úprav bylo zvýšení maximálního množství vytěžitelných mincí na čtyřnásobek. Od svého vzniku ale feathercoin prošel zajímavým vývojem. Stávající těžební algoritmus je NeoScrypt. K změně těžebního algoritmu ze Scryptu na Neoscrypt došlo proto, aby se měna stala zajímavější pro CPU a GPU těžaře. (81)

V roce 2013, bylo provedeno mnoho 51% útoků na blockchain v jehož důsledku byly smazány realizované transakce za mnoho dní. Jako reakce na útoky byl zaveden pokročilý systém CheckPointů („Advanced CheckPointing“). (81)

5.1.4.9 ByteCoin (BTE)

Datum spuštění: červenec 2012
Množství mincí: 184.46 miliard
Metoda ověření transakcí: Proof of Work
Těžební algoritmus: CryptoNight
Průměrná doba vytvoření nového bloku: 2 minuty

Jedná se o první alternativní kryptoměnu založenou na technologii cryptonote. Oproti moneru je průměrná doba vytvoření nového bloku dvojnásobná.(83)
Zajímavostí je, že sdílí jméno s úplně jinou kryptoměnou, která se snaží být přímou kopií bitecoinu. (82)
Další alternativní kryptoměny využívající technologie CryptoNote jsou například Aeon (AEON), Boolberry (BBR), DashCoin (DSH), Dosh (DOSH), DarkNote (XDN). (84)

5.1.4.10 PrimeCoin (XPM)

Datum spuštění: 7. červenece 2013
Množství mincí: Bez limitu
Metoda ověření transakcí: Proof of Work
Těžební algoritmus: Cunninghamové řetězce (Řetězce prvočísel)
Průměrná doba vytvoření nového bloku: 1 minuta

Jeden z argumentů proti kryptoměnám může být problém energetické náročnosti. Výpočetní výkon potřebný pro správný chod bitcoinové sítě je ohromný, s čímž také souvisí podstatná energetická stopa. Přitom veškerý výkon je využit pouze pro výpočet hashe.

Této nehospodárnosti si všichni tvůrci primecoinu, kteří přišli s myšlenkou, že by se výkon sítě mohl využít pro dva účely. Chod sítě a zároveň pro hledání řešení nějakého vědeckého problému. (85)
Podstata primecoinu tkví v hledání řetězců prvočísel tzv. Cunnighamové a bi-twin řetězce. V průběhu došlo k překonání několika světových rekordů, dne 16.5.2014 došlo například k nalezení první 14 místného Cunninghamova řetězce. (85)
Podobné kryptoměnou je například Curecoin(CURE), těžbou kterého můžeme pomoci se simulací interakce proteinů. A nebo Gridcoin(GRC) využívající výpočetního výkonu v řadě vědeckých oborů. (86)

5.1.4.11 Quark (QRK)

Datum spuštění: 21. červenece 2013
Množství mincí: Bez limitu
Metoda ověření transakcí: Proof of Work
Těžební algoritmus: Quark
Průměrná doba vytvoření nového bloku: 0.5 minuty

Tento altcoin využívá specifického těžebního algoritmu Quark, který se skládá z 9 kol 6 hashovacích funkcí. Algoritmus byl zvolen tak, aby těžba měny byla nejefektivnější za pomocí CPU a neumožňovala těžbu prostřednictvím zařízení ASIC. (87)
Quark byl terčem kritiky hlavně z důvodu distribuce velkého množství mincí před zpřístupněním altcoinu širší veřejnosti. (88)

5.1.4.12 ReddCoin (RDD)

Datum spuštění: 26. ledna 2014
Množství mincí: 27,5 miliard
Metoda ověření transakcí: Proof of Stake Velocity
Těžební algoritmus: Quark
Průměrná doba vytvoření nového bloku: 1 minuta

Reddcoin je označován jako společenská měnu („Social Currency“), protože míří primárně na uživatele a systémy sociálních sítí, kde je potenciál jejího využití v mikrotransakčních platbách jako forma spropitného za přidání zajímavého obsahu. (89)
Jako metodu ověření transakcí využívá upravenou verzi Proof of Stake, která motivuje uživatele k většímu utrácení a tím oběhu mincí.

5.1.4.13 VertCoin (VTC)

Datum spuštění: 10. ledna 2014
Množství mincí: 84 milionů
Metoda ověření transakcí: Proof of Work
Těžební algoritmus: Scrypt-N
Průměrná doba vytvoření nového bloku: 2,5 minut

Vývojáři vertcoinu vidí největší hrozbu kryptoměn v centralizaci většiny těžebního výkonu do rukou několika málo společností, které vyrábí těžební zařízení typu ASIC.
Aby se zabránilo možností těžby zařízeními ASIC, využívá upravenou verzi těžebního algoritmu Scrypt-N. (90)
Další zajímavou technologickou inovací je skrytí adres, díky kterému je zajištěna vyšší anonymita transakcí.

5.1.5 Příklady dalších alternativních kryptoměn

Při sestavování následujícího vzorku alternativních kryptoměn, jsem čerpal ze stránek směnárny Cryptsy.com. Všechny dále zmíněné altcoiny je možné prostřednictvím cryptsy směnit za bitcoiny. Nemělo by se tedy jednat o projekty neaktivní. Zdroj hodnot tržní kapitalizace je web Coinmarketcap ze dne 9/12/2014. (18) (60)

Tabulka č. 5 Tabulka dalších altcoinů výraznou technickou inovací. Zdroj: (Autor)

Tržní kapitalizace	Název kryptoměny	Charakteristické vlastnosti
$2,000,000	BlackCoin	Smart kontrakty, decentralizovaná aukce, pěkný design webu
$525,000	InfiniteCoin	Obrovská odměna za vytěžený blok
$333,000	MaxCoin	Anti ASIC
$190,000	DigiByte	Náročnost těžby podle DigiShield, Kombinovaný těžební algoritmus, maskot Digiman
$180,000	DigitalCoin	Kombinovaný těžební algoritmus (SHA256, Scrypt, X11)
$130,000	Hyperstake	Experimentální měna, roční uročení mincí 750%
$120,000	Diamond	Anti ASIC, možnost vytěžit superblok (Několikanásobná odměna)
$120,000	Copperlark	Těžební algoritmus SHA3
$120,000	BoostCoin	Těžební algoritmus x13
$65,000	FlutterCoin	Využití metody Proof of Transaction
$50,000	MyriadCoin	Kombinovaný těžební algoritmus
$40,000	Cinni	Integrace sociálních sítí
$33,000	LuckyCoin	Možnost vytěžit superblok (Několikanásobná odměna)
$30,000	EarthCoin	Výše odměny za těžbu stanovena podle oběhu země kolem slunce
$7,000	Guerillacoin	Metoda ověření transakcí Proof of Strenght

Tabulka č. 6 Další alternativní kryptoměny typické výrazným brandigem. Zdroj: (Autor)

Tržní kapitalizace	*Název kryptoměny*	*Charakteristické vlastnosti*
$1,225,000	Hobonickels	Charita, motiv uměleckých mincí
$700,000	IXCoin	Web velmi strohý, název není unikátní, první klon bitcoinu.
$500,000	Megacoin	Web v mnoha jazycích, propagační videa, silná podpora komunity
$400,000	CannabisCoin	Mince slouží k nákupu marihuany
$260,000	GoldCoin	Marketingové přirovnání ke zlatu
$250,000	Devcoin	Podpora a financování programátorů a umělců
$130,000	GameleagueCoin	Měna do online farmářské hry
$101,000	NautilusCoin	Stabilizační fond, který nákupy a prodeji reguluje cenu mincí
$100,000	Noblecoin	Zaměření se na vzdělání, filantropii, transparenci
$70,000	Navajo	Marketing založen na šifře z 2. světové války
$70,000	Deutsche eMark	Zaměřeno na německé občany
$70,000	CheckCoin	Propojeno s aktuální polohou, odměny za objevení nových míst, podobné jako geocaching
$48,000	Einsteinium	Cílem je financování vědeckého výzkumu
$37,000	Electronic Gulden	Zaměřeno na holandské občany
$35,000	Mazacoin	Zameřeno na americké indiány
$30,000	Munne	Snaha o vytvoření vizuálně atraktivního altcoinu
$30,000	CryptoBuk	Zaměřeno na kryptonadšence a pracovníky
$25,000	Murraycoin	Název altcoinu podle známého herce, charita
$11,000	Minerals	Inspirováno počítačovou hrou Starcraft, podpora e-sportu
$8,000	CatCoin	Využití kočičího motivu

5.1.6 Několik příkladů alternativních řetězců

5.1.6.1 Ripple (XRP)

Datum spuštění: 26. září 2013
Celková nabídka mincí: 100 miliard

Ripple je platební protokol umožňující provádět platby okamžitě a v jakékoliv měně. Vytvořila jej společnost Ripple Labs Inc., která se zároveň stará o jeho další vývoj. Stejně jako v případě bitcoinu, i systém ripple využívá pro svůj chod veřejnou databázi podobnou blockchainu. Na provozu systému se podílí autory určení uživatelé, kteří provozují uzly. Konkurenční kryptořetězec pracující na stejném principu je Stellar. (91)

V systému je využito mincí, které jsou označeny názvem Ripple Credity (XRP). Maximální počet mincí je pevně stanoven, tím pádem se jedná o systém deflační. Vytvořené peníze jsou vlastněny autorskou společností, která je dále rozděluje mezi vývojáře, uživatele a obchodníky. Ripple Labs Inc. Rozděluje peníze tak, aby se co nejvíce zvyšovalo obecné povědomí o tomto systému. O další distribuci se pak starají nižší články systému – již zmiňovaní obchodníci nebo třeba přímo vývojáři, kteří tyto mince rozdávají uživatelům nejenom v rámci různých propagačních akcí. Rozdělení měny tak není založeno na těžbě jako třeba u Bitcoinu, ale podle „zásluh“. (91)

Jednou z výhod protokolu ripple je možnost zaúčtování běžně používaných měn, jako je např. EUR nebo USD. Tento proces je však zároveň i rizikový z důvodu možného nesplacení závazků. Další velkou výhodou je rychlé vypořádávání, a to v rozmezí 2 – 20 sekund. To tomuto systému zajišťuje potenciál nahradit současné vypořádání, které využívá jako mezičlánek různé platební instituce. Celý tento platební protokol zaujal mimo jiné společnost Google Venture Capital, která do něj posléze investovala. (92)

5.1.6.2 MaidSafeCoin (MAID)

Datum spuštění: duben 2014

Cílem sítě MaidSafe vytvořené společností SAFE network je vytvoření decentralizované internetové platformy sloužící k ukládání dat. Celý systém MaidSafe se skládá ze dvou hlavních částí – ze sítě a uživatelských (klientských) aplikací. Na síti se v současné době aktivně pracuje a cílem je její kompletní spuštění na konci roku 2014. (93)

Uživatelé se dělí na 2 základní skupiny, a to na (v anglické terminologii) „farmers“ a na „builders“. „Farmers“ jsou běžní koncoví uživatelé připojení do sítě, kteří mohou sdílet volné místo na svých lokálních discích, na které jsou pak ukládána data dalších uživatelů. Za využívání jejich volného místa jsou odměňování mincemi maidsafecoin. Druhá skupina, vývojáři aplikací nazývaní „builders“, vydělávají mince na základě toho, jak často jsou jejich aplikace používány. Poslední skupinou jsou lidé podílející se na tvorbě samotného systému, ti mohou maidsafecoin získat například opravou chyb nebo tvorbou nových funkcí. (93)

Volný úložný prostor získaný od „farmers“ je naopak analogicky možné získat výměnou za mince maidsafecoin. Mince je možné buď koupit (nemáte-li je vydělané), nebo vytěžit metodou Proof of Resources, která je založená na sdílení volného úložného prostoru. (93)

5.1.6.3 CounterParty (XCP)

Datum spuštění: leden 2014

CounterParty je protokol pro vytváření a používání decentralizovaných finančních nástrojů, který používá bitcoiny jako transportní vrstvu. Hlavním cílem je umožnit podnikatelům, vývojářům, umělcům a dalším vybudovat novou, produktivní ekonomiku. (94) (95)

CounterParty poskytuje uživatelům první funkční decentralizovanou směnárnu na světě. V současné době tento protokol podporuje a realizuje tvorbu aktiv, zároveň vydává známky těchto aktiv, dále vyplácí dividendy, sázky atd. (96)

Základní měnou tohoto protokolu je netěžená XCP. Celkem bylo vydáno 2,6 milionu jednotek této měny, a to v krátkém období během ledna 2014. (94)

Jak již bylo zmíněno výše, tento protokol je založen na softwaru bitcoinu. V průběhu ledna až února 2014 bylo „spáleno“ 2130 bitcoinů, které byly nahrazeny právě měnou XCP. Od této úpravy bylo pod hlavičkou CounterParty provedeno již 77 000 transakcí v Bitcoin síti. (94)

5.2 Porovnání alternativních kryptoměn

Při průzkumu ekosystému alternativních kryptoměn jsem narazil na mnoho set různých projektů a i tak se jedná pouze o zlomek z jejich celkového množství. Podrobné porovnání více jak několika desítek alternativních kryptoměn by znamenalo investici nejenom mnoha set hodin, ale také by zabrala většinu této práce. Vzhledem k tomu, že hlavním cílem této práce není podrobný průzkum trhu s altcoiny, ale analýza jejich těžby, jsem byl nucen omezit množství zkoumaných kryptoměn na několik desítek.

Abych obsáhl celou škálu alternativních kryptoměn od těch nejúspěšnějších po altcoiny téměř zkrachované, tak jsem musel podrobněji prozkoumat přibližně stovku různých projektů.

Porovnávaný vzorek se skládá z deseti těžitelných projektů s největší tržní kapitalizací podle CoinMarketCap a dále pak náhodného výběru jednoho sta dalších projektů, jejíž mince se obchodují na směnárně Cryptsy za Bitcoiny. Řadu ze zkoumaných alternativních kryptoměn jsem představil v předešlé sekci.

Ke každé zvolené alternativní kryptoměně jsem vyhledal oficiální stránku a ohlášení o vzniku z fóra bitcointalk. Nejprve jsem všechny zmíněné zdroje podrobně prozkoumal a následně porovnal informace, které tyto zdroje obsahovaly a jakým způsobem je prezentovaly.

Ekosystém alternativních kryptoměn je tak rozmanitý, že jsem zcela jistě opomenul mnohé zajímavé altcoiny, které budou v následujících letech velmi úspěšné. I přesto, že jsem nahlédnul pod pokličku více jak stovky projektů, nemusí být výsledky srovnání platné za všech okolností.

Typově se rozdíly drtivé většiny alternativních kryptoměn dají rozlišit na rozdíly v technickém zpracování a rozdíly v brandingu.

5.2.1 Typické rozdíly v technickém zpracování

Po bližším průzkumu nejenom deseti alternativních kryptoměn s největší tržní kapitalizací a následném srovnání s bitcoinem můžu s určitostí prohlásit, že každý z altcoinů má technické zpracování jiné. Některé se odlišují v nastavení základních parametrů, jiné zase například v použitém težebním algoritmu.

Rozdíly v technickém zpracování se dají rozdělit do několika skupin.

5.2.1.1 Různé nastavení parametrů PoW a PoS

Jeden z největších rozdílů je patrný v druhu použité metody k ověření transakcí. V minulosti byla nejčastěji využívaná metoda Proof of Work. Novější projekty využívají spíše kombinace metod Proof of Work a Proof of Stake. Můžeme se ale setkat i s altcoiny, které využívají metody další.

Parametry PoW, ve kterých se nejčastěji altcoiny liší:

Maximální počet mincí – S vysokou cenou bitcoinu je pro uživatele běžný platební styk nepraktický v tom, že je při něm třeba neustále kontrolovat správný počet desetinných míst. Tento problém je jedním z důvodů, proč alternativní měny raději přistupují k vyššímu počtu maximálních mincí.

Rychlost vytváření nového bloku – Tento parametr určuje, s jakou průměrnou rychlostí jsou transakce ověřeny a označeny za platné. Bitcoin v průměru vytváří nové bloky každých deset minut. Téměř všechny alternativní kryptoměny nové bloky vytváří rychleji a umožňují tak svižnější zpracování plateb. Nové altcoiny typicky vytváří nové bloky v časovém intervalu od půl do tří minut.

Výše těžební odměny – Mnoho alternativních kryptoměn se snaží nové těžaře motivovat ze začátku zvýšenou odměnou za vytěžené nové bloky. Některé kryptoměny dokonce umožňují těžbu superbloků. Superbloky jsou bloky, které když vytěžíme tak získáme několikanásobně větší odměnu. Na tyto bloky zpravidla můžeme narazit náhodně. Těžbu superbloků umožňuje například LuckyCoin.

