Kryptoměny

Filip Kotopulos

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

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

Jméno a příjmení:	**Filip Kotopulos**
Osobní číslo:	**A16021**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Kryptoměny**
Téma anglicky:	**Cryptocurrencies**

Zásady pro vypracování:

1. **Vypracujte literární rešerši dané problematiky.**
2. **Nastudujte a popište historii, základní vlastnosti a principy kryptoměn, včetně jejich zasazení do právního rámce.**
3. **Nastudujte a popište možnosti těžby kryptoměn, jejich směny a plateb.**
4. **Vytvořte přehled nejrozšířenějších či nějakým způsobem zajímavých druhů kryptoměn.**
5. **Pro vybrané druhy kryptoměn porovnejte náročnost těžby a jejich rentabilitu.**
6. **U vybraných druhů kryptoměn analyzujte aktuální možnosti využití na trhu.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **NARAYANAN, A., J. BONNEAU, E. FELTEN, A. MILLER a S. GOLDFEDER. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press, 2016.**
2. **Kryptomagazin.cz – Bitcoin, Blockchain, zpravodajský portál o kryptoměnách [online]. Praha: MEDIA BASE, 2018 [cit. 2018-11-11]. Dostupné z: https://kryptomagazin.cz**
3. **Kryptoměny – bitcoin a další virtuální měny | E15.cz [online]. Praha: CZECH NEWS CENTER, 2018 [cit. 2018-11-11]. Dostupné z: https://www.e15.cz/kryptomeny**
4. **KRAUSE, Max J. a Thabet TOLAYMAT. Quantification of energy and carbon costs for mining ryptocurrencies. Nature Sustainability, 2018, DOI 10.1038/s41893-018-0152-7.**
5. **EXTANCE, Andy. The future of cryptocurrencies: Bitcoin and beyond. Nature News, 2015, roč. 526, č. 571, s. 21-23.**

Vedoucí bakalářské práce: **doc. Ing. Radek Matušů, Ph.D.**
Ústav automatizace a řídicí techniky

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Ing. Martin Sysel, Ph.D.
garant oboru

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně Filip Kotopulos, v.r.

ABSTRAKT

Cílem této práce je zpracovat problematiku týkající se kryptoměn, jejich historie, možností využití, náročnosti jejich získání a držení. Teoretická část je zaměřena na obecné seznámení se s kryptoměnami a na jejich popis. Praktická část se dále věnuje procesu jejich těžby a způsobům směny za zboží, služby a případným burzovním spekulacím. V praktické části byla porovnána návratnost vložených investic do těžby a na základě získaných údajů je možné vyvodit závěr, že valná většina kryptoměn je již v této oblasti neperspektivní. Zároveň však nutno říci, že v oblasti obchodu se kryptoměny rozvíjejí rychlým tempem.

Klíčová slova: kryptoměny, blockchain, těžba, směna, platby

ABSTRACT

The aim of this work is to process the issues related to cryptocurrencies, their history, possibilities of use, difficulty of their acquisition and possession. The theoretical part is focused on general introduction to cryptocurrencies and their description. The practical part also deals with the process of their mining and the ways of exchange for goods, services and possible stock exchange speculation. In the practical part, the return on invested investment was compared and based on the obtained data it can be concluded that most cryptocurrencies are already in this area unpromising. At the same time, however, cryptocurrencies are developing at a fast pace.

Keywords: cryptocurrencies, blockchain, mining, trading, payments

Tímto bych chtěl poděkovat svému vedoucímu panu doc. Radku Matušů za pomoc při tvorbě práce a za zodpovězení všech mých dotazů. Dále bych chtěl poděkovat rodině za klid, kterého se mi dostalo během psaní bakalářské práce, a za jejich podporu při mých studiích.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Dnešní doba se neustále posouvá mílovými kroky kupředu a pokrok v oblasti počítačové techniky je k nezastavení. Tento rychlý posun vpřed s sebou přináší mnohé klady i zápory. V mnoha případech se snaží člověku usnadnit život, či zjednodušit práci. Není tomu tak dávno, co se objevila možnost platit na internetu (a později nejen na něm) virtuální měnou, kterou si mohl člověk buďto koupit anebo pomocí svého počítače vytěžit, díky výpočtům matematicky náročných algoritmů.

Řeč je zde o velmi rychle se rozmáhajícím poli kryptoměn, se kterými se v dnešní době doslova roztrhl pytel a na trhu se objevují neustále nové a nové kryptoměny, nabízející svým těžitelům, či kupcům mnohdy až závratné zbohatnutí.

Autorovu volbu tohoto tématu ovlivnilo, že se na trhu objevuje mnoho kryptoměn, které se snaží člověka přesvědčit, že díky nim zbohatne a v budoucnu s nimi bude moci platit téměř za všechno, ale reálná situace je taková, že peníze, či jakékoliv prostředky v investované do této měny, již nikdy neuvidí.

Cílem této práce je vypracovat literární rešerši na téma kryptoměn, vysvětlit čtenáři tento pojem, představit jejich historii a ve stručnosti předvést principy fungování, vytvořit seznam dnes používaných kryptoměn a ukázat perspektivní kryptoměny, které by mohly býti v budoucnu zajímavé.

