ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická
Katedra ekonomiky, manažerství a humanitních věd

Energetická náročnost a ekonomické zhodnocení těžby kryptoměn

Energy consumption and economic appraisal of cryptocurrency mining

Diplomová práce

Studijní program: Elektrotechnika, energetika a management
Studijní obor: Ekonomika a řízení elektrotechniky

Vedoucí práce: Ing. Martin Dobiáš, Ph.D.

Bc. Ondřej Malý

Praha 2018

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Malý** Jméno: **Ondřej** Osobní číslo: **420165**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra ekonomiky, manažerství a humanitních věd**

Studijní program: **Elektrotechnika, energetika a management**

Studijní obor: **Ekonomika a řízení elektrotechniky**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Energetická náročnost a ekonomické zhodnocení těžby kryptoměn

Název diplomové práce anglicky:

Energy consumption and economic appraisal of cryptocurrency mining

Pokyny pro vypracování:

- Popište kryptoměny - historie, současný stav, očekávaný vývoj
- Charakterizujte proces těžby kryptoměn a jeho energetickou náročnost
- Analyzujte proces směny a obchodování s krypotměnami
- Pro konkrétní zadání proveďte ekonomickou analýzu těžby

Seznam doporučené literatury:

NORMAN, Alan T. Cryptocurrency mining: The ultimate guide to understanding Bitcoin, Ethereum, Litecoin, Monero, Zcash mining technologies. 2017.
CAUGHEY, Michael. Bitcoin Mining Step by Step. Amazon Digital Services, 2013.
WHITE, Abraham K. Cryptocurrency: Mining, Investing and Trading in Blockchain, including Bitcoin, Ethereum, Litecoin, Ripple, Dash and others. Amazon Digital Services, 2017.

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Martin Dobiáš, Ph.D., katedra ekonomiky, manažerství a humanitních věd FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **08.10.2018** Termín odevzdání diplomové práce: **08.01.2019**

Platnost zadání diplomové práce: **20.09.2020**

Ing. Martin Dobiáš, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

Datum převzetí zadání Podpis studenta

 © ČVUT v Praze, Design: ČVUT v Praze, VIC

Abstrakt

Tato práce poskytuje ucelený pohled na problematiku kryptoměn. Největší pozornost je přitom věnována jejich těžbě a problematice s ní spojenou. Rešerše obsahuje tři části, ve kterých je vysvětlen princip kryptoměn, popsán obchod s nimi a představena těžba virtuálních měn včetně jejích dopadů na životní prostředí. V práci je kladen důraz na vysvětlení důležitých spojitostí, jejichž znalost je klíčová ke správné analýze situace a učinění uváženého ekonomického rozhodnutí. Na tyto poznatky navazuje ekonomické zhodnocení těžby Bitcoinu. To vychází z vlastní navržené metodiky, aktuálně dostupných technologií a předpokládaného vývoje v oblasti kryptoměn. Výsledky jsou následně zhodnoceny z pohledu postoje rozhodovatele k riziku podle jeho osobního odhadu na vývoj ceny. Dále je těžba porovnána s alternativní investicí, kterou je nákup kryptoměn.

Klíčová slova

Bitcoin, kryptoměny, těžba kryptoměn, ekonomické zhodnocení, obtížnost těžby, cena kryptoměn, ASIC, čistá současná hodnota, spotřeba elektrické energie

Abstract

This diploma thesis provides a comprehensive view of issues connected with cryptocurrencies, while the most attention is paid to cryptocurrency mining. The research deals with both technical aspects of mining and states of affairs, which must be known before doing proper analysis and economic decision. The economic appraisal is based on these findings, using own-designed methodology and considering current situation, available technologies and assumptions of the future evolution. The results are then evaluated from the point of view of the risk-maker's attitude and his personal estimate of price development. Finally, cryptocurrency mining is compared with an alternative, that is purchasing cryptocurrencies instead of minig it.

Keywords

Bitcoin, cryptocurrencies, cryptocurrency mining, economic appraisal, mining difficulty, cryptocurrency price, ASIC, net present value, energy consumption

Poděkování

Děkuji tímto vedoucímu diplomové práce panu Ing. Martinu Dobiášovi, Ph.D. za ochotu, odborné vedení, konzultace, cenný čas a návrhy, které mi poskytl při tvorbě práce. Rád bych tímto vyjádřil i dík vyučujícím, z jejihž strany jsem při studiu vždy cítil podporu a vůli pomáhat. Můj velký dík patří rovněž škole ČVUT, na které jsem získal vědomosti potřebné k vytvoření práce a která poskytla mi možnost studovat v zahraničí, na což nikdy nezapomenu.

V Praze dne 4. 1. 2019 . . . . . .

(podpis autora)

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a v souladu s Metodickým pokynem o dodržování etických principů pro vypracování závěrečných prací, a že jsem uvedl všechny použité informační zdroje.

V Praze dne 4. 1. 2019 . . . . . .

(podpis autora)

Obsah

Seznam pojmů a zkratek

Zkratka	Pojem	Vysvětlení
BTC	Bitcoin	Referenční, první a největší kryptoměna
P2P	Peer-to-peer	Označení typu počítačových sítí, ve kterém jsou si všechny uzly rovnocenné a jednotliví klienti spolu komunikují přímo bez existence centrálního uzlu – serveru
LN	Lightning network	Vylepšení sítě zajišťující bleskové transakce
PoW	Proof-of-work	Způsob, kterým uživatel platebního systému dokazuje hodnotu platebního prostředku pomocí vynaložené práce
PoS	Proof-of-stake	Způsob, kterým uživatel platebního systému dokazuje hodnotu platebního prostředku pomocí vlastnictví měny
ASIC	Application Specific Integrated Circuit	Zařízení používané k těžbě kryptoměn, u nichž ověření transakcí vyžaduje velké množství výpočetního výkonu
FPGA	Field Programmable Gate Array	Programovatelná hradlová pole
SHA 256	-	Těžební algoritmus, který používá Bitcoin
PH, TH	Petahash, Terahash	10^{15}, 10^{12} hashů za sekundu
NPV	Net present value	Čistá současná hodnota – metoda hodnocení investic
S1	Strategie 1	Strategie okamžitého prodeje v této práci
S2	Strategie 2	Strategie kumulování kryptoměny v této práci
p.a.	Per annum	Z latiny – roční, za rok. U úvěru i vkladu značí úrok za jeden rok.
	Hashrate	Počet pokusů za sekundu, kterou je těžební soustava schopna provést; základní parametr pro výběr těžebního vybavení
	Decentralizace	Stav, ve kterém v síti neexistuje žádný nadřazený řídící uzel
	Kryptografie	Nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí
	Altcoin	Alternativní měna; kryptoměna jiná než Bitcoin
	Blockchain	Druh decentralizované databáze, kde jsou záznamy chráněny proti neoprávněnému zásahu jak z vnější strany, tak i ze strany samotných uzlů peer-to-peer sítě
	Pool	Skupina spolupracujících těžařů za účelem zpravidelnění zisků
	Fork	Oddělení od původní měny, lišící se ve změně, kvůli které došlo k odtržení. Vznikne při neshodě uživatelů.
	Fiat money	Peníze s nuceným oběhem (oběh vynucuje stát)
	Miner	Zařízení určené k těžbě kryptoměn nebo člověk těžař

Seznam obrázků

Seznam tabulek

1 Úvod

Kryptoměny, neboli elektronické či digitální peníze, zaznamenaly v posledních letech obrovský rozmach, především díky referenční měně Bitcoin. Zatímco počátkem roku 2014 Bitcoin neznalo téměř 60 % Američanů [1], dnes bychom už stěží hledali někoho, kdo o tomto fenoménu neslyšel. Může za to především rok 2017, během kterého se celková tržní kapitalizace kryptoměn znásobila více než třicetkrát. [2] Po vlně mediální pozornosti došlo k obrovskému přílivu investorů z řad veřejnosti. K dočtení byly příběhy o lidech, kteří na raketovém růstu cen kryptoměn vydělali miliony. Jelikož však tyto peníze musel někdo zaplatit, existují i lidé, kteří kvůli neuvážené investici ztratili doslova střechu nad hlavou. Mnoho těchto lidí pravděpodobně své peníze investovalo, aniž by věděli, co nebo kdo za kryptoměnami stojí, jak vůbec fungují a jaká rizika s sebou nesou.

Základní myšlenkou první kryptoměny – Bitcoinu je nepřítomnost finanční instituce, tedy třetí strany, kterou v případě dnes používaných peněz představují banky. Výsledkem je jeho decentralizace. To ve stručnosti znamená, že nemůže být nikým ovládán, ovlivňován, ani kontrolován. Na rozdíl od tradičních měn jsou kryptoměny jsou zcela virtuální a neexistují tedy žádné fyzické mince či bankovky. Vše jsou jen čísla kolující po internetu. Jejich hodnota není ničím krytá a cena je tak závislá výhradně na poptávce a nabídce. K obchodu s kryptoměnami dochází na k tomu určených burzách a ve směnárnách. Jejich uchování potom v k tomu určených peněženkách.

Investice do kryptoměn však není jediným způsobem, jak se lze na těchto měnách profitovat. Celý chod sítě zajišťují takzvaní těžaři. Jsou to lidé, kteří za určitou odměnu propůjčují výkon svého počítače k fungování sítě. Touto odměnou je kryptoměna, kterou daný těžař těží. Proces těžby většiny kryptoměn je založen na podobném principu, jako je skutečná těžba např. drahých kovů. Dopředu je známo nějaké konečné množství konkrétní kryptoměny, která se během času uvolňuje. Při vzniku měny je jí k vytěžení velké množství, které se však postupně zmenšuje, jak její zásoby docházejí. Při dosažení předem určeného data je kryptoměna vytěžena úplně a nikdy už ji víc nebude. Jelikož je množství uvolňované kryptoměny předem dáno, zvyšuje se s výkonem moderních technologií i náročnost těžby, aby poměr zůstal zachován. Těžba kryptoměn je proto nesmírně energeticky náročná. Pokud tak investor uvažuje o těžbě kryptoměn za účelem dosažení zisku, je cena elektrické energie klíčovým parametrem. Tím dalším může být volba použité technologie. Použití klasického procesoru v běžném PC už totiž se zvyšující se náročností nemusí být dostačující. Proto se dnes používají těžební sestavy z grafických karet, programovatelná hradlová pole FPGA nebo mikročipy ASIC. Ty jsou navržené speciálně za účelem těžby kryptoměn.

Nesmírně důležitý je také výběr samotné kryptoměny. V současnosti existuje kromě Bitcoinu obrovské množství takzvaných Altcoinů, lišících se zcela zásadně nebo jen v nepatrných detailech, jako je např.

název měny. Kryptoměnu dnes může velice jednoduše vytvořit každý, jelikož k tomu existují krom podrobných návodů i aplikace. O kvalitě a přínosnosti velkého množství takových elektronických peněz může být sporu a těžba nebo investice do nich by se nemusela finančně vyplatit. Pokud se však autorovi povede produkt dobře propagovat a investoři ho kupují, cena strmě stoupá. To se v minulosti již mnohokrát stalo. Výběr kryptoměny tak může být největším oříškem. Je totiž možné, že i neinovativní a prakticky nepoužitelné měny se mohou na čas dostat na výsluní, zatímco ty s velkým potenciálem zůstat navždy zapomenuty.

O kryptoměny jsem se začal zajímat v roce 2016 během studií v Asii, kde jsou kryptoměny obecně velmi populární. Rozhodl jsem se zkusit do nich investovat, zjistil jsem však, že nevím, kde začít. Nevěděl jsem, kterou kryptoměnu si vybrat, kde ji nakoupit abych se vyhnul vysokým poplatkům, ani kde ji bezpečně uchovat. Před mým prvním nákupem jsem proto strávil hodiny rešerší a vyhledáváním informací. Těch je na internetu sice již poměrně velké množství, většinou ale jeden zdroj poskytuje jen určitou část problematiky. Ne všechny zdroje jsou navíc důvěryhodné. Uvědomil jsem si, že přestože jsou kryptoměny velkým fenoménem, je tato bariéra pro mnoho potencionálních investorů velkou překážkou. Nemusí mít totiž čas, chuť, ani schopnosti tyto informace vyhledávat. Formou internetového inzerátu jsem proto nabídl pomoc a několik zájemců se skutečně ozvalo. Během rozhovoru se přirozeně zajímali i o věci, které jsem nevěděl. Patřili k nim záležitosti spojené s těžbou kryptoměn, návratností investice do ní a parametrech, na nichž závisí. To mě dovedlo k rozhodnutí věnovat se této nové problematice do větší hloubky a vytvořit dokument, který by potenciálním těžařům pomohl v jejich začátcích.

Cílem této práce je proto především poskytnutí *uceleného pohledu* na problematiku kryptoměn. Předmětem nebude pouze co, ale také proč, jak a za kolik. Poskytnuté informace nebudou propagovat konkrétní kryptoměnu, ani nikoho nabádat k určitým investičním krokům. Aktuální situace se navíc v tomto odvětví mění tak rychle, že by za několik málo měsíců či let stejně nebyly použitelné. Pokusím se proto hlavně srozumitelně popsat neměnné principy, na kterých kryptoměny stojí, a jakým směrem lze očekávat jejich vývoj.

Ze stejného důvodu se při ekonomickém zhodnocení nebudu zaměřovat na nalezení nejvýhodnější varianty současnosti. Pokud by se situace neměnila, těžba se v současnosti z ekonomického pohledu s největší pravděpodobností nevyplatí. To je ale možné zjistit prostým zadáním aktuálních hodnot do internetové kalkulačky. Všechny parametry ale konstantní nejsou a během těžby se neustále mění. Místo toho v této práci popíšu, jak by se tyto parametry musely měnit, aby se těžba z ekonomického pohledu vyplatila. Poté zhodnotím, zda je tento vývoj vůbec reálný. Pro každého čtenáře pak bude možné dosadit vstupní parametry podle aktuální situace a rozhodnout se dle svého osobního očekávání na vývoj situace. Třeba tak jednou práce usnadní něcí investičním rozhodnutí.

2 Princip a vývoj kryptoměn

Na úvod je nutné podotknout, že pojmy kryptoměna a Bitcoin byly na počátku jejich existence velmi dobře zaměnitelné. Bitcoin je skutečně první kryptoměnou, průkopníkem, na jehož základech vznikla naprostá většina ostatních kryptoměn, neboť jeho zdrojový kód je od začátku veřejný. Tyto následovníci jsou označovány jako Altcoiny. K vysvětlení principu kryptoměn tedy použiji Bitcoin, který přišel s novou, inovativní myšlenkou. Ostatní kryptoměny se už jen v lepším případě snaží tuto myšlenku posunout dále nějakým vylepšením nebo odstraněním nedostatků. V tom horším se pak pouze snaží přiživit na jeho popularitě a nic nového nepřinášejí.

2.1 Jak funguje Bitcoin

Bitcoin byl představen v roce 2008 jako čistě peer-to-peer[1] verze elektronických peněz, které umožňují, aby online platby byly posílány přímo mezi dvěma stranami bez průchodu finanční institucí. [3] V případě dnes používaného systému papírových peněz jsou touto třetí stranou banky. Ty zajišťují, aby nedocházelo k podvodům a padělání. Banky bojují s problémem padělatelství tak, že zavádí neustále těžko napodobitelnější způsoby výroby papíru a metod tisku. Tento problém Bitcoin řešit nemusí, neboť představuje měnu čistě digitální. I klasické peníze bývají ale stále častěji uloženy a přenášeny digitálně. Tím vzniká riziko, že by byla měna zároveň utracena na více místech najednou. S dvojitým utrácením se v případě peněz vypořádávají centrální autority, které mají přehled o měně v oběhu, vlastnících účtů i o jejich zůstatcích. V případě Bitcoinu, kde chod žádná třetí strana nekontroluje, je tento problém vyřešen vytvořením tzv. blockchainu. [4]

Blockchain si lze představit jako účetní knihu, ve které jsou v blocích[2] zaznamenané všechny transakce, které kdy od vzniku Bitcoinu proběhly. Tento seznam je veřejný, a kdokoli tak může sledovat, odkud a kam každá transakce jde. Na počátku byly všechny Bitcoiny na jedné adrese. Ta může být považována za alternativu bankovního účtu. Postupem času se měna začala šířit na další a další adresy, jak si ji jednotliví uživatelé sítě posílali až do stavu, ve kterém je dnes. Pokud má tedy některý uživatel sítě zaplatit Bitcoiny, je možné v blockchainu zpětně dohledat, jestli tyto prostředky opravdu někdy nabyl a jestli s nimi ještě nezaplatil na jinou adresu. [5]

Bitcoinové adresy jsou anonymní, což prakticky znamená, že systém funguje naopak než u bankovních účtů. U bankovních účtu jsou jejich vlastníci veřejně známí, nikdo ale nevidí, jak se svými prostředky

[1]Peer-to-peer je označení typu počítačových sítí, ve kterém jsou si všechny uzly rovnocenné a jednotliví klienti spolu komunikují přímo bez existence centrálního uzlu – serveru. [5]

[2] Blok je skupina několika transakcí

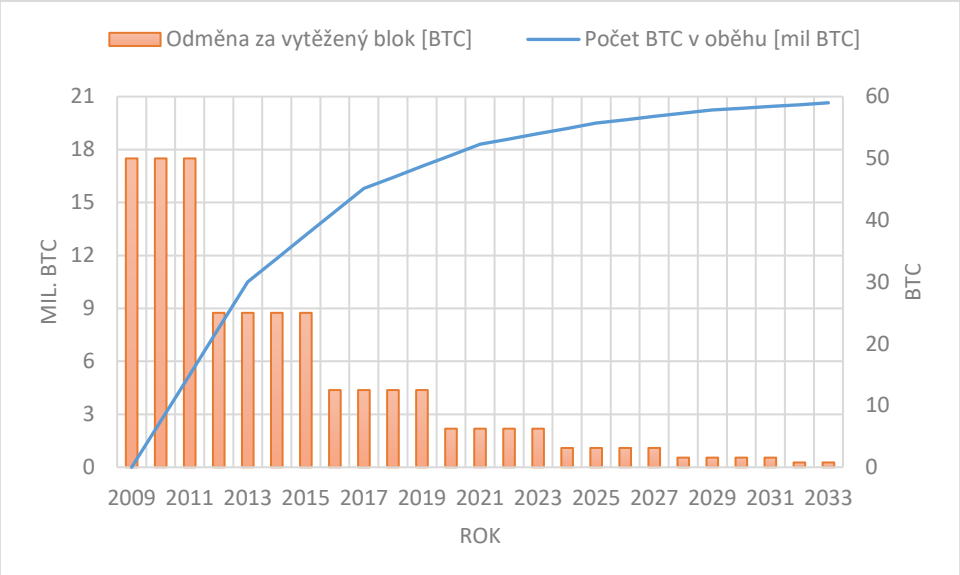
hospodaří. U Bitcoinových adres naopak nikdo neví, komu patří. Všichni ale mohou vidět, jaké transakce na nich probíhají. V praxi je k vytvoření účtu a získání adresy většinou potřeba registrace a prokázání se platným dokladem, což brání využívání kryptoměn pro trestnou činnost. V případě podezření je tak možné majitele adres dohledat.

Jak bylo naznačeno, díky blockchainu je tento systém elektronických plateb založen na důkazu, nikoliv na důvěře. [3] Zde by mohla vyvstat otázka kdo, když ne nadřazená třetí strana, tento důkaz přinese a proč. Tento úkol na sebe berou tzv. těžaři. Jsou to lidé, kteří za odměnu propůjčují výkon svého počítače k ověřování transakcí a tím k fungování sítě. Tento proces se nazývá těžba (4). Těžaři se snaží do blockchainu zanést nový soubor transakcí, jejichž správnost ověřili strojově náročným výpočtem. Transakce jsou shlukovány do bloků, které požadují vysoké množství výpočtů pro jeho správné vytvoření. Potřebují ale pouze malé množství výpočtů pro ověření jeho správnosti. Těžař, kterému se podaří blok vytvořit, získá určitý počet Bitcoinů jako odměnu. Protože je šance na vyřešení problému jako první nesmírně malá, těžaři by čekali na odměnu i několik let. Proto se sdružují do větších celků, kterým se říká pooly. Pokud jeden z počítačů v poolu vyřeší problém, rozdělí si odměnu všichni těžaři v poolu podle výkonu (hashrate)[3], který skupině poskytli. Ostatní těžaři v síti pak lehce ověří správnost nově vytvořeného bloku, tento blok akceptují jako součást historie transakcí a celý proces začne nanovo. [4]

Tímto způsobem se měna stává decentralizovanou – neexistuje zde žádný centrální bod, který by byl klíčový k chodu sítě. To je důležitá vlastnost pro odolání proti zásahům protivníku, ať již jde o pokus o regulaci zásahem legálních vlád nebo o útok kriminálních živlů. Útoky totiž nejsou kam zaměřit. [4]

Obtížnost výpočtů je nastavená tak, aby k nalezení řešení došlo průměrně jednou za deset minut. Pokud se to podaří rychleji nebo naopak pomaleji, obtížnost se upraví tak, aby tento čas zůstal zachován. Počet uvolňovaných Bitcoinů i časový interval uvolnění je znám. Je tak velmi jednoduše spočítatelné, kolik Bitcoinů je v oběhu a jestli jejich počet sedí. [5] Odměna za získání Bitcoinu se snižuje na polovinu zhruba každé čtyři roky. Díky tomu je přesně možné určit, kdy bude kolik jednotek měny vytěženo, i kdy budou zásoby vyčerpány. Předpokládaný počet Bitcoinů v oběhu a odměny za vytěžený blok v čase znázorňuje obrázek 1.

[3] *Počet pokusů za sekundu, kterou je těžební soustava schopna provést, se označuje jako hashrate a je to základní parametr pro výběr těžebního vybavení.*



Obrázek 1) Počet Bitcoinů v oběhu v čase [6]

Celkový počet Bitcoinů, který kdy bude v oběhu, je stanoven na 21 milionů. Jejich úplné vytěžení se předpokládá v roce 2140. V současnosti je jeden Bitcoin dělitelný na osm desetinných míst, přičemž nejmenší jednotka se nazývá satoshi. Jelikož se počet uvolňovaných Bitcoinů bude půlit až do uvolnění posledního satoshi, ke konci se bude uvolňovat jen velmi malé množství Bitcoinů. Proto dojde k vytěžení drtivé většiny měny už kolem roku 2033. [7] Na rozdíl od peněz, kterých banky mohou natisknout neomezené množství, je tak Bitcoin měnou deflační. To znamená, že by měl postupem času zvyšovat svou hodnotu. [5] Až budou veškeré Bitcoiny vytěženy, budou odměnou pro těžaře pouze transakční poplatky, které uživatelé sítě platí za provedení každé transakce.

Představil jsem základní vlastnosti a parametry první kryptoměny Bitcoinu. Ostatních Altcoinů už dnes existuje takové množství, že je prakticky nemožné všechny třeba jen zmínit. Často ale fungují na podobném principu, pouze se změnou některých parametrů. Těmi jsou např. druh použité metody k ověření transakcí, maximální počet mincí v oběhu, rychlost vytváření nového bloku, výše těžební odměny, způsob kalkulace náročnosti těžby, anonymita, přidání nové funkcionality, jméno měny či těžební algoritmus. Algoritmus je faktorem, který určuje, jestli těžba měny potřebuje výpočetní výkon, operační paměť nebo jiný parametr. [8] Některým z těchto alternativních kryptoměn, které přinášejí inovativní nebo zajímavé vylepšení, se budu věnovat v dalších kapitolách.