Způsob kalkulace náročnosti těžby – Změnou kalkulace náročnosti těžby se snaží vývojáři nastavit systém tak, aby případná těžba prostřednictvím multipoolu, nerozhodila celý systém. Blíže se tomuto tématu budu věnovat v analýze těžby.

Altcoin využívající PoS, mění hlavně:

Rychlost úročení nových mincí – Například u altcoinu HyperStake jsou mince úročeny 750% ročně. Jedná se o experimentální altcoin, jehož tvůrci chtěli zkusit, co takové nastavení udělá.

Výše zmíněné parametry často ovlivňují především měnovou bázi.

5.2.1.2 Měnová báze

Existují tři základní typy nastavení měnové báze:

- Budoucí měnová báze je fixní, počet vytvořených mincí je předem jasně stanovený. Rychlost těžby nových mincí závisí na nastavení systému. Po určitém čase jsou všechny mince dané kryptoměny vytěženy a je tak dosaženo předem definovaného maximální množství mincí. Tato metoda je inflační, ale ve chvíli dosažení maximálního počtu mincí, se systém začne potýkat s deflací. Toto nastavení pravidel měnové báze je využito například v případě bitcoinu a litecoinu. (97)

- Maximální měnová báze není stanovená. Proces těžby a generování nových mincí je nekonečný, ale se zvyšujícím se množstvím nově vytvořených mincí, roste zároveň i náročnost těžby. Kryptoměna využívající tohoto přístupu k měnové bázi se dá charakterizovat jako inflační. Zmíněnou variantu neomezené měnové báze využívá kryptoměna Peercoin. Pravidla těžby této měny jsou nastavena tak, aby se inflace rovnala přibližně 5% ročně. (97)
- Některé alternativní projekty využívají ještě třetího způsobu nastavení měnové báze. V tomto případě jsou všechny plánované mince vytvořeny okamžitě při vzniku a další mince tak těžit nelze. Tento systém je z podstaty deflační. Příkladem je systém Ripple, v rámci které bylo na počátku autory vytvořeno 100 miliard mincí, z nichž bylo 80% darováno společnosti RippleLabs, která centrálně spravuje chod systému. Kryptoměna Ripple není deflační a ani inflační, je to dáno velice specifickým způsobem fungování. (91)

5.2.1.3 Podle typu využitého těžebního algoritmu

Typ použitého těžebního algoritmu rozděluje alternativní kryptoměny do dvou skupin. Na altcoiny, které využívají SHA 256 nebo Scrypt a ty ostatní. Toto rozdělení vzniklo jako reakce na těžbu zařízeními ASIC.

Těžební algoritmy typu X11, X13, Quark a dalších se nedají efektivně těžit zařízením ASIC. Altcony jsou proto tzv. resistentní proti těžbě ASICem.

5.2.1.4 Anonymita

Ztížení možnosti dohledání transakcí je velké téma. Mnoho vývojářů vidí prostor pro vylepšení bitcoinového protokolu právě ve zvýšení anonymity všech transakcí. U řady nových altcoinů je vidět snaha o implementaci různých technologií, které by účastníky transakcí účinně skryly. Tato technická inovace je možná vidět u DarkCoinu a Monera. (77,69)

5.2.1.5 Další funkcionality

Některé alternativní kryptoměny jsou typické v tom, že u nich došlo k implementaci nějaké další nové funkcionality. Cinni například umožňuje zasílání šifrovaných zpráv. (98)

Dalším příkladem je viacoin, který umožňuje pomocí implementace protokolu ClearingHouse, obchodování na bázi klient-klient. (99)

5.2.2 Typické brandingové rozdíly

Při vzájemném porovnání některých altcoinů, jsem v technickém zpracování nedokázal najít žádný skutečně významný rozdíl. I přesto se však tyto altcoiny výrazně odlišovaly. Rozdíl byl patrný nejen ve kvalitě zpracování prezentačních materiálů, ale také například v širších možnostech využití mincí.

Řada alternativních kryptoměn se odlišuje od konkurence nejenom technickým zpracováním, ale především brandigem a jeho kvalitou. Obsahem brandingu je vše, co vede k vybudování větší popularity altcoinu. Jako příklad mohu zmínit grafické zpracování webových stránek a loga, stanovení konkrétní cílové skupiny uživatelů, způsob propagace, podpora komunity a mnoho dalších.

5.2.2.1 Název a logo

První setkání s každou alternativní kryptoměnou probíhá přečtením jeho názvu, případně pohledem na logo. Stejně jako v případě značek různých společností, typu Coca-Cola, nebo Nike, hraje název a logo poměrně velkou roli v utvoření prvotním dojmu. Některé loga a názvy nás mohou okamžitě zaujmout, jiné zase zmást nebo kryptoměnu od počátku rovnou zesměšnit, což ale nemusí být vždy na škodu.

Typickým příkladem je úspešná alternativní kryptoměna dogecoin, která má v logu psa rasy Shiba inu, nebo cannabiscoin. U druhého okamžitě jak po přečtení názvu, tak po pohledu na logo, okamžitě tušíme, jaké bude ústřední téma altcoinu. (67, 100)

Setkal jsem se také s altcoiny, jejíž jméno a logo bylo velmi nevýrazné a nic neříkající. Podle mého názoru se jedná například o zetacoin, ixcoin nebo munne. (101,102,103)

Zároveň bylo zajímavé zjistit, že mnohé altcoiny nemají název unikátní. Například když jsem se snažil nalézt další informace o ixcoinu, tak jsem zjistil, že existují minimálně dvě různé alternativní kryptoměny se stejným jménem ale rozdílným logem. Po krátkém bližším zkoumání, bylo hned patrné, že se neliší jen v logu, ale také v mnohých technických parametrech. (103,104)

5.2.2.2 Zaměřením na učitý segment uživatelů

Bitcoin je měna globální, která cílí prakticky na všechny uživatele. Mnohé altcoiny nechtějí konkurovat bitcoinu na globální úrovni a proto se spíše zaměřují na určitý typ uživatelů.

Některé cílí na potenciální uživatele pouze z jednoho konkrétního státu, jiné zase například na uživatele konkrétních sociálních sítí.

Jako příklad mohu uvést dogecoin, který se profiluje jako měna komunitní, zábavná a cílí hlavně na uživatele sociálních sítí typu Reddit. Altcoiny jako electronic gulden nebo mazacoin, se zaměřují na občany konkrétních států, případně etnik. (67)

Zaměření pak určuje hlavně grafickou podobu materiálů, využití různých motivů a další.

5.2.2.3 Způsob, rozsah a kvalita prezentace

Existují tisíce alternativních kryptoměn, o mnohých ale nikdy neuslyšíme a ani se snimi nesetkáme. Pokud se ale o těžbu a problematiku altcoinů budeme zajímat a informace aktivně vyhledávat, narazíme na velké rozdíly v tom, jakým způsobem a kde jsou základní charakteristiky jednotlivých projektů prezentovány.

Podrobnější informace o konkrétním altcoinu získáme zadáním jeho názvu do jednoho z internetových vyhledávačů. Mezi prvními výsledky se ve většině případů nachází oficiální propagační web a odkaz na fórum bitcointalk. Dalším častým místem ohlášení nového projektu je také web cryptocointalk. (105,106)

Některé altcoiny mají vytvořenou vlastní stránku na wikipedii a můžeme je také najít v databázi na informačních webech typu crypto-coins-table.com.(107)

Srovnáním jsem došel k názoru, že nejpatrnější rozdíl v případě místa prezentace, je v existenci prezentačního webu, případně pak wikipedie. Například altcoin bitmark samostatný prezentační web nemá. (108)

Mezi jednotlivými altcoiny je velmi výrazný rozdíl v kvalitě prezentačních materiálů. Setkal jsem se s prezentací, kde byla pouze obecně popsána technická specifika, ale také s altcoiny, jejíž princip, vlastnosti a zaměření bylo prezentováno formou krátkého videa nebo infografiky.

Velmi dobře zpracované materiály nabízí například megacoin, na jehož webu můžeme nalézt vysvětlující infografiku a různá prezentační videa. Oproti tomu offciálni web altcoinu BitCoinDark podává prezentaci jen strohým textem, ale zase má technickou inovaci zpracovanou ve vědecké práci („White paper“), kterou můžeme z webu stáhnout. (109)

Různý byl také rozsah podpory a způsob prezentace na sociálních sítích

5.2.2.4 Možnosti směny mincí a jejich využití

Velké rozdíly jsou patrné i v možnostech využití mincí. Množství obchodníků akceptující konkrétní altcoin jako formu platby se velmi liší případ od případu. Stejně tak počet směnáren, které umožňují jejich směnu.

Některé altcoiny se nechtějí stát jen dalším prostředkem směny a snaží se prezentovat trochu jiným směrem. Konkrétním příkladem je již zmíněný reddcoin a jeho využití na sociálních sítích. (89)

5.2.3 Faktory určující úspěšnost a popularitu altcoinů

Zkoumaný vzorek se skládal z altcoinů, jejichž tržní kapitalizace byla různého rozsahu od pár desítek tisíc do milionů dolarů. Což ve své podstatě znamená, že se jednalo o různě úspěšné alternativní kryptoměny, nikoliv o altcoiny bezcenné.

Základní typy rozdílů jsem úspěšně identifikoval, avšak z tohoto zběžného srovnání není možné přesně určit faktory, které významně ovlivňují úspěšnost altcoinů. Než budeme schopni tyto faktory specifikovat, je nutné porozumět tomu, jakým způsobem jednotlivé rozdíly ovlivňují úspěšnost alternativní kryptoměny.

Míra úspěšnosti odpovídá výši tržní kapitalizace, která závisí na aktuálním množství a ceně jednotlivých mincí. Celkové množství mincí ve většině případů neustále roste určitým tempem, což znamená, že tržní kapitalizace v případě nezměněné tržní ceny mincí musí také růst.

Z toho vyplývá, že hlavní vliv na výši tržní kapitalizace má cena, která je určena aktuální uživatelskou nabídkou a poptávkou po mincích.

Nabídka mincí je z převážné části tvořena těžaři, kteří prodejem vytěžených mincí pokrývají těžební náklady. Při vzniku nového altcoinu, který nebyl předem zčásti vývojáři vytěžen, se mince dají získat jediným způsobem, a to těžbou. V tento moment je ale jejich tržní cena rovna nule, což trvá do té doby, než se najde někdo, kdo bude chtít daný altcoin koupit.

Z toho plyne, že se cena alternativních kryptoměn odvíjí hlavně od poptávky. Ta je tvořena uživateli, kteří altcoiny nakupují s určitým očekáváním, nebo za účelem jejich spotřeby. Zásadní otázkou proto je, které vlastnosti alternativních kryptoměn, mají největší vliv na jejich poptávku a proč.

5.2.3.1 Různé pohledy na faktory úspěchu

Na internetu můžeme narazit na celou řadu teorií, které se snaží podmínky úspěchu altcoinů určit. Zmínit mohu například infrastrukturní a inovační teorie, společně s konceptem „nomen est omen“. Úspěšná alternativní kryptoměna musí mít dobrou infrastrukturu, být inovativní a méně náročná na údržbu. Koncept „nomen est omen“ podmiňuje úspěch kryptoměny jejím zajímavým názvem, myšlenkou a pamětihodnou obchodní historií. (110)

Tvůrce litecoinu Charlie Lee vysvětluje příčiny úspěchu jím vytvořené měny na pěti krocích. Nejdřívě je důležité najít ten správný název, nejlépe takový aby vystihoval podstatu altcoinu. Jako příklad uvádí darkcoin, který se zaměřuje na větší anonymitu transakcí nebo zábavný dogecoin. Zadruhé je důležitý kvalitní branding, pomocí kterého dokázali uživatele psychologicky přesvědčit, že je hodnota litecoinu ku bitcoinu stejná, jako stříbro ke zlatu. Třetí podstatný bod je zvolení takového těžebního algoritmu, aby nedocházelo ke vzájemnému konkurování s dalšími altcoiny. Další důležitý parametr úspěšné měny je její férové spuštění, což znamená, že by neměly být žádné mince vytěženy jejich tvůrcem před oficiálním startem. Závěrečným doporučením je také to, že by se alternativní kryptoměny neměly snažit konkurovat bitcoinu. (111)

V dalším článku se můžeme dočíst, že se úspěch kryptoměny odvíjí od pětí věcí: (112)

1. *„Dobrého vývojového týmu a podpory komunity.“*
2. *„Technických vlastností (Počet mincí, férová těžba, rychlost transakcí, atd.)*
3. *„Obchodovatelností a likviditou na hlavních směnárnách.“*
4. *„Širokým přijetím a infrastrukturou. (Rostoucí kolem altcoinových služeb.)“*
5. *„Název altcoinu a jeho identita (Nezapomenutelná obchodní historie a vývoj mince).“*

Oproti tomu jiný článek kriticky poukazuje na to, že většina nových altcoinů se zaměřuje pouze na kryptografické nadšence. Jsou přidávány nové funkcionality, které ale nejsou vůbec podstatné, protože pro obyčejného uživatele nepřináší žádnou přidanou hodnotu. A právě širší adopce více uživatelů, než jen kryptonadšenců, je podmínkou k úspěchu altcoinu. (113)

Jak je patrné, ani v kritériích úspěchu nepanuje napříč ekosystémem kryptoměn naprostá shoda a můžeme se proto setkat s řadou různých vysvětlení.

5.2.3.2 Stanovení faktorů úspěšnosti nových altcoinů

Cílem je stanovit faktory a kritéria, která nám mohou pomoci v odhadu toho, zda má nově vznikající alternativní kryptoměna dostatečný potenciál na to, aby byla v budoucnu úspěšná.

Podle mého názoru je největším faktorem neúspěchu nově vznikajících kryptoměn to, že nenabízí žádné konkrétní využití, což je ve své podstatě spojené nulovou poptávkou po těchto mincích. Základem faktorů úspěšnosti je tedy vše, co má přímý vliv na poptávku po mincích.

A za hlavní faktory úspěchu považuji:

1. Využití nejenom jako prostředek směny – využití například při nějaké činnosti
2. Zaměření se na silnou skupinu uživatelů. – snaha o uspokojení poptávky
3. Dobrá dostupnost a likvidita mincí. – jak složité bude minci nakoupit
4. Kvalita zpracování a různorodost prezentačních materiálů. – vybudování dojmu
5. Zajímavý název a motiv. – branding, vybudování psychologické poptávky

Jak je patrné, tak tyto faktory jsou spíše kvalitativního charakteru, je to dáno tím, že je velmi těžké například kvantifikovat zajímavost názvu a kvalitu loga.

Z těchto faktorů jsem sestavil 5 otázek, jejichž kladné zodpovězení, nám může pomoci určit, zda má nově vznikající altcoin dostatečný potenciál k budoucímu úspěchu.

1. Bude možné nově vzniklé mince využít nejen k nákupu zboží a služeb?
2. Je vývoj nově vznikajícího altcoinu podporován významnou komunitou?
3. Budeme moci mince získat krátce po startu jednoduchým způsobem?
4. Jsou prezentační materiály graficky estetické a zajímavé?
5. Je název kryptoměny dostatečně zajímavý?

6 Těžba kryptoměn

6.1 Úvod do analýzy těžby

Bitcoin podobně jako mnohé další alternativní kryptoměny využívá pro ověření transakcí principů Proof of Work. Proto nejjednodušší cestou jak porozumět těžbě alternativních kryptoměn je skrze těžbu bitcoinu. Nejdetailnější a nejucelenější popis mechaniky těžby bitcoinu zpracoval autor Andreas M. Antonopoulos ve své práci Mastering bitcoin. Při zpracování následující části jsem proto čerpal především z této práce.

6.1.1 Těžba obecně

Těžba je proces, jehož prostřednictvím jsou vytvářeny nové mince, a pomocí kterého dochází k ověření pravosti uskutečněných transakcí. Ověření transakcí je hlavní smysl těžby, vytváření nových mincí slouží pouze jako pobídka uživatelům k obětování výpočetního výkonu v těžbě použitém. Proces se nazývá těžbou, protože podobně jako v případě vzácných kovů, se počet nově vytěžených mincí stále snižuje v závislosti na již vytěženém množství.

Princip těžby tkví ve shromáždění uskutečněných transakcí do tzv. bloků a následném zařazení tohoto nového bloku na konec hlavního řetězce bloků, neboli blockchainu. Napojením bloku na konec řetězce jsou transakce v bloku obsažené konfirmovány a uživatelé tak mohou s nově nabytými mincemi začít volně pracovat.