V této práci uvidí přínos hlavně zájemci o pochopení principů fungování kryptoměn a lidé se zájmem o těžbu, kteří se ještě nerozhodli, do které kryptoměny by rádi investovali jejich čas a peníze. Dále může být tato práce podkladem pro výuku ať už na střední, či vysoké škole

Teoretická část této práce bude věnována historii, základním vlastnostem a principům kryptoměn. Dále se zaměří na jejich ekonomické aspekty a jejich zasazení do právního rámce u nás a ve světě. V neposlední řadě probere možnosti těžby měn a jejich směny na trhu.

Praktická část se následně bude zabývat vybranými druhy kryptoměn, které jsou buďto aktuálně používané nebo přišly autorovi z určitých hledisek zajímavé. Tyto měny budou následně podrobněji představeny, bude u nich porovnána návratnost vložených investic a nastíněny možné způsoby útraty těchto měn.

I. TEORETICKÁ ČÁST

1 Kryptoměna

Kryptoměny jsou v dnešním světě často zmiňovaným tématem. Velká popularizace měny Bitcoin přilákala na tento trh spoustu malých a středních investorů s vidinou velkého zisku.

Pod pojmem kryptoměna bychom si měli představit virtuální měnu nebo platidlo, které je založeno na kryptografii[1)]. Její hodnota je dána nabídkou a poptávkou po této měně, přičemž toto platidlo nemá žádnou hmatatelnou formu a vyskytuje se čistě ve virtuálním prostředí jako sekvence nul a jedniček. [1]

Cílem jejich vzniku bylo zvýšit bezpečnost, rychlost a anonymitu plateb. Při klasickém převodu u bankovního účtu odesilatel nikdy neví, co se s penězi děje a kudy peníze putují, než dorazí ke svému adresátovi. Ku příkladu platí-li člověk kartou, všechny transakce jsou evidovány a banka nebo zprostředkovatel platby tak přesně ví, co si osoba kupuje. Pokud bychom mluvili o rychlosti, určitě si všichni vybaví rychlost, s jakou mezi sebou banky posílají peníze a jak drahé a pomalé jsou platby do zahraničí. [1]

Jako důležitý pojem je třeba zmínit decentralizaci, což znamená, že kryptoměny nemají (až na výjimky) žádný centrální uzel, který by řídil jejich chod. Základem je peer-to-peer komunikace mezi jednotlivými uzly (počítači), proto když jeden uzel vypadne, neohrožuje to chod systému, jako například u běžné banky, kdy pád systému na hlavní pobočce může vyřadit z činnosti pobočky ostatní. [2]

Všechny tyto neduhy klasického bankovnictví řeší nebo se snaží řešit právě kryptoměny. Platby jsou rychlé, bezpečné, transparentní a obsahují téměř nulovou informaci o odesilateli. Další z velkých výhod je omezené množství, kdy se měna nedá těžit/tisknout donekonečna, jak je tomu u běžných bankovek. [1]

1.1 Historie

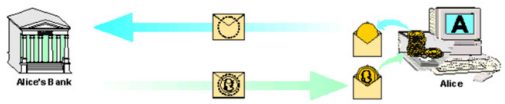
Spousta lidí pokládá za počátek kryptoměn vznik dnes asi nejznámější kryptoměny Bitcoin v roce 2009. První vize kryptoměn se však začaly objevovat o více než 20 let dříve. V roce 1982 publikoval ve své práci první vizi kryptoměny David Chaum, který si představoval virtuální měnu, se kterou by se daly platit malé finanční částky, tzv. mikro transakce. O několik let později se podobným směrem vydal i systém Cybercash, v obou případech však můžeme říci, že ještě nešlo o plnohodnotnou kryptoměnu a systémy se snažily spíše konkurovat kreditním kartám, směnkám a šekům. Následovala spousta dalších pokusů o tvorbu virtuálních měn jako třeba NetCash, Digigold, ale šlo buď o pouhé vize, nebo se měna neuchytila. [3]

[1)] Vědní obor věnující se utajení obsahu zpráv a vytváření šifrovacích systémů.

1.1.1 Ecash

Kryptoměna Ecash vznikla v roce 1989 společně se společností DigiCash, kterou založil David Chaum. Kryptoměna Ecash měla sloužit jako elektronická měna pro platby menších rozměrů a byla to první elektronická off-line měna[2]. Projekt od svého vzniku podpořilo v USA jen málo bank. Do Evropy se dostala měna v červnu roku 1998, na konci tohoto roku však společnost DigiCash zbankrotovala kvůli uživatelsky většímu zájmu o kreditní karty. [3, 4]

Princip fungování Stejně jako se dnes setkáváme s Bitcoinem, či dalšími kryptoměnami, i s Ecash bylo možné platit pouze v obchodech přijímajících tuto měnu. Oproti novějším druhům kryptoměn však samotné získání kryptoměny nezahrnuje těžení, ale jedná se o pouhou směnu reálných peněz za peníze elektronické.