2.2 Historie kryptoměn

Historie digitálních měn není příliš dlouhá. První pokusy o jejich vytvoření přišly koncem 80. let minulého století, kdy začala být šířeji dostupná a srozumitelná kryptografie, tedy nauka o šifrování. [4]

Kryptografie se zabývá metodami a technikami zabezpečené komunikace za účasti třetí strany, se kterou však nechceme sdílet obsah. Jejím základním cílem je zašifrování určité zprávy do nečitelného textu, který je následně možné rozšifrovat pouze pomocí určitého klíče. Klíč je návodem ke zjištění, jakým způsobem má být zpráva transformována do výsledného zašifrovaného textu. Prostřednictvím kryptografie je u kryptoměn zabráněno pokusům o podvod, jako jsou například realizace fiktivních transakcí či dvojité platby stejnými prostředky. U digitálních měn si totiž peníze můžeme představit jako data, která je možné zkopírovat a odeslat dvěma lidem zároveň. Určení pravosti takové transakce je možné právě díky šifrování. [8]

2.2.1 Měny před Bitcoinem

První velkou digitální měnou historie byla měna E-cash, vytvořená kryptografem Davidem Chaumem, přezdívaném otec digitálních měn. V roce 1982 představil kryptografický systém pro anonymní transakce a v roce 1990 ho uvedl do provozu právě pod názvem E-cash. Jeho systém nebyl určen pro nahrazení celého peněžního systému, ale přišel pouze s alternativou k současným peněžním mikro transakcím, které považoval za složité a nedostatečně anonymní. O několik let později však vyhlásil bankrot. K tomu byl nucen možná právě kvůli tomu, že požadoval příliš anonymity pro uživatele a nepodařilo se mu tak vtáhnout do své měny státní peníze. [5]

Brzy začaly vznikat další měny. Mnoho z nich skončilo velmi neslavně a ukazují, proč se pravděpodobně autor Bitcoinu nikdy ke svému brilantnímu nápadu nepřihlásí. Ukázalo se totiž, že není možné vytvořit konkurenci státním penězům bez toho, aby autor neskončil jako obžalovaný u soudu. Skončili tak například autoři digitální měny E-gold. Ta byla krytá skutečným zlatem, které společnost nakupovala a skladovala. Bylo tak známo její sídlo i tvůrci a pro vládu nebyl velký problém tento projekt zarazit. Podobně dopadl i tvůrce Liberty Dolaru. Ten si všiml, že americké dolary nejsou již desítky let ničím kryté a nemají stanovený limit zásob. Vytvořil proto alternativní peníze kryté drahým kovem. Obžaloba tvrdila, že se autor snažil zničit měnu vlastní země a byl odsouzen za padělání peněz a terorismus. [5]

Autor digitální měny Liberty Reserve byl pro změnu odsouzen za praní špinavých peněz, když mu byla společnost v roce 2013 zabavena. Šlo přitom o nejstarší existující digitální měnu, jelikož vznikla již v roce 2001. Její pointou bylo znovu ukládání peněz do zlata, ale také do dolaru či eura. Digitální měny přesto nepřestaly být populární a o jejich zavedení se pokoušely i velké firmy jako jsou Visa nebo

MasterCard. Visa přišla s vlastním konceptem Visa Cash a MasterCard zakoupil elektronický peněžní systém Mondex. Tyto platební systémy se ale neukázaly jako životaschopné, brzy skončily a obě společnosti se nadále soustředily na tradiční bankovnictví. [5]

Tyto příběhy jasně ukázaly, že pokud má být některá digitální měna úspěšná, nesmí být centralizovaná. Zároveň však muselo docházet k zabezpečení celé sítě i bez pomoci tohoto centra. Tento problém vyřešil až příchod Bitcoinu a s ním technologie blockchain.

2.2.2 Příchod Bitcoinu

První zmínka o Bitcoinu se objevila v říjnu roku 2008 v článku „Bitcoin: A Peer-to-Peer Electronic Cash System" sepsaný autorem vystupujícím pod jménem Satoshi Nakamoto. Tento dokument popisuje Bitcoin jako elektronickou měnu založenou na důkazu prací, jeho výhody i princip funkce. [3] I přes obrovský úspěch kryptoměny a mediální zájem Satoshi Nakamoto nikdy neodhalil svou totožnost, čemuž se po osudu jeho předchůdců nemůže nikdo divit. Tento tvůrce nebo i skupina tvůrců předal krátce po rozšíření Bitcoinu internetovou doménu vývojářům projektu a nemá tak nad Bitcoinem žádnou moc. Stejně jako nikdo jiný, díky jeho decentralizaci. [5]

Bitcoin jako takový existoval od počátku roku 2009. Aby se ale stal platidlem, musel být nejprve někdo ochotný nabídnout za něj své zboží nebo službu. K tomu došlo až v květnu 2010, kdy se na internetovém fóru objevila nabídka na zaplacení 10 000 BTC za dvě pizzy. Trvalo to čtyři dny a první platba kryptoměnou byla na světě. Zpráva o transakci v Bitcoinech se internetem rozšířila velmi rychle. Díky ní se s Bitcoinem seznámilo velké množství nadšenců, inovátorů i autorů konkurenčních digitálních měn. Ještě v tomtéž roce došlo k mnohým zásadním zlomům. Byla založena jedna z největších burz obchodujících Bitcoin – Mt.Gox. Uskutečnila se první půjčka a první transakce mezi telefony. Objevila se bitcoinová opce, vzniknul první těžební pool a státy také poprvé varovaly před touto decentralizovanou měnou. Dle jejich zprávy lze tuto měnu efektivně využívat k financování terorismu. Na počátku roku 2011 dosáhl Bitcoin parity s americkým dolarem a jeho tržní kapitalizace překročila jeden milion USD. Tyto zprávy způsobily, že se o Bitcoin nezajímali již pouze nadšenci, ale začali ho akceptovat i prví e-shopy. S popularitou přišly také první krádeže, jako například napadení burzy Mt.Gox. Při té byly odcizeny stovky tisíc Bitcoinů. [5] Podobné krádeže jsou možné zejména proto, že si lidé nechávají své prostředky uložené na burzách chráněné slabými hesly. Pokud dojde k ukradení informací o uživatelských jménech, e-mailových adresách a zašifrovaných heslech, je možné je snadno rozklíčovat a účty vykrást.

Dalším významným krokem k propagaci kryptoměn bylo v roce 2012 oznámení možnosti nákupu placených funkcí pomocí Bitcoinu na jednom z nejpoužívanějších redakčních systému na světě, webu

WordPress.com. Po tomto velikánovi se začali přidávat další obchodníci jako restaurace, lékaři, právníci, první taxi služby i větší obchody s různým fyzickým zbožím. Pro ty, kteří s Bitcoinem nechtěli spekulovat nebo ho nechtěli vlastnit, byla založena společnost Bitpay.com. Ta na stránkách zákazníka vygeneruje jednoduché prostředí, které umožňuje platby v BTC dle kurzu v daný okamžik. Bitcoiny pak převede do peněženky serveru BitPay, který vám obratem zašle na bankovní účet peníze. I tato služba udělala Bitcoin zas o něco dostupnější. [5]

Vznikaly však také ilegální servery umožňující nákup za Bitcoiny, jako například server Silk Road. Ten nabízel na deset tisíc ilegálních produktů, hlavně drog. Když byl v roce 2013 dopaden jeho provozovatel, vypočítala FBI dvouleté tržby tohoto serveru na více než miliardu amerických dolarů. Stále více se tak ukazovalo, že Bitcoin funguje v reálném světě. Vznikaly první knihy, časopisy a pořady. To s sebou přinášelo jak dobré, tak špatné zprávy, které významně ovlivňovaly cenu Bitcoinu. Ta tak kolísala jako na horské dráze. Jednou z nejhorších zpráv byl krach největší burzy Mt.Gox, která v té době zprostředkovávala až tři čtvrtiny všech obchodů s Bitcoiny. Její klienti přišli dohromady o statisíce Bitcoinů a cena kryptoměny se propadla více než o 60 %. [5]

Říká se, že neexistuje špatná reklama. Všechny tyto zprávy přinášely Bitcoinu stále větší pozornost a popularitu až do stavu, ve kterém se nachází dnes.

2.2.3 Vznik alternativních kryptoměn

I přes to, že je Bitcoin bezpochyby geniální myšlenkou, má i své četné nedostatky. Těmi nejvýznamnějšími je například relativně pomalé ověřování transakcí, které je překážkou běžného platebního styku. Kvůli nastavené složitosti ověřování je čas k tomu potřebný kolem deseti minut, což je pro použití Bitcoinu k platbě například v supermarketu nemyslitelné. Dalším problémem jsou vysoké transakční poplatky. Bitcoinová síť je se rozrostla natolik, že v jednom okamžiku někdy čeká na potvrzení i několik desítek tisíc transakcí. Obecně platí, že čím déle transakce čeká na potvrzení, tím má větší přednost. Čekací dobu je ale možné významně zkrátit pomocí navýšení transakčního poplatku. Aby transakce proběhla v relativně rozumném čase, je nutné uhradit poplatek až v řádu desítek amerických dolarů. To činí použití Bitcoinu k platbám malých částek velmi nevýhodné, až nepoužitelné. V neposlední řadě musím zmínit obrovskou energetickou spotřebu při těžbě, které se budu podrobněji věnovat vpříslušné pokapitole (4.4). Všechny tyto závažné nedostatky i nápady na různá lepší vylepšení vedli vývojáře z celého světa k tomu, aby navrhovali vlastní kryptoměny. Ty jsou obecně označované jako alternativní měny neboli Altcoiny.

Pokud ale řešení na tyto problémy existují, proč vytvářet nové kryptoměny a jednoduše neupravit stávající Bitcoin? Tato řešení nikdy nejsou dokonalá a nesou s sebou různá omezení současných

vlastností Bitcoinu. Ne všichni by se tak shodli, zda je navrhovaná změna skutečně přínosnou. Jelikož v Bitcoinové síti neexistuje žádný centrální bod, který by rozhodoval o budoucnosti této měny, rozhoduje o ni většina uživatelů. Síť je však natolik rozsáhlá, že získat podporu většiny uživatelů je téměř nemožné. Pokud se tak objeví návrh na změnu, který není všeobecně akceptován, může se skupina podporovatelů rozhodnout od původní měny odtrhnout. Je vytvořena nová měna, od které všichni držitelé původní měny obdrží stejný počet mincí, jaký drželi. Nadále tak existují dvě různé měny, lišící se ve změně, kvůli které se rozdělili. Tato rozdělení se nazývají „forks“. [9]

První alternativní kryptoměny začaly vznikat kolem roku 2011 jako reakce na vzrůstající popularitu Bitcoinu i jeho nedostatky. Obecně lze říci, že kryptoměny se liší hlavně v protokolu[4], na kterém jsou založeny. Kryptoměny založené na stejném protokolu jsou si velmi podobné a liší se většinou pouze v několika znacích. Z počátku se objevovaly jen kryptoměny vycházející z Bitcoinu, používající stejnojmenný protokol Bitcoin. [8]

Protokol Bitcoin

Tento protokol je charakteristický hlavně tím, že jako metodu ověření transakcí používá metodu důkazů prací (proof-of-work) a jeho základní datovou strukturou je blockchain. Jedna z prvních měn založená na tomto protokolu, která je pravděpodobně také nejznámější, je Litecoin (2.3.2). Litecoin je téměř klonem Bitcoinu s tím rozdílem, že místo 21 milionů mincí bude v oběhu čtyřnásobek, tedy 84 milionů. Průměrná doba ověření transakce je naopak čtvrtinová čili 2,5 minuty. Největším rozdílem je těžební algoritmus, který používá. Díky němu nevyžaduje těžba Litecoinu tolik výpočetního výkonu, ale je při ní využito větší množství operační paměti. Tímto způsobem tak Litecoin řeší problém obrovské spotřeby výpočetního výkonu a elektrické energie. [8], [10] Litecoinu a dalším Altcoinům se budu více věnovat v dalších kapitolách.

Kryptoměn vycházejících z protokolu Bitcoin, které se snaží měnu vylepšovat, přibývalo. V roce 2012 jich bylo okolo dvaceti, zatímco o rok později už kolem dvou set. Motivací k tomu byl pravděpodobně ohromný nárůst ceny Bitcoinu. Některé kryptoměny vznikly však pouze za účelem rychlého zisku. V praxi jim stačilo pouze okopírovat volně přístupný kód Bitcoinu a propagovat novou měnu napříč internetovou komunitou. Rozšířili tak bázi uživatelů a zvýšili cenu. Jakmile se jim podařilo cenu zvýšit, prodali obrovské množství kryptoměny, o kterou jako tvůrci neměli nouzi. Cena tak spadla a kryptoměna mnohdy i úplně zanikla. Serióznější projekty kryptoměn, obecně vyvýjené často celými skupinami vývojářů, spotřebovávají při své snaze velké množství zdrojů, času a peněz. Častý způsob

[4] Protokol je standart, který definuje princip, jak daná síť funguje a co je společné pro všechny kryptoměny založené na daném protokolu. [10]

pokrytí těchto nákladů je proces tzv. první nabídky mincí („Initial Coin Offering“), což je pojem převzatý z veřejné nabídky prvně vydávaných akcií. Jedná se 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. [8]

Kryptoměn vycházejících z protokolu Bitcoin je stále většina, protože se jedná o nejjednodušší způsob vytvoření nové měny. Velmi přehledný graf měn vycházejících z Bitcoinu je k nalezení na adrese: http://mapofcoins.com/bitcoin#. V roce 2015 jich tento server evidoval téměř sedm set a v současné době je to tak pravděpodobně ještě víc. [11]

Protokol Ripple

Jiným protokolem, který vznikl v roce 2011, je protokol Ripple. Ten dostal své jméno podle první měny na něm založené. Je definovaný jako internetový protokol pro spojování bank and platebních systémů. Měny založené na tomto protokolu se významně odlišují od všech ostatních, protože postrádají základní vlastnost – decentralizaci. V Ripple síti vždy existuje tzv. Gateway, tedy uzel, který propojuje síť se zbytkem světa. Typicky se jedná o bankovní instituci, která zprostředkovává nákup a prodej peněz. Protokol byl skutečně navržen pro bankovní instituce a mezibankovní převody a bývá tak považován za produkt snahy bank o omezení kryptoměn, které jsou jejich obrovskou konkurencí. Mnozí uživatelé je tak ani nepovažují za kryptoměny. [10], [11] Protože s tímto názorem souhlasím, nebudu se již měnám založeném na tomto protokolu dále věnovat.

Protokol CryptoNote

V roce 2012 byl vymyšlen další protokol, jehož snahou je dosažení kompletně anonymních kryptoměn. Stejně jako u Bitcoin protokolu je zde využíváno metody důkazu prací a blockchainu, i když s malými odlišnostmi. U Bitcoinu mohou všichni uživatelé vidět cestu transakcí. Cryptonote ale zabraňuje aby kdokoli věděl, který účet byl odesílatelem a který příjemcem transakce. Toho je dosaženo díky tomu, že účty jsou uspořádávány do skupin. Navíc se používá tzv. ring signature. To je podpis, u kterého je výpočetně nezvládnutelné zjistit, kdo ze skupiny ho vytvořil. Odesílatel ani příjemce tak nemůže být jednoznačně identifikován. Nejznámějšími zástupci tohoto protokolu jsou měny Monero, Dashcoin (2.3.2) a Bytecoin. [10]

Protokol NXT

Rovněž v roce 2012 vznikla nová kryptoměna a s ní i nový protokol NXT, který používají kryptoměny založené na stejném principu. Tento Altcoin byl první, který použil k ověření transakcí metodu proof-of-stake neboli důkaz vkladu. Lidé, kteří ověřují transakce v tomto případě nejsou těžaři propůjčující výkon svého počítače, jako v případě metody proof-of-work. Jsou to lidé, kteří tuto kryptoměnu prostě vlastní. Stačí k tomu mít v počítači stažený kompletní historii transakcí (blockchain) a počítač pak plní funkci uzlu sítě. Za to, že měnu prostě držíte tak získáváte odměnu. Tento způsob je mnohem ekologičtější, neboť k chodu potřebuje zlomek spotřeby energie sítě používající metodu důkazu prací. Je tím tak opět řešena obrovská energetická náročnost Bitcoinu. [11]

Systém proof-of-stake není jedinou snahou o vylepšení metody proof-of-work. Další je například proof-of-burn, kde transakce ověřuje držitel mincí, které jsou „spalovány“. U proof-of-importance je zase důležitost ověřovatele vypočítána z počtu provedených transakcí a u proof-of-capacity je rozhodující místo na disku účastníkova počítače. [6] Otázkou samozřejmě zůstává, zda se jedná skutečně o vylepšení metody proof-of-work, nebo jde pouze o snahu zviditelnění se. Osobně se spíše přikláním k druhé možnosti.

Protokol Ethereum

Dalším protokolem, založeným v roce 2014 nad stejnojmennou měnou je Ethereum (2.3.2). Tento systém nemá za cíl pouze chod kryptoměny, ale umožňuje navíc vybudovat chytré kontrakty nad touto měnou. Za chytrý kontrakt je označován jakýkoliv protokol či software, jenž zajišťuje neboli vynucuje provedení kontraktu (smlouvy). Lze tak provádět i složitější, uživatelem definované akce. K tomu má Ethereum definovaný vlastní výpočetní jazyk, nazvaný EVM kód (Ethereum virtual machine). Pomocí tohoto jazyka je možné definovat vlastní pravidla pro přístup k penězům a jejich řízení. [10]

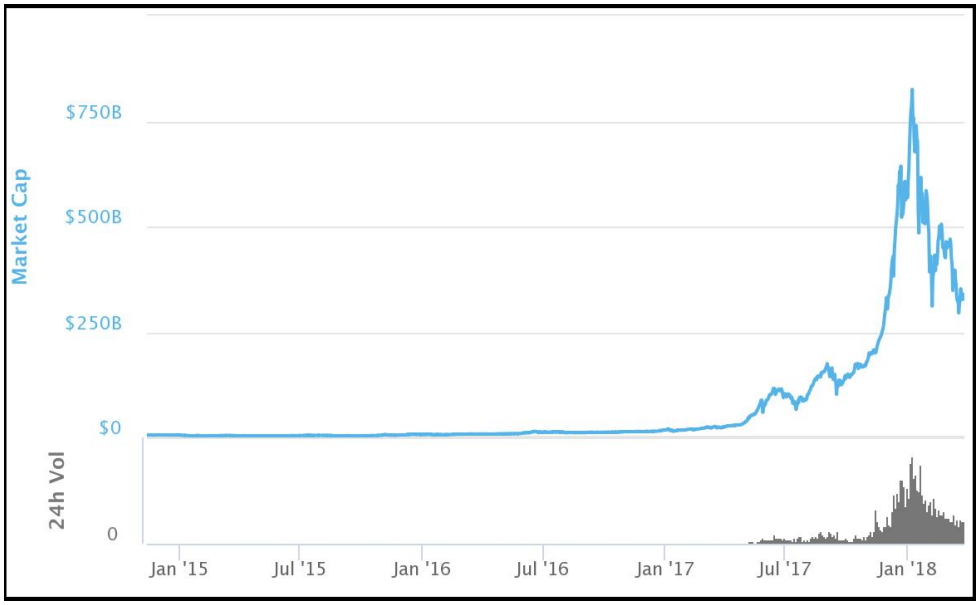
Další protokoly

Mezi další protokoly patří například Zerocash, který se liší od Bitcoinu v sestavení a ověření platebních transakcí. BitShares zase poskytuje možnost směny s tržními aktivy. Existuje také protokol XC hlásící „odvážně pragmatický, reálný přístup“. [11] Protokolů, na kterých kryptoměny fungují je více a stejně jako kryptoměny samotné neustále vznikají i zanikají. Kryptoměn je v současnosti na webu coinmarketcap.com evidováno více než 1500, ale konečné číslo bude pravděpodobně ještě vyšší. [2]

2.3 Současný stav

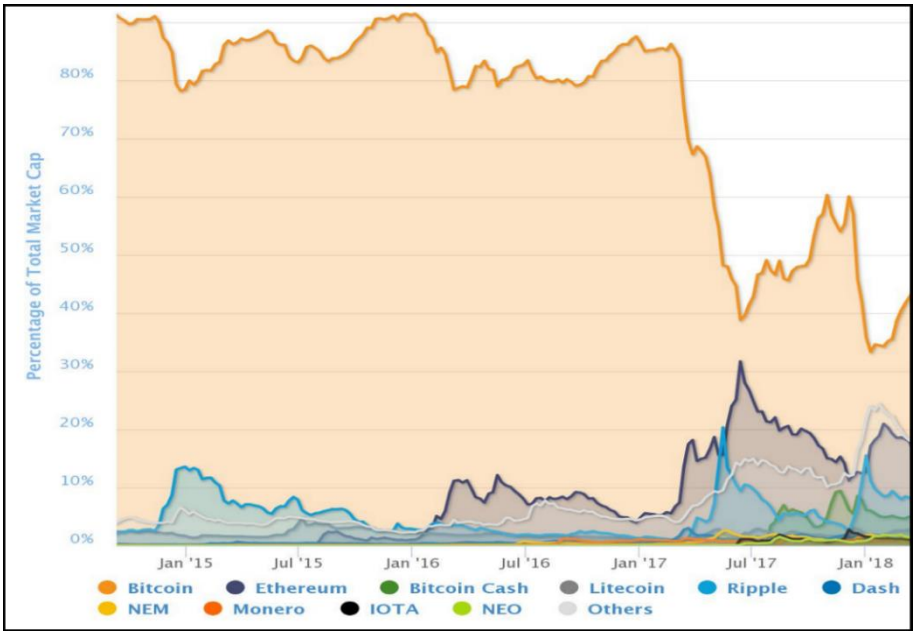
2.3.1 Tržní kapitalizace

Celková tržní kapitalizace všech kryptoměn je v době psaní této práce více než 326 bilionů amerických dolarů. [2] Koncem roku 2017 byla přitom hodnota téměř třikrát vyšší. Kryptoměny ale podle mého názoru zažívají recesi, která je přirozenou reakcí na nepřirozený růst ceny po mediálním boomu a vzniku cenové bubliny během roku 2017. Obrázek 2 zachycuje vývoj tržní kapitalizace kryptoměn během doby jejich existence. Je na něm možné pozorovat obrovský nárůst během posledního roku. Tomuto jevu se budu podrobněji věnovat v kapitole obchodování s kryptoměnami (3).



Obrázek 2) Tržní kapitalizace kryptoměn [2]

Tržní kapitalizace, neboli součin počtu vydaných mincí kryptoměny s její cenou, je jedním z parametrů, podle kterých je možné porovnat úspěšnost dané měny. Procentuální zastoupení deseti největších měn na celkové tržní kapitalizaci kryptoměn ukazuje obrázek 3. Je na něm viditelné, jak se postupem času snižuje dominance referenčního Bitcoinu ve prospěch ostatních alternativních měn. Ta klesla z původních 100 % na současných méně než 45 %. Naopak se v poslední době zvyšuje popularita kryptoměny Ethereum. V neposlední řadě je možné pozorovat, že deset největších měn tvoří více než 80 % celkové tržní kapitalizace všech kryptoměn. Existuje jich přitom na 1500. [2] To jen podporuje tvrzení, že většina Altcoinů nepřináší žádnou přidanou hodnotu a snaží se pouze přiživit na popularitě kryptoměn obecně. Takových měn existuje obrovské množství a není je tudíž všechny možné v této



Obrázek 3) Tržní kapitalizace největších kryptoměn [2]

práci pokrýt. Z těchto důvodů jen stručně představím několik mnou vybraných kryptoměn s nejvyšší tržní kapitalizací a pokusím se popsat jejich odlišnosti, které mohly mít za následek jejich popularitu.

2.3.2 Vybrané kryptoměny

Bitcoin

- Vznik: 2009
- Množství mincí: 21 milionů
- Metoda ověření transakcí: Proof of work
- Těžební algoritmus: SHA256
- Průměrná doba vytvoření nového bloku: 10 minut

Bitcoin je v současnosti nejrozšířenější a neznámější kryptoměna světa a bývá označován za průkopníka v oblasti kryptoměn. Těžební algoritmus SHA256 je náročný na výpočetní výkon a pro klienty s běžným počítačem nemá příliš smysl se snažit o těžbu. Na tu je za potřebí speciální hardware zvaný ASIC. [10]

Litecoin

- Vznik: 2011
- Množství mincí: 84 milionů
- Metoda ověření transakcí: Proof of work
- Těžební algoritmus: Scrypt
- Průměrná doba vytvoření nového bloku: 2.5 minuty [12]

Tato odnož Bitcoinu se snaží o zrychlení svého předchůdce a liší se hlavně využitím jiného těžebního algoritmu. Díky tomu těžba Litecoinu nevyžaduje tolik výpočetního výkonu, nýbrž operační paměti.

Ethereum

- Vznik: 2014
- Množství mincí: není pevně stanoveno
- Metoda ověření transakcí: Proof of work (v budoucnu možná změna na Proof of stake)
- Těžební algoritmus: Ethash
- Průměrná doba vytvoření nového bloku: 12 sekund [10]

Ethereum má za cíl kromě chodu kryptoměny navíc možnost vybudování chytrých kontraktů. Používá vlastní algoritmus náročný na operační paměť těžebního vybavení. Během jednoho až dvou let by však Ethereum mělo přejít na metodu Proof of stake, se kterou přišel protokol NXT. To by mělo za následek konec možnosti těžby metodou, jaká se používá dnes. Změna by měla přinést hlavně snížení spotřeby elektrické energie a vyšší míru decentralizace. [13]

Bitcoin Cash

- Vznik: 2017
- Množství mincí: 21 milionů
- Metoda ověření transakcí: Proof of work
- Těžební algoritmus: SHA256
- Průměrná doba vytvoření nového bloku: 9,5 minuty

Tento fork[5] Bitcoinu vznikl v reakci na pomalé ověřování transakcí a vysoké poplatky svého předchůdce. Jedná se o téměř totožnou měnu s tím rozdílem, že velikost bloku Bitcoin Cash je 8 MB namísto původního 1 MB u Bitcoinu. Těžaři tak za vteřinu zpracují až osmkrát více transakcí. [14] Odpůrci BCH však tuto měnu neuznávají, jelikož toto řešení považují pouze za dočasné a způsobující snížení decentralizace, která je hlavní myšlenkou kryptoměn. [15] Já s tímto názorem souhlasím.