Vytváření nových bloků je spojeno s řešením složitého matematického problému, jehož podstatu tvoří kryptografický hash algoritmus. Správné řešení tohoto problému se nazývá Proof of Work a v nově vytvořeném bloku plní funkci důkazu o tom, že k vytvoření bloku bylo spotřebováno významné množství výpočetního výkonu. Řešení je pro každý blok jiné a v jeho hledání si těžaři vzájemně konkurují. Za úspěšné nalezení výsledku je těžař odměněn formou nově vytvořených mincí a také sumou transakčních poplatků v nově vytěženém bloku obsažených. Aktuálně je 99.5% příjmu těžařů tvořen nově vytvořenými mincemi. Dá se ale očekávat, že se stále se zmenšující odměnou za nově vytvořené bloky, začnou hrát poplatky větší roli.

Těžbe kryptoměn se věnuje celá řada typů lidí: (114, str. 2)

- Nadšení středoškolští a vysokoškolští studenti, kteří využívají levnou elektřinu a hardware z domova (Platí rodiče.) nebo ve školách.
- Hráči počítačových her, kteří chtějí naplno využít výkon svých počítačů ve chvíli, kdy se hrám aktivně nevěnují.
- Kryptoměnoví nadšenci, kteří ve sklepě sestavují velká těžební zařízení o mnoha grafických kartách.
- Hackeři, kteří prostřednictvím malware a jiných nežádoucích programů, vytváří sítě ovládnutých cizích počítačů, které následně využívají k těžbě kryptoměn.

- Internetové skupiny nadšenců, kteří společně nakupují těžební hardwarové řešení a dělí se o zisk.
- Profesionální společnosti, které získali finance na vývoj nových těžebních stanic a uskutečnění těžebních operací.

Tvorba alternativních kryptoměn nemusí probíhat pouze pomocí metody Proof of Work. Řada altcoinů využívá pro ověření transakcí kombinaci metod, nebo metody zcela unikátní. Termín těžba je typická pro metodu Proof of Work. V případě Proof of Stake jsou mince vytvářeny úročením neboli ražbou.

6.1.1.1 Podrobné vysvětlení procesu těžby na příkladu

Veškeré informace jsou napříč bitcoinovou sítí propagovány prostřednictvím uzlů. Abychom tedy mohli začít nové transakce uspořádávat do bloků, musíme nejprve zprovoznit plného bitcoinového klienta. Bitcoin klient plní roli uzlu, díky kterému jsme schopni přijímat a dále přeposílat nezkonfirmované transakce. Tyto transakce však zatím nejsme schopni organizovat do bloků, k tomu potřebujeme připojit výpočetní jednotku, která bude schopna efektivně řešit hashovací algoritmus. Může se jednat o například o procesor nebo grafickou kartu.

Kromě nezkonfirmovaných transakcí se celou sítí propagují i nově vytvořené bloky. Informace o tom, že byl vytvořen nový blok, má pro nás dva významy. Prvním je, že někdo jiný dokázal vytvořit nový blok dříve než my a druhým, že byl odstartován závod, kdy na jeho konci po deseti minutách dojde k vytvoření bloku dalšího.

Aktivní uzel všechny proběhnuté transakce eviduje v zásobníku, který se nazývá „memory pool“, nebo také „transaction pool“. Ve chvíli kdy bude vytvořen nový blok, automaticky porovnáme všechny shromážděné transakce s transakcemi obsaženými v nově vytvořeném bloku. Transakce, které v bloku nejsou uvedeny, jsou nezkonfirmované a čekají tak na zařazení do bloku nového. Náš uzel následně vytvoří kandidáta na nový blok, který se stane blokem potvrzeným pouze tehdy, pokud nalezneme správné řešení algoritmu Proof of Work.

Kandidát na nový blok se skládá z výběru nezkonfirmovaných transakcí, podle jejich stáří a velikosti. Tedy čím je nezkonfirmovaná transakce starší a obsahuje větší množstvím mincí, tím má vyšší prioritu a šanci na to stát se součástí bloku. Některé transakce mohou obsahovat poplatek za zpracování. V případě zahrnutí takovéto transakce do bloku nám bude daný poplatek při úspěšném vytěžení bloku vyplacen.

První transakce v bloku slouží jako generátor nových mincí a je vytvořena uzlem automaticky. Množství nově vytvořených mincí odpovídá součtu velikosti aktuální odměny za nový blok a případně vyplacených transakčních poplatků.

Posledním krokem ve vytvoření kandidáta na nový blok je sestavení hlavičky bloku. Struktura hlavičky je následující:

Tabulka č. 7 Složení hlavičky bloku. Zdroj: (32)

Velikost	Pole	Popis obsahu pole
4 bity	Verze	Číslo indentifikující verzi protokolu.
32 bitů	Hash předchozího bloku	Odkaz na hash hodnotu předchozího bloku v řetězci bloků.
32 bitů	Merkle Root	Hash hodnota kořene merkle stromu transakcí bloku.
4 bity	Časová známka	Čas vytvoření bloku.
4 bity	Cílová obtížnost	Náročnost bloku určená pomocí Proof of Work
4 bity	Nonce	Hodnota použitá pro sestavení hashe bloku. V základu je nulová.

Pokud je hlavička zcela vyplněná, může začít proces těžby. Úkolem je najít hodnotu nonce s jejíž pomocí bude hash hlavičky bloku menší než cílová obtížnost („Difficulty target“). Dá se najít pouze pomocí náhodného zkoušení různých hodnot, což v praxi může znamenat i triliony pokusů.

Po nalezení správné hodnoty nonce dojde k propagaci námi vytvořeného bloku do zbytku sítě. Ostatní uzly v síti tento blok otestují a přepošlou dál. Ověřuje se například to, zda je opravdu hash hlavička bloku menší než cílová obtížnost. Nové bloky jsou ověřované na každém uzlu zvlášť, což v principu brání snahám o podvádění.

Může se stát, že blok nebude v některém z testovaných parametrů vyhovovat a bude tak odmítnut. Nestane se proto součástí žádného řetězce bloků.

Nové bloky jsou buď rovnou napojeny na hlavní řetězec bloků, blokchain nebo začnou tvořit řetězce nové. Takovéto řetězce v síti vzájemně soupeří o zařazení na konec hlavního řetězce. Vítěz je vybrán nezávisle podle porovnání náročnosti s jakou došlo k jeho vytvoření.

6.1.2 Náročnost těžby

Náročnost („Difficulty“) se udává jako abstraktní číslo, které vyjadřuje, jak těžké je nalézt hash menší než cílová obtížnost.

Průměrná doba za jakou dojde k vytvoření nového bloku je stále stejná, a to bez ohledu na to, kolik výpočetního výkonu máme pro řešení těžebního algoritmu k dispozici. Toho je dosaženo pomocí cílové obtížnosti, která určuje, jaká bude náročnost nalezení správného řešení. Jedná se o proměnlivý parametr, jehož hodnota se často mění v závislosti na celkovém výkonu celé sítě.

Výpočetní výkon se udává jako **hash rate**, tedy kolikrát jsme schopni za jednu vteřinu nalézt řešení konkrétního těžebního algoritmu. Celkové množství spotřebovaného výpočetního výkonu se dá vypočítat jako násobek hash rate a doby, po kterou jsme výsledek hledali.

K periodickému přepočtu cílové obtížnosti dochází na všech uzlech automaticky. To jak často a jak přesně bude k přepočtu docházet, závisí na konkrétním nastavení jednotlivých altcoinů.

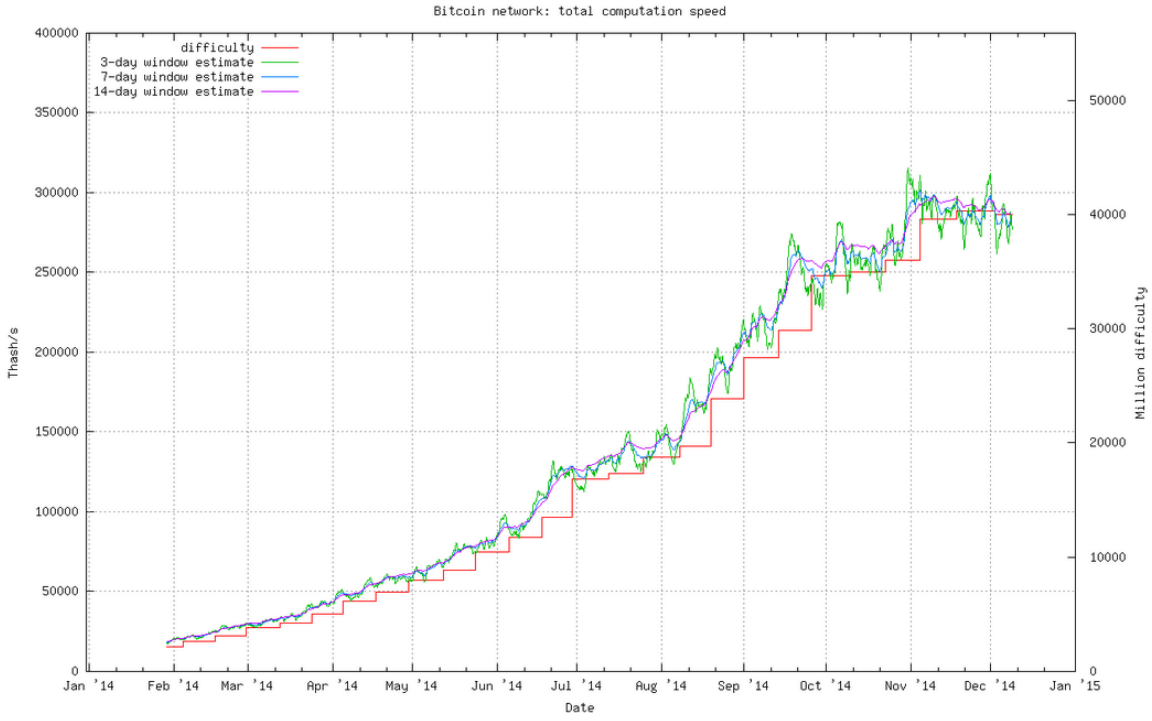
U bitcoinu dochází k přepočtu cílové obtížnosti pokaždé po vytěžení 2016 bloků. Způsob přepočtu vystihuje vzorec:

Cílová obtížnost = původní obtížnost * (Délka těžby posledních 2016 bloků / 20160 minut)

K zvýšení nebo snížení náročnosti dochází podle toho, zda jsou nové bloky vytvářeny rychleji, nebo pomaleji než za stanovenou periodu 10 minut.

Občas může dojít na situaci, kdy se výpočetní výkon celé sítě skokově zvýší. Typickým příkladem je zahájení prodeje nového těžebního zařízení, v tomto případě ASIC.

Aby se zabránilo extrémním změnám náročnosti, je výrazná změna hodnoty cílové obtížnosti u bitcoinu vynásobena nebo vydělena čtyřmi. K plnému promítnutí změny celkového hash rate tak může dojít až po několika dalších přepočtech.



Obrázek č. 6 Vývoj výpočetního výkonu a náročnosti těžby u bitcoinu. Zdroj: (60)

6.1.2.1 Různé způsoby stanovení náročnosti těžby

Hledání nových způsobů jak stanovit náročnost těžby začalo být středem zájmu zhruba na začátku roku 2014. Hodnota řady alternativních kryptoměn vzrostla a v reakci nato začal být populární nový druh těžby prostřednictvím multipoolu. Tento způsob je typický tím, že výpočetní výkon uživatelů alokuje dynamicky do altcoinů tak, aby vždy docházelo k nejvýnosnější těžbě. (115)

Problém nastává ve chvíli, pokud se do tohoto multipoolu shlukne velké množství těžařů. Když má multipool velké množství výpočetního výkonu, a tento výkon začne být využit v těžbě ne příliš známého altcoinu, může dojít k zahlcení systému a výraznému skokovému

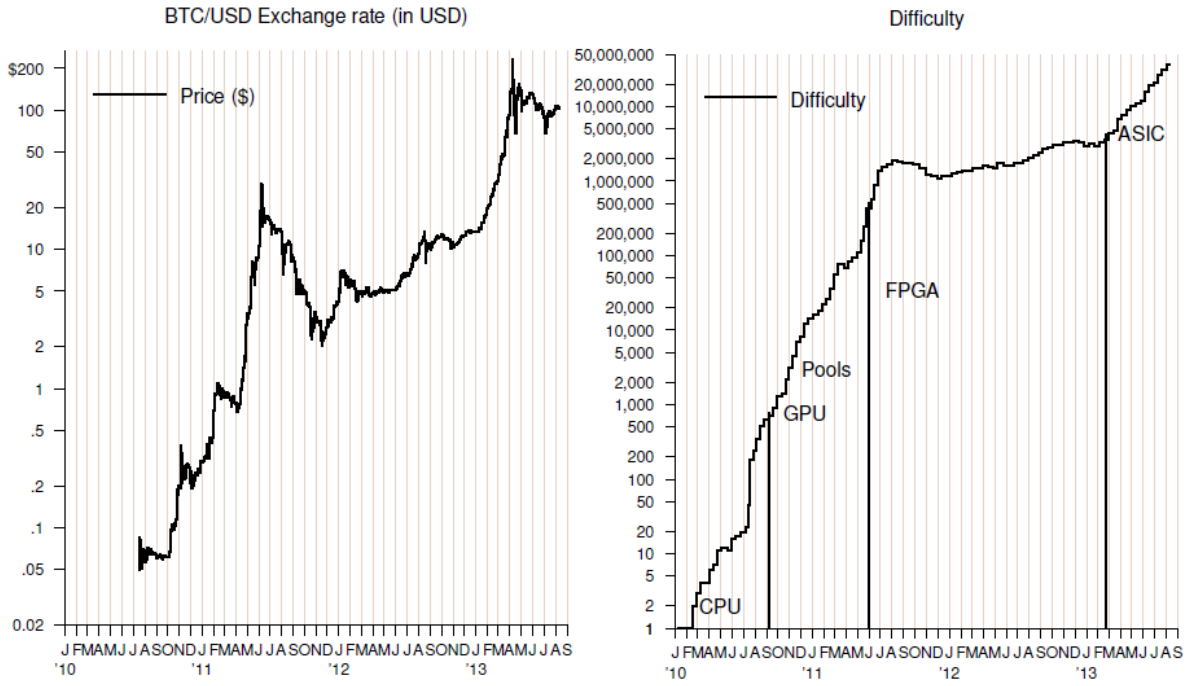
nárůstu náročnosti těžby a poklesu rychlosti vytvoření nového bloku. Ve chvíli kdy se tak stane, se těžba přesouvá znovu k jinému altcoinu. (115)

Což zanechá původní cíl těžby v problematickém stavu, protože se její těžba nevyplatí až do chvíle, než dojde k dalšímu přepočtení náročnosti. To může trvat i podstatně dlouhou dobu, v rámci které může dojít k naprosté paralyzaci funkcí a ukončení činnosti altcoinu. (115)

Řešením je častější přepočítání náročnosti těžby a použití jiného výpočetního mechanismus, než je patrný třeba u bitcoinu. Příkladem je třeba tzv. způsob Kimotovi gravitační studny („Kimotos gravity well“), kdy dochází k přepočtu náročnosti těžby nikoliv po vytěžení 2016 bloků, jako v případě bitcoinu, ale po bloku každém. Můžeme to vidět například u altcoinu Megacoin.(116)

6.1.2.2 Faktory ovlivňující výši náročnosti

Faktory, které mají vliv na výši náročnosti těžby, jsou dva. Prvním je cena mincí, protože s rostoucí cenou mincí se začíná vyplácet těžit pomocí i těch zařízení, které mají vyšší náklady na provoz. Druhý faktor je inovace technologií, tedy hardwaru a softwaru, který se používá k těžbě. (114)



Obrázek č. 7 Vývoj ceny bitcoinu a náročnosti těžby. Zdroj: (str. 7, 113)

První graf ukazuje závislost ceny mincí bitcoinu v čase a druhý graf zobrazuje vývoj náročnosti v čase, s vyznačenými body, kdy došlo k počátku těžby novým druhem technologií.

6.1.3 Těžební hardware a software

K realizaci těžby kryptoměn je potřeba dvou základních věcí. Zařízení, které bude řešit konkrétní těžební algoritmus. A také softwarového programu, který bude hardware ve skutečnosti ovládat.

Těžit se dá pomocí 4 typů hardwarových zařízení.

6.1.3.1 CPU – Těžba procesorem

Jedná se o těžbu pomocí standardního procesoru, který se nachází v každém PC. V počátcích kryptoměn se jednalo o jedinou cestu, jak kryptoměny těžit. Kryptoměny využívající těžebního algoritmu SHA-256 nebo Scrypt se těžit tímto zařízením nevyplatí, z důvodu malého výkonu v porovnání s ostatními. U jiných těžebních algoritmů se těžba může stále vyplácet..