Obr. 1.1 Popis získání měny [5]

Alice odešle do banky prázdnou minci s hodnotou, kterou požaduje. Tato mince má unikátní seriové číslo, které však banka nevidí. Banka jí následně strhne z účtu požadovanou hodnotu a zpět odešle sadu mincí podepsanou digitálním podpisem ztvrzujícím platnost mincí a jejich hodnotu. Tyto mince pak může Alice použít při platbě u obchodníka. [5]

Obr. 1.2 Platby mezi uživateli [5]

Podobný systém následně funguje i u plateb mezi uživateli mince. Pokud chce například Alice poslat peníze Cindy, odešle jí mince v požadované hodnotě, ty se ze Cindina počítače odešlou do Cindiny banky, která kontaktuje banku Alice a zjistí pravost mincí. Pokud vše souhlasí, odešle Cindina banka mince na Cindin účet, jak je vidět na obrázku výše. [5]

Pro uživatele kryptoměny byla tato měna zdarma na rozdíl od obchodníků, kteří platili poplatek z každé provedené platby, jako je tomu dnes u plateb kartou. Za 3 roky beta testování si měna získala okolo 5 000 uživatelů. [3, 5]

[2] Off-line měna je taková měna, u které obchodník nemusí při přijímání platby kontaktovat třetí stranu (banka, společnost spravující kreditní karty).

Zabezpečení Zabezpečení bylo provedeno pomocí tzv. slepého podpisu, což je forma digitálního podpisu, kdy je obsah zprávy skrytý před tím, než je podepsán. Vymyslel ho David Chaum společně s Amosem Fiatem a Mori Naorem a poprvé jej využili právě u kryptoměny Ecash. V praxi se tento systém stále ještě používá např. při elektronických volbách. [4]

1.1.2 Cybercash

CyberCash nebo CyberCash Secure Payment System byla platforma určená pro platby na internetu, kde si uživatel mohl nabít svou virtuální peněženku pomocí kreditní karty nebo později pomocí virtuálních mincí. [3]

Stejně jako Ecash CyberCash nabízel možnost plateb mikro transakcí pomocí jejich virtuálních mincí. Zajímavostí u tohoto systému je, že díky zákazu americké vlády vyvážet kryptografii (byla považována za zbraň) se nemohl CyberCash šířit za hranice USA. Nicméně ve finále se podařilo společnosti dostat od vlády výjimku. [3]

Kvůli chybě v systému zvané Y2K[3)], která postihla nejen společnost CyberCash a způsobovala zdvojnásobení placených částek u některých zákazníků, společnost zkrachovala v roce 2001. Její know-how pak odkoupila společnost PayPal a využívá jej dodnes. [3]

1.2 Princip fungování

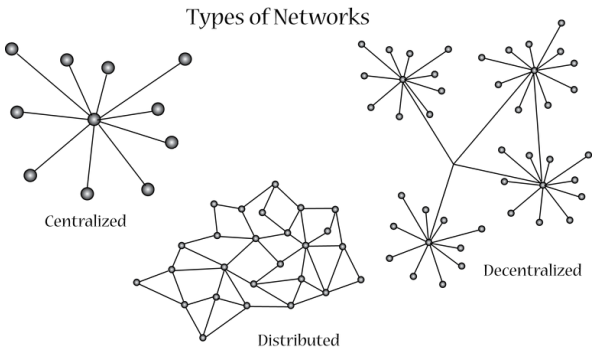
Kryptoměny by se velmi jednoduše daly přirovnat ke zlatu, či jinému nerostnému bohatství. Tak jako zlato, či další nerosty i kryptoměny je možné těžit. Nebudete je však těžit s krumpáčem a lopatou někde v dole, nýbrž se se svým počítačem zapojíte do složitých výpočtů, za jejichž výpočet dostanete řádnou odměnu ve formě kryptoměny. [2]

Téměř všechny dnešní kryptoměny jsou založeny na technologii blockchain a o její existenci už určitě každý slyšel minimálně v souvislosti s kryptoměnou Bitcoin.

1.2.1 Blockchain

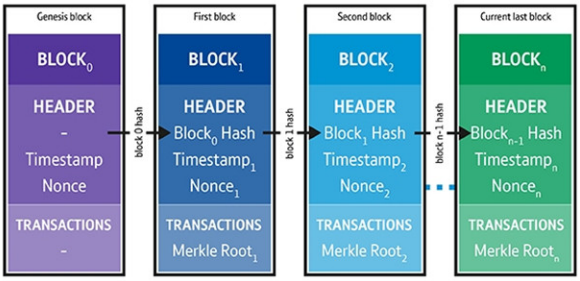
Při doslovném překladu by blockchain mohl být vyložen jako řetězec bloků a nebudeme daleko od pravdy. Blockchain je distribuovaná databáze skládající se z po sobě jdoucích bloků, které vždy obsahují odkaz na blok předchozí. Tato databáze se nemusí výlučně omezovat pouze na kryptoměny, ale je použitelná například v logistice pro sledování pohybu nákladu. [6]

[3)] Problém spojený s přechodem na nové milénium, kdy počítače špatně interpretovaly rok 2000. Zápis roku byl totiž složen jen ze 2 posledních číslic a počítač tak nebyl schopen rozeznat rok 1900 a 2000 nebo interpretoval rok jako 19100.