Monero

- Vznik: 2014
- Množství mincí: 18.4 milionu
- Metoda ověření transakcí: Proof of Work
- Těžební algoritmus: CryptoNight
- Průměrná doba vytvoření nového bloku: 1 minuta

[5] *Oddělení od původní měny, lišící se ve změně, kvůli které došlo k odtržení. Vznikne při neshodě uživatelů.*

Hlavním znakem této měny je zvýšená anonymita. Jeho charakteristikami jsou nevysledovatelné platby, zcela anonymní transakce a resistence blockchainu proti analýzám historie transakcí. Použitý těžební algoritmus CryptoNight je náročný na operační paměť. [12]

IOTA

- Vznik: 2015
- Množství mincí: 2,78 x 10^{15}
- Metoda ověření transakcí: Proof of Work
- Těžební algoritmus: -
- Průměrná doba vytvoření nového bloku: -

IOTA přišla s novou myšlenkou kryptoměny bez blockchainu. Místo toho používá technologii Tangle, která umožňuje chod sítě bez transakčních poplatků či limitů. Funguje tak, že při odeslání jedné transakce uživatelův počítač zpracuje a potvrdí dvě transakce jiné. IOTA tedy nelze těžit. Nevýhodou je nižší výpočetní síla jednotlivých uzlů. Ta způsobuje, že útok specializovaných zařízení by mohl tento systém prolomit. Na druhou stranu platí, že čím více připojených zařízení, tím větší bezpečnost celé sítě. [16]

Dash

- Vznik: 2014
- Množství mincí: 22 milionů
- Metoda ověření transakcí: Proof of Work/Proof of Service
- Těžební algoritmus: X11
- Průměrná doba vytvoření nového bloku: 2,5 minuty

Dash, dříve Darkcoin, kombinuje metodu Proof of work s metodou Proof of Service. To se projeví tak, že někteří uživatelé (Master Nodes), splňující určité podmínky, mají v síti vyšší postavení než jiní a poskytují speciální služby. Těžba této kryptoměny je stejně jako Bitcoin náročná na výpočetní výkon. Těžební algoritmus X11 však brání těžbě na zařízeních ASIC a vyplatí se tak na osobních počítačích. [12]

EOS

- Vznik: 2017
- Množství mincí: 1 miliarda
- Metoda ověření transakcí: Delegated proof of Stake
- Těžební algoritmus: -
- Průměrná doba vytvoření nového bloku: 3 sekundy

EOS je platforma pro chytré kontrakty a jedná se o pokus vylepšení Etherea, především v jeho rychlosti. Dokáže totiž zpracovat až 50 000 transakcí za vteřinu, oproti třiceti transakcím Etherea. Využívá novou metodu ověřování, která stanoví jednadvacet delegátů zajišťujících chod sítě. Ty jsou voleni na základě hlasování. Platí přitom, že čím více mincí uživatel vlastní, tím více má hlasů. [17] Z mého pohledu zde opět dochází ke snížení decentralizace, hlavní myšlenky kryptoměn. Jak tomu chodí u Proof of Stake, tato kryptoměna se netěží a odměnu získávají uživatelé za její držení.

Popsané kryptoměny bychom podle [2] mohli zařadit do žebříčku TOP 10 s nejvyšší tržní kapitalizací. Z tohoto žebříčku jsem záměrně vynechal Ripple a jeho odnož Stellar, které podle mnohých nesplňují parametry kryptoměn. Popsáno nebylo rovněž NEO, které bývá nazýváno jako čínské Ethereum a Cardano, navrženo na základě akademického výzkumu. Popularita měn je často sezónní záležitostí a kdybychom se podívali na žebříček tři roky starý, figurovali by v něm pouze Bitcoin a Litecoin. [8] Z toho důvodu není tolik podstatné znát konkrétní kryptoměny, jako spíše chápat v čem se mohou lišit a jaká úskalí s sebou jejich „vylepšení“ nesou.

2.4 Budoucnost kryptoměn

Kryptoměny představují možnou alternativu k současnému peněžnímu systému. Obecně jsou nyní velkým trendem, což může, avšak nemusí pokračovat. Ať už v budoucnu současný systém peněz nahradí nebo ne, myslím, že nelze očekávat jejich naprostý konec. Na to je v kryptoměnách už příliš mnoho práce a hodně lidí má zájem na jejich pokračování. Je možné, že žádná z měn, které známe dnes nebude z dlouhodobého hlediska úspěšná. Nové a nové kryptoměny s sebou přinášejí inovace, který celý systém posouvají vpřed. Jejich úspěch a neúspěch však bude pravděpodobně záviset na tom, jak si dokážou poradit se svými problémy nebo naopak jak dokáží využít své přednosti. Z toho důvodu se pokusím stručně vystihnout jejich hlavní výhody a nevýhody ve srovnání se současným peněžním systémem.

2.4.1 Nevýhody

Jedním z největších problémů kryptoměn je bezpochyby jejich obrovská energetická spotřeba (4.4) nutná k ověřování transakcí a k chodu sítě. V roce 2017 padlo na těžbu kryptoměn kolem 29,5 TWh elektrické energie, což odpovídá polovině spotřeby celé České republiky. [18] Tato energie by podle mnohých mohla být využita k mnohem významnějším problémům. K tomu více než polovina této spotřeby připadá na Čínu. Ta je světovou velmocí v těžbě kryptoměn a téměř 60 % elektřiny zde pochází z uhelných zdrojů. [18], [19] To s sebou nese i velkou uhlíkovou stopu a znečištění životního prostředí.

Tím, že je u mnohých kryptoměn stanoveno jejich konečné množství se jedná o deflační měny. Mnoho ekonomů varuje, že deflační ekonomika je neštěstím. Lidé podle nich hromadí peníze místo jejich utrácení. Zastánci naopak tvrdí, že deflace není špatná sama o sobě, ale je jen negativně spojována s poklesem poptávky. V praxi prý platí, že instinkt hromadění způsobený deflační měnou lze přemoci slevami obchodníků, které překonají instinkt hromadění zákazníků. [4]

Dalším důvodem je již zmíněné relativně pomalé ověřování transakcí a vysoké transakční poplatky u některých kryptoměn. Ty jsou překážkou běžného platebního styku. Některé kryptoměny jsou schopné efektivně řešit některý z těchto problémů, často ale na úkor problémů jiných. Pokud by některá měna cílila až k nahrazení současných peněz, musela by bezpochyby perfektně vyřešit všechny tyto problémy.

2.4.2 Výhody

Někteří příznivci kryptoměn vyvrací jejich ohromnou energetickou spotřebu porovnáním se současným systémem peněz. Podle nich by se v případě peněžního systému měly započítat veškeré jeho náklady. Těmi jsou např. energie potřebná k výrobě, distribuci a skartaci peněz nebo energie k výstavbám bank a k jejich provozu. Ta totiž u kryptoměn odpadá. Tato energie nelze nikterak spočítat. Je však opravdu možné, že v celkovém součtu nejsou kryptoměny o mnoho horší než současný systém.

Mimo to jsou kryptoměny teprve na počátku své existence a mají velké množství chyb. To je však součástí pokroku a taková fáze se nedá přeskočit. Pokud by se jim podařilo odstranit všechny problémy, mohly by se mnohem lepším platidlem díky decentralizaci a dohledatelnosti plateb v blockchainu. Jejich hlavním přínosem jsou tedy především teoretické možnosti, které by mohly přinést.

Lightning Network

Nevýhody se navíc vývojáři neustále snaží odstraňovat. Pravděpodobně největším posunem vpřed by bylo zavedení takzvané Lightning Network. Ta by umožnila zachování současné decentralizace při zrychlení plateb a snížení poplatků, což by s sebou přineslo i snížení množství spotřebované energie. Tato síť by fungovala tak, že by spolu dvě strany vytvořily soukromý obousměrný platební kanál. Přes něj by si navzájem mohly posílat neomezené množství plateb bez poplatků, jelikož transakce by probíhaly mimo blockchain. Až v případě, že by se jedna ze stran rozhodla kanál uzavřít, by se konečné zůstatky zapsaly do blockchainu (s poplatkem). LN navíc zajišťuje nalezení nejkratší cesty k cíli. Pro představu uvažujme situaci, kdy uživatel 1 má otevřený kanál s uživatelem 2, uživatel 2 má otevřený kanál s uživatelem 3 a ten s uživatelem 4. Potom může uživatel 1 zaslat uživateli 4 platbu napřímo skrz kanály mezi uživateli 2 a 3, aniž by o tom musel tyto uživatele informovat. Tato síť by tak mohla být skutečně efektivní a optimistické odhady hovoří o jejím spuštění během roku 2019. [20]

3 Obchodování s kryptoměnami

Kryptoměny vznikly především jako alternativa k dnes používanému systému peněz, nazývanému anglicky jako fiat money[6]. Proč by ale vůbec někdo chtěl dnes fungující systém nahradit? I klasické peníze se potýkají s problémy, kterých si někteří všímají více, jiní méně. Názoru jejich odpůrců se budu věnovat v první části této kapitoly (3.1). K tomu, aby se s kryptoměnami dalo platit, je nutné nejprve jejich pořízení a uschování. Popis tohoto procesu bude náplní druhé části této kapitoly (3.2). Na závěr se zaměřím na tržní cenu kryptoměn, její vývoj v čase a na názor dvou různých táborů v její predikci (3.3).

3.1 Problémy peněz s nuceným oběhem

Je poměrně známým faktem, že peníze už dlouhou dobu nejsou kryty drahými kovy jako v minulosti a tím pádem nemají žádnou skutečnou hodnotu. Hodnota je dána pouze vírou uživatelů v jejich cenu. Peníze představují měny vynucené. Znamená to, že příslušný stát rozhodne o používané měně a jakákoliv alternativní platidla zakáže. [21] Někteří odpůrci volají po zrušení systému a obnovení peněz krytých drahými kovy. Jiní argumentují tak, že obnovení úplného krytí peněz zlatem je v současné době nereálné a navíc zcela nežádoucí. Historie podle nich jednoznačně ukázala neudržitelnost plného krytí peněz. Hlavním důvodem je rozvoj peněžní směny a z toho vyplývající potřeba růstu peněz v ekonomice. Vzhledem k omezené nabídce zlata byly všechny systémy na něm založené postupně nahrazovány systémem emise a oběhu nekrytých peněz, a to především na základě tržní poptávky po penězích. [22]

Současné bankovnictví lze popsat jako dvoustupňový systém. První stupeň reprezentují centrální banky. Druhý stupeň, označovaný jako komerční, představují obchodní a další banky. Hlavním cílem centrální banky není zisk, jak je tomu u bank komerčních, nýbrž zajištění cenové stability při provádění měnové politiky. [22]

Možná už tak známým faktem ale není, jak peníze vznikají. Intuitivní představa by mohla být taková, že obchodní banky půjčují své peníze, získané například vklady majitelů účtů a že peníze jsou uložené v centrální bance, která tak kontroluje jejich množství. Ve skutečnosti ale centrální banka množství peněz v oběhu vůbec nekontroluje a komerční banky peníze samy vytvářejí. K tomu dochází typicky v momentě, kdy komerční banka poskytne klientovi úvěr. Současně s připsáním nových peněz účet klienta, vytvořených „tahem pera“, vznikne jeho závazek vůči poskytující bance. Banky samozřejmě

[6] *Česky také označovány jako peníze s nuceným oběhem (oběh vynucuje stát).*

nemohou půjčovat neomezené množství peněz a jsou povinné držet určité rezervy. Hodnota těchto rezerv je však v současnosti např. v České republice pouze 2 %. [23] V praxi to znamená, že na každý půjčený milion korun musí banka držet pouze 20 000 Kč. Tím ale dochází k potenciálnímu problému zvanému multiplikační efekt. Pokud si například pan A do banky uloží 1 000 000 Kč, banka si ponechá 20 000 Kč jako rezervu a zbylých 980 000 Kč může půjčit (převést je na účet) panu B. Pan B tyto peníze utratí u obchodníka C a převede peníze na jeho účet, který se pro zjednodušení nachází u stejné banky. Tím pádem se ale v bance teoreticky nachází 1 980 000 Kč, které mohou chtít vybrat pan A a C. Stejným způsobem se částka může neomezeně zvyšovat. [24]

Pokud už banka nemá dostatečné množství rezerv k půjčování (2 %), může si je půjčit u centrální banky za měnově politickou úrokovou sazbu. Pokud si chce klient peníze z banky vybrat v hotovosti a banka tyto peníze nemá, může si o ně opět požádat u centrální banky, která bankovky natiskne. Centrální banka tedy nekontroluje ani množství bankovek v oběhu, na jejichž emisi má ze zákona výhradní monopol. [23]

Skutečný problém by nastal, kdyby chtěli své účty vybrat naráz všichni klienti. Hotovostní peníze totiž tvoří jen okolo jedné sedminy peněžní zásoby. [22] Taková situace by tak znamenala obrovský problém, pokud ne pád celého systému peněz s nuceným oběhem.

V současné době je vytvářeno stále větší a větší množství peněz, což má nevyhnutelně za následek i růst inflace a zadluženosti populace. Říká se, že každý cent, který někdo vlastní, je zároveň něčím dluhem. Zvyšující se množství peněz je současným nástrojem k růstu ekonomiky. V dřívějších dobách k tomu docházelo automaticky například po období válek nebo epidemií, kdy klesal počet lidí. Těchto událostí v dnešní době ubývá a ekonomiku je tak nutné stimulovat přílivem nových peněz. [25]

Myslím, že tato kapitola stručně vysvětluje to, proč se někteří lidé obávají o budoucnost, nevěří současnému systému nucených peněz a hledají z něj různá východiska. Jedním z těchto východisek je i použití kryptoměn, kde jsou banky zcela nepotřebné. Pokud ale uvážíme například výše zmíněnou situaci s půjčkou milionu korun, dostaneme se s uvažováním úroku 5 % a dobou splatnosti osm let na splatnou částku 1 211 045 Kč. [24] Pro banku to tedy znamená výdělek přes dvě stě tisíc korun, a to za povinnosti držet rezervu pouze dvacet tisíc Kč. Je tak jasné, že provozovatelé bank se nebudou chtít vzdát svého živobytí zadarmo a kryptoměny budou mít ještě trnitou cestu.

3.2 Nákup a uložení kryptoměn

Pokud se nový uživatel rozhodne začít používat kryptoměny, je prvním krokem jejich nákup. Ten lze provést prakticky dvěma způsoby. Jedním z nich je jejich nákup přímo od někoho, kdo kryptoměny již vlastní. Tento způsob s sebou samozřejmě nese zvýšené riziko podvodu. Neexistuje zde totiž třetí,

dohlížející strana, nemluvě o složitosti hledání takové osoby. Nejčastějším způsobem je tedy použití směnárny.

3.2.1 Směnárny

Web Crypto Coin Charts eviduje ve své databázi téměř dvě stě směnáren po celém světě. Největší z nich je v současnosti Bitfinex se sídlem v Hong Kongu. Na té denně proběhnou obchody za více než 1,5 miliardy amerických dolarů, což odpovídá tržnímu podílu přes 25 %. Dalšími známými směnárnami jsou např. americký Coinbase nebo lucemburský Bitstamp. [26] Velká směnárna ovšem neznamená velké množství obchodovatelných měn. Někteří obchodníci se soustředí především na Bitcoin, popřípadě na jiné velké Altcoiny jako je Litecoin nebo Ethereum. I v případě, že směnárna nabízí velké množství měn, není většinou možný jejich nákup přímo za peníze. Nejprve musí dojít k nákupu největší kryptoměny Bitcoinu. Až poté je za něj možné směnit ostatní kryptoměny.

V drtivé většině směnáren musí nákupu předcházet registrace. Ta kromě běžných registračních údajů vyžaduje také osobní doklad jako je pas, občanský nebo řidičský průkaz. Směnárny se tak snaží zamezit praní špinavých peněz a použití kryptoměn k trestné činnosti.

Některé směnárny fungují na principu shromažďování a párování nabídek s poptávkami uživatelů, a vystupují tak v roli prostředníka. V takovém případě nejsou většinou účtovány žádné poplatky za směnu. Místo toho je zpoplatněn výběr vložených financí, nebo nakoupených kryptoměn. Druhým případem jsou směnárny, které plní přímo roli protistrany. Uživatel zde platí za rozdíl mezi nákupní a prodejní cenou a směnárny tak vydělávají na daném kurzovém rozdílu. V každém případě vždy uživatel zaplatí určitý poplatek. [8]

Pokud se uživateli podaří u směnárny registrovat, není už problém poslat na její bankovní účet peníze, případně kryptoměny nakoupit přímo platební kartou. Nechávat své peníze nebo kryptoměny ve směnárně je ale značně rizikové. Již mnohokrát došlo k jejich krachům nebo vykradením. Proto je dalším krokem převod kryptoměn do bezpečného úložiště.

3.2.2 Transakce a adresa

Chce-li uživatel odeslat nakoupenou kryptoměnu ze směnárny pryč, musí k tomu nutně znát cílovou adresu. Ta je identifikátorem účtu, na který chce měnu převést. Každý účet má svou nezaměnitelnou adresu podobně jako má bankovní účet své číslo. Různé kryptoměny mají různé adresy. Například ta Bitcoinová se skládá z 26 až 34 alfanumerických znaků. V těchto znacích je obsažena informace o tom, pro jakou síť je adresa určena, kontrolní součet pro zajištění integrity dat a hash veřejného klíče vlastněného uživatelem. Toto číslo je veřejné a pouze s ním nelze získat ke kryptoměnám přístup.

S konkrétními adresami jsou matematicky svázány privátní klíče. Ty slouží k ovládání veškerých mincí, které jsou tímto klíčem zabezpečené. I ve směnárně leží kryptoměny na určité adrese. Zadá-li uživatel příkaz k převodu na adresu jinou, je v blockchainu (pokud ho měna používá) zkontrolováno, zda adresa směnárny tímto obnosem disponuje. Pokud ano, dojde v blockchainu ke snížení zůstatku na kontě směnárny, a naopak k jeho navýšení na cílové adrese. [8]

3.2.3 Klient a peněženka

Klient je software, který slouží ke komunikaci se zbytkem kryptoměnové sítě. Jeho součástí je kromě databáze uskutečněných transakcí a nástrojem pro jejich ověření i funkce peněženky. Ta je rozhraním umožňujícím přijímání a uchování kryptoměn a realizaci nových transakcí. Každá peněženka umožňuje vygenerování nové adresy, na kterou je možné kryptoměny poslat, i jejich odeslání na adresu jinou. Měla by být chráněna velmi silným heslem, aby bylo zamezeno k přístupu kohokoli kromě jejího vlastníka. Některé peněženky umožňují uchování několika různých kryptoměn. Většinou je ale nutné ke každé kryptoměně založit odlišnou peněženku. Nejjednodušší je vysvětlení na příkladu Bitcoinu, přičemž ale ne všechny kryptoměny fungují úplně stejně. [4]

Bitcoinové klienty můžeme rozdělit na úplné, odlehčené nebo webové. Liší se v tom, do jaké míry spoléhají na třetí strany, a do jaké na vlastní informace. Úplný klient uchovává celou historii blockchainu a spravuje uživatelské peněženky. Ty spravuje i odlehčený klient, který ale neuchovává kopii všech transakcí a musí tak při ověřování transakcí věřit serverům vlastněným třetí stranou. Webový klient potom uchovává na serverech třetích stran i peněženky. Volba závisí na tom, jakou kontrolu chce mít uživatel nad svými prostředky. Úplný klient je nejbezpečnější, je ale náročný na úložné místo a vyžaduje zálohy a zabezpečení. Pokud by došlo k poškození počítače, jsou data navždy ztracena. Webový klient naproti tomu není na uživatelově počítači závislý vůbec. Může však dojít k ztrátě prostředků při prolomení webového zabezpečení služby, jak se tomu již mnohokrát stalo. [4]

Pokud uživatel nechce spoléhat na software, je možné vytvořit papírovou peněženku. Jedná se de facto o papír s vytištěnou adresou pro zaslání prostředků a privátním klíčem pro jejich výběr. Vlastnictví většiny kryptoměn je vlastně pouhý zápisem o této skutečnosti v blockchainu. Proto se mohou kryptoměny nacházet i na adrese, kterou uživatel vytvoří a napíše na papír bez použití softwarové peněženky. Vytvoření papírových peněženek je možné na k tomu určených webových stránkách.

Další nesoftwarovou možností je zakoupení takzvané hardwarové peněženky. Tu si lze představit jako běžné USB, na kterém je nahraný program fungující stejně jako běžná softwarová peněženka. Lze ji ale jednoduše odpojit od počítače a uchovávat off-line, což se považuje za nejbezpečnější způsob.

3.3 Tržní cena

Cena kryptoměn je faktorem, který jednoznačně určuje jejich úspěšnost. Myslím, že i přes jejich technický přínos v nich stále většina lidí vidí pouze možnost zbohatnutí. Pokud by cena významně klesla, znamenalo by to obrovský odliv uživatelů.

3.3.1 Korelace mezi kryptoměnami

Sledovat a popisovat tržní cenu stovek kryptoměn by bylo velmi obtížné. Naštěstí se ale cena většiny kryptoměn vyvíjí velmi podobně. Jejich vzájemný lineární vztah může být pozorován pomocí korelační koeficientu, který se používá ve statistice. Ten nabývá hodnot od -1 do 1. Pokud je korelační koeficient kladný, znamená to, že s jednou rostoucí veličinou roste i ta druhá. Pokud je naopak záporný, při růstu jedné veličiny druhá klesá. Korelační koeficient 1 potom značí zcela přímou závislost, kdy při změně jedné veličiny o jednu jednotku se druhá veličina změní přesně ve stejném poměru. Korelace ale nestanovuje, která veličina je příčinou a která následkem.

Na základě dat z [2] jsem provedl výpočet korelačních koeficientů mezi Bitcoinem a vybranými alternativními měnami popsanými výše. Použil jsem přitom denní data za dva časové úseky. Nejprve jsem využil data za uplynulý rok, tedy období, ve kterém došlo k největším absolutním změnám cen kryptoměn. Následně jsem aplikoval i denní data od začátku roku 2018. Ten byl zatím charakteristický největšími propady v cenách měn. Výsledek výpočtů, které jsou součástí přílohy 1, ukazuje tabulka 1. Výpočet byl proveden k 9.4.2018.

Tabulka 1) Korelace vybraných kryptoměn (zdroj: vlastní)

Období	**9.4.2017 - 9.4.2018**	**1.1.2018 - 9.4.2018**
Měna	*BTC*	*BTC*
BTC	1,00	1,00
ETH	0,50	0,78
BCH	0,25	0,82
LTC	0,53	0,79
IOTA	0,49	0,78
XMR	0,51	0,81
Dash	0,45	0,85
EOS	0,35	0,68
ADA	0,30	0,66
NEO	0,31	0,70

Obecně platí, že korelační koeficienty v rozmezí 0,3 – 0,7 značí středně silnou korelaci a koeficienty nad 0,7 korelaci silnou. Na první pohled je viditelné, že korelační koeficienty mezi Bitcoinem a všemi vybranými Altcoiny jsou kladné. Platí tedy, že pokud stoupá cena Bitcoinu, stoupá i u ostatních měn

(nebo naopak). To už samo o sobě ukazuje, jak moc jsou kryptoměny spjaté jako celek. Přihlédneme-li ještě k velikostem korelačních koeficientů, které jsou zejména pro rok 2018 skutečně významné, lze usuzovat, že se buď bude dařit všem kryptoměnám, nebo žádné. Navíc se jedná o průřezová data, u kterých bývají korelační koeficienty menší. Nic nenasvědčuje tomu, že by bylo možné považovat některou kryptoměnu za náhradu jiné a využít tak diverzifikaci rizika. Z těchto důvodů se místo na ceny jednotlivých měn zaměřím na cenu Bitcoinu, jako největší kryptoměny. Předpokládám totiž, že změny v jeho ceně se projeví poměrnou změnou i v cenách ostatních měn.

3.3.2 Predikce cen

Cena Bitcoinu i ostatních kryptoměn není ničím podložena ani kryta a je tak dána především poptávkou a nabídkou. O její predikci se pokouší mnoho odborníku i nadšenců, jedná se však spíše o hádání z neexistující křišťálové koule. Obecně existují dva tábory – ti kteří předpokládají, že cena půjde nahoru a ti věřící v její pád.

Mezi známé zastánce teorie o růstu ceny Bitcoinu patří např. programátor a businessman John McAfee, zakladatel stejnojmenné softwarové společnosti. Podle něj se cena jednoho Bitcoinu v roce 2018 zdesetinásobí a do roku 2020 vidí jeho cenu až na milionu amerických dolarů. [27]

Zcela opačný názor zastává ekonom Nouriel Roubini, přezdívaný „Dr. Doom“. Ten patří k osobám, které opakovaně upozorňují na možný pád Bitcoinu i ostatních kryptoměn až na jejich pravou hodnotu, tedy na nulu. Také nazval Bitcoin největší bublinou v historii lidstva. [28]

S názorem, že kryptoměny jsou ekonomická bublina souhlasí i další lidé, včetně mne. Zaměřím se proto na tuto problematiku podrobněji.

Cenová bublina

Cenové bubliny jsou definovány jako „ceny kurzů (akcií, dluhopisů, komodit, měn apod.) vyhnané spekulacemi nad ekonomicky ospravedlnitelnou úroveň, přičemž většina investorů sice ví, že ceny jsou přehnané, přesto daný investiční instrument dále nakupují ve víře, že se svezou na dalším cenovém růstu a stačí prodat dříve, než cenová bublina praskne.“ [29]

Podle této definice jsou ale bublinou i v současnosti používané peníze, neboť jejich jediná ospravedlnitelná úroveň je cena papíru, na kterém jsou natištěny. I když jsou tak kryptoměny pravděpodobně bublinou, neznamená to nutně jejich konec.