6.1.3.2 GPU – Těžba grafickou kartou

S vývojem a optimalizací těžebního softwaru se začalo využívat výkonu počítačových grafických karet. Ze začátku se k těžbě využívalo jednotek grafických karet, standardní byla situace, kdy uživatel těžil na svém výkonném herním PC v době, kdy nehrál hry. Postupem času začali těžaři nakupovat velké množství grafických karet, ze kterých skládali těžební sestavy o mnoha grafických kartách.

Obrázek č. 8 Těžební zařízení s grafickými kartami. Zdroj: (str. 6-7, 117)

Na obrázku vlevo je vidět těžební sestava složená z 5 ti grafických karet, základní desky, procesoru, paměti, zdroje a dvou ventilátorů. Pravý obrázek je ukázkou sestavy o 69 grafických kartách.

Postavení takovéto těžební sestavy není příliš náročné, zvládne to i středně počítačově znalý uživatel. Vzhledem k tomu, že těžbu kryptoměn v počátku provozovali hlavně nadšenci a nikoliv firmy, tak je na internetu možné najít celou řadu návodů, jak těžební sestavu postavit.

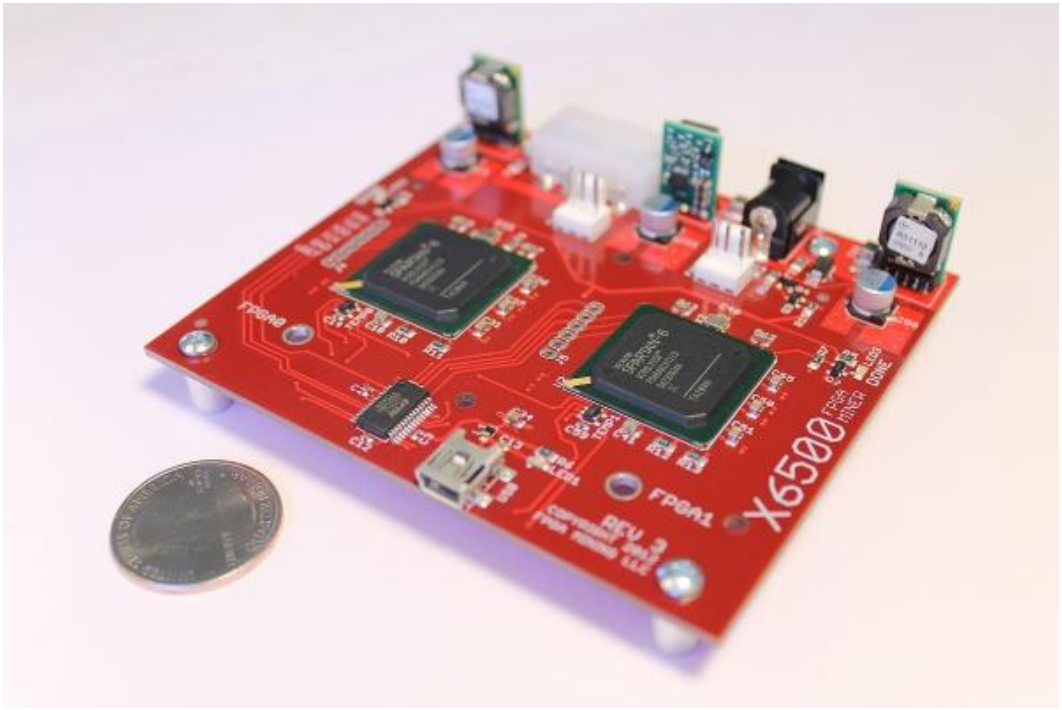
Zájem těžařů o grafické karty v určitých momentech stát také za tím, že hlavní dodavatel společnost AMD nestíhala pokrýt poptávku a docházelo tak k dlouhým čekacím lhůtám na určité modely. (118)

Zajímavostí také je, že oproti kartám společnosti Nvidia, dosahovaly karty od AMD mnohem většího výkonu při těžení bitcoinů. Je to dáno jiným technologickým postupem při výrobě karty.(119)

Nevýhodou ale bylo, že tyto sestavy produkují poměrně velké množství hluku a spotřebovávají mnoho elektřiny, s čímž souvisí také řada problémů typu přehřívání karet.

6.1.3.3 FPGA – Těžba programovatelným hradlovým polem

Podobně jako ASIC je i FPGA specializovaný typ hardwaru navržený na řešení konkrétního problému. FPGA se využívali k těžbě před příchodem další technologie ASIC. Dosahovaly podobného výkonu jako nejnovější těžební sestavy grafických karet. Výhodou těchto zařízení je, že jsou skladná ovládaná přes USB přístup. (114, str.)



Obrázek č. 9 Těžební zařízení typu FPGA. Zdroj: (115)

Na obrázku se nachází zařízení x6500 Rev 3 od společnosti FPGA Mining LCC.

6.1.3.4 ASIC – Těžba čipy, navrženými pro specifické užití

Zařízení typu ASIC, je ve své podstatě mikročip navržený k řešení velmi konkrétního problému. V našem případě k hledání řešení těžebního algoritmu. Ničeho jiného tyto zařízení

nejsou schopny. Oproti ostatním zařízením dosahují mnohonásobně vyššího těžebního výkonu a velmi nízké spotřeby elektřiny, což z nich dělá nejefektivnější těžební zařízení. (114, str. 8)

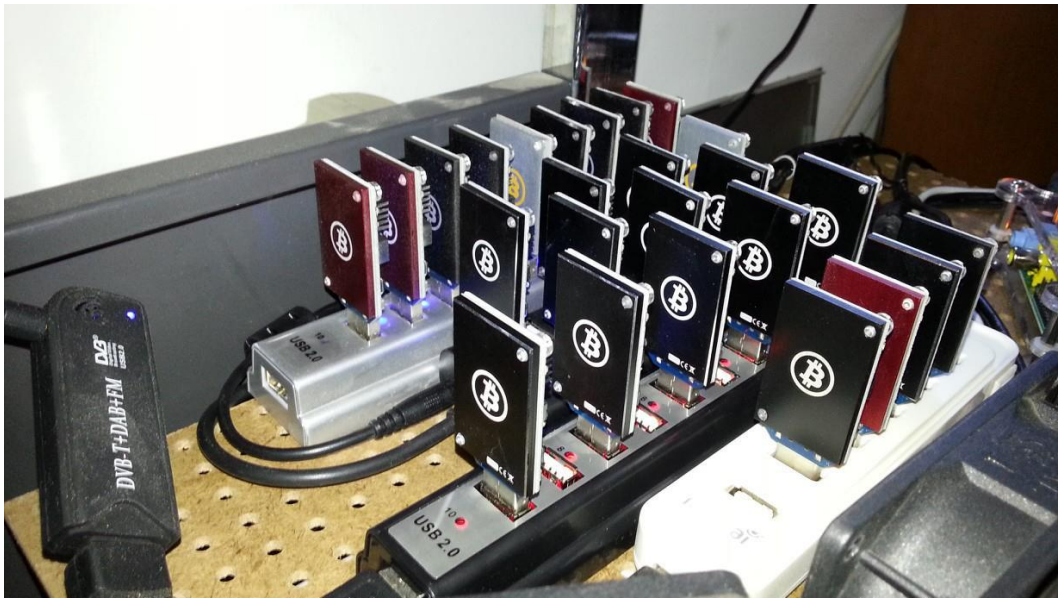
Jejich výhodou kromě vysokého výkonu a malé spotřebě elektřiny, je i mnohdy malá velikost a fakt, že se připojují prostřednictvím USB. Existují ale i velké asic sestavy, dosahující obrovského těžebního výkonu. (114, str. 9)

Hlavním omezením je ale to, že dokážou řešit pouze jeden konkrétní těžební algoritmus. Aktuálně jsou dostupná zařízení ASIC pouze pro těžbu SHA-256 a Skrypt. (120)

Společností, které vyrábějí ASIC, je na celém světě pouze kolem deseti. Známé jsou například Butterfly Labs a Zeus. (121, 122)

Tito výrobci se neustále snaží vyvinout novější zařízení, která by spotřebovávala menší množství elektřiny a byla výkonnější.

Dodávky ASIC zákazníkům jsou často zpožděny, někdy i o několik týdnů, což s rostoucí náročností těžby může velmi ovlivnit očekávanou výnosnost těžby.



Obrázek č. 10 Ukázka zařízení typu ASIC. Zdroj: (121)

6.1.3.5 Výkonnost jednotlivých typů těžebního hardwaru

V případě těžebních algoritmů SHA-256 a Scrypt, se dnes vyplatí jenom zařízení typu ASIC, které dosahují výkonu v řádech tisíců megahashů za jednu vteřinu a přitom spotřebovávají v průměru pouze pár wattů na jednu GH/s. (123)

Oproti tomu těžbou prostřednictvím různých CPU, GPU a FPGA můžeme dosáhnout řádově stovek Mhash/s. (124)

Přesunem těžby z technologie CPU na GPU došlo zhruba k 70 násobnému zvýšení výkonnosti těžby. Technologie FPGA oproti GPU zase spotřebovává pětinásobně méně elektřiny. Technologie ASIC oproti všem předešlým zvýšila v průměru výkon těžby stonásobně a třistanásobně snížila množství spotřebu elektřiny. (124)

Těžba většiny alternativních kryptoměn s těžebním algoritmem jiným, je tedy dnes výhodná jen pomocí GPU a CPU.

6.1.3.6 Těžební software

Programů umožňujících těžbu existuje velké množství. Vzájemně se liší nejen grafickou úpravou, operačním systémem, ale hlavně optimalizací výkonu těžby určitého druhu zařízení a algoritmu.

Pro těžbu pomocí grafických karet od společnosti AMD se často využívá Cgminer. U karet od výrobce Nvidia cudaMiner.(125, 126)

V těžbě prostřednictvím CPU je často doporučován cpuMiner. (127)

6.2 Způsoby realizace těžby

Těžit alternativní kryptoměny můžeme několika způsoby, které se liší hlavně v pravidelnosti, s jakou získáme odměnu za vytěžení mincí.

6.2.1 Solo těžba

Odměnu za nově vytvořený blok získává v případě těžby pouze ten, kdo najde správné řešení těžebního algoritmu jako první. Všichni těžaři si tak v tomto procesu vzájemně konkurují. Problém je v tomto případě to, že řešení nacházíme po náhodně dlouhých intervalech a získáváme tak odměnu nepravidelně. (128)

Těžaři se proto začali sdružovat do tzv. poolu. Kde jsou odměny vypláceny pravidelně v poměru podle množství výpočetního výkonu využitého k nalezení konkrétního řešení.

6.2.2 Těžba v poolu

Těžba v poolu funguje na principu sdružení více těžařů do jednoho uskupení, které využívá při řešení algoritmu výpočetní výkon všech těžařů dohromady. Pool tímto způsobem získá velké množství výpočetního výkonu, díky čemuž častěji vytěží nový blok a nové mince. Tyto mince jsou poté následně rozděleny mezi jednotlivé těžaře podle množství výpočetního výkonu, jakým jednotlivý těžaři přispěli v nálezu správného řešení. Část z vytvořených mincí jde pak provozovateli poolu jako poplatek. (128)

6.2.3 Težba v multipoolu

Multipool je podobný druh těžby jako těžba v poolu, pouze s tím rozdílem, že nedochází k těžbě jedné konkrétní kryptoměny, ale několika. Výběr toho, která kryptoměna bude těžena, závisí na její aktuální profitabilitě. (128)

6.2.4 Cloudová těžba

Těžba jakékoliv kryptoměny je spojena nejenom s koupí a správným nastavením hardwaru, optimalizací těžebního softwaru a nalezením ideálních prostor, kam veškerou techniku umístit. Řada lidí nemá dostatečné technické znalosti nebo prostředky k tomu, aby dokázali celou těžební operaci naplánovat a uvést do provozu. Přesně na tento typ uživatelů míří služby cloudové těžby. O veškeré technické provedení a zázemí se stará společnost, od které si můžeme koupit těžební kontrakty. Na základě těchto kontraktů dojde k okamžitému započetí těžby kryptoměny, jejíž výsledky jsou přesouvány na zaregistrované účty uživatele. (129)

Tři základní druhy cloudové těžby jsou: (129)

- Hostovaná těžba - Měsíční pronájem konkrétního těžebního zařízení. Nájemce zařízení může využít k těžbě jakékoliv měny a za veškeré nastavení těžby nese plnou zodpovědnost
- Virtuální hostovaná těžba – Instalace těžebního software na pronajatých virtuálních serverech. Typickým a velmi populárním příkladem byla těžba na pronajaté cloudové platformě od Amazonu.
- Pronajmutí hashovacího výkonu – Pronajmutí čistého těžebního výkonu, bez nutnosti spravovat fyzický hardware nebo virtuální servery. Jedná se o nejčastější způsob cloudové těžby.

Výhody cloudové těžby jsou: (129)

- Nízké počáteční náklady, protože není potřeba pořizovat drahý těžební hardware.
- Úspora času a starostí s nákupem a zprovozněním těžební operace.
- V případě zanechání činnosti, je prodej těžebního kontraktu podstatně jednoduší, než prodej těžebního hardwaru.

Rizika a problémy: (129)

- Renomé a zabezpečení cloudové společnosti. Těžební kontrakty mohou mít dobu trvání od několika málo dní do několika let, proto je důležité využívat služeb pouze renomovaných společností, u kterých je malé riziko krachu, a jsou dobře zabezpečené proti napadení hackery.
- Nižší zisk. Cena kontraktů se může výrazně lišit, někteří poskytovatelé mohou nabízet těžební výkon za takovou cenu, u které bude doba návratnosti investice nepřiměřeně dlouhá. Do kalkulace musíme rovněž započítat odhad toho, jak se bude v budoucnu vyvíjet náročnost těžby dané kryptoměny.

- Systémové riziko centralizace sítě. Jedná se o riziko tajného spolčení společností s velkým těžebním výkonem, které by pak mohli síť prostřednictvím útoku 51% ovládnout.

6.3 Výnosnost těžby a těžební strategie

Investovat do kryptoměn se dá dvěma způsoby. Buď můžeme kryptoměnu jednoduše nakoupit, nebo pořídíme vybavení, kterým altcoiny budeme těžit. Oba způsoby mají svá specifika.

Pokud očekáváme, že cena konkrétní kryptoměny bude stoupat, tak nejjednodušším způsobem jak této situace využít, je altcoin nakoupit přímo a později ho se ziskem prodat.

V případě těžby existuje několik strategií, kterými se dá na těžbě vydělat.

Buď můžeme těžit altcoiny nově vznikající, a doufat, že jejich hodnota v následujícím čase poroste. U většiny nových altcoinů nemáme šanci mince získat způsobem jiným, než těžbou krátce po spuštění. Je to dáno tím, že tyto altcoiny často nemají zařízenou podporu směnáren. A proto jejich případný nákup, můžeme realizovat jen pomocí přímého obchodu s nějakým těžařem, což může být velmi rizikové. Těžaři v tomto případě většinou spekulují nato, že si nově vznikající kryptoměny všimnou velcí spekulanti, kteří rychlým přísunem peněz, vytvoří na kryptoměně cenovou bublinu.

Dalším těžebním způsobem je specializace na jednu hlavní kryptoměnu, například bitcoin. V tomto případě těžaři nakupují neustále nejnovější a nejvýkonnější ASIC zařízení a doufají, že se jim investice vrátí dřív, než budou muset začít vyprodávat svoje těžební zařízení kvůli zvyšující se těžební náročnosti.

Výpočet návratnosti investice v případě jednotlivých kryptoměn je vcelku jednoduchý. Musíme ale znát několik důležitých proměnných.

- Počáteční náklady na zprovoznění těžebního zařízení, které se skládají z nákupu hardware a zařízení těžebních prostor, kam hardware umístíme.
- Výkon těžebního zařízení, kterého jsme schopni dosáhnout při řešení konkrétního těžebního algoritmu.
- Variabilní těžební náklady, pomocí kterých dosahujeme těžebního výkonu. Jedná se hlavně o spotřebu elektrické energie, případně nájem prostor a další.
- Stávající náročnost těžby a očekávaná náročnost těžby v budoucnu. S vyšší náročností dokážeme na stejném zařízení vytěžit menší počet mincí, čímž se nám při jejich nezměněné cenně sníží i výše zisku z těžby.
- Samozřejmě velkou neznámou je také odhadovaná cena bitcoinu.

Výpočet je možný například pomocí vnbitcoin.org.