Obr. 1.3 Typy sítí [27]

Základním prvkem je blok. Jak bylo již řečeno, každý blok obsahuje transakce, či nějaké informace a odkaz na blok předchozí. Tento odkaz je ve formě hash[4)] otisku celého předchozího bloku, to znamená, že díky těmto hash otiskům se můžeme dostat až k prvnímu bloku nazývanému genesis block. [6]

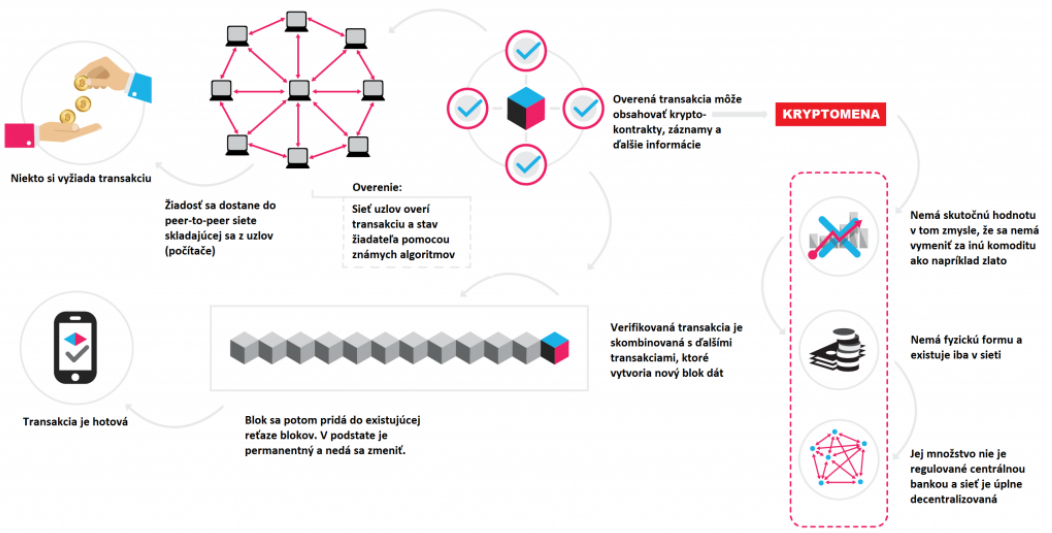


Obr. 1.4 Řetězení bloků [30]

Díky odkazům na předchozí blok je tedy nemožné již vygenerovaný a připojený blok jakkoliv změnit, jelikož by se následně změnil hash otisk tohoto bloku, ten by změnil další otisk a toto řetězení by pokračovalo až k poslednímu bloku. [2, 3]

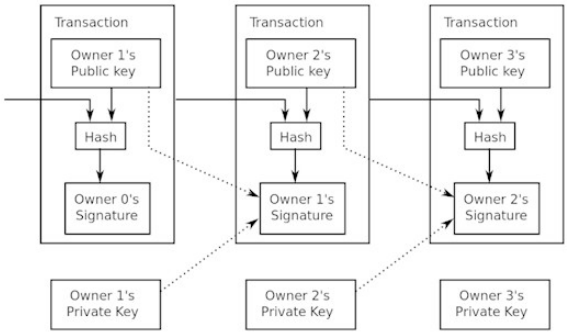
Pro zajištění ještě vyšší bezpečnosti se k těmto informacím připojuje také hodnota nonce. Nonce je číslo, které by mělo být v celé síti unikátní, avšak v praxi nedokážeme zaručit, že tomu tak vážně bude, a proto k tomuto číslu připojujeme ještě časové razítko. [2, 3] Celý koloběh krásně popisuje obrázek ze serveru Kryptomagazín.cz (Obr. 1.5)

[4)] Je výstup hashovací funkce, která mění vstup o různé délce na výstup o délce jednotné. Tento proces je nevratný a je prakticky nemožné z něj vyluštit původní zprávu.



Obr. 1.5 Technologie blockchain [6]

Transakce Samotná transakce uvnitř blockchainu se dosti podobá digitálně podepsanému dokumentu. Pro příklad, rozhodneme se odeslat mince z peněženky A do peněženky B. Nejdříve potřebujeme veřejný klíč peněženky adresáta. Pomocí našeho privátního klíče k transakci vytvoříme digitální podpis, do kterého uložíme detaily transakce. Takto připravenou transakci můžeme odeslat do světa. Po vytěžení bloku, ve kterém figuruje naše transakce, je ověřena zbytkem sítě pravost této transakce. [2, 3]



Obr. 1.6 Schéma transakce [31]

Proof-of-Work (PoW) Aby námi navrhovaný (vytěžený) blok byl přijat do blockchainu a schválen jako platný, musí se na něm shodnout určité množství jednotlivých nodů (uzlů). Stavu, kdy se jednotlivé nody shodnou na tom, že námi navrhovaný blok je platný, se říká konsenzus. [3]

Postup konsenzu:

1. Nové transakce jsou vysílány do sítě.
2. Každý uzel transakce sesbírá a uloží do bloku.
3. Náhodně je vybrán uzel, který smí navrhnout svůj blok.
4. Ostatní uzly schválí nebo zamítnou navrhovaný blok.
5. Blok je přidán do blockchainu.

Jak ale vybrat férově, který node může navrhnout svůj blok? K tomuto účelu právě slouží proof-of-work. Aby byl zaručen náhodný výběr, jsou nody vybírány podle veličiny, kterou si nemůžeme monopolizovat, a tou je v našem případě výpočetní výkon. Nody tedy mezi sebou soutěží o možnost navrhnout následující blok. [3]

Proof-of-Stake (PoS) Jiným způsobem výběru nodu, je proof-of-stake. U tohoto způsobu výběru nehraje roli výpočetní výkon, ale počet držených mincí, jež těžař má. Existuje více variant, které zohledňují například délku držení mincí apod. Zároveň se zde zaměňuje pojem těžař za pojem razič. [3]

Mezi kryptoměny, u kterých se můžeme setkat s tímto systémem, se řadí Ethereum, Peercoin nebo například Nxt. [2]