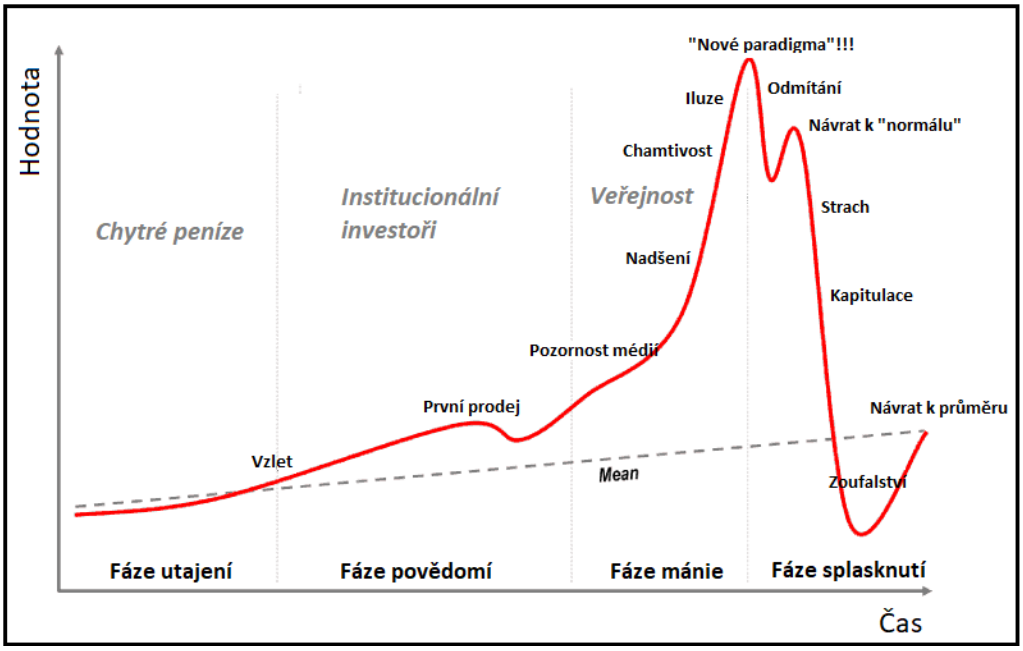
Podle investiční společnosti Goldman Sachs by vývoj kryptoměn mohl mít podobný scénář jako tzv. internetová bublina (.com bubble) na přelomu tisíciletí. Během ní lidé neuvážlivě investovali do nově vznikajících internetových firem, které neměly promyšlený obchodní model a brzy zkrachovaly. Po

splasknutí bubliny došlo k pádům cen a zániku drtivé většiny firem. Některé z nich, jako Amazon, Google nebo Yahoo, se však vyvinuly v celosvětově úspěšné firmy. Je tak dobře možné, že z dnešních tisíců kryptoměn přežije pouze několik nejsilnějších, které se stanou neméně úspěšnými. [30]

Ritvik Vasudevan se tyto dvě bubliny pokusil srovnat statistickými metodami. Výsledná hodnota R^2 v jeho regresní analýze přitom činí 0,92. Tato hodnota popisuje, jaký podíl celkové variability v závislé proměnné se podařilo vysvětlit použitým modelem. Z toho by bylo skutečně možné vyvodit závislost mezi těmito dvěma událostmi. Na druhou stranu zde autor počítá s několika předpoklady, které nemusí platit. Ceny akcií a kryptoměn totiž nejsou totéž. Internetová bublina se navíc vyvíjela několik let a její tržní kapitalizace byla okolo 6,7 bilionu USD. Oproti tomu bitcoinová bublina bývá vymezována do období zhruba jednoho roku s tržní kapitalizací pod 1 bilion amerických dolarů. [31]

Vznik bubliny

Z mého pohledu je možné současný stav kryptoměn nejlépe pochopit z práce, kterou vytvořil Jean-Paul Rodrigue. Ten vysvětluje, že cenové bubliny v historii opakovaly již mnohokrát (tulipánová horečka, nemovitostní bubliny, internetová bublina). Přestože byla každá odlišná, v něčem byly naprosto stejné. Podle něj má každá bubliny čtyři fáze, viz obrázek 4. [32]

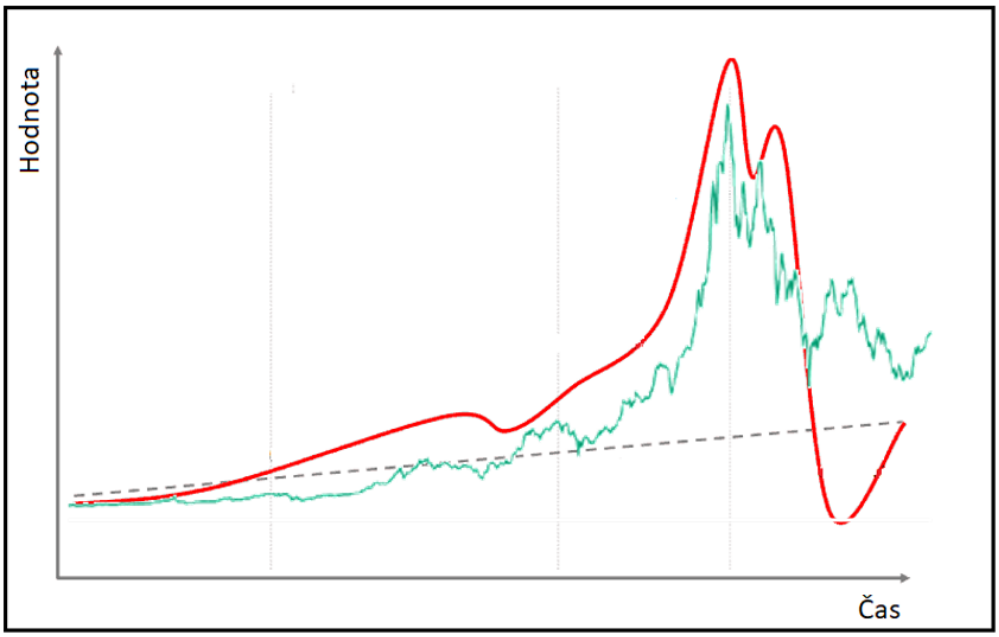


Obrázek 4) Fáze bubliny [32]

1) **Utajení.** Ti, kdo rozumí novým základům, si uvědomí příležitost zhodnocení. Ta je však s riskem, neboť předpoklady zatím nejsou potvrzeny. Tito investoři zvaní "chytré peníze" mají obvykle lepší přístup k informacím a jsou schopni je správně vyhodnotit. Investují proto první peníze a ceny postupně rostou, avšak bez zájmu širší veřejnosti. [32]

2) **Povědomí.** Více a více investorů, zejména institucionálních, si začíná všímat pohybu. Přinášejí další peníze, které tlačí ceny vzhůru. Mohou se objevit krátkodobé fáze prodeje, kdy „chytré peníze“ inkasují první zisky. [32]
3) **Mánie.** Každý si uvědomuje, že ceny letí nahoru a veřejnost povzbuzená zájmem médií skáče po investiční příležitosti života. Tato fáze není o logice, nýbrž o psychologii. Záplavy peněz vzbuzují ještě vyšší očekávání a nadšení tlačí ceny do nebes. Čím vyšší je cena, tím více investic přichází. Nově příchozí přitom ani často nemají tušení o základním fungování trhu. Aktiva jsou nabízeny se všemi možnými finančními prostředky, zejména s pákovým efektem a dluhem. Mezitím „chytré peníze“ a institucionální investoři potichu prodávají svá aktiva. [32]
4) **Splasknutí.** Moment prozření přichází a všichni si najednou uvědomí, že se situace změnila. Očekávání se hroutí, ne však bez fáze odmítání. Při té se mnozí snaží utěšovat tím, že se jedná pouze o dočasný ústup. Někteří jsou ošálení, ne však nadlouho. Všichni očekávají pokles cen a kupců je málo. Situace je tak špatná, že se cena může dostat pod dlouhodobý průměr, což je situace výhodná k nákupu. Široká veřejnost však už tento sektor považuje za nejhorší možnou investici. [32]

Na obrázku 5 je stejná linie jako na obrázku 4, zobrazující typickou bublinu. Tentokrát je však doplněná o cenu Bitcoinu za poslední rok. [2], [32]

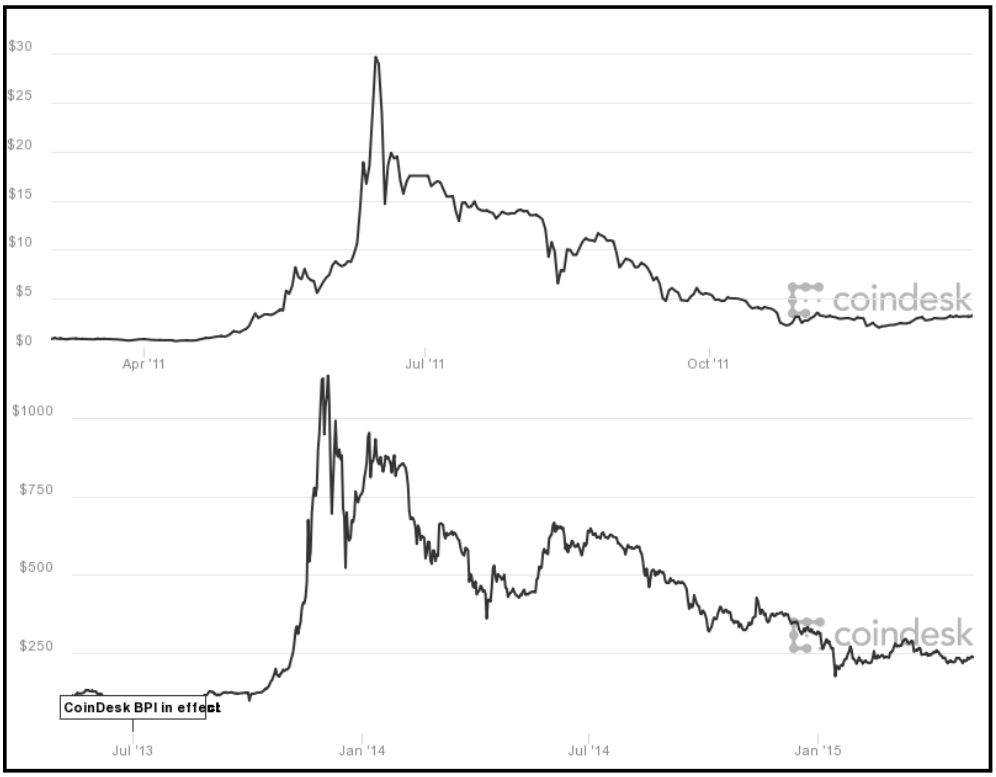


Obrázek 5) Bublina a Bitcoin (zdroj: vlastní)

Myslím, že ceny kryptoměn během minulého roku vcelku přesně následovaly jednotlivé fáze bubliny, včetně popsaného chováním lidí, médií a investorů. Otázkou ale zůstává, jak se bude situace vyvíjet dál. Jedna z možností je taková, že jsou kryptoměny stále ve fázi sestupu a dostanou

se až na cenu, kterou měly před fází mánie. To by např. pro Bitcoin mělo být kole 3-4 tisíc dolarů za kus. Je ale možné i to, že už na dně byl a čeká ho opět pozvolný nárůst. S ním by pravděpodobně rostly ceny i ostatních kryptoměn.[7]

Nikde není psáno, že splasknutí bubliny musí nutně znamenat konec. Bitcoin už podobné chování zažil v minulosti, pouze v menším měřítku. To ukazuje obrázek 6. Poprvé to bylo v roce 2011 kolem hodnoty 30 USD. O dva roky později už cena dosáhla 1000 USD a v roce 2017 to byla již zmíněná bublina, která dosáhla 20 000 amerických dolarů. Tržní kapitalizace kryptoměn na vrcholu poslední bubliny byla zhruba jedna sedmina té, které dosáhla bublina internetová. V dnešní době je navíc v oběhu daleko více peněz, takže ve srovnatelných cenách by se jednalo o číslo ještě menší. Je tak možné, že za několik let se dočkáme dalšího razantního nárůstu cen. Pokud by to bylo podobným tempem jako doposud, odpovídalo by to cenám ve stovkách tisíc USD.



Obrázek 6) Bitcoinové bubliny v minulosti [62]

Podle mého názoru si kryptoměny prošly fází bubliny a jsou momentálně spíše v období recese. Nemyslím si ale, že by to znamenalo jejich sestup k nule. Po ustálení ceny na nějaký čas očekávám opět vzestup ceny Bitcoinu a s tím i vzestup cen ostatních kryptoměn. Z dlouhodobého hlediska ale nejspíš přežije přibližně jedna kryptoměna ze sta.

[7] *Psáno v květnu 2018 při ceně kolem 8000 USD. V lednu 2019 při odevzdání práce je cena skutečně 3 900 USD. [2]*

Téměř roční období stoupajících cen s sebou přineslo i zvýšený počet těžařů. Po velkém pádu ceny jich ale pravděpodobně zůstalo více, než je síť schopná uživit. Cena kryptoměn je zcela zásadním faktorem ovlivňujícím rentabilitu těžby a tento jev se zde negativně projeví.

3.4 Daně a kryptoměny

Problematika nákupů, prodejů či jiných operací s kryptoměnami je oblastí, která zatím není jednoznačně a jasně definovaná. Dle ustanovení Evropského soudního dvora z roku 2015 nepodléhá směna kryptoměn na burze DPH a je jako oběživo osvobozená. Těžba kryptoměn jako taková pravděpodobně DPH také nepodléhá – není jasné, kdo je koncový zákazník, není jasné místo uskutečněného plnění a nelze ani ovlivnit svou činností výši příjmu. V České republice jsou kryptoměny považovány ze strany státních orgánů za nehmotný movitý majetek. Česká národní banka se vyjádřila, že kryptoměny nejsou peněžní prostředky. Podle ní jejich nákup a prodej nepředstavují žádnou platební službu, elektronické peníze, ani cizí měnu. Kryptoměny nemají ani povahu cenného papíru. [33]

Zdanění virtuálních měn tak v ČR není v současnosti přímo ošetřené zákonem a jasná pravidla neexistují. K dispozici je pouze vyjádření Finanční správy. Podle té by veškeré výnosy z obchodování s kryptoměnami měly podléhat dani z příjmů. Podle odborníků ale vyjádření nepostihuje všechny situace. Tento stav se dá přisuzovat rychlému vývoji, na který legislativci zatím nestačili reagovat. Lze tedy očekávat, že v dohledné době nastane ze strany Finanční správy nová úprava daňových zákonů s výslovnou úpravou virtuálních měn. Ta by měla reflektovat aktuální potřeby vznikající v souvislosti operací s kryptoměnami. [34]

Zpeněžení vytěžené kryptoměny nebo rozdíl mezi nákupní a prodejní cenou by pravděpodobně měl být zdaněn. Je ale třeba řídit se pouze obecnými právními předpisy. Operace s kryptoměnami jsou však natolik specifické, že je často možné si jednu situaci vyložit z více úhlů pohledu. Navíc chybí praktické zkušenosti a v řadě případů tak lze očekávat ustálení praxe až na základě soudních rozhodnutí. [34]

3.4.1 Obecně platné zásady – nepodnikatel

Každá směna podléhá podle aktuální legislativy dani z příjmu. Zisk z ní je tak nutno zdanit. Postup zdanění záleží na tom, zda se jedná o jednorázový či pravidelný příjem. Dále záleží, zda má daná osoba kryptoměny zahrnuty v podnikání či funguje jako fyzická osoba. K obchodu je většinou výhodnější přistupovat jako fyzická osoba, kdy příjmy nepodléhají zdravotnímu a sociálnímu pojištění a náklady se uplatňují pouze přímé na pořízení kryptoměny. Nevýhodou je, že nelze uplatňovat ztrátu. Pokud obchody vyjdou do mínusu, základ daně je nula. V případě, že se jedná o jednorázovou činnost, je

možné využít osvobození příjmů do výše třiceti tisíc korun za rok. Většinou ale lidé obchodují soustavně a operace s kryptoměnami se nedají považovat za činnost nepravidelnou. V situaci, kdy s kryptoměnami obchoduje fyzická osoba, zdaňuje své příjmy jako takzvané ostatní příjmy (15 %). Výdaje na zajištění příjmů může být problém stanovit, pokud došlo k nakoupení vícekrát za jinou cenu. V takovém případě se výdaje stanoví jako aritmetický průměr nebo jako First in First out. V takovém případě má přednost dříve nakoupené množství. [34]

3.4.2 Obecné platné zásady – podnikatel

V některých případech může mít osoba zahrnuty kryptoměny ve svém podnikání. I když to zákon jasně nespecifikuje, může to být těžba kryptoměn. Tato činnost se už totiž netýká pouze správy vlastního majetku. Dala by se považovat za poskytovanou službu, která naplňuje znaky podnikání. V takovém případě by bylo nutné zřídit si živnostenské oprávnění a přihlásit se k sociálnímu a zdravotnímu pojištění. Příjem se pak zdaňuje podle §7 Zákona o dani z příjmu. Druh živnosti je pravděpodbně živnost volná. Zdanitelný příjem je směna vytěžené kryptoměny (za FIAT nebo něco jiného), tedy jen následné zhodnocení. Náklady proti příjmům lze pak použít paušální ve výši 60 % nebo skutečné náklady na těžbu (elektrická energie, hardware apod.). V případě podnikání lze i uplatnit ztrátu a v budoucnu ji odečítat (po dobu pěti let – viz §34 Zákona o dani z příjmu). Případný zisk se daní také 15 %. [33]

3.4.3 Těžba kryptoměn a účetnictví

V případě podnikání jako právnická osoba je rovněž nejasné vedení podvojného účetnictví. V současné době je doporučeno, aby se kryptoměny účtovaly jako zásoby. Spekuluje se však také o zařazení jako cenné papíry, nehmotný majetek nebo dokonce jako ceniny. Jednotná právní úprava však aktuálně neexistuje. Ministerstvo financí také prosazuje, aby se v případě snížení hodnoty kryptoměn vytvářely opravné položky. Problematické může být rovněž doložení zůstatků účtů s kryptoměnami při účetní závěrce. Zůstatek účtu by měl souhlasit se zůstatkem na výpisu z elektronické peněženky. Ne u všech typů kryptoměn však tato peněženka existuje, a tak je potřeba mít alespoň čestné prohlášení dané osoby nebo mít výpis z burzy. To je však editovatelný excelový soubor, a proto je možné, že takový dokument nemusí obstát před kontrolou z finančního úřadu. [34]

4 Těžba kryptoměn

V první kapitole jsem vysvětlil, že těžba je proces, při kterém na sebe těžaři berou úlohu dohlížející, třetí strany. Propůjčují totiž výkon svého počítače k ověřování transakcí. To umožnil vynález blockchainu. Blockchain si lze představit jako účetní knihu, do které smí zapisovat pouze těžař, který vyřeší výpočtově náročnou úlohu. Blockchain přitom zdaleka nemusí být využíván pouze u kryptoměn, ale v budoucnu by mohl být použit například pro hlasování demokratických systémů (znemožnění zfalšování hlasování), nepopíratelné vlastnictví digitálních komodit, pro finanční transakce nebo náhradu centrálních databází a úložišť. Zařízení by pak komunikovala přímo mezi sebou. [35] Dnes už existují i kryptoměny, které blockchain nepoužívají a těží se jiným způsobem nebo je nelze těžit vůbec.

V této kapitole se podrobněji zaměřím na celý proces těžby technologií využívající blockchain a v jednotlivých podkapitolách popíšu, jakým způsobemse těží (4.2), jaké technologiejsou k tomu využívány (4.3), i kolik elektrické energie spotřebují (4.4).

4.1 Princip těžby

Základem těžby je takzvaná hashovací funkce. Jedná se o převedení vstupních dat na určitý výstup, který by měl být velmi snadno spočitatelný. Zároveň by ale mělo být velmi obtížné, ze znalosti pouze výstupu, zjistit podobu původních dat. Problém může být vysvětlen na příkladu, kdy se snažíme námi vytvořenou funkcí přijít na hash prvočísla. Při použití kalkulačky a spočtení odmocniny ze tří dostaneme výsledek 1.7320**508075**68877293527446341 50. Pokud bychom vzali páté až desáté desetinné číslo (zvýrazněno ve výsledku), dostaneme číslo 508075. To je hash. Je snadné získat hash, pokud známe prvočíslo a danou funkci. Je ale mnohem komplikovanější přijít na to, z jakého prvočísla určitý hash pochází. Pokud bychom např. znali pouze hash 087518, bylo by komplikované bez zkoušení přijít na to, že původní prvočíslo je 9973. A to i přesto, že známe funkci, jak hash vyprodukovat. [36]

Kryptoměny využívají podobný systém, jen výrazně složitější. Bitcoin začal s těžebním algoritmem SHA-256 a jeho nástupci používají mnoho dalších. Některé z nich jsou pouze upravené, jiné zcela odlišné. Algoritmus SHA-256 převede jakýkoliv text na hash dlouhý dvaatřicet znaků. Pokud se změní třeba jen jediný znak v původním textu, výsledný hash je naprosto nepředvídatelně změněn. Neexistuje žádný jiný způsob než prosté zkoušení, jak přijít na text, jehož hash začíná nulou. K přijití na tento hash je vynaložena práce zkoušením. Proto se těžení říká "proof of work" neboli "metoda důkazu prací". V praxi se na hash převádí text v podobě počítačového kódu, který obsahuje informace o transakcích v bloku. Výsledný hash musí mít na začátku 17 nul. K tomu je potřeba obrovské množství pokusů (hashů), které provádí naráz všichni těžaři připojení do sítě. Ten, kterému se to podaří jako prvnímu,

zašle výsledný text všem ostatním, kteří ho velmi snadno ověří. Blok transakcí je potvrzen, zanesen do blockchainu a uznán všemi uživateli sítě. Vítězný těžař obdrží odměnu a začíná se znovu dalším blokem jenž obsahuje transakce čekající na potvrzení. [36]

Každý další potvrzený blok, zanesený do blockchainu vítězným těžařem, je svou existencí závislý na těch předchozích. V hashovaném textu je totiž i údaj o minulém bloku. Při jakékoliv úpravě původního textu by se hash změnil a neodpovídal. Nelze tak měnit jakékoliv údaje. Všichni mohou jednoduše ověřit, že výsledný hash u jakéhokoliv bloku sedí, a že potvrzení transakce proběhlo v pořádku. Nové mince vznikají pouze těžbou jako odměna, kdy je potvrzen blok. Není tak možné je padělat nebo uměle vytvářet. Každý má totiž možnost si přesně spočítat, kolik mincí je v oběhu a jestli jejich počet sedí. Blockchain je zcela veřejný a transparentní. Jeho správnost je možné snadno a relativně rychle spočítat, o což se starají všichni uživatelé provozované sítě. [36]

Síť je nastavená tak, aby k vytěžení bloku došlo pravidelně za určený časový úsek. Počet těžařů i výkon jejich vybavení se ale neustále mění. Jelikož jsou výpočty založené na metodě pokus-omyl, záleží do jisté míry i na štěstí. Proto se kontroluje průměr času vyřešení jednoho bloku za poslední dva týdny. Pokud interval neodpovídá tomu zadanému, přidá se nebo odebere počet nul na začátku hledaného hashe. Každá přidaná nula obtížnost zdvojnásobí a naopak. Touto samoregulací se udržuje časový interval, při němž vznikají nové mince a je tak známo jejich konkrétní množství v oběhu. [36]

Některým odpůrcům vadí, že zkoušení při těžbě je extrémně energeticky náročné. Spotřebovává tak výpočetní výkon počítačů, který by mohl být využit lépe. Proto vznikají kryptoměny, které se spotřebu snaží snížit používáním metody proof of stake. Jiné, v čele s měnou IOTA, zase nelze těžit. Kryptoměny jako je Primecoin se těžbu pro změnu snaží dělat těžbu přínosnou. Těžaři Primecoinu totiž při těžbě hledají nová prvočísla, která jsou potřebná v matematice, fyzice i řadě dalších věd.