Třetí možností těžby je těžba alternativních kryptoměn. Většinou se jedná o střídavou těžbu altcoinů podle toho, který se aktuálně nejvíce vyplatí těžit. Na tomto principu jsou postaveny hlavně multipooly. Rozdílem oproti zaměření se na jednu konkrétní kryptoměnu je v tom, že

při střídavé těžbě více měn, nedokážeme příliš odhadnout nárůst náročnosti těžby. Dalším problémem je to, že rozhodování o koupi těžebního zařízení, nejsme schopni přesně odhadnout, jakého výpočetního výkonu při jaké spotřebě elektrické energie dosáhneme.

Právě na tento případ těžby se zaměřuji v následujícím praktickém úkolu.

6.4 Realizace reálné těžební operace

6.4.1 Cíl těžební operace

Zjistit, zda je možné pomocí konkrétního testovaného hardwaru dosáhnout profitabilní těžby v některém z různých druhů altcoinů.

6.4.1.1 Metoda dosažení cíle

Nejprve popíšu, jaký konkrétně testovaný těžební hardware mám k dispozici.

Před tím, než budu schopen vypočítat výnosnost těžby, musím vědět, jakého těžebního výkonu mohu dosáhnout a za jaké spotřeby elektrické energie.

Tyto dva parametry zjistím tak, že zprovozním několik testovacích těžebních operací, u kterých si poznamenám, jakého těžebního výkonu jsem dosáhl a za jaké spotřeby elektrické energie. Těžební výkon změřím v těžebním softwaru a spotřebu elektřiny změřím pomocí měřiče spotřeby elektrické energie.

Poté s pomocí zjištěných výsledků a internetového kalkulátoru výnosnosti těžby CoinWarz určím, zda aktuálně existuje alternativní kryptoměna, kterou mohu se ziskem těžit.

6.4.2 Těžební hardware

Využité těžební zařízení k těžbě se dá nazvat výkonným herním PC.

Procesor: Intel Core i5-4670K (3.4 GHz, 6MB, LGA 1150) BOX

Grafická karta: ATI Sapphire R9 280X Vapor-X 3GB DDR5, PCI-E

Chladič procesoru: Gelid Solution Tranquillo, CPU cooler – revise 2

Paměť: Kingston 2x4GB DDR3 1600MHz CL9 (KHX16C9T3K2/8X)

Základní deska: Gigabyte Z87-HD3 – Z87, DDR3, s 1150, ATX

Zdroj: Fortron AURUM S, 80+ Gold, 700W

Pevný Disk: Kingston SSDNow V+100 SVP100S2/96G 2.5“ 96GB

Systémové informace viz. Příloha č.1 a Příloha č.2

6.4.3 Výběr způsobu těžby

Přesný těžební výkon daného hardwaru můžeme zjistit pouze samotným zrealizováním těžební operace. Na internetu je možné najít od ostatních těžařů popis toho, jakého výkonu dosahovali se svými zařízeními, za jakých podmínek a s jakým nastavením těžebního softwaru.

Mnohdy se jedná o popis nastavení a výkonu velkých těžebních sestav, skládajících se z mnoha grafických karet se specifickým druhem chlazení. Tyto informace od ostatních uživatelů nám mohou pomoci určit, zda při zprovoznění těžby neděláme nějakou chybu. Protože pokud ano, náš těžební výkon nebude ani zdaleka odpovídat hodnotám, kterých dosahovali ostatní.

K realizaci těžební operace potřebujeme několik základních věcí. Těžební hardware a těžební software, ale hlavně si musíme zvolit způsob, jakým začneme těžit.

Vzhledem k tomu, že zatím nevím, jakého výkonu a spotřeby elektrické energie můžu dosáhnout, tak budu pouze realizovat těžbu, která mi tyto informace dokáže jednoduše poskytnout.

Jednou z variant, jak toho můžu dosáhnout, je výběr několika různých alternativních kryptoměn, u kterých započnu s jejich těžbou. Tímto způsobem bych musel stáhnout a zprovoznit pro každou konkrétní kryptoměnu klienta a následně pak složitě nastavit těžební software tak, abych byl schopen samostatné těžby.

Mnohem jednodušší způsob je využít některého z těžebních multipoolů, nebo těžebního cloudu, kterému budu dodávat svůj výpočetní výkon.

Zvolil jsem způsob poslední, tedy realizaci těžby prostřednictvím cloudového řešení, kdy nebudu těžit konkrétní kryptoměny, ale namísto toho svůj těžební výkon dodám cloudovému poskytovateli.

Pro tento účel jsem vybral server nicehash.com, kterému mohu dodávat těžební výkon v algoritmech Scrypt, SHA256, Scrypt-A.-Nf, X11, X13, Keccak, X15, Nist5, NeoScrypt, Lyra2RE. (131)

6.4.3.1 Cloudová těžba NiceHash

NiceHash poskytuje dvě základní služby. Nabízí k prodeji těžební kontrakty, kdy si můžeme koupit kontrakt o určitém výkonu, který následně můžeme využít v těžbě konkrétní kryptoměny. Druhou službou je to, že těžařům nabízí odkup jejich výpočetního výkonu.

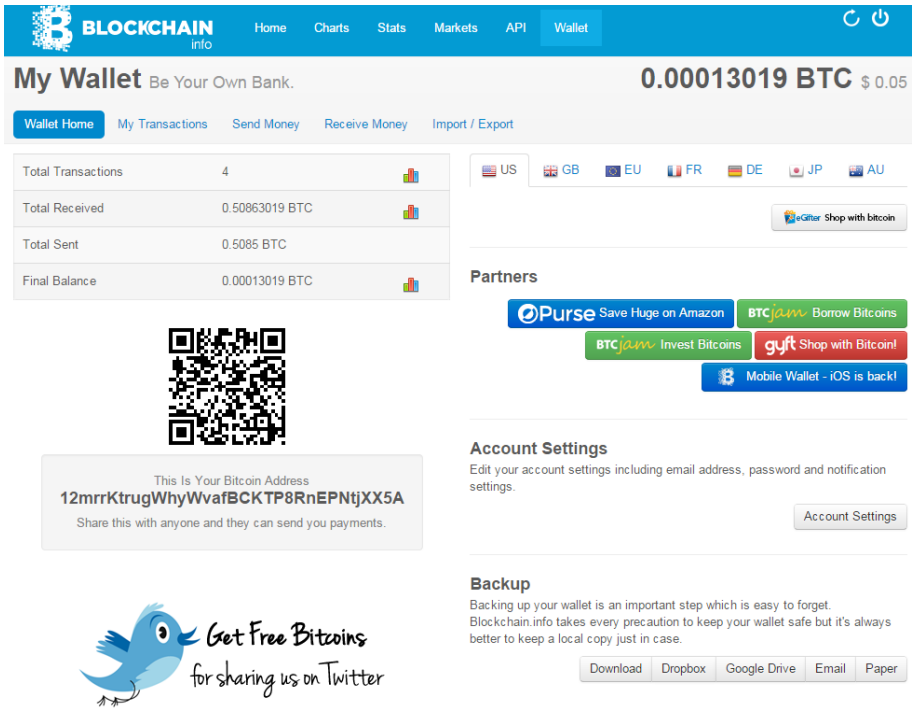
K tomu aby mohl těžař dodávat cloudu svůj výkon, musí mít nejprve založenou bitcoinovou pěněžeku s adresou, kam mu bude za dodaný výkon přicházet výplata v bitcoinech. Tato adresa slouží také jako identifikátor našeho těžebního zařízení.

Vzhledem k tomu, že zatím potřebujeme zjistit pouze výkon, kterého můžeme naším zařízením dosáhnout, tak nás výše odměny za námi dodaný výpočetní výkon nemusí příliš zajímat.

6.4.3.2 Založení bitcoinové peněženky na blockchain.info

Proces založení peněženky je velmi snadný.

1. Na adrese https://blockchain.info/wallet/new vyplníme email a přístupové heslo na novou peněženku. (130)
2. Po vyplnění hesla a emailové adresy nás web požádá o uložení série slov, která nám může pomoci v případě ztráty přístupového hesla k peněžence.
3. Jakmile potvrdíme úspěšné uložení dané série slov, přivítá nás úvodní přihlašovací stránka do peněženky.
4. Poté co vyplníme správně heslo, obdržíme na email, který jsme vytvořili při zakládání peněženky, zpráva. V této zprávě musíme kliknout na konfirmační odkaz, který nám zaktivní přístup do peněženky na daném PC.
5. Po úspěšném přihlášení do peněženky se setkáme s touto obrazovkou.



Obrázek č. 11 Bitcon peněženka na serveru Blockchain.info. Zdroj:(129)

6. V levém dolním rohu vidíme naší bitcoinovou adresu, kterou budeme potřebovat ke správnému nastavení těžebního softwaru.

6.4.4 Výběr a zprovoznění těžebního softwaru

Každý těžební pool, kryptoměna, či cloudová služba doporučuje různé druhy těžebního softwaru. V případě NiceHash je doporučováno k těžbě několik druhu softwaru.(132)

Tzv. PIMP, který se nahrává na USB disk, ze kterého se pak spouští jako operační systém.

Další je MultiMiner, software s grafickým rozhraním podporující mnoho platforem, který je založen na těžebním softwaru BFGMiner.

A poté klasický SGminer, který nejlépe optimalizuje těžbu pomocí grafických karet značky AMD. Pro těžbu pomocí karet značky Nvidia je doporučován software Cuda.

Pro těžbu zařízením ASIC, je připraven software cgminer.

V našem případě vlastníme výkonnou grafickou kartu od výrobce AMD, proto jsem zvolil těžební software **SGminer-5.1-dev-2014-11-13-win32.**

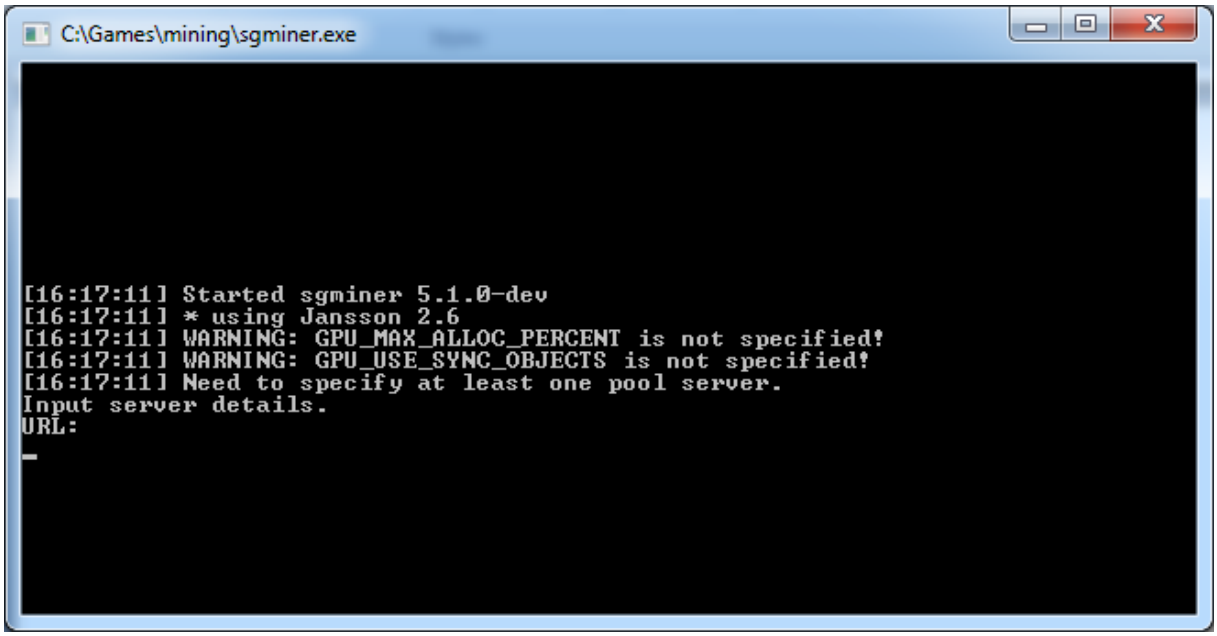
6.4.4.1 Instalace těžebního software SGminer 5.1

Tento těžební software můžeme stáhnout z odkazu, který je zveřejněn na NiceHash.(132)

Po stažení zkomprimovaného souboru typu zip, musíme tento soubor rozbalit do nové námi vytvořené složky například na disku C:\.

Obsah nově vytvořené složky je nyní složka, která se skládá z cca 60 různých souborů.

Spouštěcím souborem SGmineru 5.1 je SGminer.exe. Po jehož spuštění se otevře následující okno.



Obrázek č. 12 Aplikace SGminer po jeho úspěšném spuštění. Zdroj: (Autor)

V případě, že se nám program úspěšně spustil, je instalace hotova.

V některých případech může antivirový program hlásit, že se jedná o virus, proto je nutné přidat tento spouštěcí soubor do výjimek z kontrol.

6.4.4.2 První nastavení těžebního software SGminer 5.1

Abychom mohli začít s těžbou, je nutné software SGminer nastavit tak, aby došlo k jeho připojení k těžebnímu poolu (v našem případě NiceHash).

Veškeré hlavní nastavení softwaru se provádí při spuštění formou přidaných parametrů.

Nejvíce doporučovaný způsob jak SGminer nastavit je vytvořením spouštěcího bat souboru, do kterého všechny potřebné parametry uvedeme.

Ve složce, kde máme program rozbalený, vytvoříme prostřednictvím textového editoru (Ideálně Notepad.) soubor nazvaný například Start.txt.

Abychom mohli začít s úplně základním způsobem těžby, musíme v tomto souboru identifikovat cílový těžební pool, kterého se chceme stát součástí, a na kterém budeme těžit.

Na stránkách NiceHash jsou uvedeny následující adresy poolů, které se liší zpracovávaným těžebním algoritmem. (133)

Tabulka č. 8 Podporované těžební algoritmy službou NiceHash. Zdroj: (133)

Algoritmus	*Adresa poolu*
Scrypt	stratum+tcp://stratum.nicehash.com:3333
SHA256	stratum+tcp://stratum.nicehash.com:3334
Scrypt-A.-Nf.	stratum+tcp://stratum.nicehash.com:3335
X11	stratum+tcp://stratum.nicehash.com:3336
X13	stratum+tcp://stratum.nicehash.com:3337
Keccak	stratum+tcp://stratum.nicehash.com:3338
X15	stratum+tcp://stratum.nicehash.com:3339
Nist5	stratum+tcp://stratum.nicehash.com:3340
NeoScrypt	stratum+tcp://stratum.nicehash.com:3341
Lyra2RE	stratum+tcp://stratum.nicehash.com:3342

Nejprve se zkusíme připojit na pool, který řeší těžební algoritmus Scrypt. Do textového souboru Start.txt napíšeme:

SGminer -o stratum+tcp://stratum.nicehash.com:3336 -u „BitcoinAdresa“ -p x

Tento řádek říká, spustit SGminer s dalšími parametry.

Parametr „–o xxxx“ specifikuje adresu těžebního poolu, na který se připojujeme.

Parametr „–u BitcoinAadresa“ je jméno našeho těžebního zařízení, v tomto případě ho identifikuje bitcoinová adresa námi založeného účtu na blockchain.info.

Parametr „–p x“ je heslo, které v tomto konkrétním případě žádné není. Proto je jeho hodnota x, může tam být ale prakticky cokoliv.

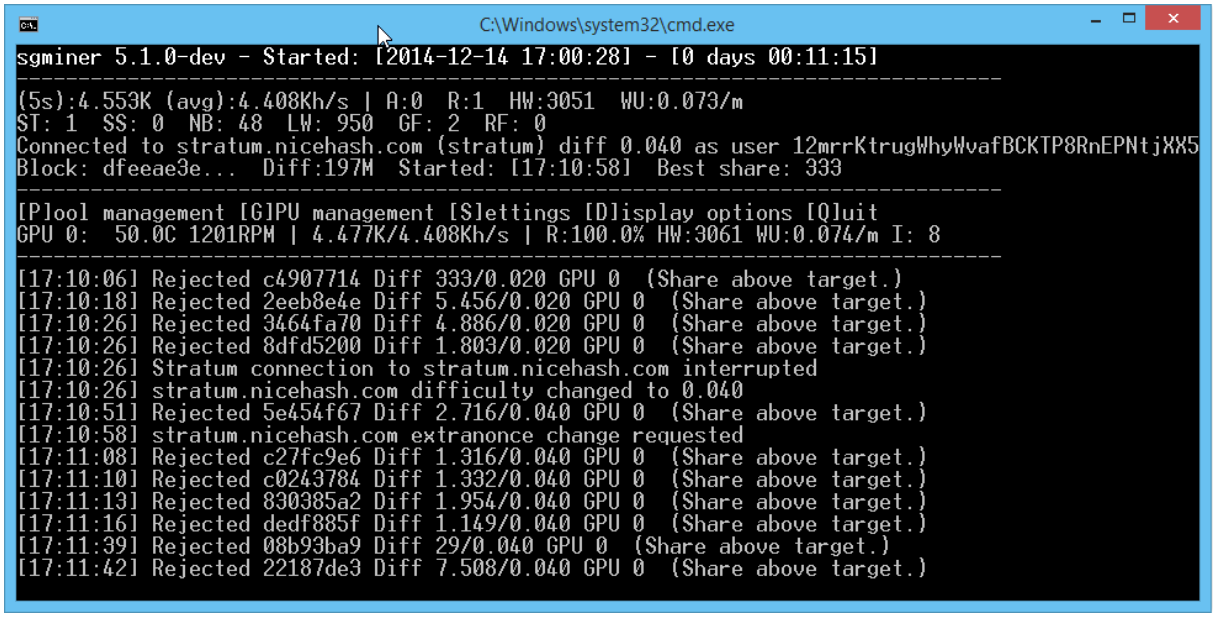
V případě jiných poolů musíme registrovat naše těžební zařízení pod jménem a heslem. Proto existují parametry –u a –p.