Škálování (fork) Fork neboli vidlička je situace, kdy se více těžařům podaří v podobný okamžik vytěžit blok, který se snaží zapojit do blockchainu, aniž by o sobě věděli. Nastává zde situace, kdy již nemáme řetězec po sobě jdoucích bloků a řetězec se nám dělí (název vidlička proto, že následující uskupení vypadá jako vidlička s hroty). [2, 3]

Pokud nastane tato situace, je potřeba ji urychleně vyřešit, neboť by mohlo dojít ke dvojité útratě jedné mince. Aby bylo jasně rozhodnuto, který blok se zapojí do řetězce, používá se pravidlo bloku, na který byl vynaložen vyšší výpočetní výkon. Blok, který nebyl použit k rozvoji blockchainu, se následně pojmenovává jako orphan (sirotek). [3]

K forkování může také dojít při aktualizaci protokolu blockchainu a v tomto případě můžeme rozlišovat dva typy forku, a to měkký a tvrdý fork. [3]

Soft fork Jako soft fork se označuje stav, kdy byla pozměněna struktura protokolu blockchainu a tato nová struktura zůstává kompatibilní se starším protokolem. Nově vytěžené bloky jsou tedy uznávány i starší verzí softwaru jako validní. [3]

Hard fork Hard fork je naproti tomu stav, kdy změna struktury protokolu zapříčiní, že starší verze softwaru neuznává nové bloky jako validní a zpětná kompatibilita již není možná. V takovém případě musí na novou verzi softwaru přejít všichni uživatelé nebo dojde k rozdělení (splitu) blockchainu trvalým forkem. [2, 3]

Pokud takováto situace nastane a blockchain je rozdělen trvalým forkem, vznikají z původní měny dvě měny nové, hovoříme pak o škálování měny. Typickým příkladem hard forku může být rozdělení Bitcoinu na Bitcoin, Bitcoin cash nebo Bitcoin gold. [2, 3]

1.3 Ekonomie kryptoměn

Spousta ekonomů se proti kryptoměnám ohrazuje a ptají se, čím jsou tyto měny kryty. Odvolávají se na tzv. zlatý standard, kdy je měna kryta zlatem, což teoreticky zaručuje její sílu a nemožnost stále tisknout nové a nové bankovky. [2, 7]

Se zlatým standardem se v dnešní době však setkáme jen málo. Dnes jsou ve světě měny (pasiva) zajištěny především aktivy národních bank. Tato aktiva už netvoří jako dřív zlato (i když v některých případech má stále svůj podíl), ale jsou tvořena především pohledávkami vůči zahraničí včetně cenných papírů v cizí měně. Pod tímto pojmem si můžeme představit dluhopisy, cenné papíry a další cenné listiny vydávané zahraničními bankami a státy. [7]

Na rozdíl od běžných měn, kterým byly věnovány předchozí řádky, kryptoměny nejsou ničím kryty a jsou decentralizované. Tedy nemají žádné centrum, které by řídilo jejich cenu a počet mincí v oběhu. [2]

Jak tedy vzniká cena jednotlivé mince? Její cena je dána nabídkou a poptávkou po dané měně a její vzácností. Tak jako zlato a další nerosty, i kryptoměny mají omezené množství, a proto se mince stávají vzácnými. V dnešní době se můžeme setkat s velkou volatilitou[5)] u kryptoměn jako je například Bitcoin. Tato volatilita je dána velkou popularizací měny a nárustem poptávky v posledních letech. Ona značná poptávka a snaha investorů zbohatnout během krátkého období má však za následek rychlé kolísání měny a její nestabilitu. Vytváří se zde následně tzv. bubliny, kdy se cena neustále zvyšuje a bublina se nafukuje, dokud bublina nepraskne a cena opět rapidně poklesne. [8]

Dají se však kryptoměny klasifikovat jako peníze? Příznivci kryptoměn tuto klasifikaci podporují a i zákon se v mnoha případech vyjadřuje o kryptoměně jako o formě cizí měny, ale bude ještě chvíli trvat než kryptoměny vstoupí do povědomí lidí jako reálné peníze pro běžné platby. [2, 9]

[5)] Volatilita je pravděpodobnost, že se cena bude v průběhu daného časového období měnit. Se zvyšující se volatilitou se zvyšuje rozpětí, ve kterém cena kolísá.

1.3.1 Kryptoměny u nás

Česká legislativa zatím neumí s kryptoměnami pracovat a nijak je nezakazuje. Pokud však budeme chtít kryptoměnu směnit za zboží či koruny, vždy musíme tuto směnu zdanit. Jako fyzická osoba odvedeme státu 15% daň, zatímco právnická osoba odvádí 19% daň. [2]

Pokud kryptoměnu prodáváme, z finančního pohledu se jedná o příjem z prodeje. Tento příjem nemusíme danit, pokud během zdaňovacího období (tedy jednoho roku) nepřesáhne 30 000 Kč. [2]

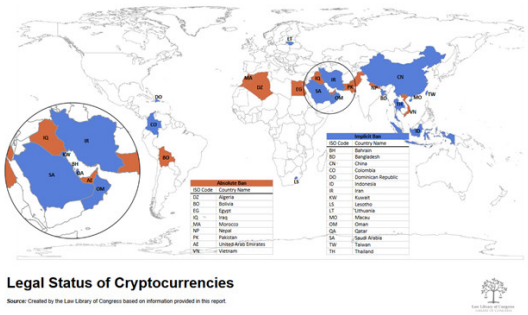
Zákon také rozlišuje, zda se jedná o jednorázový prodej, či opakovanou činnost. Ve druhém případě tedy budeme muset na konci zdaňovacího období vyplnit daňové přiznání, i když náš výdělek nepřesáhne částku 30 000 Kč. [2]