4.2 Způsoby těžby

4.2.1 Podle způsobu zapojení se do sítě

Sólo těžba

Jak jsem uvedl při vysvětlování principu, těžaři se snaží získat odměnu za vyřešení výpočtu. K tomu používají metodou pokus-omyl. Čím lepší vybavení těžař má, tím vyšší je šance na získání odměny. Jelikož je však celkový výpočetní výkon sítě obrovský, ani skvělé vybavení nezaručí více než nepatrné procento tohoto výkonu. Pokud tak někdo kryptoměny těží sám, dá se jeho snaha přirovnat k loterii. Existuje určitá šance, že se těžaři podaří najít hledaný hash. V tom případě si sám ponechá odměnu, která mnohonásobně pokryje investiční náklady i spotřebovanou energii. Na druhou stranu se ale může

stát, že řešení nenalezne vůbec nikdy. Proto se drtivá většina těžařů uchyluje do tzv. těžebních poolů čímž se sníží jejich riziko. Odměnu totiž dostanou sice menší, zato ale zcela jistě. [12]

Těžba v poolu

Těžební pooly (skupiny) spojují mnoho stovek až tisíc těžařů pomocí specializovaných protokolů. Jejich těžební hardware zůstává připojen ke skupinovému serveru během těžby a synchronizuje tak jejich úsilí s ostatními těžaři. Jejich spojený výkon poskytuje větší šanci, že některý z nich získá odměnu, kterou poté sdílejí. Ta je připsána bitcoinové adrese skupiny, místo individuálnímu těžaři. Z té jsou poté zasílány periodické platby na bitcoinové adresy těžařů, pokud na ni mají nárok. Obvykle je tato odměna snížena o procentní poplatek jako odměnu za poskytování služeb. [4]

Pooly jsou otevřené všem těžařům bez ohledu na velikost dosaženého hashe nebo profesionalitu. Aby těžař získal podíl na zisku, je nastavena mnohonásobně nižší obtížnost, než je obtížnost sítě. Princip je podobný, jako kdyby všichni těžaři házeli kostkou. Odměna by přitom byla skupině připsána, pokud by některý z nich hodil číslo například menší než tři. Nárok na podíl by měl ale zároveň každý, kdo by hodil alespoň číslo menší než pět. To zajistí, aby se těžba vyplatila i menším těžařům. Kryptoměny totiž mají fungovat decentralizovaně. Čím více těžařů je zapojeno, tím menší je šance na napadení tak, že by se část těžařů pokusila převzít kontrolu. Pokud by totiž nějaký pool dosáhl více než 50 % podílu na celkovém výkonu sítě, mohl by teoreticky do blockchainu zanést nepravdivé informace. Tomu se pochopitelně všichni poctiví účastníci snaží předejít. [4]

V současnosti se nejvíce těžebních poolů nachází v Číně. Uvádí se, že u Bitcoinu působí více než 80 % těžařů ve skupinách provozovanými právě Čínou. Mezi největší patří BTC.com, AntPool nebo ViaBTC. Desetina připadá údajně na Českou republiku, zejména díky skupině SlushPool, která byla vůbec prvním těžebním poolem na světě. [37] U Litecoinu dva největší (čínské) pooly dosahují podílu na výkonu přes 60 % a u Etherea dosahují tohoto podílu pooly tři. [38] To ukazuje, že kryptoměny jsou sice decentralizované, většina těžby se však odehrává ve skupinách. Tyto skupiny jsou ještě k tomu většinou organizovány na jednom území. To s sebou nese hrozbu, na kterou opět odpůrci často upozorňují.

Těžba v multipoolu

Tento způsob je podobný jako těžba v poolu. Rozdílem je to, že nedochází k těžbě jedné konkrétní kryptoměny, ale několika. Výběr toho, která kryptoměna bude těžena, závisí na její aktuální profitabilitě. Těžba v multipoolu tak využívá změny náročnosti jednotlivých kryptoměn. Problém ale může nastat ve chvíli, kdy se v multipoolu shlukne velké množství těžařů. Pokud nepříliš známý Altcoin začne být těžen obrovským výpočetním výkonem, může dojít k zahlcení systému a výraznému

skokovému nárůstu náročnosti těžby. Tím pádem dojde i k poklesu rychlosti vytvoření nového bloku. Ve chvíli, kdy se tak stane, se multipoolu přesune k jiné kryptoměně. Těžba původní měny se ale stane nerentabilní až do chvíle, než dojde k dalšímu přepočtení náročnosti. To může trvat i velmi dlouho, což může mít za následek paralyzaci funkcí nebo i ukončení činnosti kryptoměny. Z toho důvody jsou některé kryptoměny navrženy tak, aby byla jejich náročnost přepočítávána a měněna podstatně častěji. [8]

Cloudová těžba

Cloudová těžba cílí na uživatele, kteří nechtějí nebo nemají možnost či schopnosti zprovoznit vlastní těžební soustavu. O veškeré technické provedení a údržbu se stará společnost, od které si uživatel může koupit těžební kontrakty. Největší výhodou je úspora počáteční investice, času i starostí s provozováním těžebního vybavení. Na druhou stranu je zisk logicky výrazně menší kvůli platbám za službu. Cloudovou těžbu je možné využít několika způsoby. Je možný pronájem těžebního zařízení, které si nájemce nastaví na libovolnou kryptoměnu a nese za něj veškerou odpovědnost. Druhým způsobem je pronájem pouze těžebního výkonu bez nutnosti spravovat hardware. Naopak je možný i způsob, kdy poskytovatel služeb nabízí těžařům odkup jejich výpočetního výkonu. [8]

4.2.2 Podle těžebního vybavení

Těžební vybavení určuje, jakého výkonu je těžař schopen dosáhnout. Výkon se vyjadřuje jako hodnota hashrate. Ten udává, kolikrát je možné nalézt řešení konkrétního těžebního algoritmu za jednu vteřinu. Pokud je např. hashrate celé sítě 10 TH/s, znamená to, že je schopna provést deset bilionů výpočtů za sekundu. [39] Spotřebovaný výpočetní výkon pak odpovídá násobku hashrate a doby nutné k nalezení výsledku. Hashrate, kterého je konkrétní těžební hardware schopen dosáhnout se liší pro jednotlivé kryptoměny, protože se liší jejich těžební algoritmy. Pro každou jednotlivou kryptoměnu je tak nutné vybrat nejvhodnější vybavení podle toho, jestli algoritmus k výpočtům využívá výpočetní výkon nebo operační paměť.

Procesory (CPU)

Nejzákladnější myšlenkou kryptoměn je jejich decentralizace. Původní představa byla tedy taková, že k těžbě kryptoměn budou využívány standartní procesory. Ty se nacházejí ve všech osobních počítačích lidí po celém světě. Jelikož je však doba vytěžení bloku konstantní, je odměna za to stále stejná bez ohledu na celkový výkon, který těžaři dodávají. V případě, že jeden těžař zvýší svůj hashrate, se tedy jeho odměna zvýší na úkor ostatních. Je-li proto vynalezena nová technologie, musí na ni přejít každý těžař, aby držel krok s konkurencí. Celkový dodávaný hashrate se zvýší, což vede k navýšení obtížnosti těžby tak, aby doba vytěžení bloku zůstala zachována. Těžaři tak pouze dodají větší výkon za stejnou

odměnu, kterou by dostali, kdyby nikdo z nich na novou technologii nepřešel. Protože došlo k vyvinutí nových komponent, procesory se dnes pro výpočty už prakticky nepoužívají.

Grafické karty (GPU)

Po procesorech se začalo přecházet na grafické karty. Nejprve se využívalo jednotek grafických karet umístěných např. ve výkonných herních počítačích. Později těžaři začali skládat soustavy z mnoha grafických karet, zvaných těžební Rigy. Rig se může skládat z nosné konstrukce, zdroje, harddisku, paměti RAM, procesoru, základní desky pro osazení grafických karet a samotných karet. Těch může být v řádu jednotek až několika desítek. [40] Rig složený z šesti grafických karet je na obrázku 7.

Obrázek 7) Těžební Rig s grafickými kartami [40]

Přechodem těžby z procesorů na grafické karty došlo obecně k navýšení výkonosti těžby zhruba sedmdesátkrát. [41] Těžba pomocí grafických karet se používá i v současnosti, a to především pro kryptoměny, jejichž těžba je náročná na operační paměť.

Programovatelná hradlová pole (FPGA)

FPGA (Field Programmable Gate Array) jsou logické integrované obvody, které se skládají z konfigurovatelných logických bloků (CLB). Tato polovodičová zařízení jsou programovatelná až po výrobě, takže mohou být nastavena podle požadavků zákazníka. Propojením logických bloků lze vytvořit zařízení jako je mikroprocesor, paměť atd. [42]

Programovatelná hradlová pole dosahovala srovnatelného výkonu jako sestavy grafických karet, avšak při zhruba pětinové spotřebě elektřiny. [41] Dnes už se ale nevyužívají, protože byla nahrazena technologií ASIC.

ASIC (Application Specific Integrated Circuits)

ASIC čipy se od FPGA liší v tom, že jsou naprogramovány pro specifické použití již během výroby. Mohou proto být vyrobeny tak, aby jejich jediným úkolem bylo řešení těžebního algoritmu. Stovky takových čipů se potom osazují do tzv. minerů. Díky tomu jsou schopné dosáhnout až stonásobného výkonu s třistanásobně nižší spotřebou energie oproti ostatním technologiím. Zároveň ale nemohou být použity k ničemu jinému. [42] Obrázek 8 ukazuje Antminer S9, který se požívá typicky k těžbě Bitcoinu.

Obrázek 8) Antminer S9 [43]

ASIC se navíc programují pouze k řešení algoritmů SHA-256 a Scrypt. S jejich pomocí tak nelze těžit všechny kryptoměny. Z kryptoměn, které jsem představil, je požívají pouze Bitcoin, Bitcoin Cash (oba SHA-256) a Litecoin (Scrypt). Existuje řada dalších alternativních měn používajících tyto algoritmy, z mého pohledu se však jedná o natolik neznámé až nedůvěryhodné měny, že bych o jejich těžbě ani neuvažoval. [44]

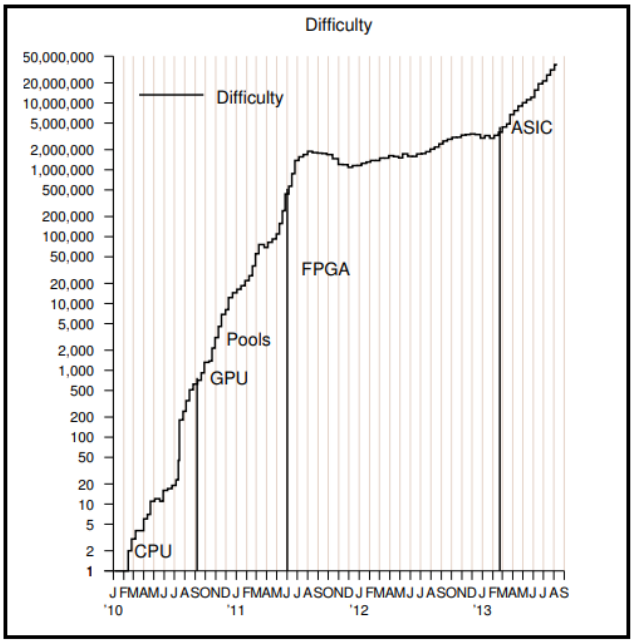
Čipy ASIC jsou jednoznačně nejdražší technologií, což činí těžbu s jejich pomocí privilegovanou. Nemohou si je totižu dovolit všichni těžaři-investoři. Tento fakt opět narušuje myšlenku decentralizace kryptoměn, neboť vede ke stavu, v jakém je dnes např. bitcoinová síť. U té až 80 % všech těžařů působí v poolech v Číně. [37] Z toho důvodu přicházejí vývojáři s takovými algoritmy, aby nové kryptoměny nebylo možné těžit na zařízeních ASIC. Výsledkem je, že kromě Bitcoinu a Bitcoinu Cash se dnes více známějších kryptoměn těží pomocí Rigů z grafických karet.

Těžební hardware musí být samozřejmě oživen programem podporujícím těžbu vybrané kryptoměny. Na trhu je jich velké množství, jako například Nice Hash nebo Miner Gate, softwarem se však v této práci nebudu zabývat.

4.3 Technická náročnost těžby

Už v předešlém textu jsem vysvětlil, že většina kryptoměn je navržena tak, aby k vytěžení bloku docházelo pravidelně za předem stanovený časový úsek. Ať už se tedy na těžbě podílí jediný osobní počítač, jehož hashrate se pohybuje v jednotkách MH/s nebo tisíce nejmodernějších těžebních soustav, musí být složitost výpočtu nastavená tak, aby byl tento čas zachván. Z toho důvodu se cílová obtížnost často mění podle výkonu celé sítě. Náročnost těžby vyjadřuje, jak těžké je nalézt hash menší než cílová obtížnost. [8]

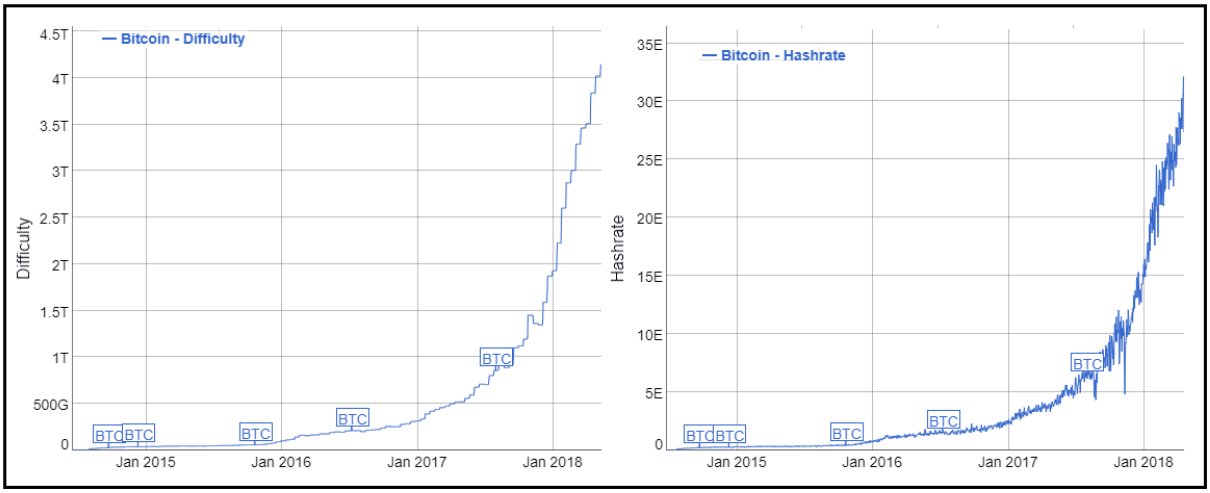
Proces změny obtížnosti je dobře pozorovatelný u Bitcoinu, který byl postupně těžen všemi vynalezenými technologiemi. V roce 2010 došlo k obrovskému nárůstu výkonu a tím i ke změně náročnosti těžby vinou přechodu z technologie CPU na GPU. Ke stejné situaci došlo i o rok později, kdy grafické karty nahradila FPGA. Následovaly dva roky bez větších změn a poté příchod technologie ASIC (vše 4.2.2) s dalším obrovským nárůstem těžební síly. Změnu obtížnsti s příchodem nových technologií zachycuje obrázek 9. [45]



Obrázek 9) Obtížnost těžby Bitcoinu v čase [45]

ASIC umožnila umístění funkce SHA256 přímo na křemíkové čipy specializované pro účely těžby. Jeden takovýto čip může vyvinout více těžebního výkonu, než celá bitcoinová síť v roce 2010. Po roce 2013 se ASIC stávaly stále hustšími, blíže technologickým možnostem výroby křemíku s rozlišením dvaadvacet a později šestnáct nanometrů. Poté byl závod o hustotu čipů nahrazen závodem o vyšší hustotu výpočetních center, ve kterých mohou být umístěny tisíce těchto čipů. Prostory jsou omezeny především potřebou odvádění tepla a poskytování odpovídající elektrická energie. [4]

K opravdu velkým nárůstům výkonu (hashrate) a náročnosti (difficulty) však začalo docházet až po roce 2016, jak ukazuje obrázek 10. Náročnost těžby je dnes více než 80 000krát vyšší, než tomu bylo při příchodu čipů ASIC. [46]



Obrázek 10) Změna hashrate a náročnosti u BTC po roce 2015 [46]

Podle mého názoru je to zapříčiněno hlavně obrovským nárůstem zájmu o kryptoměny a růstem jejich cen (3.3.2). Cena kryptoměn je totiž klíčovým parametrem ovlivňujícím náročnost těžby. Pokud je cena vysoká, je těžba rentabilní i s pomocí zařízení, které mají vyšší pořizovací i provozní náklady. Pokud navíc těžař očekává růst cen, může se rozhodnout dočasně těžit i se ztrátou a očekávat zhodnocení kryptoměny v čase. Cena je ale i naopak ovlivňována náročností těžby, protože nové mince vznikají pouze při těžbě. Nelze tedy očekávat, že by je těžaři prodávali levně, pokud museli vynaložit velké finanční úsilí k jejich získání.

Jak je vidět z obrázku 10, obtížnost těžby zatím neustále stoupá, zatímco cena kryptoměn obecně stoupala pouze do konce roku 2017. Během roku 2018 zažívá spíše sestup, což by se mělo negativně projevit na rentabilitě těžby.

Pokud bude cena kryptoměn nadále klesat, mělo by to vést k odlivu části těžařů, jejichž náklady na energii jsou nejvyšší. Celkový hashrate sítě a tím i náročnost by měli klesat, aby byli těžaři ochotni prodávat nové mince za tržní cenu. Pokud bude naopak poptávka po nových mincích dostatečná, budou je investoři ochotni nakupovat i za vyšší cenu, která odpovídá současným vysokým nákladům na těžbu. Cena kryptoměn by potom mohla začít opět růst.

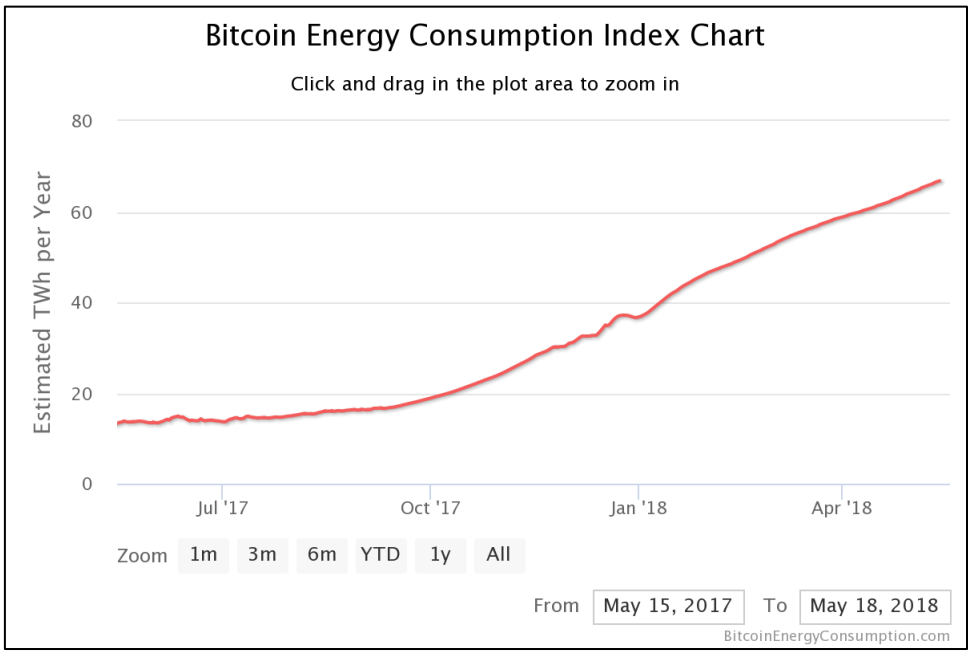
Který ze scénářů nastane ukáže až čas. Myslím si ale, že současný stav vysokého růstu náročnosti těžby a nižší ceny kryptoměn není dlouhodobě udržitelný.

4.4 Energetická náročnost těžby

Těžba kryptoměn, která zajišťuje jejich chod, spotřebovává velké množství elektrické energie. Platí to zejména u měn využívající metodu proof-of-work. Tou je referenční Bitcoin a měny ním inspirované jako je Litecoin, Ethereum nebo Monero. Bitcoin, jako stále největší kryptoměna, má na této spotřebě jednoznačně největší podíl. Podle serveru "Bitcoin Energy Consumption Index", který poskytuje aktuální odhady spotřeby energie nejen bitcoinové sítě, spotřebuje jen Bitcoin ročně přes 66 TWh elektrické energie. Toto číslo navíc velmi rychle roste. [47]

Jak rychle spotřeba roste dokládá následující případ. V březnu roku 2016 provedl environmentální výzkumník Sebastiaan Deetman výzkum ohledně předpokládané spotřeby energie v roce 2020. Deetman výzkum provedl v optimistické a pesimistické variantě, přičemž vycházel ze spotřeby a tempa růstu těžení. Uvažoval přitom i zvyšující se účinnost těžebních čipů ASIC. [48]

Výsledky byly alarmující. I při optimistické variantě by v roce 2020 vytěžení jediného Bitcoinu spotřebovalo okolo 5 500 kWh, což je zhruba půlroční spotřeba běžné americké domácnosti. Pokud by polovina této energie byla vyrobena z fosilních paliv, uvolnilo by se tím do ovzduší na 4 000 kg oxidu uhličitého. Pesimistická varianta předpokládala takový průběh, kdy bitcoinová síť spotřebuje za rok více energie než celé Dánsko. Daleko horší je ale fakt, že tohoto stavu bylo dosaženo již v prosinci 2017. Pesimistická varianta tedy nastala více než o dva roky dříve, než autor předpokládal. Současných 66 TWh již odpovídá roční spotřebě České republiky. Více už spotřebuje pouze čyřicet zemí světa. [48] Odhad energetické spotřeby bitcoinové sítě za minulý rok je zachycen na obrázku 11.



Obrázek 11) Odhadovaná spotřeba bitcoinové sítě [47]

Podle odhadů by se roční spotřeba bitcoinové sítě na během roku 2019 mohla vyšplhat až na 125 TWh, což je zhruba roční spotřeba Holandska. Již teď přitom jediná bitcoinová transakce vypotřebuje pětkrát více energie než 100 000 transakcí VISA. [47]

Tabulka 2 uvádí některé statistiky dvou největších kryptoměn Bitcoin a Ethereum. Ty využívají energeticky náročnou metodu důkazu prací.

Tabulka 2) Statistiky sítě Bitcoin a Ethereum [47]

Statistika	Bitcoin	Ethereum
Odhadovaná roční spotřeba elektřiny [TWh]	66,81	19
Roční příjmy z těžby [USD]	7 013 774 044	6 293 866 568
Roční náklady na těžbu [USD]	3 340 362 318	2 279 557 354
Celkový hashrate sítě [PH/s]	32 502	0,27
Spotřeba energie na transakci [KWh]	895	65
Počet domácností, které by energie sítě poháněla	6 185 856	1 758 918
Spotřeba elektřiny jako % celosvětové spotřeby	0,30 %	0,09 %
Roční uhlíková stopa [Kilotun CO2]	32 736	-

Z tabulky je zřejmé, že přestože je energetická náročnost obrovská, roční náklady na těžbu jsou stále významně menší než její profit. Za těchto okolností tedy nelze očekávat výrazné snížení počtu těžařů. Ti se však často stěhují do míst s velmi nízkou cenou elektřiny, jako je například Venezuela nebo Čína. Zde se cena elektřiny za kWh pohybuje mezi 3-6 centy USD. Konktrétně v Číně, která se na těžbě kryptoměn odhadem podílí z 60-80 %, pochází až téměř 60 % energie z uhelných zdrojů. To s sebou nese i významnou uhlíkovou stopu. Ta je podle tabulky 2 v případě Bitcoinu až třicet dva tisíc kilotun oxidu uhličitého ročně. [49] Kryptoměny tak nejenže spotřebovávají energii, která by mohla být využita k přínosnějším účelům, ale zároveň se nezanedbatelně podílejí na znečišťování planety. Pokud se tak mají z dlouhodobého hlediska prosadit, bude nutné tyto problémy odstranit.

Jako reakce na tuto ohromnou spotřebu vznikají kryptoměny založené na jiných metodách ověřování transakcí s nižší spotřebou energie, jako je proof-of-stake (2.2.3). Tyto Altcoiny se však ještě neprokázaly být tak promyšlenými jako jejich předchůdci. Řešením by bylo rovněž zprovoznění takzvané Lightning Network (4.2), na které se však zatím pouze pracuje.

I když existuje více kryptoměn, princip hodnocení investice je pro všechny stejný. Z toho důvodu provedu výpočty pouze pro jednu kryptoměnu, tržního vůdce Bitcoin. Pro zhodnocení investice do těžby jiné kryptoměny by bylo možné postupovat podle stejné metodiky (5.1), pouze se změnou některých vstupních parametrů. Výsledek je navíc silně ovlivněn cenou zkoumané kryptoměny a jak jsem uvedl, ceny kryptoměn mají obecně vysoký korelační koeficient (3.3.1). Jelikož budu při výpočtech zkoumat změnu ceny Bitcoinu, byl by tak závěr pravděpodobně podobný i pro většinu ostatních kryptoměn.

5 Ekonomické zhodnocení těžby BTC

V této části práce se pokusím odpovědět na často pokládanou otázku, zda se v současnosti stále ještě vyplatí těžit Bitcoin. Už nyní ale musím upozornit, že jednoduchá odpověď neexistuje. Jak jsem uvedl v úvodu práce (1), pokud by všechny parametry zůstaly konstantní, těžba se v současnosti z ekonomického pohledu nevyplatí. To je ale možné zjistit prostým zadáním hodnot do internetové kalkulačky a není to cílem této práce. Výnos z těžby ale záleží na mnoha vstupních parametrech, které jsou pro každého člověka jiné, nebo se během doby investice nepředvídatelně mění. Do první skupiny patří například velikost vstupní investice, cena elektrické energie nebo hashrate (4.2.2) a spotřeba zakoupeného vybavení. Tyto hodnoty zvolí těžař na začátku a poté se již nemění. Ve své práci dosadím do těchto proměnných typické nebo průměrné hodnoty. Ve skutečnosti bude mít ale každý člověk vstupy o něco odlišné. Druhou skupinou jsou proměnné, které se mění během návratnosti investice. Jsou jimi prodejní cena Bitcoinu (3.3) a obtížnost jeho těžby (4.3). Na tyto dva parametry zaměřím největší pozornost při svých výpočtech.