Finální řádek může vypadat například následovně:

SGminer -o stratum+tcp://stratum.nicehash.com:3336 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x

Takto upravený textový soubor Start.txt uložíme jako Start.bat. Tím se z něj stane soubor spouštěcí.

Když tento soubor spustíme, po chvíli načítání SGminer začne s těžbou.



Obrázek č. 13 Aplikace SGminer při těžbě. Zdroj: (Autor)

Z okna programu je patrné, že jsme se úspěšně připojili na pool a začali s těžbou. Bohužel je na obrazovce vidět, že naším těžebním zařízením vykonaná práce je odmítána s tím, že výkon s jakým algoritmus řešíme, je pouze kolem 4Kh/s. Což je naprosto nedostačující. Znamená to, že není SGminer nastavený správně.

6.4.4.3 Správné nastavení softwaru SGminer k těžbě

SGminer nabízí velmi mnoho různých parametrů, které můžeme nastavit a ovládat tak výkon grafické karty. Pro pokročilejší nastavení se využívá konfiguračního souboru. Pokud SGminer spustíme, můžeme jednoduše zmáčknutím klávesy „S“ otevřít nabídku nastavení. Po dalším stisknutí klávesy „W“, bude vytvořen konfigurační soubor, který se uloží do stejné složky, kde máme SGminer. Tento soubor se jmenuje „SGminer.conf“ a můžeme ho otevřít pomocí textového editoru.

Soubor bude obsahovat následující text:


```
{
  "pools": [
    {
      "url": "stratum+tcp://stratum.nicehash.com:3336",
      "user": "12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A",
      "pass": "x"
    }
  ],
  "profiles": [],
  "failover-only": true,
  "algorithm": "ckolivas",
  "device": "all",
  "temp-cutoff": "95",
  "temp-overheat": "85",
  "temp-target": "75",
  "gpu-memdiff": "0",
  "shares": "0",
  "kernel-path": "/usr/i586-mingw32msvc/bin",
  "api-mcast-port": "4028",
  "api-port": "4028",
  "expiry": "28",
  "failover-switch-delay": "60",
  "gpu-dyninterval": "7",
  "gpu-platform": "-1",
  "hamsi-expand-big": "4",
  "keccak-unroll": "0",
  "log": "5",
  "no-pool-disable": true,
  "no-client-reconnect": true,
  "queue": "1",
  "scan-time": "7",
  "tcp-keepalive": "30",
  "temp-hysteresis": "3"
}
```


Na začátku je specifikace poolu, na který jsme se připojili. V další části jsou podstatné parametry, které definují způsob jak SGminer bude řešit daný těžební algoritmus.

Zásadní problém, na který jsem při nastavování SGmineru narazil, tkvěl v tom, že primárně začala těžba nikoliv hlavní grafickou kartou, ale kartou, která je integrovaná na základní desce.

Tento problém vyřešilo nastavení hodnoty 1 k parametru gpu-platform.

Poté jsem se setkal s problémem, že nebyla správně nastavená intenzita těžby. Přidáním parametru „intensity“: „15“, se těžební výkon mnohonásobně zvýšil.

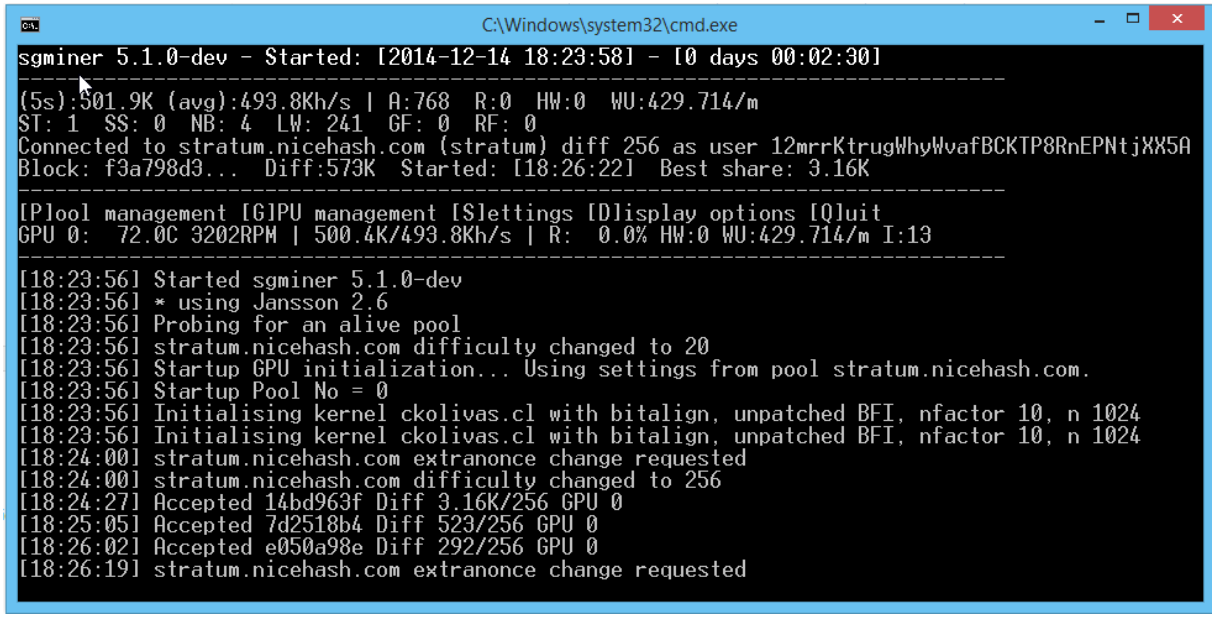
Při těžbě ostatních těžebních algoritmů typu x11 a dalších, bylo potřeba správně nastavit cestu ke kernelu, který se má při těžbě využít.

Po upravení spouštěcího souboru Start.bat tak, aby obsahoval dva řádky

set GPU_MAX_ALLOC_PERCENT 100

SGminer -k scrypt -o stratum+tcp://stratum.nicehash.com:3333 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 13 -g 2 -w 256 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan

SGminer začal těžit Skrypt výkonem zhruba 500Kh/s.



Obrázek č. 14 Aplikace SGminer při úspěšné těžbě. Zdroj: (Autor)

6.4.4.4 Měření spotřeby elektrické energie

Ke změření kolik počítač spotřebovává při těžbě elektrické energie, jsem použil výrobek Silverscrest Z 30412.

Obrázek č. 15 Měřič spotřeby elekrické energie značky Silvercrest. Zdroj: (Autor)

6.4.5 Měření výkonnosti těžby

Po zprovoznění funkční těžební operace jsem postupně zkoušel těžit různé algoritmy a zaznamenával jsem spotřebu elektrické energie. Dosahovaný výpočetní výkon zcela jistě nebude výkon maximálně možný, protože jsem při těžbě počítač využíval i k jiným činnostem.

Tabulka č. 9 Naměřené hodnoty výkonu a spotřeby. Zdroj: (Autor)

Algoritmus	Dosahovaný výkon	Spotřeba	Nastavení SGmineru
Scrypt	500 Kh/s	**290 W**	SGminer -k scrypt -o stratum+tcp://stratum.nicehash.com:3333 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 13 -g 2 -w 256 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan
SHA256	550 Kh/s	**300 W**	SGminer -k SHA256 -o stratum+tcp://stratum.nicehash.com:3333 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 16 -g 2 -w 256 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan
Scrypt-A.-Nf.	270 Kh/s	**300 W**	SGminer --pool-algorithm zuikkis --pool-nfactor 11 -o stratum+tcp://stratum.nicehash.com:3335 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 13 -g 2 -w 256 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan
X11	2 800 Kh/s	**190 W**	SGminer --pool-algorithm darkcoin-mod -o stratum+tcp://stratum.nicehash.com:3336 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 13 -g 2 -w 256 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan
X13	2 700 Kh/s	**210 W**	SGminer --pool-algorithm marucoin-mod -o stratum+tcp://stratum.nicehash.com:3337 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 18 -g 2 -w 256 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan
Keccak	340 000 Kh/s	**300 W**	SGminer --pool-algorithm maxcoin -o stratum+tcp://stratum.nicehash.com:3338 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 13 -g 2 -w 256 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan
X15	2 500 Kh/s	**200 W**	SGminer --pool-algorithm bitblock -o stratum+tcp://stratum.nicehash.com:3339 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 20 -g 2 -w 128 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan
Nist5	10 000 Kh/s	**200 W**	SGminer --pool-algorithm talkcoin-mod -o stratum+tcp://stratum.nicehash.com:3340 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 20 -g 2 -w 128 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan --gpu-powertune 30
NeoScrypt	240 Kh/s	**220 W**	SGminer --pool-algorithm neoscrypt -o stratum+tcp://stratum.nicehash.com:3341 -u 12mrrKtrugWhyWvafBCKTP8RnEPNtjXX5A -p x --gpu-platform 1 -d 0 -I 16 -g 2 -w 64 --thread-concurrency 8192 --gpu-engine=1020 --gpu-memclock=1500 --auto-fan --gpu-powertune 30

6.4.6 Výsledky měření a jejich vyhodnocení

Z předešlé tabulky je patrné, jakého výpočetního výkonu mohu dosáhnout v případě těžby konkrétních těžebních algoritmů. Díky tomu, že jsem zjistil také výši spotřeby elektrické energie, tak mohu využít jeden z mnoha srovnávacích serverů, který mi dokáže říct, zda a případně která alternativní kryptoměna se mi vyplatí těžit.

Samozřejmě je nutné znát ještě jeden důležitý parametr a tím je cena elektrické energie. Aktuální sazbu, kterou platím je 4.2Kč na 1 kWh elektřiny. Při kurzu 22 korun za 1 americký dolar, je to přibližně 0.191$/kWh.

Když zadám výsledné hodnoty z těžby do kalkulátoru na serveru CoinWarz.com, vyjde mi následující tabulka:

Tabulka č. 10 Výnosnost těžby podle CoinWarz.com. Zdroj: (133)

	Crypto Currency Current Profitability Position	Current Difficulty 14 Day Difficulty Chart	Est. Coins (Current / 24 Hr Avg)	Exchange Rate BTC 14 Day Exchange Rate Chart	Exchange Volume	Revenue / Profit (per day)	Earn 1 BTC (in days)	Profit Ratio vs. BTC (Current / 14 Day Average)
1	Darkcoin (DRK) Network Hashrate: 76.72 GH/s Block Reward: 6.00 Blocks: 186,349 Block Time: 2.50 minute(s) X11	2,813.9764 -10.91 %	0.1201 / 0.1070	0.00633610 (Bittrex) +0.37 %	5.28 BTC 836.71 DRK	$0.27 / ($0.60) $0.87 for electricity	1,314.12 0.00076097 BTC / day	156.42 % / 152.39 %
2	StartCoin (START) Network Hashrate: 11.53 GH/s Block Reward: 40.00 Blocks: 109,651 Block Time: 1.00 minute(s) X11	185.5489 -12.34 %	12.1427 / 10.6437	0.00004401 (Bittrex) +0.73 %	2.31 BTC 52,779.83 START	$0.19 / ($0.68) $0.87 for electricity	1,871.26 0.00053440 BTC / day	150.51 % / 147.81 %
3	CannabisCoin (CANN) Network Hashrate: 8.52 GH/s Block Reward: 52.50 Blocks: 386,441 Block Time: 42.00 second(s) X11	74.9443 -16.81 %	39.4578 / 32.8249	0.00001321 (Cryptsy) -0.75 %	1.56 BTC 117,343.97 CANN	$0.19 / ($0.68) $0.87 for electricity	1,918.51 0.00052124 BTC / day	150.16 % / 147.28 %
4	Sterlingcoin (SLG) Network Hashrate: 1.53 GH/s Block Reward: 50.00 Blocks: 106,834 Block Time: 2.00 minute(s) X13	45.2815 -34.56 %	59.9746 / 39.2479	0.00001273 (Cryptsy) +0.47 %	0.17 BTC 13,476.73 SLG	$0.27 / ($0.69) $0.96 for electricity	1,309.80 0.00076348 BTC / day	149.81 % / 142.64 %
5	Digitalcoin-X11 (DGC) Network Hashrate: ? Block Reward: 5.00 Blocks: 1,039,707 Block Time: 40.00 second(s) X11	18.9385 -31.47 %	14.8709 / 10.1917	0.00003400 (Cryptsy) +9.76 %	0.28 BTC 9,153.16 DGC	$0.18 / ($0.69) $0.87 for electricity	1,977.81 0.00050561 BTC / day	149.76 % / 143.57 %
6	Phoenixcoin (PXC) Network Hashrate: 23.30 MH/s Block Reward: 50.00 Blocks: 520,302 Block Time: 1.50 minute(s) Neo Scrypt	0.2675 +4.44 %	902.5483 / 944.4389	0.00000091 (Cryptsy) 0.00 %	0.07 BTC 74,637.40 PXC	$0.29 / ($0.71) $1.01 for electricity	1,217.55 0.00082132 BTC / day	147.98 % / 146.95 %
7	Feathercoin (FTC) Network Hashrate: 1.80 GH/s Block Reward: 80.00 Blocks: 500,418 Block Time: 1.00 minute(s) Neo Scrypt	29.5790 +27.12 %	13.0579 / 17.9158	0.00006000 (BTCe) +2.10 %	13.49 BTC 229,581.80 FTC	$0.28 / ($0.73) $1.01 for electricity	1,276.37 0.00078347 BTC / day	146.99 % / 151.00 %
8	Cryptcoin (CRYPT) Network Hashrate: 2.40 GH/s Block Reward: 31.25 Blocks: 352,151 Block Time: 1.50 minute(s) X11	107.9286 -19.44 %	16.3089 / 13.1392	0.00002415 (Bittrex) +1.74 %	0.19 BTC 7,807.41 CRYPT	$0.14 / ($0.73) $0.87 for electricity	2,538.97 0.00039386 BTC / day	146.84 % / 144.03 %

Z dané tabulky zcela jasně vyplývá, že těžba jakékoliv alternativní kryptoměny využívající jeden ze zadaných těžebních algoritmů, by byla ztrátová. Dokázal bych sice natěžit určité množství mincí, ale jejich prodejem bych nebyl schopný pokrýt náklady na elektrický proud. Vyplatilo by se mi to, kdybych náklady na elektrický proud neměl, ale i v tomto případě bych za 24 hodin těžby, byl schopný vydělat pouze zhruba 5 Kč.

Tento kalkulátor zároveň nezapočítává různé další poplatky spojen například s těžbou prostřednictvím multipoolu. Tudíž i bez nákladů na elektřinu, by výsledný zisk byl nižší.

7 Závěr

Ekosystém alternativních kryptoměn se skládá ze stovek až tisíců různých projektů. Technickou revoluci zažehl bitcoin, který jako první dokázal nahradit do té doby centralizované platební systémy. Každým měsícem vznikají nové projekty, které využívají technologického základu bitcoinu k decentralizovanému řešení i jiných problémů, jakým je například ověření vlastnictví konkrétní věci. Do budoucna se dá očekávat, že tyto technologie zasáhnou do života nás všech.

Cílem mojí práce bylo nejenom tento rozsáhlý ekosystém zanalyzovat a představit tak další úspěšné projekty, ale také zjistit, zda je možné profitabilně alternativní kryptoměny těžit pomocí konkrétní grafické karty.

Ekosystém kryptoměn se skládá z celé řady projektů, které můžeme rozlišovat primárně podle jejich účelu, který se snaží naplnit. Většinu projektů můžeme dělit na alternativní kryptoměny a alternativní řetězce. Účelem alternativních kryptoměn je primárně plnit roli prostředníka směny, tedy peněz. Zatímco alternativní řetězce mohou mít za cíl například správu internetové domény .bit.