Obchody uskutečňované právnickými osobami jsou pod přísným státním dohledem a je s ním spojená složitá agenda. Dnešní zákony si nevědí moc rady s nákupem a držením kryptoměn a pro firmu tak vzniká velmi komplikovaná situace, kdy není zcela jasné, co se s kryptoměnou má stát po jejím nákupu. [2]

Česká legislativa se snaží na kryptoměny stále adaptovat, ale nynější situace jejich rozmachu u nás moc nepomáhá. Běžný občan s velkou pravděpodobností ani neví, že i po zaplacení za službu či zboží musí z tohoto obchodu odvést státu daň. V budoucnu se snad dočkáme větší adaptace virtuálních měn do českého finančního systému. [2]

1.3.2 Kryptoměny ve světě

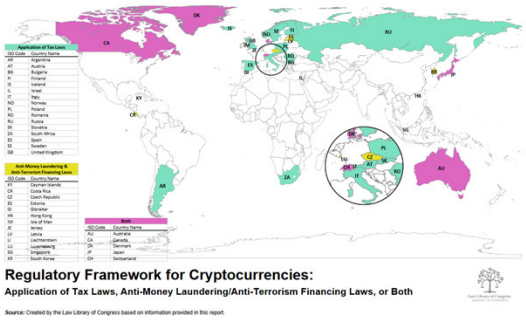
Názory na kryptoměny se ve světě různí. Tak jako v České republice, i ve světě si spousta států neví rady, jak tyto virtuální měny zařadit do svých finančních systémů. Spousta států kryptoměny uznává jako legální a liší se zde jen forma zdanění. [9]



Obr. 1.7 Legálnost kryptoměn ve světě [24]

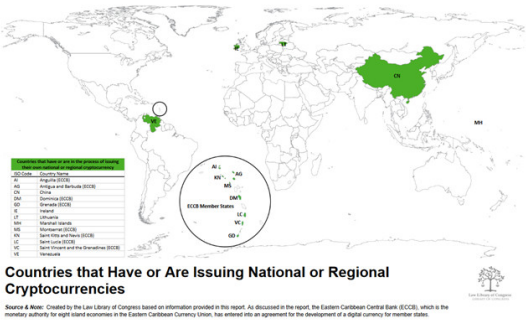
Některé státy zavedly přísná pravidla a omezení pro obchodování s kryptoměnami z důvodu obav o napojení těchto obchodů na teroristickou činnost nebo praní špinavých

peněz. Z těchto důvodů musí banky a instituce provádějící transakce pomocí kryptoměn státu hlásit všechny obchody. Mezi tyto státy patří například Austrálie nebo Kanada. [9]



Obr. 1.8 Státy regulující obchod s kryptoměnou [25]

Státy jako Čína, Irsko či Litva šly v této problematice ještě o krok dál a zavedly nebo se snaží zavést svou vlastní kryptoměnu. Čína je v problematice kryptoměn sporná, jelikož veškeré další virtuální měny zakazuje. [9]



Obr. 1.9 Státy vyvíjející vlastní kryptoměnu [26]

2 Těžba a směna kryptoměn

Než začneme kryptoměnu používat, musíme si jako u klasické měny pořídit peněženku. Jednotlivé mince můžeme považovat za unikátní kód, či posloupnost čísel. Takto uložené mince můžeme uložit na harddisk, flashku či vytisknout na papír a uložit do šuplíku. Pro jednodušší práci s kryptoměnou je však nejlepší pořídit si peněženku elektronickou. Zde máme na výběr hned z několika variant. Můžeme si pořídit peněženku:

1. Softwarovou
2. Hardwarovou
3. Webovou
4. Mobilní

2.1 Pěněženky

2.1.1 Softwarová peněženka

Softwarová peněženka je velmi populární, hlavně v kombinaci s peněženkou mobilní. Jedná se o software vyvíjený pro uchování, přijímání a odesílání kryptoměn. První možnost, která se nabízí, je stáhnout si peněženku z oficiálních stránek měny. Tady však často nastává problém, že tento klient v sobě uchovává kompletní řetězec blockchainu a zabírá tak zbytečně moc místa. [2, 3]

Proto je dobré se poohlédnout po úspornějším softwaru. Tím by mohla být například populární peněženka Electrum, Jaxx, Exodus a další. Tyto softwarové peněženky nabízejí intuitivní ovládání, líbivý design a v mnoha případech i mutaci pro mobilní zařízení. [2, 6]

Jelikož osobní počítače čelí útokům v podobě virů, malwarů a dalšího invazivního softwaru, je třeba svou peněženku zabezpečit. Peněženka nám zpravidla vygeneruje soubor, ve kterém máme uloženy své mince a přístupové údaje k nim. Tento soubor je dobré zálohovat, abychom předešli možné ztrátě nebo zničení a také bychom jej měli zašifrovat, aby se k němu útočník nedostal. V minulosti bylo takto již zcizeno mnoho mincí hlavně kryptoměny Bitcoin. [2, 6]

2.1.2 Hardwarová peněženka

Další z možností, jak uložit naše mince, je pořízení hardwarové peněženky, což je jednoúčelové zařízení podobné flashdisku, na kterém jsou uloženy naše soukromé klíče k softwarové peněžence.