Změna obtížnosti těžby je proces, který se děje na základě vývoje celkového výkonu sítě. Ten závisí na počtu těžařů v síti a na právě dostupné technologii. Díky tomu lze, i když obtížně, náročnost těžby predikovat. O to se pokusím na základě historických dat a vlastních předpokladů. Prodejní cena je ale závislá pouze na nabídce a poptávce trhu. I když existují různé nástroje k hledání trendů, například vývoje cen akcií, jedná se o metody založené na předpokladech, které nemusí platit. Věřím, že nikdo na světě není schopen ceny kryptoměn spolehlivě předpovídat, a proto se o to nebudu pokoušet ani já.

Z toho důvodu jsem vytvořil vlastní obecnou metodiku pro kalkulaci zisku, která počítá se změnou prodejní ceny a změnou náročnosti během těžby (5.1). Cílem nebude zjistit, zda se těžba vyplatí se současnými, neměnnými hodnotami. Místo toho se pokusím určit, jakým tempem by cena musela růst při předpokládaném zvyšování náročnosti těžby tak, aby se čistá současná hodnota investice rovnala nule. Výsledek bude tedy například takový, že při zakoupení běžně dostupného zařízení by cena Bitcoinu musela stoupnout na X Kč, aby byla investice rentabilní i se započítáním časové ceny peněz a příplatkem za riziko. Jeden rozhodovatel pak bude možnost považovat za zajímavou, zatímco druhý ne. Záleží na jejich osobním založení a predikci ceny (3.3.2). Dále uvažuji dva způsoby monetizace, kdy k prodeji kryptoměny dochází buď hned, jakmile je to možné, nebo až po ukončení činnosti.

5.1 Metodika

Pro výpočet provozního zisku z těžby Bitcoinu za N dní vyjdu z rovnice 1, kterou jsem sestavil na základě informací z diskuzních fór. Měla by odpovídat vzorci, který používá většina internetových kalkulaček. [50]

$$Zisk_N = \frac{N * S * H * R * (1 - f) * P_{BTC}}{D * 2^{32}} - N * P_E * C * h \qquad 1$$

N… počet dní při nichž těžba probíhá
S… počet sekund za den (86 400)
H... hashrate použité těžební soustavy [H/s]
R… odměna za jeden vytěžený blok [BTC]
f… poplatek těžebnímu poolu [%]
P_{BTC}... prodejní cena jednoho Bitcoinu [Kč]
D… obtížnost těžby [-]
*2^{32}… pomocné číslo (čas = obtížnost * 2^{32}/hashrate)*
P_E… cena elektřiny [Kč/kWh]
C… spotřeba elektřiny použité těžební soustavy [kW]
h… počet hodin za den (24)

Žlutou barvou je znázorněno množství vytěžené kryptoměny, zeleně její prodejní cena a červeně výdaje na těžbu (viz rovnice 2). Co se týká jednotlivých parametrů v rovnici, téměř všechny mohu jednoduše vyčíslit. U Bitcoinu se obtížnost těžby kontroluje podle průměru času vyřešení za poslední 2 týdny a poté dojde k její úpravě. Počet dní N tedy nastavím na čtrnáct dní, protože po tuto dobu se obtížnost nebude měnit. Samotná obtížnost D je číslo veřejně dostupné na internetu. Počet sekund za den S a počet hodin za den h je znám. Hashrate H a spotřebu C každého těžebního zařízení udává výrobce. Tyto parametry dosadím až provedu výběr nejoptimálnějšího mineru ASIC. Výběr je popsaný v podkapitole těžební vybavení (5.2.1). Odměna za vytěžený blok R je v současné době konstantní a sníží se na polovinu až koncem května 2020. Zůstane proto po celou dobu těžby neměnná. Poplatek těžebnímu poolu se pohybuje typicky od 0 do 2 %. Cena elektrické energie P_E vychází v rovnici 1 z ceny za kWh, stejně jako u internetových kalkulaček. Ve skutečnosti ale probíhají platby za elektřinu formou záloh. Tuto skutečnost zachycuji v rovnici 3. Ke stanovení výše záloh provedu důkladnější průzkum trhu, popsaný v podkapitole cena elektrické energie (5.2.2).

Jedinou neznámou v rovnici zůstává cena Bitcoinu P_{BTC} v době prodeje. Ostatní, konstantní parametry z rovnice 1 lze sloučit a vzorec tak zjednodušit na rovnici 2. Ta popisuje obecný zisk z těžby za dva týdny. Během této doby se nemění obtížnost a tím pádem jsou množství vytěžené kryptoměny a výdaje k tomu vynaložené známé.

$$Zisk_{14} = množství_{14} * P_{BTC} - výdaje_{14} \qquad 2$$

Těžba bude samozřejmě probíhat déle než dva týdny. Fyzická životnost hardwaru může dosahovat až tří let. Její stanovení pro výpočet bude popsáno v podkapitole životnost zařízení (5.2.5). Stav z rovnice 2 bude platit vždy jen čtrnáct dní, poté dojde ke změně obtížnosti o x procent, čímž se změní množství vytěžené kryptoměny. Cashflow za G čtrnáctidenních časových úseků během životnosti zařízení tak popisuje rovnice 3.

$$CF_G = \left(\sum_{i=1}^{G} \frac{Q * P_{BTC}}{D * (1+x)^{i-1}} \right) - m * záloha \qquad 3$$

Q… člen $N * S * H * R * (1-f)/2^{32}$ z rovnice 1
x… změna obtížnosti za 14 dní [%]
G… počet čtrnáctidenních časových úseků za životnost zařízení
m… počet měsíců za životnost zařízení
záloha… pravidelná platba dodavateli energií [Kč]

Změnu obtížnosti těžby x se pokusím predikovat v podkapitole obtížnost těžby (5.2.3) na základě historických dat a vlastního názoru. Měsíční zálohu spočítám v podkapitole cena elektrické energie (5.2.2). Nalezené hodnoty potom dosadím do rovnice 3.

Jediným faktorem ovlivňujícím příjem z těžby tak zůstane prodejní cena Bitcoinu. Jsou tak možné dvě různé strategie: prodávat kryptoměnu po částech hned jakmile ji vytěžím nebo ji kumulovat a prodat všechnu najednou až po ukončení těžby.

5.1.1 Strategie okamžitého prodeje (S1)

Při aplikování této strategie bude k prodeji vytěženého množství Bitcoinu docházet hned, jakmile to bude možné. Cena kryptoměn se sice mění neustále, k prodeji však bude docházet jen jednou za časový úsek. Minimální výběr při těžbě v poolu totiž bývá omezen, typicky hodnotu kolem 0,01 BTC. Nabízí se tak prodej jednou za čtrnáct dní. V tomto případě znám cenu Bitcoinu na začátku těžby, která se bude měnit o y procent jednou za čtrnáctidenní období. Těch je za životnosti zařízení počet G. K prodeji dojde vždy na konci této periody. Zálohy jsou placené dopředu měsíčně, celkem m-krát za životnost. Doplnění této skutečnosti do rovnice 3 dostanu rovnici 4, která popisuje cashflow z těžby za životnost zařízení při aplikaci strategie 1.

$$CF_{\check{z}iv,S1} = \left(\sum_{i=1}^{G} \frac{Q * P_{zac} * (1+y)^{i}}{D * (1+x)^{i-1}} \right) - m * záloha \qquad 4$$

P_{zac}… cena Bitcoinu v den začátku těžby [Kč]
y… změna ceny za 14 dní [%]

Ke zhodnocení investice použiji ukazatel "čistá současná hodnota" NPV[8]. Ta bere v úvahu časovou hodnotu peněz, závisí na předvídaných hotovostních tocích a alternativních nákladech kapitálu. NPV je dáno předpisem:

$$NPV = -I + \sum_{i=1}^{n} \frac{CF_i}{(1+r)^i} \qquad 5$$

I… počáteční investice [Kč]
CF… hotovostní toky v průběhu investice [Kč]
r… diskontní úroková míra [-]

Diskontní úrokovou míru (5.2.4) stanovím dále v této práci v příslušné podkapitole. Počáteční investice bude známá po výběru těžebního vybavení (5.2.1). CF_i je v tomto případě rovno členům na pravé straně rovnice 4. Jejich dosazením do rovnice 5 dostanu rovnici 6.

$$NPV = -I + \sum_{i=1}^{G} \frac{\frac{Q * P_{zac} * (1+y)^i}{D * (1+x)^{i-1}}}{(1+r_p)^i} - \sum_{j=1}^{m} \frac{záloha}{(1+r_q)^{j-1}} \qquad 6$$

r_p… diskontní úroková míra pro období 14 dní [-]
r_q… diskontní úroková míra pro období 1 měsíc [-]

V této rovnici jsou na pravé straně známé všechny parametry kromě y. Abych y nalezl, položím NPV rovno nule a použiji řešitele v excelu. Získám tak číslo vyjadřující, o kolik procent by se cena musela průměrně měnit za čtrnáct dní, aby příjmy pokryly počáteční investici i se započítáním diskontní úrokové míry. Jelikož je NPV rovno nule, je tato míra rovna vnitřnímu výnosovému procentu investice. Rozhodnutí se pak bude lišit pro každého rozhodovatele podle jeho předpokladu vývoje ceny a postoji k riziku.

5.1.2 Strategie kumulování (S2)

Při aplikování této strategie bude vytěžené množství Bitcoinu uchováváno a k jeho prodeji dojde najednou až po ukončení těžby. V tomto případě je důležité pouze množství vytěžené kryptoměny za životnost a výdaje na těžbu. Vyjdu-li z rovnice 1, mohu vynechat prodejní cenu P_{BTC}, neboť v tomto případě nebude k prodeji docházet. Rovnici dále rozdělím na dvě nové. Rovnice 7 udává vytěžené množství Bitcoinu za G čtrnáctidenních období. Rovnice 8 uvádí počáteční investici a výdaje na elektrickou energii za m měsíců.

[8] Net Present Value

$$Množství_G = \sum_{i=1}^{G} \frac{N * S * H * R * (1-f)}{D * (1+x)^{i-1}} \quad (7)$$

$$Výdaje_m = I + \sum_{i=1}^{m} \frac{záloha}{(1+r_q)^{i-1}} \quad (8)$$

Parametry v obou těchto rovnicích jsou známé. Dopředu bude tedy možné spočítat, kolik Bitcoinů lze za rok vytěžit, i kolik korun to bude stát. Čistá současná hodnota této investice je:

$$NPV = -Výdaje_m + \frac{Množství_G * P_{BTC}}{(1+r)^j} \quad (9)$$

j… počet let mezi začátkem těžby a prodejem (životnost)
r… roční diskontní úroková míra
P_{BTC}… cena Bitcoinu v době prodeje [Kč]

V této rovnici jsou na pravé straně známé všechny parametry kromě P_{BTC}. Abych ho nalezl, položím NPV rovno nule a použiji řešitele v excelu. Získám tak prodejní cenu, které musí Bitcoin dosáhnou za j let, aby příjmy pokryly počáteční investici i se započítáním diskontní úrokové míry. Rozhodnutí se pak bude lišit pro každého rozhodovatele podle jeho předpokladu vývoje ceny a postoji k riziku.

5.2 Dosazení neznámých parametrů

V této části popíšu výběr parametrů I, H, C, x, r, m, G a záloha, které dosadím do vzorců popsaných v části metodika (5.1).

5.2.1 Těžební vybavení

Při těžbě kryptoměn se předpokládá použití toho nejlepšího možného vybavení, aby už od začátku nebyla konkurence ve výhodě. To, který ASIC je v dané chvíli nejlepší, závisí ale na více parametrech. Těmi jsou jeho cena neboli investice I, hashrate H, kterého je stroj schopen dosáhnout a spotřeba C, kterou při tom má. Dostupná zařízení přitom většinou dominují pouze v jednom parametru na úkor ostatních. K výběru proto použiji vícekriteriální hodnocení variant, konkrétně metodu globálního kritéria.

Tato metoda pracuje se subjektivně stanovenými vahami kritérií. Je schopná porovnat parametry, i když jsou některé maximalizační, zatímco jiné minimalizační. Myslím, že nejdůležitějším parametrem je hashrate, protože ten jediný ovlivňuje množství vytěžené kryptoměny. Závisí na něm tak velikost příjmů po celou dobu investice. Jeho podíl na celkovém rozhodnutí proto nastavím na 50 %.

Pořizovací cena je naopak vynaložena jednorázově a v případě velmi kvalitního vybavení by mělo dojít k jejímu rychlému navrácení. Váhu pro I proto uvažuji 20 %. Zbylých 30 % rozhodnutí bude záviset na spotřebě C, která ovlivňuje výdaje v celém průběhu těžby a je proto druhým nejdůležitějším parametrem.

Podle mého průzkumu je nyní jedničkou na trhu Bitmain Antminer S9. Tento ASIC dosahuje hashratu 14,5 TH/s, při spotřebě 1365 W. Jeho cena se přitom pohybuje kolem 16 000 Kč. [51]

Nově se však mají na trhu objevit také minery GMO Miner B3 a Whatsminer M10 s termínem doručení 25.10.2018. Oba mají dosahovat hashrate 33 TH/s. [52], [53] ASIC B3 to zvládne se spotřebou 3417 W za cenu 1999 USD. ASIC M10 stojí 1488 USD a spotřebovává 2145 W. S použitím kurzu 22 Kč/1 USD a započítáním dopravy budu počítat s cenami 44 500 Kč za B3 a 33 000 Kč za M10. Přehled parametrů ASIC, mezi nimiž se budu rozhodovat, a použitých kritérií i s jejich vahami a typem je shrnut v tabulce 3.

Tabulka 3) Parametry ASIC (zdroj: vlastní)

	Investice [Kč]	**Hashrate [TH/s]**	**Spotřeba [W]**
Typ	MIN	MAX	MIN
Váha	0,2	0,5	0,3
S9i	16000	14,5	1365
GMO B3	44500	33	3417
M10	33000	33	2145

Aby se různá kritéria dala porovnávat, je nejprve nutné všechna převést na maximalizační. Toho dosáhnu tak, že pro každé kritérium vždy vynásobím jejich maximum a minimum a následně ho podělím převáděnou hodnotou. Tabulka 4 ukazuje parametry jednotlivých zařízení s maximalizačními kritérii.

Tabulka 4) Parametry ASIC s MAX kritérii (zdroj: vlastní)

	Investice [Kč]	**Hashrate [TH/s]**	**Spotřeba [W]**
Typ	MAX	MAX	MAX
Váha	0,2	0,5	0,3
S9i	44500	14,5	3417
GMO B3	16000	33	1365
M10	21576	33	2174

Dalším krokem je pak normování hodnot. Pro každé kritérium se nejprve vybere maximální hodnota a tou se poté podělí příslušné normované hodnoty. V posledním kroku se pro každý ASIC provede součet vážených hodnot jednotlivých kritérií a výsledky se porovnají. Nejvyšší hodnota značí nejlepší výsledek, přičemž nejvyšší teoretická hodnota je 1. Výsledky metody globálního kritéria ukazuje tabulka 5.

Tabulka 5) Výsledek metody globálního kritéria (zdroj: vlastní)

	Investice [Kč]	Hashrate [TH/s]	Spotřeba [W]	Vážený součet
Typ	MAX	MAX	MAX	
Váha	0,2	0,5	0,3	
S9i	1,00	0,44	1,00	0,72
GMO B3	0,36	1,00	0,40	0,69
M10	0,48	1,00	0,64	0,79
Maximum	44500	33	3417	

Metoda globálního kritéria vícekriteriálního hodnocení variant vybrala jako nejlepší ASIC Whatsminer M10. Přestože ani v jednom z kritérií nebyl jednoznačně nejlepší, při započítání vážených, normovaných hodnot všech kritérií vyšel jako vítěz. Výpočet je k dispozici v dokumentu excel v listu VH, který je přílohou této práce. Pokud by tak někdo např. chtěl volit jiné váhy pro použitá kritéria, hodnoty jsou snadno nahraditelné. Výsledek ale odpovídá mému očekávání. Domnívám se, že nejvýhodnější je začít těžit s novým produktem. Jak jsem nastínil v kapitole těžba kryptoměn (4), těžba je hra s nulovým součtem. Přejitím na novější produkt dříve, než konkurence znamená vyšší výnos na jejich úkor, neboť se zvýší obtížnost sítě při zachování stejné odměny.

Při výpočtech budu tedy uvažovat se zakoupením jednoho Whatsmineru M10 za cenu 33 000 Kč. Jeho hashrate H bude 33 TH/s při spotřebě 2145 W. S termínem doručení 25.10.2018 a týdenní rezervou na zprovoznění uvažuji se začátkem těžby k 1.11.2018.

5.2.2 Cena elektrické energie

Cena elektrické energie je rozdílovým parametrem mezi jednotlivými těžaři. Technologie jsou víceméně dostupné všem stejně, cenu elektřiny ale může mít každý odlišnou. V České republice jsou ceny bohužel obecně vyšší, než tomu je v některých zemích světa. Díky tomu mají tamní těžaři konkurenční výhodu. Naopak ale jistě existují i země, kde se těží v nepříznivějších podmínkách. V této práci budu počítat s takovou cenou elektřiny, kterou bych si mohl jako soukromá osoba sjednat v Praze. Různí dodavatelé nabízejí v různých krajích odlišné ceny, někdo proto zaplatí více, někdo méně. Dosazení mírně odlišných hodnot do rovnic pak může provést každý podle svých osobních podmínek.

Při výpočtech budu kalkulovat s cenami elektřiny, které odpovídají dvěma různým sazbám: D02d a D57d. Uvažuji přitom, že cena elektrické energie zůstane po dobu těžby konstantní. Obecně má ale spíše rostoucí tendeci a v horizontu několika let tak pravděpodobně nebude možné se stanovenými cenami počítat. Z toho důvodu je součástí práce i citlivostní analýza na změnu ceny elektrické energie (5.3.4).

D02d

Jedná se o jednotarifovou distribuční sazbu elektřiny pro běžně vybavenou českou domácnost se střední spotřebou. Nejsou zde žádné podmínky pro přiznání. Najdeme ji ve zhruba 65 % všech domácností. [54] Spotřeba mnou vybraného mineru M10 je 2,145 kW, což při nepřetržitém provozu odpovídá spotřebě 18 790 kWh/rok[9]. Pro příkon M10 postačí i s rezervou pro ostatní domácí spotřebiče hlavní jistič do 40 A. Pro tyto parametry odběru nabízí kalkulátor cen energií nejvýhodnější nabídku od Bohemia Energy. Rozpis dodávky elektřiny a regulovaných služeb pro tuto nabídku je na obrázku 12. [55]

Položka	Sazba	Období	Počet jednotek	Jednotka	Jednotková cena bez DPH (Kč)	Celkem (Kč)
Silová energie	VT	od 18.10.2018 do 18.10.2019	18790	kWh	0,89900	16 892,21
	NT		0		0,00000	0,00
Měsíční poplatek za odběrné místo			12	měsíc	0,00000	0,00
Daň z elektřiny			18790	kWh	0,02830	531,76
Obchod s elektřinou						17 423,97
Použití sítí	VT	od 18.10.2018 do 18.10.2019	18790	kWh	1,64417	30 893,95
	NT		0		0,00000	0,00
Měsíční poplatek za odběrné místo			12	měsíc	155,00000	1 860,00
Distribuční služby						32 753,95
Systémové služby	SS	od 18.10.2018 do 18.10.2019	18790	kWh	0,09363	1 759,31
Obnovitelné zdroje	PoZE		18790		0,49500	9 301,05
Poplatek OTE za odběrné místo	OTE					64,80
Regulované služby						43 879,11
Celkem bez DPH						61 303,08

Dodávka elektřiny	Základ DPH	DPH	Celkem
Obchod s elektřinou	17 423,97	3 659,03	21 083,00
Regulované služby	43 879,11	9 214,61	53 093,73
Celkem	**61 303,08**	**12 873,65**	**74 176,73**

Obrázek 12) Rozpis dodávky elektřiny a regulovaných služeb v D02d [55]

Cena elektrické energie je podle nabídky 74 176 Kč ročně. Poplatek za odběrné místo 1 860 Kč bez DPH, tedy 2 250 Kč s DPH 21 %, lze ale považovat za utopené náklady. Platili bychom ho totiž i v případě, že by k těžbě nedocházelo. Měsíční zálohu stanovím jako jednu dvanáctinu této ceny.

$$Záloha_{D02d} = \frac{(74176 - 2250)}{12} = \underline{6181\ Kč} \qquad 10$$

[9] *2,145 kW*24 h*365 dní=18 790 kWh*

Zálohy se většinou počítají z předpokládané spotřeby a zaokrouhlují se mírně nahoru. Pro jednoduchost počítám s teoretickým předpokladem, že částka bude 6200 Kč měsíčně. Cena za kWh je v tomto případě 3,82 Kč[10].

D57d

Tato distribuční sazba je dvoutarifová, střídá se zde tedy vysoký a nízký tarif. Nízký tarif přitom platí po dobu 20 h denně. Tato sazba nahrazuje D45d, která musela být přiznána nejpozději do 31. 3. 2016. Je ale určena pro vytápění některými typy topných elektrických spotřebičů a k její získání tak musí být splněny určité podmínky. V odběrném místě musí být používány hybridní nebo přímotopné elektrické spotřebiče pro vytápění objektu nebo systém vytápění s tepelným čerpadlem. Zároveň musí součtový instalovaný příkon těchto spotřebičů činit nejméně 40 % příkonu odpovídajícího hodnotě hlavního jističe před elektroměrem v odběrném místě. [56] Tyto podmínky nesplňuje každý, pokud ale někdo topí elektřinou, lze v jeho případě počítat s cenami této sazby.

Aby byla splněna druhá podmínka, musí příkon těžebního vybavení a ostatních domácích spotřebičů kromě vytápění dosahovat maximálně 60 % celkového odběru. Pokud budu opět uvažovat 2,145 kW pro těžbu a rezervu 10 kW pro domácí spotřebiče, musí celkový odběr domácnosti být alespoň 20,2 kW[11]. Velikost vstupního jističe tak musí být alespoň 63 A[12].

Z celkové spotřeby 18 790 kWh bude 83,3 % odebráno v nízkém tarifu, zatímco 16,6 % v tarifu vysokém[13]. To odpovídá 15 658 kWh v nízkém a 3 131 kWh ve vysokém tarifu. Po dosazení hodnot do kalkulačky energií je opět nejvýhodnější nabídka od Bohemia Energy. Rozpis dodávky elektřiny a regulovaných služeb pro tuto nabídku je na obrázku 13. [55]

Cena elektrické energie je podle nabídky 53 653 Kč. Poplatek za odběrné místo 13 704 Kč bez DPH, tedy 16 581 Kč s DPH, lze ale považovat za utopené náklady. Platili bychom ho totiž i v případě, že by k těžbě nedocházelo. Měsíční záloha je tak:

$$\text{Záloha}_{\text{D57d}} = \frac{(53653 - 16581)}{12} = \underline{3089\ \text{Kč}} \qquad 11$$

Po zaokrouhlení budu počítat s částkou 3100 Kč měsíčně. Cena za kWh je v tomto případě 1,97 Kč[14].

[10] *(74176-2250) Kč/18790 kWh = 3,82 Kč/kWh*
[11] *(2145+10000) W*(100/60) = 20 241 W*
[12] *20 241 W / 400 V = 50,6 A*
[13] *20/24 h = 0,833, 1-0,833 = 0,166*
[14] *(53653-16581) Kč/18790 kWh = 1,97 Kč/kWh*

Položka	Sazba	Období	Počet jednotek	Jednotka	Jednotková cena bez DPH (Kč)	Celkem (Kč)
Silová energie	VT	od 18.10.2018 do 18.10.2019	3131	kWh	0,89900	2 814,77
	NT		15658		0,89900	14 076,54
Měsíční poplatek za odběrné místo			12	měsíc	0,00000	0,00
Daň z elektřiny			18789	kWh	0,02830	531,73
Obchod s elektřinou						17 423,04
Použití sítí	VT	od 18.10.2018 do 18.10.2019	3131	kWh	0,15780	494,07
	NT		15658		0,10190	1 595,55
Měsíční poplatek za odběrné místo			12	měsíc	1 142,00000	13 704,00
Distribuční služby						15 793,62
Systémové služby	SS	od 18.10.2018 do 18.10.2019	18789	kWh	0,09363	1 759,21
Obnovitelné zdroje	PoZE		18789		0,49500	9 300,55
Poplatek OTE za odběrné místo	OTE					64,80
Regulované služby						26 918,19
Celkem bez DPH						44 341,23

Dodávka elektřiny	Základ DPH	DPH	Celkem
Obchod s elektřinou	17 423,04	3 658,84	21 081,88
Regulované služby	26 918,19	5 652,82	32 571,01
Celkem	**44 341,23**	**9 311,66**	**53 652,89**

Obrázek 13) Rozpis dodávky elektřiny a regulovaných služeb v D57d [55]

5.2.3 Obtížnost těžby

Obtížnost D je k 1.11.2018, tedy v okamžiku začátku těžby, 7 184 404 942 701. [57] Z tohoto čísla je možné spočítat, kolik Bitcoinu lze vytěžit během příštích dvou týdnů, během nichž se obtížnost nezmění. Co se ale stane dál mohu a musím jen odhadovat. Vyjdu proto z historie změn v obtížnosti za minulý rok. [57] Data jsou k nahlédnutí pod listem změna_D v excelu, který je přílohou této práce. Z dat vychází následující výpočty.

Průměr

Nejjednodušší metodou odhadu z historických dat je stanovení prostého aritmetického průměru, například pomocí excelu. Ten pro data za poslední rok vychází na změnu +6,07 % každých čtrnáct dní. Výpočet je přílohou této práce.