Velké množství projektů však není úspěšných. Zajímalo mě proto, proč některé projekty úspěšné jsou a jiné ne. V rámci této diplomové práce jsem podrobně prozkoumal velké množství alternativních kryptoměn a na základě zjištěných poznatků definoval hlavní typy rozdílů mezi nimi. Poté jsem stanovil vlivy, které mají na úspěšnost kryptoměn největší dopad.

V praktické části jsem testoval možnost použití konkrétní grafické karty k těžbě alternativních kryptoměn. Nejprve jsem musel zprovoznit těžební software, s jehož pomocí jsem poté začal testovat těžební výkon dané karty. S pomocí naměřeného těžebního výkonu a spotřeby elektrické energie jsem zjistil, že se těžba alternativních kryptoměn tímto způsobem nevyplatí. Je to dáno hlavně vysokými náklady na elektrickou energii.

Přínos mé práce tkví nejen v uceleném popisu ekosystému alternativních kryptoměn, ale také v praktické ukázce toho, jak lze zjistit výkonnost těžebního zařízení.

Dalším velice zajímavým tématem z oblasti kryptoměn by mohlo být podrobné popsání toho, jak se s těmito finančními instrumenty spekulativně obchoduje.

Seznam použitých zdrojů

[1] Bitcoin. BITCOIN COMMUNITY. *Bitcoin wiki* [online]. Media wiki, 2013 [cit. 2014-12-11]. Dostupné z: https://en.bitcoin.it/wiki/Bitcoin

[2] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System – Satoshi Nakamoto* [online]. 2013 [cit. 2014-12-14]. Dostupné z: http://bitcoins.info/bitcoin.pdf

[3] Digital currency. BITCOIN COMMUNITY. *Bitcoin wiki* [online]. Media wiki, 2013 [cit. 2014-12-11]. Dostupné z: https://en.bitcoin.it/wiki/Digital_currency

[4] Cryptocurrency. INVESTOPEDIA. *Investopedia* [online]. Investopedia LLC, 2013 [cit. 2014-12-11]. Dostupné z: www.investopedia.com/terms/c/cryptocurrency.asp

[5] Cryptocurrency. TECHOPEDIA. *Techopedia* [online]. Techopedia, 2013 [cit. 2014-12-11]. Dostupné z: www.techopedia.com/definition/27531/cryptocurrency

[6] Silk Road: Theory & Practice. GWERN.NET. *Gwern.net* [online]. 2011, 8.12.2014 [cit. 2014-12-11]. Dostupné z: http://www.gwern.net/Silk%20Road

[7] STASTNA, Kazi. WikiLeaks bypasses donations boycott. CBC NEWS. *CBC News: Technology & Science*[online]. 2012, 18.7.2012 [cit. 2014-12-11]. Dostupné z: http://www.cbc.ca/news/technology/wikileaks-bypasses-donations-boycott-1.1170719

[8] KANAI, Gen. Update on the cost of monoculture in Korea. KANAI, Gen. *Mozilla in Asia: Gen Kanai's Mozilla weblog* [online]. 2007 [cit. 2014-12-11]. Dostupné z: http://blog.mozilla.org/gen/2007/09/21/update-on-the-cost-of-monoculture-in-korea/

[9] European Central Bank. *Virtual Currency Schemes* [online]. 2012 [cit. 2014-12-11]. Dostupné z: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[10] KING, Sunny a Scott NADAL. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake* [online]. 2012. [cit. 2014-12-11] Dostupné z: http://peercoin.net/assets/paper/peercoin-paper.pdf

[11] PŘISPĚVATELÉ WIKIPEDIE. Cryptography. In: *Wikipedia, the Free Encyclopedia* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://en.wikipedia.org/wiki/Cryptographic_hash_function

[12] MENEZES, Alfred J., Paul C. VAN OORSCHOT a Scott A. VANSTONE. Handbook of applied cryptography. Vyd. 1. Boca Raton: CRC Press, 1997, 780 s. ISBN 08-493-8523-7.

[13] PŘISPĚVATELÉ WIKIPEDIE. Cryptographic hash function. In: *Wikipedia, the Free Encyclopedia* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://en.wikipedia.org/wiki/Cryptographic_hash_function

[14] Comparison between Litecoin and Bitcoin/Alternative work in progress version. LITECOIN WIKI. *Litecoin wiki*[online]. Media wiki, 2013 [cit. 2014-12-11]. Dostupné z: https://litecoin.info/Comparison_between_Litecoin_and_Bitcoin/Alternative_work_in_progress_version

[15] BRITO, Jerry a Andrea CASTILLO. BITCOIN: A Primer for *Policymakers* [online]. Arlington: Mercatus Center at George Mason University, 2013 [cit. 2014-12-11]. Dostupné z: http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf

[16] Private key. BITCOIN COMMUNITY. *Bitcoin wiki* [online]. Media wiki, 2011, 19.8.2014 [cit. 2014-12-11]. Dostupné z: https://en.bitcoin.it/wiki/Private_key

[17] Technical background of version 1 Bitcoin addresses. BITCOIN COMMUNITY. *Bitcoin wiki* [online]. Media wiki, 2011, 15.9.2014 [cit. 2014-12-11]. Dostupné z: https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

[18] Developer Guide. BITCOIN PROJECT. *Bitcoin* [online]. 2014 [cit. 2014-12-11]. Dostupné z: https://bitcoin.org/en/developer-guide#escrow-and-arbitration

[19] Wallet. BITCOIN COMMUNITY. *Bitcoin wiki* [online]. Media wiki, 2011, 2.12.2014 [cit. 2014-12-11]. Dostupné z: https://en.bitcoin.it/wiki/Wallet

[20] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System – Satoshi Nakamoto* [online]. 2013 [cit. 2014-12-14]. Dostupné z: http://bitcoins.info/bitcoin.pdf

[21] HURŤÁK, Petr. *Analýza virtuální měny Bitcoin* [online]. Praha, 2013 [cit. 2014-12-14]. Bakalářská práce. Vysoká škola ekonomická. Vedoucí práce Radim Brixí. Dostupné z: http://www.vse.cz/vskp/show_file.php?soubor_id=1244711.

[22] ŠKODA, Dominik. *Bitcoin jako forma digitálních peněz* [online]. Praha, 2014 [cit. 2014-12-14]. Vysoká škola ekonomická. Vedoucí práce Zbyněk Revenda. Dostupné z: https://www.vse.cz/vskp/show_file.php?soubor_id=1247693. Diplomová práce.

[23] SKUDNOV, Rostislav. *Bitcoin Clients: Bachelor´s Thesis* [online]. Turku, 2012 [cit. 2014-12-11]. Bakalářská práce. Turku University of Applied Sciences. Vedoucí práce Raija Tuohi. Dostupné z: http://publications.theseus.fi/bitstream/handle/10024/47166/Skudnov_Rostislav.pdf.

[24] Proof of Stake. BITCOIN COMMUNITY. *Bitcoin wiki* [online]. 2012, 8.6.2014 [cit. 2014-12-12]. Dostupné z: https://en.bitcoin.it/wiki/Proof_of_Stake

[25] REN, Larry. *Proof of Stake Velocity: Building the Social Currency of the Digital Age* [online]. www.reddcoin.com, 2014 [cit. 2014-12-12]. Dostupné z: https://www.reddcoin.com/papers/PoSV.pdf

[26] COINMARKETCAP. *Crypto-Currency Market Capitalizations* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://coinmarketcap.com/

[27] *Bitcoin and Altcoin price charts/ graphs* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://cryptocoincharts.info/

[28] PŘISPĚVATELÉ FÓRA. Re: Total Coins - Nov 15th 2014. In: *Bitcoin Forum* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://bitcointalk.org/index.php?topic=858783.20

[29] PŘISPĚVATELÉ FÓRA. Necronomicon thread: Altcoins which are dead. In: *Bitcoin Forum* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://bitcointalk.org/index.php?topic=588413.0

[30] Altcoin Definition. INVESTOPEDIA, LLC. *Investopedia* [online]. 2014 [cit. 2014-12-12]. Dostupné z:http://www.investopedia.com/terms/a/altcoin.asp

[31] Cryptocurrency 2.0. ALTCOIN HERALD. *Altcoin Wiki* [online]. 2014 [cit. 2014-12-12]. Dostupné z: https://altcoinherald.com/wiki/index.php?title=Cryptocurrency_2.0

[32] Mastering bitcoin. O'REILLY MEDIA, Inc. *O'Reilly* [online]. 2013 [cit. 2014-12-12]. Dostupné z: http://chimera.labs.oreilly.com/books/1234000001802/ch04.html

[33] NXT ORGANIZATION. *Nxt.org: Decentralized & Trustless Financial Ecosystem* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://nxt.org/

[34] KELLEHER, John. Who Is Satoshi Nakamoto, Mysterious Bitcoin Founder?. INVESTOPEDIA, LLC. *Investopedia* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://www.investopedia.com/articles/general/032614/who-satoshi-nakamoto-mysteriousbitcoin-founder.asp

[35] Overview. THE BITCOIN FOUNDATION. *The Bitcoin Foundation* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://bitcoinfoundation.org/about/overview/

[36] Who controls the Bitcoin network?. BITCOIN PROJECT. *Bitcoin* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://bitcoin.org/en/faq#who-controls-the-bitcoin-network

[37] FAQ. BITCOIN COMMUNITY. *Bitcoin Wiki* [online]. 2010, 12.12.2014 [cit. 2014-12-13]. Dostupné z: https://en.bitcoin.it/wiki/FAQ

[38] PŘISPĚVATELÉ FÓRA. *** Complete Guide on How to Create a New Alt Coin ***. In: *Bitcoin Forum* [online]. 2013 [cit. 2014-12-13]. Dostupné z: https://bitcointalk.org/index.php?topic=225690.0

[39] Trade. BITCOIN COMMUNITY. *Bitcoin Wiki* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://en.bitcoin.it/wiki/Trade

[40] THE TOR PROJECT, Inc. *Tor Project: Anonymity Online* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://www.torproject.org/docs/trademark-faq.html.en

[41] Darknet Market Chart. VAULT-TEC CORPORATION. *Vault43* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://vault43.org/chart.php

[42] FOXTON, Willard. So how much was Silk Road worth?. TELEGRAPH MEDIA GROUP LIMITED. *Telegraph Blogs* [online]. 2013 [cit. 2014-12-13]. Dostupné z: http://blogs.telegraph.co.uk/technology/willardfoxton2/100010940/so-how-much-was-silk-road-worth/

[43] WONG, Joon Ian. Dark Markets Grow Bigger and Bolder in Year Since Silk Road Bust. COINDESK. *CoinDesk* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://www.coindesk.com/dark-markets-grow-bigger-bolder-year-since-silk-road-bust/

[44] WONG, Joon Ian. China's Market Dominance Poses Questions About Global Bitcoin Trading Flows. COINDESK. *CoinDesk* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://www.coindesk.com/chinese-markets-dominance-poses-questions-global-bitcoin-trading-flows/

[45] HAJDARBEGOVIC, Nermin. Yuan Trades Now Make Up Over 70% of Bitcoin Volume. COINDESK. *CoinDesk* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://www.coindesk.com/yuan-trades-now-make-70-bitcoin-volume/

[46] MAULDIN, John. Mauldin: What is Bitcoin. BUSINESS INSIDER INC. *Business Insider* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://www.businessinsider.com/mauldin-what-is-bitcoin-2014-12

[47] Map of coins [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://mapofcoins.com/NAMECOIN. *Namecoin* [online]. [cit. 2014-12-12]. Dostupné z: http://namecoin.info/

[48] PŘISPĚVATELÉ FÓRA. *** Complete Guide on How to Create a New Alt Coin ***. In: *Bitcoin Forum* [online]. 2013 [cit. 2014-12-13]. Dostupné z: https://bitcointalk.org/index.php?topic=225690.0

[49] COINCREATOR.NET. *CoinCreator* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://coincreator.net/

[50] CZECH CROWN COIN. *Czech Crown Coin* [online]. [cit. 2014-12-12]. Dostupné z: http://www.czechcrowncoin.com/?page_id=65

[51] KELLEHER, John. Who Is Satoshi Nakamoto, Mysterious Bitcoin Founder?. INVESTOPEDIA, LLC. *Investopedia* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://www.investopedia.com/articles/general/032614/who-satoshi-nakamoto-mysteriousbitcoin-founder.asp

[52] ICOs. ALTCOIN HERALD. *Altcoin wiki* [online]. 2014 [cit. 2014-12-12]. Dostupné z: https://altcoinherald.com/wiki/index.php?title=ICOs

[53] Developer Guide. BITCOIN PROJECT. *Bitcoin* [online]. 2014 [cit. 2014-12-11]. Dostupné z: https://bitcoin.org/en/developer-guide#escrow-and-arbitration

[54] CRYPTOCOINCHARTS. *Bitcoin and Altcoin price charts/ graphs* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://cryptocoincharts.info/

[55] Cryptocurrency Charts by Market Capitalization. *Cryptocoinrak Altcoin List* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://www.cryptocoinrank.com/

[56] WORLD COIN INDEX. *WorldCoinIndex.com - Latest crypto coin trade prices and market cap* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://worldcoinindex.com/

[57] BTC-E.COM. *BTC-E | Bitcoin Exchange, Litecoin Exchange, BTC Exchange* [online]. 2014 [cit. 2014-12-14]. Dostupné z: https://btc-e.com/

[58] PROJECT INVESTORS INC. *Cryptsy* [online]. 2014 [cit. 2014-12-12]. Dostupné z: https://www.cryptsy.com/

[59] EXCHANGE WAR. *Exchange war: list of crypto-exchanges* [online]. 2014 [cit. 2014-12-14]. Dostupné z:http://exchangewar.info/

[60] BITCOINCHARTS.COM. *Bitcoin Charts* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://bitcoincharts.com

[61] HAJDARBEGOVIC, Nermin. Bitcoin Scammers Held by Chinese Authorities. COINDESK. *CoinDesk* [online]. 2013 [cit. 2014-12-12]. Dostupné z: http://www.coindesk.com/bitcoin-scam-china-authorities/

[62] BRADBURY, Danny. Czech bitcoin exchange Bitcash.cz hacked - 4,000 user wallets emptied. COINDESK. *CoinDesk*[online]. 2013 [cit. 2014-12-12]. Dostupné z: http://www.coindesk.com/czech-bitcoin-exchange-bitcash-cz-hacked-4000-user-wallets-emptied/

[63] HERN, Alex. How a bug in bitcoin led to MtGox's collapse. THE GUARDIAN. *The Guardian* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://www.theguardian.com/technology/2014/feb/27/how-does-a-bug-in-bitcoin-lead-to-mtgoxs-collapse

[64] What is the Difference Between Litecoin and Bitcoin?. COINDESK. *CoinDesk* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://www.coindesk.com/information/comparing-litecoin-bitcoin/

[65] OPENSTREETMAP CONTRIBUTORS. *Coinmap* [online]. [cit. 2014-12-13]. Dostupné z: http://coinmap.org/

[66] PŘISPĚVATELÉ WIKIPEDIE. Dogecoin. In: *Wikipedia, the Free Encyclopedia* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://en.wikipedia.org/wiki/Dogecoin

[67] PARKER, David. The Pros and Cons of the X11 Algorithm. PARKER, David. *CryptoCoinsNews* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://www.cryptocoinsnews.com/pros-cons-x11-algorithm/

[68] PŘISPĚVATELÉ FÓRA. [ANN][DRK] Darkcoin | First Anonymous Coin | Inventor of X11, DGW and Darksend | Instant TX.*Bitcoin Forum* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://bitcointalk.org/index.php?topic=421615.0

[69] Darkcoin Added To Darknet Drug Marketplaces. LUCRATIVELY LLC. *Coin Brief* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://coinbrief.net/darkcoin-darknet-markets/

[70] Peercoin. BITCOIN COMMUNITY. *Bitcoin Wiki* [online]. 2014 [cit. 2014-12-13]. Dostupné z: http://en.bitcoinwiki.org/Peercoin

[71] PŘISPĚVATELÉ FÓRA. [ANN] BitcoinDark (BTCD)--Teleport/Telepathy Privacy Tech--SuperNET Core Coin. In: *Bitcoin Forum* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://bitcointalk.org/index.php?topic=684090.0

[72] KING, Sunny a Scott NADAL. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake* [online]. 2012. [cit. 2014-12-11] Dostupné z: http://peercoin.net/assets/paper/peercoin-paper.pdf

[73] PŘISPĚVATELÉ FÓRA. [ANN] BitcoinDark (BTCD)--Teleport/Telepathy Privacy Tech--SuperNET Core Coin. In: *Bitcoin Forum* [online]. 2014 [cit. 2014-12-13]. Dostupné z: https://bitcointalk.org/index.php?topic=684090.0