Pokaždé, když chceme provést platbu, je potřeba mít fyzicky u sebe právě toto zařízení, kterým digitálně podepíšeme transakci, a transakce tak může být provedena. Při tomto podepsání jen připojíme peněženku pomocí USB k počítači, na peněžence zadáme své heslo a dáme potvrdit. Díky tomu, že se soukromé klíče nacházejí právě na tomto zařízení a nikdy se neodesílají do počítače, je tak zabráněno možnému odchycení klíče útočníkem. [2]

Obr. 2.1
Trezor
One [28]

Revoluci v hardwarových peněženkách přinesl český vynález Trezor. V dnešní době vyrábí firma 2 verze, a to Model T a Trezor One. Další velmi populární hardwarovou peněženkou je Ledger, který nabízí více modelů a pro některé designově líbivější vzhled. [2, 6]

Obr. 2.2 Ledger
Nano X [29]

2.1.3 Webová peněženka

Jednou z méně doporučovaných peněženek je peněženka webová, či cloudová. Jedná se o druh peněženky, kdy máme mince uloženy na webu nějakého zprostředkovatele a máme k ní přístup prakticky odkudkoliv. Mnoho lidí ale už neví, že mince, které si takto uloží u třetí strany nejsou nikdy technicky úplně jejich. Náleží provozovateli webu a pokud by se stalo, že bude mít majitel webu s našimi mincemi nekalé úmysly, jen těžko se pak budeme domáhat svých mincí zpět. [2, 3]

2.1.4 Mobilní peněženka

Poslední kategorií peněženek jsou ty pro mobilní platformy. Nemusíme se obávat absence peněženky pro jednotlivé platformy, jelikož základní platformy jako Android, iOS, Windows, či Blackberry mají aplikace peněženek k dispozici. Jediné omezení, se kterým se zde můžeme setkat, je nízký počet aplikací podporujících danou platformu. [2]

Na platformě Android se můžeme setkat s aplikacemi jako Blockfolio, BitPay, Coinomi, Mycelium a mnoha dalšími. Díky rozšířenosti platformy máme možnost si vybrat z nemalého počtu aplikací. [2, 6]

Platforma iOS nám poskytuje také spoustu nativních aplikací jako Bread wallet, Airbitz, Bither či Copay. Jak už tomu u těchto dvou nejpopulárnějších platforem bývá, v nabídce jsou i více platformní aplikace jako Jaxx, Coinbase, Blockchain wallet apod., díky kterým můžeme mít přehled o svých transakcích na obou platformách. [2, 6]

Na posledních platformách Windows a Blackberry si budeme muset vystačit jen s aplikací Coin.space pro Windows a Bitcoin Wallet pro Blackberry. [2]

2.2 Těžba

Těžba je podle knihy pana Stroukala a Skalického: *„. . . proces, při kterém se pomocí strojově náročného výpočtu hledá další blok pro napojení do blockchainu.“*. [2]

Snaha těžaře tedy je, aby pomocí svého zařízení vypočítal hash hodnotu celého bloku tak, aby jeho hodnota byla nižší, než je požadovaný cíl. Tato hodnota se odvozuje od aktuální náročnosti těžby a v pravidelných intervalech se mění. [2, 3]

Pokud bychom se chtěli věnovat těžbě na vyšší úrovni, už nám nebude stačit klasický počítač, jelikož náročnost těžby populárních měn, jako je Bitcoin, je velmi vysoká. Postupem času se těžba přesunovala z procesorů (CPU) na procesory grafických karet (GPU), následně na programovatelná hradlová pole (FPGA) a nyní až k obvodům ASIC, což jsou obvody speciálně navrhované pro výpočet jednoho typu výpočtu. [2]

2.2.1 CPU Těžba

Je nejjednodušší a nejstarší forma těžby. Tato forma těžby je velmi pomalá a při dnešní náročnosti těžby již nepoužitelná. Kdokoliv, kdo by se pokoušel těžit pomocí CPU, brzy zjistí, že je tato forma těžby ztrátová a zisk můžeme generovat pouze u začínajících měn s nízkou obtížností nebo u měn zakazujících těžbu ostatními způsoby. [3]

2.2.2 GPU Těžba

Dalším vývojovým stupněm těžby je těžba pomocí grafické karty. Její výhody jsou hlavně v paralelním výpočtu jednotlivých hash hodnot, kdy na více aritmetických logických jednotkách (ALU) grafické karty řešíme více výpočtů najednou. Také tento způsob je přijatelný i pro úplné začátečníky, jelikož téměř všechny moderní počítače obsahují výkonnou grafickou kartu, která může být ve většině případů ještě přetaktována na vyšší výkon. [3]

Obr. 2.3 Domácí GPU stanice [3]

Další výhodou grafických karet je možnost připojení více karet na jedno CPU, získáváme tak vyšší výkon a vyšší pravděpodobnost vytěžení bloku. To vedlo k vytvoření mnoha domácích těžebních stanic. Problém však nastává s chlazením a spotřebou elektrické energie takovéto stanice. Zároveň i pořizovací náklady výkonných grafických karet nejsou malé a můžeme se zde opět octnout ve ztrátě. [3]