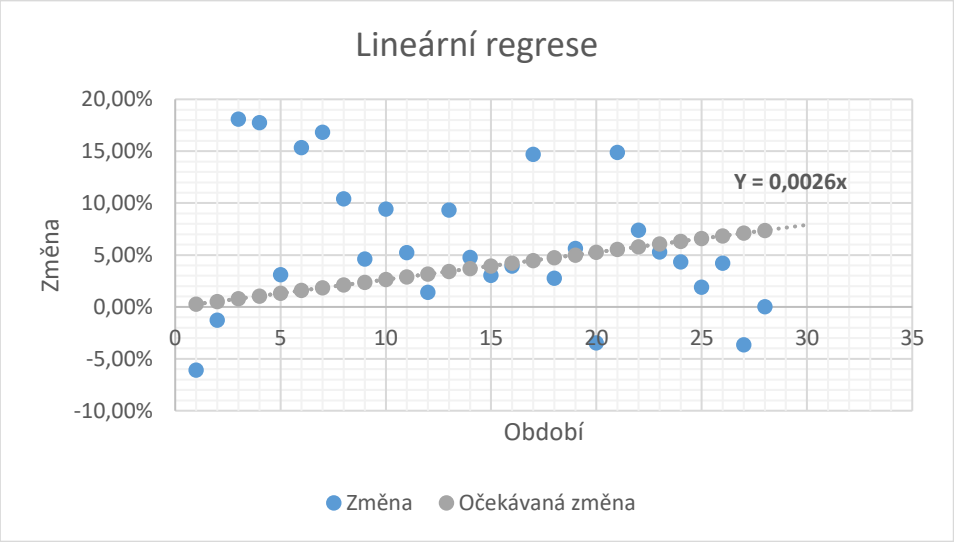
Lineární regrese

Druhou použitou metodou je regresní analýza. Ta zkoumá lineární vztah mezi dvěma či více proměnnými. Nezávislou proměnou je v tomto případě čas, tedy počet čtrnáctidenních období za poslední rok. Závislou proměnou je potom procentuální změna obtížnosti těžby. Lineární regrese proloží zkoumané hodnoty přímkou ve tvaru:

$$Y = ax + b \qquad 12$$

Y… závislá proměnná
x… nezávislá proměnná
b… konstanta (zde 0)
a… parametr určující vztah mezi závislou a nezávislou proměnnou

Výpočet byl proveden pomocí nástroje v dokumentu excel a je opět přílohou této práce. Graf rovnice výsledné přímky ukazuje obrázek 14.



Obrázek 14) Graf rovnice přímky lineární regrese (zdroj: vlastní)

Jak je vidět z obrázku 14, rovnice přímky má tvar Y = 0 + 0,00263x. To může být chápáno tak, že obtížnost v n-tém období (Y) je rovna číslu 0,00263 * n-té období (x). Jelikož jsem tedy vyšel celkem z 28 vzorků, je příští očekávaná změna rovna:

$$Změna_{29} = 0{,}00263 * 29 = 7{,}6\ \% \qquad 13$$

Pro ověření regresní analýzy se používá významnost F. Výsledky považovat za statisticky průkazné, pokud je F menší než 0,05. V mém případě má F hodnotu 0,007. Hodnota R^2, která říká kolik procent změn v závislé proměnné je vysvětleno použitým modelem, je v tomto případě 0,24. Jen 24 % změn ve vývoji obtížnosti je tak vysvětleno časem. Myslím, že v tomto čísle je obsažen hlavně přirozený příliv nových těžařů, jak se těžba kryptoměn stává známější. Zbylých více než 75 % modelu je tak nevysvětleno a nelze se na něj z velké části spoléhat.

Vícenásobná regrese

Do regresní analýzy lze zařadit i více nezávislých proměnných. Když jsem jako druhý parametr zkusil zahrnout cenu Bitcoinu v příslušném období, vyšplhala se hodnota R^2 nad 70 %. Budoucí cena je ale pro mne neznámým parametrem, a proto mi její zahrnutí do modelu bohužel nepomůže. Odměna za vytěžený blok je v předpokládané době těžby neměnná a na modelu se tak neprojeví.

Do modelu proto zařadím pod druhou nezávislou proměnnou x_2 také hashrate nejvýkonnějšího vybavení, který byl v daném období dostupný. Provedením výsenásobné regrese dostanu následující výslednou přímku:

$$Y = ax_1 + bx_2 + c = -0{,}0024x_1 + 0{,}0068x_2 \qquad 14$$

Výpočet je v příloze práce. Významnost F je opět v pořádku. Hodnota R^2 je nad 51 %, tedy již více než polovina změn v závislé proměnné je vysvětlena tímto modelem. Pokud za x_1 dosadím příští časové období 29 a za x_2 hashrate ASICu "Antminer S9i" 14 TH/s, který byl až doposud nejvýkonnějším zařízením na trhu, je příští předpokládaná změna obtížnosti 2,56 %. Pokud budu ale uvažovat, že x_2 je nyní již 33 TH/s, je předpokládaná čtrnáctidenní změna 15,5 %.

Rozhodnutí

Myslím, že výsledek vícenásobné regrese s uvažováním přechodu i ostatních těžařů na výkonnější zařízení je jasným ukazatelem, kterým směrem by se měla obtížnost brzy měnit. Na druhou stranu nepředpokládám, že dojde k okamžitému přestupu všech těžařů na nový hardware. Nabídka je omezena a mnozí těžaři zajisté nebudou chtít ihned nahrazovat nedávno zakoupené vybavení. S příchodem nové technologie je ale rozhodně při odhadu třeba počítat. Jelikož se stále jedná pouze o odhad na základě historických dat a domněnek, budu počítat se třemi různými odhady – pesimistickým, realistickým a optimistickým. Výpočty potom provedu pro každý z nich a výsledky zhodnotím z pohledu racionálního rozhodovatele.

Jako realistickou variantu vidím změnu obtížnosti o 6 % za čtrnáct dní, tedy průměr za poslední rok. Pro pesimistickou variantu budu počítat se změnou o 10 % za stejný časový úsek. Jedná se totiž o průměrný nárůst po celou dobu těžby a výsledných 15 % z metody vícenásobné regrese nevidím jako udržitelný stav. Je ale možné, že v některých obdobích po příchodu nové technologie bude obtížnost skokově narůstat o desítky procent. Jako optimistický odhad vidím situaci s nárůstem pouze o 2 % za období. Takový stav by mohl být způsoben například nedostatkem hardwaru na trhu nebo zákazem těžby v některých zemích.

5.2.4 Diskontní úroková míra

Použitá metoda hodnocení investic NPV počítá s budoucími peněžními toky, u nichž může zohlednit změnu hodnoty v čase. Ta se v čase mění ze dvou důvodů. Jednak znehodnocením peněz vlivem inflace a rovněž možností jejich uložení s určitým úrokem. Proto se u NPV budoucí peněžní toky diskontují neboli se adekvátně ponížují o diskont. Diskont reprezentuje ušlou příležitost, měl by ale být vyšší než úroková sazba příležitosti (např. Státní dluhopisy). Ty lze totiž víceméně považovat za bezrizikový

finanční instrument, což o těžbě kryptoměn říci nelze. [58] Diskont proto stanovím jako bezrizikovou úrokovou sazbu + prémii za riziko, které realizací projektu podstupuji. To stanovím čistě subjektivně, což by měl udělat každý potenciální investor. Hledat pak budu prodejní cenu, kterou by Bitcoin musel dosáhnout, aby se čistá současná hodnota investice rovnala nule. Jinými slovy se bude jednat o cenu, při které bych dosáhl právě požadovaných X % (diskont).

Strategie S1

Diskontování peněžních toků obvykle probíhá na roční bázi a míra je tedy stanovena per annum. V mém případě je však nutné kladné peněžní toky (příjmy z prodeje) diskontovat jednou za čtrnáct dní a ty záporné (zálohy) jednou měsíčně. To je vidět z rovnic 6 a 8. Nejprve proto stanovím požadovanou efektivní úrokovou míru, tedy úrok, kterého bych dosáhl při ročním úročení. Podle vzorce 15 poté vypočítám úrok r_p odpovídající době čtrnácti dnů nebo r_q pro jeden měsíc (zde pro r_p).

$$1 + r_{ef} = (1 + \frac{r_p}{p})^p \qquad 15$$

r_{ef}… efektivní úroková míra [-]
p… počet čtrnáctidenních období v roce (pro q měsíčních)

Jelikož se v mém případě jedná o poměrně malou investici na krátký časový úsek, počítám jako bezrizikovou příležitost uložení peněz na spořící účet s úrokem 1 % p.a. [59] K tomu požaduji, aby má investice vynesla 5 % ročně jako příplatek za riziko. Efektivní úroková míra je tedy 6 % p.a. Abych zjistil, kolika procenty je nutné peněžní toky diskontovat za období p, q, vyjádřím $r_{p,\,q}$ z rovnice 15, a dosadím za r_{ef}, p a q. To zobrazuje rovnice 16 (pro případ s parametrem p).

$$r_p = \left(\sqrt[p]{(1 + r_{ef})} - 1\right) * p = \left(\sqrt[26]{(1 + 0{,}06)} - 1\right) * 26 = 0{,}05833 \qquad 16$$

Pro r_q je výsledek 0,05841. Vypočtené úrokové míry jsou ale s úročením p.a. Abych je mohl použít v rovnicích 6 a 8, je nutné je převést na čtrnáctidenní/měsíční úročení. Toho se dosáhne prostým podělením počtem období v roce, tedy šestadvaceti nebo dvanácti. Výsledné diskontní úrokové míry jsou tak 0,00224 (r_p) a 0,00487 (r_q).

Strategie S2

Jak je vidět z rovnic 8 a 9, pro použití strategie S2 potřebuji k výpočtu znát parametry r_q a r_{ef}. Úroková míra r_q je stejná jako v případě strategie S1, tedy 0,00487. K těžbě totiž dochází naprosto stejně. Diskont r_p není potřeba znát, neboť k prodeji nebude během těžby docházet. Prodej se uskuteční až po n letech od počáteční investice. Na podělení z něho plynoucích peněžních toků proto použiji r_{ef}, tedy 0,06.

5.2.5 Životnost zařízení

Racionální těžař bude zařízení provozovat pouze v případě, kdy příjem z těžby (množství krát cena) bude vyšší než výdaje. Množství je sice na základě odhadu vývoje obtížnosti možné dopředu stanovit, cena je však stále neznámou. Spočítat dopředu, kdy se těžba přestane vyplácet tak není možné. Platí však předpoklad, že pokud racionální těžař v průběhu těžby zjistí, že jeho příjmy jsou menší než platby za elektřinu, těžbu ukončí.

Tento stav pravděpodobně nastane dříve než za fyzickou životnost zařízení, která je asi tři roky. Interval, ve kterém se obvykle na trhu objevují lepší modely je jeden až dvaroky. Poté pravděpodobně dojde ke skokovému zvýšení D o desítky procent a konci rentability provozování zařízení. Jakmile se totiž na trhu objeví výkonnější model, těžaři s ním vytěží více na úkor ostatních. Snížené příjmy už tak nepokryjí výdaje na elektřinu. V takovém případě je navíc starší zařízení prakticky neprodejné, tj. jeho zůstatková cena je nulová.

Předpoklad kratší životnosti se potvrdil, když jsem provedl kontrolní výpočty s uvažováním životnosti tři roky. Podle nich by již po roce a půl docházelo k vytěžení takřka zanedbatelného množství kryptoměny, a to i s uvažováním lineárního nárůstu obtížnosti podle odhadu v (5.2.3). I při optimistické variantě by toto množství sotva stačilo na pokrytí nákladů, zatímco při té realistické a pesimistické by téměř s jistotou nestačilo vůbec. Při svých výpočtech budu proto počítat s životností zařízení jeden a půl roku. Počet měsíců za životnost m tak bude 18 a počet čtrnáctidenních období G bude 39.[15]

5.3 Provedené výpočty

V této části použiji sestavené rovnice 6, 7, 8 a 9 k tomu, abych nalezl parametr y pro S1 a P_{BTC} pro S2. Tyto parametry udávají, o kolik procent by cena Bitcoinu musela průměrně růst každé dva týdny, respektive jaké by musela být jeho prodejní cena na konci těžby, aby investice přinesla právě požadované vnitřní výnosové procento. Výpočty v excelu jsou přílohou této práce a hodnoty proměnných lze lehce nahradit těmi aktuálními.

5.3.1 Strategie – S1

Pro tuto strategii vyjdu z rovnice 6. Vyčíslení parametrů I, G, x, r_p, m, záloha, r_q a H obsažený v členu Q jsem vysvětlil v podkapitole dosazení neznámých parametrů (5.2). Q kromě H zahrnuje rovněž N, S, R a f. Počet dní N v období G je 14. Počet sekund S za den je 86 400. Odměna R za vytěžený blok je v současnosti 12,5 BTC. (viz Obrázek 1). Odměnu těžebnímu poolu f uvažuji 1 %. P_{zac}, tedy cena Bitcoinu

[15] *(365/14) *1,5= 39,1*

v době začátku těžby, je k 1.11.2018 143 500 Kč. [60] Obtížnost D je k 1.11.2018 rovna 7 184 404 942 701. [57] NPV dosadím rovno 0 a pomocí řešitele v excelu naleznu jedinou neznámou z rovnice 6, tedy parametr y. Výpočet jsem provedl celkem pro dvě různé ceny elektřiny odpovídající tarifům D57d a D02d a tři odhady vývoje obtížnost – optimistický, realistický a pesimistický. Veškeré výpočty jsou uvedeny v příloze této práce v listu BTC_S1. Výsledky jsou shrnuty v tabulce 6.

Tabulka 6) Požadovaná prodejní cena BTC při S1 (zdroj: vlastní)

Tarif	x - Změna D	y - změna/14 dní	P - cena BTC za 1,5 roku
D57d	Optimistický	1,95%	304 670 Kč
	Realistický	5,74%	1 264 708 Kč
	Pesimistický	9,52%	4 975 545 Kč
D02d	Optimistický	4,30%	742 302 Kč
	Realistický	8,21%	3 111 971 Kč
	Pesimistický	12,10%	12 364 257 Kč

Krom procentuální změny v ceně Bitcoinu ukazuje tabulka 6 i cenu, které by Bitcoin při takovém růstu dosáhl za jeden a půl roku. Komentáři výsledků se budu věnovat více v podkapitole racionální rozhodovatel (5.4). Už na první pohled je ale vidět, že výsledky se obrovsky liší v závislosti na ceně elektřiny a odhadu růstu obtížnosti těžby. Závěr tak pravděpodobně nebude pro všechny stejný a rozhodnutí bude silně ovlivněno rozhodovatelovým odhadem a možnostmi.

5.3.2 Strategie – S2

V případě této strategie dosadím nejprve známé parametry do rovnic 7 a 8. Z rovnice 7 dostanu očekávané výdaje pro dva různé tarify odběru elektrické energie. Z rovnice 8 potom tři různá množství vytěžené kryptoměny pro tři různé odhady vývoje obtížnosti. Tento mezivýsledek ukazuje tabulka 7.

Tabulka 7) Očekávané výdaje a vytěžené množství BTC při S2 (zdroj: vlastní)

Tarif	Výdaje [Kč]	Množství [BTC]
D57d	86560	0,439283
		0,253671
		0,171813
D02d	140119	0,439283
		0,253671
		0,171813

Výdaje zahrnující počáteční investici a diskontovanou hodnotu záloh za elektřinu budou tedy pro tarif D57d 85 560 Kč a 140 119 Kč pro D02d. Za dobu těžby přitom dojde k vytěžení 0,17 BTC pro pesimistický odhad, 0,25 BTC pro realistický odhad nebo 0,43 BTC pro optimistický odhad vývoje obtížnosti. Pomocí rovnice 9 a řešitele v excelu naleznu pro každou z kombinací těchto variant cenu Bitcoinu, za kterou by po roce a půl muselo dojít k prodeji, aby investice přinesla právě vnitřní výnosové procento. Výpočty jsou přílohou této práce v listu BTC_S2. Výsledky jsou shnuty v tabulce 8.

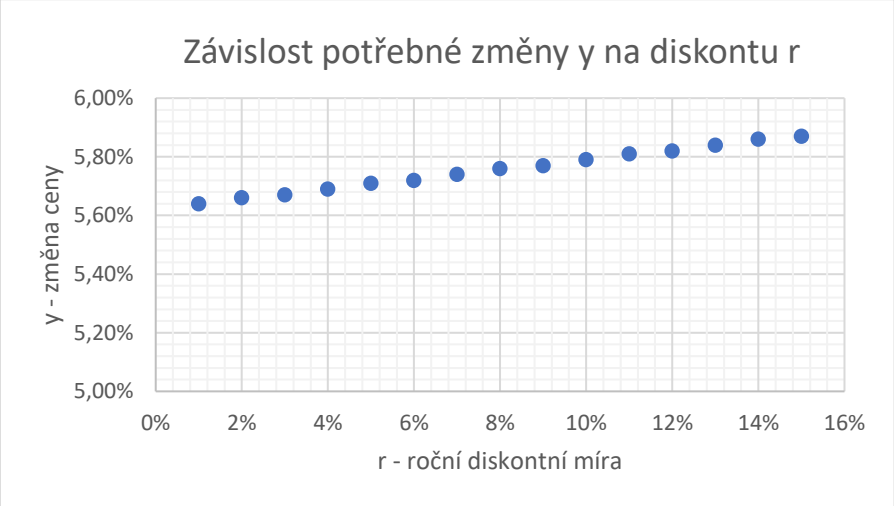
Tabulka 8) Požadovaná prodejní cena BTC při S2 (zdroj: vlastní)

Tarif	x - Změna D	P - cena BTC za 1,5 roku
D57d	Optimistický	215 045 Kč
	Realistický	372 396 Kč
	Pesimistický	549 816 Kč
D02d	Optimistický	348 107 Kč
	Realistický	602 819 Kč
	Pesimistický	890 020 Kč

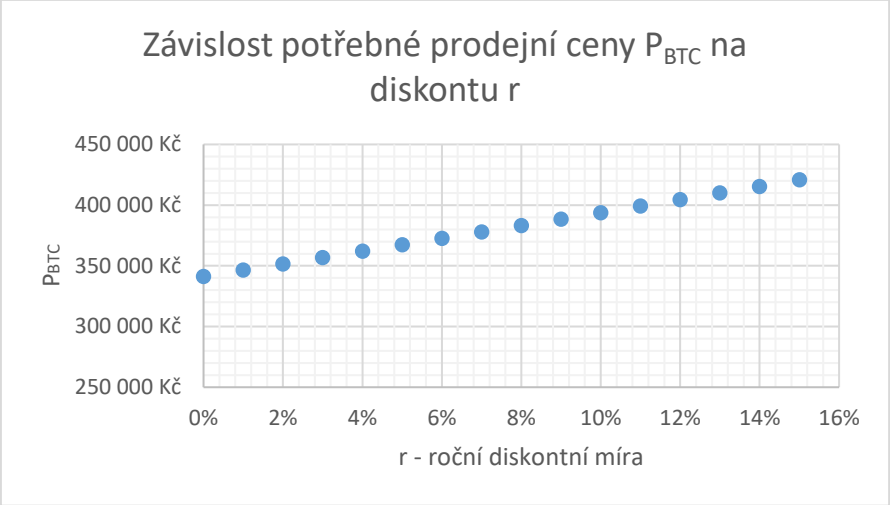
Komentáři výsledků se budu věnovat více v další podkapitole racionální rozhodovatel (5.4). Oproti strategii S1 je ale možné sledovat mnohem menší rozdíl v prodejních cenách po ukončení životnosti zařízení. To je způsobené tím, že při odhadovaném nárůstu obtížnosti dojde k vytěžení drtivé většiny celkového množství kryptoměny na počátku těžby. Pokud tak prodejce počká až na konec, prodá vše za jednotnou cenu. Pokud ale bude výtěžek zpeněžovat průběžně, prodá nejvíce kryptoměny za nízkou cenu a jen velmi malé množství za cenu vysokou (za předpokladu růstu ceny). Proto vychází pro strategii S1 konečná cena mnohem vyšší.

5.3.3 Citlivostní analýza na diskontní míru

Diskontní úrokovou míru jsem stanovil jako bezrizikovou úrokovou sazbu + subjektivně stanovenou prémii za riziko. Proto připojím ještě analýzu změnu výsledků v případě, kdy by byl právě diskont stanoven jinak. Citlivostní analýzu neprovedu kvůli velkému rozsahu pro všechny varianty odhadů změn obtížnosti a ceny elektrické energie, ale pouze pro reprezentativní situaci. Vybranný scénář je realistický odhad změny obtížnosti a cena záloh v tarifu D57d, pro obě strategie S1 i S2. Princip je přitom stejný jako v předchozích výpočtech, pouze hledám výsledek pro 15 různých diskontních úrokových mír (0-15 %). Výpočty jsou opět přílohou diplomové práce na listu CA_diskont. Výsledky ukazují obrázek 15 a obrázek 16.



Obrázek 15) Závislost potřebné změny ceny Bitcoinu na diskontní míře (zdroj: vlastní)



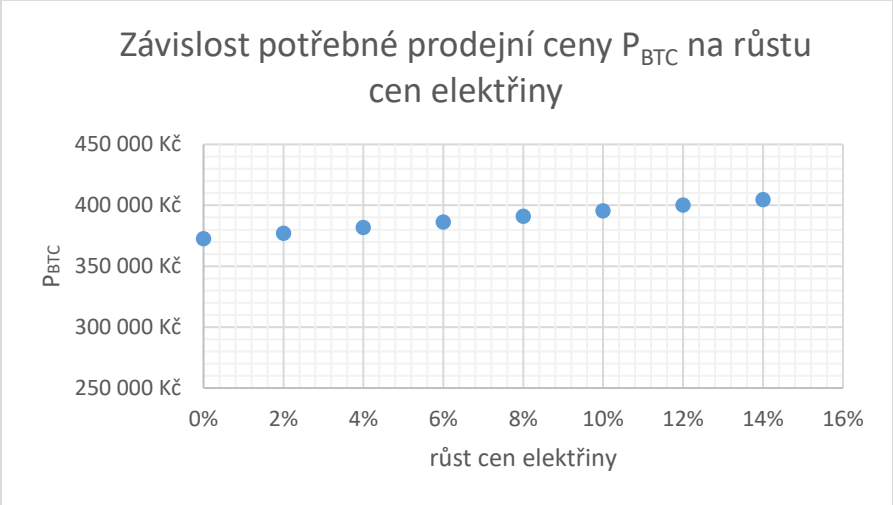
Obrázek 16) Závislost P_{BTC} na diskontní míře (zdroj: vlastní)

Z grafů je možné pozorovat, jak by se výsledky měnily v případě vyššího či nižšího očekávání, než je pro výpočet použitých 6 %. Pokud by si tak těžař stanovil místo nich například 15 %, musela by pro strategii S1 cena BTC růst tempem 5,87 % za čtrnáct dní (oproti 5,74 %). V případě S2 by cena musela dosáhnout 420 816 Kč (oproti 372 396 Kč).

5.3.4 Citlivostní analýza na cenu elektřiny

Jelikož má cena elektřiny v ČR od začátku roku 2016 vzrůstající tendenci, lze podle mého očekávat její nadálé postupné zvyšování. [63] Ve výpočtech předpokládám fixaci stanovené ceny (5.2.2) po celou dobu těžby. Pokud si však někdo bude sjednávat tarif za několik let, bude cena pravděpodobně vyšší. Proto provedu citlivostní analýzu i na cenu elektřiny. Kvůli velkému rozsahu pro všechny varianty odhadů změn obtížnosti a dva tarify elektřiny ji ale předvedu pouze pro reprezentativní situaci. Tento příklad je realistický odhad změny obtížnosti a cena záloh v tarifu D57d pro strategii S2. Princip je přitom stejný jako v předchozích výpočtech, pouze hledám výsledek pro osm různých možností růstu ceny elektrické energie (0-14 % s krokem 2 %). Výpočty jsou opět přílohou diplomové práce na listu CA_elektřina. Výsledky ukazuje obrázek 17.

Z grafu je možné pozorovat, jak by se výsledky měnily v případě navýšení ceny elektrické energie o 0-16 %. Pokud by se tak obtížnost měnila podle realistického očekávání, těžař by aplikoval strategii S2 a sjednal by si tarif D57d například o 10 % navýšený, musela by cena Bitcoinu po roce a půl dosáhnout 395 434 Kč (oproti 372 396 Kč).