[74] PŘISPĚVATELÉ FÓRA. [XMR] Monero - A secure, private, untraceable cryptocurrency - 0.8.8.6. In: *Bitcointalk* [online]. 2014 [cit. 2014-12-12]. Dostupné z: https://bitcointalk.org/index.php?topic=583449.0

[75] CryptoNight. BITCOIN COMMUNITY. *Bitcoin Wiki* [online]. Mediawiki, 2014 [cit. 2014-12-12]. Dostupné z: https://en.bitcoin.it/wiki/CryptoNight

[76] MONERO. *Monero* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://www.monero.cc/

[77] Innovation & Merits. YBCOIN DEVELOPMENT TEAM. *YBCoin* [online]. 2013 [cit. 2014-12-12]. Dostupné z: http://www.ybcoin.com/en/innovations-merits

[78] Cryptocointalk - discussing the world of cryptocurrencies. CRYPTOCOINTALK.COM. *Cryptocointalk* [online]. 2014 [cit. 2014-12-12]. Dostupné z: https://cryptocointalk.com/topic/1608-ybcoin-ybc-information/

[79] YBCoin. COINWIK.ORG. *Decentralized currencies* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://coinwik.org/YBCoin

[80] PŘISPĚVATELÉ WIKIPEDIE. User:WSF/Feathercoin. In: *Wikipedia, the free encyclopedia* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://en.wikipedia.org/wiki/User:WSF/Feathercoin

[81] BYTECOIN. *Bytecoin|SHA256 Cryptocoin* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://bytecoin.biz/

[82] BYTECOIN.ORG. *Bytecoin (BCN)* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://bytecoin.org/

[83] CryptoNote Currencies. CRYPTONOTE. *CryptoNote* [online]. 2014 [cit. 2014-12-12]. Dostupné z: https://cryptonote.org/coins/

[84] PRIMECOIN. *Primecoin* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://primecoin.io/

[85] GRIDCOIN. *Gridcoin* [online]. [cit. 2014-12-12]. Dostupné z: http://www.gridcoin.us/index.html

[86] QUARK. *Quark - Money reinvented by the people* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://www.qrk.cc/

[87] Quark. COINWIKI. *Coinwiki.info* [online]. 2013 [cit. 2014-12-12]. Dostupné z: http://coinwiki.info/en/Quark

[88] REDDCOIN. *Reddcoin* [online]. 2014 [cit. 2014-12-12]. Dostupné z: https://www.reddcoin.com/

[89] VERTCOIN. *Vertcoin – Bitcoin Upgraded* [online]. 2014 [cit. 2014-12-12]. Dostupné z: https://vertcoin.org/wp/

[90] Introduction to Ripple for Bitcoiners. RIPPLE WIKI. *Ripple Wiki* [online]. 2013 [cit. 2014-12-12]. Dostupné z: https://wiki.ripple.com/Introduction_to_Ripple_for_Bitcoiners

[91] LEWIS, Antony. Ripple Explained: Medieval Banking with a Digital Twist. COINDESK. *CoinDesk* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://www.coindesk.com/ripple-medieval-banking-digital-twist/

[92] MAIDSAFE.NET. *MaidSafe – The New Decentralized Internet* [online]. 2014 [cit. 2014-12-12]. Dostupné z: http://maidsafe.net/

[93] PŘISPĚVATELÉ FÓRA. [ANN][XCP] Counterparty - Pioneering Peer-to-Peer Finance - Official Thread. In: *Bitcoin Forum*[online]. 2014 [cit. 2014-12-14]. Dostupné z: https://bitcointalk.org/index.php?topic=395761.0

[94] COUNTERPARTY. *Counterparty* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://counterparty.io/

[95] STERRY, David R. What is Counterparty?. *David R. Sterry's Blog* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://davidsterry.com/blog/2014/10/what-is-counterparty

[96] Comparison of cryptocurrencies. BITCOIN COMMUNITY. *Bitcoin wiki* [online]. 2014, 7.11.2014 [cit. 2014-12-12]. Dostupné z: https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies

[97] CINNICOIN INC. *CinniCoin | The future of cryptocurrency* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://www.cinnicoin.com/

[98] VIACOIN. *Viacoin | The Future of Digital Currency* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://viacoin.org/

[99] CANNABIS COIN. *Cannabis Coin | The Marijuana Bitcoin | Official Canabis Coin* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://cannabiscoin.net/

[100] ZETACOIN.CC & ZBAD305. *Official Home of Zetacoin* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://zetacoin.cc/

[101] IXCOIN. *IXcoin | The First Alternative to Bitcoin. Secured with 7.2 PetaHash/s* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://www.ixcoin.co/

[102] MUNNE. *Home - Munne - A new economy is here* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://munnecoin.com/

[103] IXCOIN PROJECT. *Ixcoin P2P Virtual Currency* [online]. 2011 [cit. 2014-12-14]. Dostupné z: http://ixcoin.org/

[104] PŘISPĚVATELÉ FÓRA. Announcements (Altcoins). In: *Bitcoin Forum* [online]. 2014 [cit. 2014-12-14]. Dostupné z: https://bitcointalk.org/index.php?board=159.0

[105] Cryptocoin LAUNCH Announcements. CRYPTOCOINTALK.COM. *CryptoCoinTalk* [online]. 2014 [cit. 2014-12-14]. Dostupné z: https://cryptocointalk.com/forum/700-cryptocoin-launch-announcements/

[106] CRYPTO COINS TABLE. *Crypto Coins Table - Bitcoin, Litecoin, Peercoin, ...* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://crypto-coins-table.com

[107] PŘISPĚVATELÉ FÓRA. Bitmark. In: *Bitcoin Forum* [online]. 2014 [cit. 2014-12-14]. Dostupné z: https://bitcointalk.org/index.php?topic=660544.0

[108] MEGACOIN. *Megacoin | Tvoje globální peníze* [online]. 2013 [cit. 2014-12-14]. Dostupné z: https://www.megacoin.co.nz/

[109] PŘISPĚVATELÉ FÓRA. 'Nomen est omen' concept in altcoin economic theory. In: *Bitcoin Forum* [online]. 2014 [cit. 2014-12-14]. Dostupné z: https://bitcointalk.org/index.php?topic=655461.0

[110] GILLESPIE, Clay Michael. Charlie Lee: Litecoin's Five Steps to Creating a Successful Altcoin. CRYPTOCOINS NEWS.*Cryptocoins news* [online]. 2014 [cit. 2014-12-14]. Dostupné z: https://www.cryptocoinsnews.com/charlie-lee-litecoins-five-steps-creating-successful-altcoin/

[111] VALIS, Dick. A Name Matters: Cryptocurrency Names and Ratings. ALTCOIN PRESS. *Altcoin Press* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://altcoinpress.com/2014/11/a-name-matters-cryptocurrency-names-and-ratings/

[112] Distribution Remains The Greatest Hurdle For Altcoin Success. ALTCOIN HERALD. *Altcoin Herald* [online]. 2014 [cit. 2014-12-14]. Dostupné z: https://altcoinherald.com/distribution-remains-greatest-hurdle-altcoin-success

[113] TAYLOR, Michael Bedford. *Bitcoin and The Age of Bespoke Silicon* [online]. 2013 [cit. 2014-12-14]. ISBN 978-1-4799-1400-5. Dostupné z: http://cseweb.ucsd.edu/~mbtaylor/papers/bitcoin_taylor_cases_2013.pdf

[114] PŘISPĚVATELÉ FÓRA. The Newbie's Guide to Kimoto's Gravity Well. In: *Megacoin Forum* [online]. 2013 [cit. 2014-12-14]. Dostupné z: https://forum.megacoin.co.nz/index.php?topic=893

[115] MEGACOIN. *Megacoin | Tvoje globální peníze* [online]. 2013 [cit. 2014-12-14]. Dostupné z: https://www.megacoin.co.nz/

[116] LIMER, Eric. The crazy Bitcoin mining rings. THE UNHIVED MIND ARCHIVE 2. *The Unhived Mind Archive 2* [online]. 2013 [cit. 2014-12-14]. Dostupné z: http://theunhivedmind.com/wordpress2/the-crazy-bitcoin-mining-rigs/

[117] HRUSKA, Joel. Massive surge in Litecoin mining leads to graphics card shortage. ZIFF DAVIS, LLC. *ExtremeTech*[online]. 2013 [cit. 2014-12-14]. Dostupné z: http://www.extremetech.com/computing/172381-massive-surge-in-litecoin-mining-leads-to-radeon-shortage

[118] Why a GPU mines faster than a CPU. BITCOIN COMMUNITY. *Bitcoin Wiki* [online]. 2011, 8.1. 2013 [cit. 2014-12-14]. Dostupné z: https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU

[119] Mining. BITCOIN COMMUNITY. *Bitcoin Wiki* [online]. 2011, 10.10.2014 [cit. 2014-12-14]. Dostupné z: https://en.bitcoin.it/wiki/Mining

[120] ZEUS INTEGRATED SYSTEMS LIMITED. *Zeusminer (Scrypt) ASIC Miner* [online]. 2014 [cit. 2014-12-14]. Dostupné z: https://zeusminer.com/

[121] BUTTERFLY LABS INC. *Bitcoin Mining Hardware - ASIC Bitcoin Miner - Butterfly Labs* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://www.butterflylabs.com/

[122] Mining hardware comparison. BITCOIN COMMUNITY. *Bitcoin Wiki* [online]. 2011, 10.10.2014 [cit. 2014-12-14]. Dostupné z: https://en.bitcoin.it/wiki/Mining_hardware_comparison

[123] Non-specialized hardware comparison. BITCOIN COMMUNITY. *Bitcoin Wiki* [online]. 2011, 10.10.2014 [cit. 2014-12-14]. Dostupné z: https://en.bitcoin.it/wiki/Non-specialized_hardware_comparison

[124] PŘISPĚVATELÉ FÓRA. [ANN] cudaMiner & ccMiner CUDA based mining applications [Windows/Linux/MacOSX]. In: *Bitcoin Forum* [online]. 2013 [cit. 2014-12-14]. Dostupné z: https://bitcointalk.org/index.php?topic=167229.0

[125] PŘISPĚVATELÉ FÓRA. OFFICIAL CGMINER mining software thread for linux/win/osx/mips/arm/r-pi 4.8.0. In: *Bitcoin Forum* [online]. 2011 [cit. 2014-12-14]. Dostupné z: https://bitcointalk.org/index.php?topic=28402.0

[126] PŘISPĚVATELÉ FÓRA. An (even more) optimized version of cpuminer (pooler's cpuminer, CPU-only). In: *Bitcoin Forum*[online]. 2011 [cit. 2014-12-14]. Dostupné z: https://bitcointalk.org/index.php?topic=55038.0

[127] Solo mining, pool mining and Multi pool mining. COIN RAMBLE. *Coin Ramble* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://coinramble.com/?p=3

[128] Cloud Mining - How to Mine Bitcoin without a Miner. COINDESK. *CoinDesk* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://www.coindesk.com/information/cloud-mining-bitcoin-guide/

[129] BLOCKCHAIN.INFO. *Bitcoin Block Explorer - Blockchain.info* [online]. 2014 [cit. 2014-12-15]. Dostupné z: https://blockchain.info/

[130] NICEHASH.COM. *NiceHash* [online]. 2014 [cit. 2014-12-14]. Dostupné z: https://www.nicehash.com/

[131] Software. NICEHASH.COM. *NiceHash* [online]. 2014 [cit. 2014-12-15]. Dostupné z: https://www.nicehash.com/index.jsp?p=software

[132] Before you start - NiceHash and WestHash. NICEHASH.COM. *NiceHash* [online]. 2014 [cit. 2014-12-15]. Dostupné z: https://www.nicehash.com/?p=gstarted

[133] *CoinWarz* [online]. 2014. vyd. 2013 [cit. 2014-12-15]. Dostupné z: http://www.coinwarz.com/cryptocurrency

Seznam obrázků a tabulek

Seznam obrázků

Obrázek č. 1 Tvorba Bitcoinové adresy z veřejného klíče a klíče privátního. Zdroj: (32) ... 12
Obrázek č. 2 Princip tvorby transakcí. Zdroj: (str.6, 23) ... 14
Obrázek č. 3 Celkový počet bitcoinových mincí v závislosti na čase. Zdroj: (32) ... 21
Obrázek č. 4 Velikost tržní kapitalizace různých kryptoměn v USD Zdroj: (26) ... 29
Obrázek č. 5 Poměr množství zobchodovaných bitcoinů. Zdroj: (22) ... 31
Obrázek č. 6 Vývoj výpočetního výkonu a náročnosti těžby u bitcoinu. Zdroj: (60) ... 53
Obrázek č. 7 Vývoj ceny bitcoinu a náročnosti těžby. Zdroj: (str. 7, 113) ... 54
Obrázek č. 8 Těžební zařízení s grafickými kartami. Zdroj: (str. 6-7, 117) ... 55
Obrázek č. 9 Těžební zařízení typu FPGA. Zdroj: (115) ... 56
Obrázek č. 10 Ukázka zařízení typu ASIC. Zdroj: (121) ... 57
Obrázek č. 11 Bitcon peněženka na serveru Blockchain.info. Zdroj:(129) ... 64
Obrázek č. 12 Aplikace SGminer po jeho úspěšném spuštění. Zdroj: (Autor) ... 65
Obrázek č. 13 Aplikace SGminer při těžbě. Zdroj: (Autor) ... 67
Obrázek č. 14 Aplikace SGminer při úspěšné těžbě. Zdroj: (Autor) ... 69
Obrázek č. 15 Měřič spotřeby elekrické energie značky Silvercrest. Zdroj: (Autor) ... 70

Seznam tabulek

Tabulka č. 1 Obchodované kryptoměnové páry Zdroj: (60) ... 28
Tabulka č. 2 Pořadí padesáti kryptoměn podle jejich tržní kapitalizace. Zdroj: (26) ... 30
Tabulka č. 3 Pořadí kryptoměn v rozlišení na těžitelné a netěžitelné. Zdroj: (26) ... 30
Tabulka č. 4 Nejaktivnější směnárny za posledních 30 dní. Zdroj: (59) ... 31
Tabulka č. 5 Tabulka dalších altcoinů výraznou technickou inovací. Zdroj: (Autor) ... 40
Tabulka č. 6 Další alternativní kryptoměny typické výrazným brandigem. Zdroj: (Autor) ... 41
Tabulka č. 7 Složení hlavičky bloku. Zdroj: (32) ... 52
Tabulka č. 8 Podporované těžební algoritmy službou NiceHash. Zdroj: (133) ... 66
Tabulka č. 9 Naměřené hodnoty výkonu a spotřeby. Zdroj: (Autor) ... 71
Tabulka č. 10 Výnosnost těžby podle CoinWarz.com. Zdroj: (133) ... 72

Přílohy

Příloha 1 – Systémové informace

Příloha 2 – Verze grafického ovladače

Příloha 1 - Systémové informace

Název operačního systému	Microsoft Windows 8.1 Pro
Verze	6.3.9600 Sestavení 9600
Další popis operačního systému	Není k dispozici
Výrobce operačního systému	Microsoft Corporation
Název systému	RAJBA
Výrobce systému	Gigabyte Technology Co., Ltd.
Model systému	Z87-HD3
Typ systému	x64-based PC
SKU systému	To be filled by O.E.M.
Procesor	Intel(R) Core(TM) i5-4670K CPU @ 3.40GHz, 3401 Mhz, jádra: 4, logické procesory: 4
Verze systému BIOS/Datum	American Megatrends Inc. F6, 3. 8. 2013
Verze SMBIOS	2.7
Verze integrovaného řadiče	255.255
Režim systému BIOS	Starší verze
Výrobce základní desky	Gigabyte Technology Co., Ltd.
Model základní desky	Není k dispozici
Název základní desky	Základní deska
Role platformy	Desktop
Stav zabezpečeného spouštění	Nepodporováno
Konfigurace PCR7	Vazba není možná
Adresář systému Windows	C:\Windows
Systémový adresář	C:\Windows\system32
Spouštěcí zařízení	\Device\HarddiskVolume1
Národní prostředí	Česká republika
Vrstva HAL (Hardware Abstraction Layer)	Verze = "6.3.9600.17196"
Uživatelské jméno	Rajba\Raj
Časové pásmo	Střední Evropa (běžný čas)
Nainstalovaná fyzická paměť (RAM)	8,00 GB
Celková fyzická paměť	7,89 GB
Volná fyzická paměť	3,38 GB
Celková virtuální paměť	15,9 GB
Volná virtuální paměť	10,0 GB
Prostor stránkovacího souboru	8,00 GB
Stránkovací soubor	D:\pagefile.sys

Příloha 2 Verze grafického ovladače