Obrázek 17) Závislost P_{BTC} na růstu ceny elektřiny (zdroj: vlastní)

5.4 Racionální rozhodovatel

V této části se pokusím odpovědět na dvě otázky: kterou strategii zvolit a zda vůbec začít s těžbou kryptoměn. Odpověď na ně není ale pro každého jednotná. Každý člověk má totiž odlišnný postoj k riziku a rozhodnutí by udělal každý jinak. Rozhodovatel s averzí k riziku dává přednost méně rizikovým variantám, které mu přináší uspokojivé výsledky s vysokou pravděpodobností. Rozhodovatel se sklonem k riziku realizuje i varianty s vysokým rizikem, které mohou být hodně výnosné, ale mohou být i hodně proděločné. [61]

5.4.1 Porovnání strategií S1 a S2

V případě této diplomové práce neznám pravděpodobnosti, s kterými nastane odhadovaný vývoj obtížnosti těžby a nemohu tedy určit riziko, které těžba přinese. Celý výpočet je založen na předpokladu, že cena Bitcoinu poroste, což ale rozhodně nemusí platit. Kdyby ale cena nerostla, je za současných podmínek téměř jasné, že by se těžba z ekonomickéh pohledu nevyplatila a výpočet by neměl smysl. Je to způsobené tím, že se cena během roku psaní práce významně snížila, zatímco obtížnost těžby zůstala zachována. Důvodem bylo pravděpodobně to, že těžaři již zakoupené vybavení logicky nechtěli přestat provozovat. Výsledky tedy ukazují, že cena kryptoměny musí růst, i když ve skutečnosti nemusí. A zde právě dochází k rozdílu mezi dvěma použitými strategiemi.

Pokud by cena celou dobu rostla, vyplatí se samozřejmě více strategie S2. Nejvýhodnější by bylo prodat veškerou vytěženou kryptoměnu až na konci za co nejvyšší cenu. Z toho důvodu ukazuje strategie S2 mnohem menší potřebný nárůst ceny i rozptyl jednotlivých scénářů. Pokud by ale cena spíše klesala, celá situace se obrátí. V takovém případě by bylo výhodné prodávat Bitcoin co nejdříve to půjde a tím pádem by jasnou volbou byla strategie S1. Jednoduše řečeno se jedná o risk, zda cena stoupne nebo

ne. Výpočty počítají s cenou Bitcoinu, kterou je velmi obtížné predikovat, za rok a půl. Čím dříve tak k prodeji dojde, tím větší je jistota, že cena Bitcoinu bude blíže ceně na začátku těžby. Obecně lze tak shrnout, že rozhodovatel s averzí k riziku zvolí raději strategii S1, zatímco milovník rizik strategii S2.

5.4.2 Vyplatí se těžba?

Už dříve jsem uvedl, že odpověď na otázku, zda se Bitcoin z ekonomického pohledu vyplatí těžit, záleží hlavně na víře každého jednotlivce v růst prodejní ceny. Pokud stejně jako někteří Bitcoinoví nadšenci věříte, že cena přesáhne milion dolarů, není pro vás problém začít těžit ani s dražší elektřinou a pesimistickým odhadem vývoje obtížnosti. Tento extremistický názor ale většina lidí nesdílí. Cena Bitcoinu už na druhou stranu byla nad hranicí 400 000 Kč, a tak by víra v růst na podobnou hodnotu nebyla úplně neopodstatněná, třebaže je tato situace nepravděpodobná. Jak jsem navíc uvedl v kapitole (3.3.2), Bitcoin už několika bublinami prošel a pokaždé se jeho cena po nějaké době začala znovu zvyšovat.

Výsledky výpočtů ale hovoří jasně. I v případě optimistického rozhodovatele při realistickém vývoji obtížnosti by očekávání splnila pouze těžba v tarifu D57d. Navíc pouze při použití rizikovější strategie S2. Při rychlejším růstu obtížnosti těžby jsou z mého pohledu potřebné růsty cen mimo realitu, i když bych nerad ovlivnil ničí úsudek. Z mého pohledu by ale i nejoptimističtější rozhodovatel měl těžit pouze s levným tarifem odběru elektrické energie. Ten je však potřebné získat pouze na elektrické spotřebiče. Tarif D02d, který odpovídá ceně 3,82 Kč za kilowatthodinu, je pro těžbu velmi nevýhodný. Konkurenční těžaři v jiných zemích světa totiž pravděpodobně disponují cenami mnohem nižšími.

Porovnání s nákupem

Možností, jak rozhodnout, zda těžit či ne, je srovnat těžbu s prostým nákupem kryptoměny. Již před začátkem těžby je možné spočítat množství Bitcoinu, které těžba přinese i k tomu potřebné výdaje. Ty se rovnají počáteční investici a současné hodnotě v budoucnu zaplacených záloh, tedy jejich diskontované hodnotě. Alternativou k těžbě je nákup kryptoměny právě za tyto výdaje. K 1.11.2018 bylo Bitcoin možné nakoupit za 143 500 Kč. Za cenu odpovídající nákladům těžby tak bylo reálné nakoupit takové množství BTC, které ukazuje tabulka 9.

Tabulka 9) Množství nakoupené kryptoměny (zdroj: vlastní)

Tarif	Výdaje [Kč]	Množství [BTC]
D57d	86560	0,60321
D02d	140119	0,97644

V případě těžby bylo i při uvažování optimistického nárůstu obtížnosti vytěžené množství pouze 0,439 Bitcoinu. Nákup je tak pro všechny scénáře jednoznačně výhodnější než těžba. Ať má tedy rozhodovatel averzi či sklon k riziku, pokud je racionální, těžit Bitcoin nebude.

Výsledek je tak nakonec přeci jen jednoznačný. S použitými parametry není těžba Bitcoinu nikdy výhodnější než nákup. Zbývá proto pouze určit, jakých hodnot by některé parametry musely nabývat, aby se těžba stala výhodnější než nákup kryptoměn.

5.4.3 Těžba vs. Nákup

Parametry, které odlišují těžbu od nákupu, jsou cena elektrické energie, obtížnost těžby a hashrate se spotřebou použitého zařízení.

Obtížnost D jsem do výpočtů již zahrnul ve třech různých odhadech, a proto se jí zabývat dále nebudu. Počítat, jaká by musela být cena elektrické energie nedává z mého pohledu velký smysl. Uvažovaný tarif D57d je už tak na české poměry velmi nízký a výrazně nižší cena za kilowatthodinu není reálná. Pokud do svých výpočtů dosadím za cenu elektřiny nulu, je alternativou k těžbě nákup kryptoměny pouze za cenu vstupní investice I. V takovém případě by nákup přinesl 0,23 Bitcoinu. To je o něco méně než odpovídající vytěžené množství pro realistický scénář vývoje obtížnosti. Elektřina zadarmo ale není. I v případě, že někdo za elektřinu navíc naplatí, jako například studenti na kolejích, musí náklady na ni zaplatit někdo jiný. Jedná se tak de facto o krádež a taková varianta není solidární. Naopak lze podle mého očekávat spíše postupné zvyšování cen elektřiny, a proto byla součástí práce citlivostní analýza, která tento vývoj postihuje (5.3.4).

Zbývá se tak zaměřit na parametry těžebního zařízení. Najdu proto pro všechny scénáře takový hashrate, který by soustava ASIC musela mít, aby při zachování všech ostatních parametrů byla těžba výhodnější než nákup. Výpočet provedu tak, že pomocí nástroje řešitel budu v rovnici 7 hýbat s hodnotou H tak, aby vytěžené množství odpovídalo nakoupenému množství z tabulky 9. Výpočty jsou v příloze excel v listu S2_vs_Nakup a výsledky shrnuje tabulka 10.

Tabulka 10) Hashrate zlomu (zdroj: vlastní)

Množství [BTC]	x - Změna D	H - hashrate [TH/s]
0,60321	Optimistický odhad	45,3
	Realistický odhad	78,5
	Pesimistický odhad	115,8
0,97644	Optimistický odhad	73,3
	Realistický odhad	127
	Pesimistický odhad	187,5

Těžba Bitcoinu se za současné situace nevyplatí, protože je vždy nevýhodnější než nákup. Zda se vyplatí nákup, zhodnotí každý sám. Na rozdíl od těžby zde ale hraje roli pouze jeden parametr, a to cena. Rozhodnutí je tak mnohem jednodušší. Pokud by někdo o těžbě uvažoval, může k rozhodnutí použít tabulku 10. Pokud by všechny parametry kromě H zůstaly stejné, rozhodovatel by například měl cenu elektřiny odpovídající tarifu D57d a realistický odhad vývoje obtížnosti, měl by začít těžit pouze v případě, že se na trhu objeví ASIC dosahující minimálně hashrate 78,5 TH/s.

Tato hodnota je více než dvojnásobkem hashrate, kterého dosahují právě vyvinuté nejnovější technologie. Tato situace není příliš pravděpodobná. Na druhou stranu se ve světě kryptoměn stalo již mnoho překvapení a nelze ji tak ani úplně vyloučit. Je ale třeba stále sledovat nové trendy a vývoj kryptoměn.

Ve své práci jsem do výpočtů záměrně nezahrnul daně (3.4), protože situace kolem nich není jednoznačná. Zdanění virtuálních měn totiž v ČR není v současnosti přímo ošetřené zákonem a jasná pravidla neexistují. K dispozici je pouze vyjádření Finanční správy, podle které by veškeré výnosy z obchodování s kryptoměnami měly podléhat dani z příjmů. Podle odborníků ale nepostihuje všechny situace. Tento stav se dá přisuzovat rychlému vývoji, na který legislativci zatím nestačili reagovat. Lze tedy očekávat, že v dohledné době nastane ze strany finanční správy nová úprava daňových zákonů s výslovnou úpravou virtuálních měn, která bude reflektovat aktuální potřeby vznikající v souvislosti operací s kryptoměnami. [34]

Zpeněžení vytěžené kryptoměny nebo rozdíl mezi nákupní a prodejní cenou je v každém případě nutné zdanit, je ale třeba řídit se pouze obecnými právními předpisy. Operace s kryptoměnami jsou však natolik specifické, že je často možné si jednu situaci vyložit z více úhlů pohledu. Navíc chybí praktické zkušenosti a v řadě případů tak lze očekávat ustálení praxe až na základě rozhodnutí soudů. [34]

Pro svou nejednoznačnost a možné zanesení nepřesností do výsledku nejsou daně součástí výpočtů, je však dobré mít na paměti, že se musí platit. Zhodnocení by tak pravděpodobně bylo posunuto ještě více v neprospěch těžby kryptoměn.

6 Závěr

Cílem této práce bylo srozumitelné poskytnutí uceleného pohledu na problematiku kryptoměn a ekonomické zhodnocení jejich těžby. Ucelený pohled je shrnut v prvních třech kapitolách práce. V první kapitole popisuji princip kryptoměn a jejich vývoj od vzniku až do současného stavu, včetně výhledu do budoucna. Druhá část se zaměřuje na způsob obchodování s kryptoměnami, na rozbor jejich cen a důvodů, kvůli kterým vznikly. Třetí část už pojednává o samotné těžbě. Pozornost přitom není zaměřena pouze na princip a způsoby těžby, ale také na technický pokrok a problémy, které s sebou přináší. Nezaměřil jsem se tak pouze na technickou část problematiky, ale také na vysvětlení důležitých spojitostí, bez jejichž znalosti jsou podle mého názoru těžba a obchodování s kryptoměnami neuvážené.

Ve čtvrté části z těchto znalostí vycházím a snažím se o ekonomickou analýzu těžby kryptoměn. Když jsem práci na začátku roku 2018 začínal psát, pohybovala se cena Bitcoinu kolem 400 000 Kč. Kvůli jeho popularitě vstoupilo na pole těžby mnoho těžařů, kteří tlačili výkon sítě vzhůru. Během psaní práce se cena prudce propadla, zatímco výkon sítě zůstal vysoký. Vstup nového těžaře se tak v současnosti z ekonomického pohledu pravděpodobně nevyplatí. K tomuto zjištění je ale možné dojít prostým využitím internetových kalkulaček, které ukážou, jaká je se současnými hodnotami návratnost investice. Z toho důvodu při výpočtech v této práci vycházím ze vzorců používaných těmito kalkulačkami a rozšiřuji je o růst ceny a obtížnosti těžby v čase, stejně jako o časovou cenu peněz. S třemi odhady vývoje obtížnosti a dvěma různými cenami elektrické energie počítám potřebnou změnu ceny, aby investice přinesla právě stanovené vnitřní výnosové procento. Jelikož je toto procento z větší části stanovené subjektivně, je součástí práce citlivostní analýza na diskontní úrokovou míru. Zároveň do budoucna počítám i s možností zvyšování cen elektrické energie. Z toho důvodu je v práci i citlivostní analýza na změnu ceny elektřiny.

Kvůli rozsahu se omezuji pouze na zhodnocení nejpoužívanější kryptoměny Bitcoin. Podle internetových kalkulaček srovnávající kryptoměny se těžba Bitcoinu pohybuje mezi nejvýnosnějšími. Nelze proto uvažovat, že výběr jiné kryptoměny by přinesl výrazně lepší výsledky. Součástí práce je navíc stanovení korelačního koeficientu mezi cenami kryptoměn, který je velmi vysoký. Jelikož se při výpočtech zaměřuji právě na stanovení změny ceny, byl by závěr nejspíš podobný i pro ostatní kryptoměny.

Výpočty jsou provedeny pro dvě různé strategie: strategii okamžitého prodeje S1 a strategii prodeje až po konci těžby S2. Každá ze strategií je atraktivní pro určitý typ člověka, podle jeho založení a postoji k riziku. Obecně jsou ale výsledky takové, že aby byla těžba Bitcoinu rentabilní, rozhodnutí začít těžit

by provedl pouze hodně optimistický člověk s nízkou cenou elektrické energie. Pokud by navíc těžbu srovnal s alternativní investicí, kterou je nákup kryptoměn, těžit by nezačal nikdy. Proto je práce rozšířena ještě o hledání takových parametrů, kterých by těžební soustava musela dosáhnout, aby byla těžba Bitcoinu výhodnější než jeho nákup. Výsledek je takový, že i s nižší cenou elektrické energie by ASIC musel dosahovat výrazně vyššího těžebního výkonu, než je ten dosahovaný u současně dostupných zařízení. Nejmodernější technologie dosahuje nyní okolo 33 TH/s. Potřeba by ale bylo alespoň 45,3 TH/s s optimistickým vývojem obtížnosti, respektive 78,5 TH/s v případě realistického vývoje. Tato situace není v současnosti pravděpodobná. Začít s těžbou kryptoměn tak nelze za daného stavu doporučit.

Výnosnost těžby kryptoměn ale ovlivňuje mnoho parametrů, které se mohou neočekávaně změnit, zatímco princip zůstává stejný. I když tak za několik let budou možná na trhu úplně jiné kryptoměny, zhodnocení rentability jejich těžby bude možné na podobném principu. Výpočty jsem provedl s takovými parametry, které považuji za reálné a opodstatněné. Je ale možné, že se v budoucnu uberou naprosto odlišným směrem. V takovém případě bude možné jednoduše vstupní parametry aktualizovat a výpočty provést znovu. Doufám tak, že tato diplomová práce poslouží v budoucnu potenciálním těžařům jako pomoc k dosažení zisku, nebo alespoň k zamezení ztráty.

7 Použitá literatura

[1] N. Hajdarbegovic, „coindesk,“ 2013. [Online]. Available: https://www.coindesk.com/americans-think-bitcoin-is-xbox-game/.

[2] „Coinmarketcap,“ 2018. [Online]. Available: https://coinmarketcap.com/charts/.

[3] S. Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System,“ 2008.

[4] A. M. Antonopoulos, Mastering Bitcoin, O'Reilly, 2014.

[5] J. S. Dominik Stroukal, BITCOIN: Peníze budoucnosti, Praha: Ludwig von Mises Institut CZ&SK, 2015.

[6] FILIM, „CryptoSvět,“ Listopad 2017. [Online]. Available: https://cryptosvet.cz/navod-zacatecnika-rozdil-proof-of-work-proof-of-stake-proof-of-burn-dalsimi-proof-of/.

[7] „Bitcoinwiki: FAQ,“ [Online]. Available: https://en.bitcoin.it/wiki/Help:FAQ#How_long_will_it_take_to_generate_all_the_coins.3F.

[8] B. M. BALLEK, „Analýza těžby alternativních kryptoměn,“ Vysoká škola ekonomická v Praze, Praha, 2014.

[9] „Kryptomagazin,“ 13 1 2018. [Online]. Available: https://kryptomagazin.cz/kratky-pruvodce-bitcoin-forky/.

[10] B. M. OCENÁŠ, „ANALYTICKÉ ZPRACOVÁNÍ BLOCKCHAINU KRYPTOMEN - Diplomová práce,“ VYSOKÉ UCENÍ TECHNICKÉ V BRNE, Brno, 2017.

[11] „MAPofCOINS,“ [Online]. Available: http://mapofcoins.com/.

[12] A. K. White, Cryptocurrency 2018: Mining, Investing and Trading in Blockchain, including Bitcoin, Ethereum, Litecoin and others, Amazon, 2017.

[13] S. Buchko, „coincentral.com,“ 12 2107. [Online]. Available: https://coincentral.com/when-will-ethereum-mining-end/. [Přístup získán 4 2018].

[14] „Bitcoin Cash,“ [Online]. Available: https://www.bitcoincash.org/.

[15] Bilthon, „StackExchange.com,“ 2017. [Online]. Available: https://bitcoin.stackexchange.com/questions/62672/what-are-the-drawbacks-of-bitcoin-cash.

[16] D. Ogurcakova, „Kryptomagazin,“ 3 2018. [Online]. Available: https://kryptomagazin.cz/iota-vse-o-budoucim-piliri-pro-internet-of-things/. [Přístup získán 4 2018].

[17] „Kryptomagazín,“ 3 2018. [Online]. Available: https://kryptomagazin.cz/eos-uvod-ke-kryptomene-ktera-zpracuje-50-000-transakci-za-sekundu/. [Přístup získán 4 2018].

[18] V. Urbánek, „kurzy.cz,“ 19 1 2018. [Online]. Available: https://www.kurzy.cz/zpravy/443671-na-tezbu-kryptomen-loni-padlo-29-5-twh-elektricke-energie--polovina-spotreby-cr/. [Přístup získán 3 2018].

[19] J. Buntinx, „themerckle.com,“ 3 2018. [Online]. Available: https://themerkle.com/the-real-carbon-footprint-of-cryptocurrency/. [Přístup získán 4 2018].

[20] N. Acheson, „coindesk.com,“ 2018. [Online]. Available: https://www.coindesk.com/information/what-is-the-lightning-network/.

[21] M. Z. Buřival, „Mladý Podnikatel,“ 2012. [Online]. Available: https://mladypodnikatel.cz/jak-vznikaji-a-funguji-penize-t2289. [Přístup získán 2018].

[22] Z. Revenda, „MONOPOLY CENTRÁLNÍCH BANK A EMISE PENĚZ,“ Vysoká škola ekonomická v Praze, 2009.

[23] Tomáš Holub, „Česká Národní Banka,“ Množství peněz určuje ekonomika, nikoli centrální banka, 1 2018. [Online]. Available:

https://www.cnb.cz/cs/o_cnb/blog_cnb/prispevky/holub_kral_saxa_20180115.html. [Přístup získán 4 2018].

[24] Š. Vaněk, „Finance v klidu," 2016. [Online]. Available: https://financevklidu.cz/jak-banky-vydelavaji-diky-penezum-ktere-sami-nemaji/. [Přístup získán 2018].

[25] A. Michl, *Geoinformatika tisknutí peněz,* https://www.youtube.com/watch?time_continue=1206&v=E3YLAo3rgyY: Unicorn College open, 2017.

[26] „Crypto Coin Charts," [Online]. Available: https://cryptocoincharts.info/markets/info. [Přístup získán 2018].

[27] R. King, „BitDegree," 3 2018. [Online]. Available: https://www.bitdegree.org/tutorials/bitcoin-price-prediction/. [Přístup získán 4 2018].

[28] A. Kharpal, „CNBC," 2 2018. [Online]. Available: https://www.cnbc.com/2018/02/06/bitcoin-price-will-crash-to-zero-nouriel-roubini-says.html. [Přístup získán 4 2018].

[29] „Business Center," [Online]. Available: https://business.center.cz/business/pojmy/p3248-cenova-bublina.aspx.

[30] L. SHEN, „FORTUNE," 2 2018. [Online]. Available: http://fortune.com/2018/02/07/bitcoin-price-usd-prediction-goldman-sachs-cryptocurrency/. [Přístup získán 4 2018].

[31] R. Vasudevan, „The startup," 1 2018. [Online]. Available: https://medium.com/swlh/how-similar-is-the-crypto-bubble-to-the-dot-com-bubble-bd6f30992e60. [Přístup získán 4 2018].

[32] J.-P. Rodrigue, The Geography of Transport Systems, New York: Routledge, 2017.

[33] H. Kocourková, „Alza," [Online]. Available: https://www.alza.cz/jak-zdanit-prijmy-z-kryptomen. [Přístup získán 5 2018].

[34] M. Mareš, „ePravo," 2018. [Online]. Available: https://www.epravo.cz/top/clanky/kryptomeny-z-ucetniho-a-danoveho-hlediska-108117.html. [Přístup získán 9 2018].

[35] T. Procházka, „Finance.cz," 2017. [Online]. Available: https://www.finance.cz/493355-blockchain/. [Přístup získán 2018].

[36] Tadoch, „TradeArena," 1 2018. [Online]. Available: https://www.tradearena.cz/rubriky/kryptomeny/jak-funguje-tezba-bitcoinu-podrobne-vysvetleni-miningu_363.html. [Přístup získán 5 2018].

[37] J. Tuwiner, „Buy Bitcoin Worldwide," 4 2018. [Online]. Available: https://www.buybitcoinworldwide.com/mining/pools/. [Přístup získán 5 2018].

[38] M. Trump, „BitcoinBlog.cz," 11 2017. [Online]. Available: https://bitcoinblog.cz/stitky/tezarske-pooly/. [Přístup získán 5 2018].

[39] „MinerGate," [Online]. Available: https://minergate.com/blog/hashrate-improvement-for-cpu/.

[40] Bohemiasoft, „Webareal," 2017. [Online]. Available: https://blog.webareal.cz/stavime-rig-pro-tezbu-etherea-1-dil/. [Přístup získán 2018].

[41] Přispěvatelé, „Bitcoin Forum," [Online]. Available: https://bitcointalk.org/index.php?topic=167229.0. [Přístup získán 5 2018].

[42] „Xilinx," [Online]. Available: https://www.xilinx.com/products/silicon-devices/fpga/what-is-an-fpga.html.

[43] J. Tuwiner, „BuyBitcoiWorldwide," 4 2018. [Online]. Available: https://www.buybitcoinworldwide.com/mining/hardware/. [Přístup získán 5 2018].

[44] Přispěvatelé, „BitcoinForum," [Online]. Available: https://bitcointalk.org/index.php?topic=2591317.0.

[45] M. B. Taylor, „Bitcoin and The Age of Bespoke Silicon,“ University of California, San Diego, 2013.

[46] „BitInfoCharts,“ [Online]. Available: https://bitinfocharts.com/comparison/bitcoin-hashrate.html. [Přístup získán 5 2018].

[47] BitcoinEnergyConsumptionIndex, „Digiconomist,“ 5 2018. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption. [Přístup získán 5 2018].

[48] S. Deetman, „Motherboard,“ 3 2016. [Online]. Available: https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020. [Přístup získán 5 2018].

[49] B. Wallace, „hackernoon.com,“ 3 2018. [Online]. Available: https://hackernoon.com/what-is-the-carbon-footprint-of-crypto-1798479bcd1. [Přístup získán 4 2018].

[50] „Reddit,“ 10 2018. [Online]. Available: https://www.reddit.com/r/Bitcoin/comments/262riz/what_is_the_formula_for_mining_profitability/.

[51] „moleminer,“ [Online]. Available: https://www.moleminer.cz/antminer-asic-minery-od-bitmain/antminer-s9i-sha256-miner/. [Přístup získán 10 2018].

[52] „GMO,“ [Online]. Available: https://www.gmo.jp/en/news/article/782/. [Přístup získán 10 2018].

[53] „Pangolinminer,“ 4 10 2018. [Online]. Available: https://pangolinminer.com/product/whatsminer-m10/.

[54] „elektřina.cz,“ [Online]. Available: https://www.elektrina.cz/slovnik/distribucni-sazba-d02d.

[55] „TZBinfo,“ [Online]. Available: https://kalkulator.tzb-info.cz/cz/dodavka-elektricke-energie-porovnani-nabidek?id=1795. [Přístup získán 10 2018].

[56] „Energofin,“ [Online]. Available: http://www.energofin.cz/novinky/9/.

[57] „Bitcoinwisdom,“ [Online]. Available: https://bitcoinwisdom.com/bitcoin/difficulty. [Přístup získán 1 11 2018].

[58] M. Mařík, Diskontní míra pro výnosové oceňování podniku, Praha: OECONOMICA, 2007.

[59] „měšec.cz,“ [Online]. Available: https://www.mesec.cz/produkty/sporici-ucty/?vyse_vkladu=58000&vypovedni_lhuta=0&doba_ulozeni=547&spocitat=Spo%C4%8D%C3%ADtat&_sl1=pocatecni_vklad&_sl2=max_dosazitelny_urok&_sl3=platebni_karta_k_uctu&tridit=_calc1&smer=s. [Přístup získán 10 2018].

[60] „coimate,“ [Online]. Available: www.coinmate.io. [Přístup získán 1 11 2018].

[61] „Teorie užitku,“ [Online]. Available: http://www2.ef.jcu.cz/~jfrieb/prednasky_komplet/skriptaRM_uzitek.pdf.

[62] „Coindesk,“ [Online]. Available: https://www.coindesk.com/price/.

[63] „kuryz.cz,“[Online].https://www.kurzy.cz/komodity/cena-elektriny-graf-vyvoje-ceny/nr_index.asp?A=5&idk=142&od=24.8.2007&curr=EUR&default_curr=EUR&unit=&lg=1