2.2.3 FPGA Těžba

Postupem času se začalo upouštět i od těžby na grafických kartách a okolo roku 2011 se objevila programovatelná hradlová pole. Nabízejí vyšší výkon než grafické karty s jednodušším řešením chlazení. [3]

Na rozdíl od grafické karty můžeme teoreticky využít plný potenciál tohoto zařízení a nechybí ani možost připojení k jedné centrální jednotce. [3] Rychlost výpočtů se zvyšuje exponenciálně a v porovnání s 20 MH/s u těžby pomocí CPU se dostáváme k hodnotám okolo 1 TH/s. [3]

I přes veškeré výhody je FPGA těžba velice náročná, jelikož správné naprogramování je obtížnější než u GPU a špatná dostupnost těchto zařízení na trhu také nenahrává této těžbě do karet. Posledním hřebíčkem do rakve byl pak rychlý nástup posledního typu těžby pomocí ASIC hardwaru. [3]

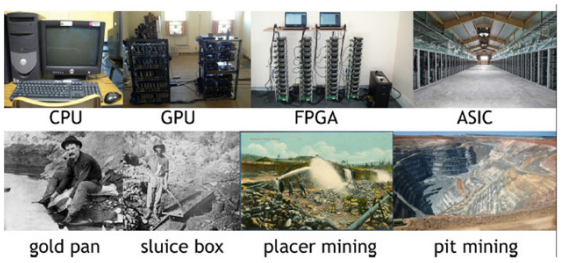
Obr. 2.4 FPGA stanice [3]

2.2.4 ASIC Těžba

V dnešní době dominantní forma těžby. Jedná se o speciálně navrhnuté obvody pro řešení jednoho typu příkladů. Tyto obvody byly již od začátku designovány pro těžbu kryptoměn a v dnešní době je na světě několik výrobců těchto zařízení, u kterých si můžeme vybrat model přesně podle našich představ. [3]

Obr. 2.5 Těžební centrum [3]

V dnešní době se přesunuje těžba od jednotlivců do speciálních těžebních center, která si silně střeží svá tajemství, a do budoucna může tento přesun těžby úplně vytlačit běžné těžaře z tohoto odvětví. [2, 3]



Obr. 2.6 Vývoj těžby kryptoměn a zlata [3]

Abychom mohli kryptoměnu těžit, musíme si k tomu pořídit příslušný software. Pro systém Windows můžeme použít například těžební program GUIMiner, který je zdarma k dostání na stránkách guiminer.org a nabízí běžným uživatelům možnost těžit v tzv. poolech (bazénech). [2]

2.2.5 Pool

Pool neboli bazén je společenství několika uživatelů (těžařů), kteří se snaží společnými silami vytěžit jeden blok. Po vytěžení bloku pool rozdělí odměnu podle vyřešených úloh mezi jednotlivé členy a těžba začíná nanovo. [3, 6]

Členství v poolu má výhody nejen v tom, že člen nemusí mít extrémní výpočetní výkon a může se tak podílet na těžbě i se stolním počítačem, ale i ve formě jakéhosi zajištění vytěžené odměny, jelikož se zde zvyšuje pravděpodobnost vytěžení bloku, oproti těžbě jednotlivce, a tím se stabilizuje pravidelný přísun kryptoměny, i když za cenu nižších výdělků. [2, 3]

Jednotlivé pooly se od sebe liší ve velikosti, v poplatcích, v politikách chodu... Do některých poolů se může těžař zapojit zdarma, zatímco jiné si účtují poplatek za vstup. Některé pooly si poplatky za transakci rozdělují, jiným tyto poplatky zůstávají jako poplatek za možnost účastnit se těžby. Při volbě vhodného poolu je rozhodnutí jen na těžaři a jelikož je konkurence mezi pooly stále narůstající, snaží se každý pool oslovit těžaře tak, aby získal vyšší pravděpodobnost vytěžení bloku. [2, 3]

2.3 Nákup, směna a platby

Způsob získání kryptoměny pomocí těžby je pro spoustu lidí zbytečně zdlouhavý, složitý anebo výpočetně náročný pro jejich zařízení. Proto existuje jako i u zlata možnost si kryptoměnu jednoduše nakoupit na burze, ve směnárně, v bankomatu nebo přímo od fyzických vlastníků měny. Jelikož je většina kryptoměn decentralizovaná, jejich kurz u jednotlivých prodejců se může velmi lišit, proto je dobré si před nákupem projít více nabídek a porovnat, která je pro vás nejvýhodnější.

V českém prostředí pro nás bude nejjednodušší nákup přes specializované směnárny, či bankomaty. Ty nám za české koruny smění kryptoměnu podle našeho výběru při kurzu daném směnárnou. Mezi nejznámější směnárny v české republice patří server simplecoin.cz, kde můžeme obchodovat s kryptoměnou bez nutnosti registrace. [1, 2]

2.3.1 Burza

Další možností je obchodování na burze, to přináší levnější kurzy, ale také rizika. Mezi největší burzy patří Coinbase, Binance, Kraken nebo třeba BitMex. Výhodou těchto

obchodů může být celosvětové měřítko, kdy opouštíme české prostředí a vrháme se do globálního obchodního systému. [1, 6]

S obchodováním na burze je však spojena spousta různých úskalí. Například registrace na burze je časově náročná, jelikož burzy vyžadují ověření identity a místa bydliště. Pro ověření identity je potřeba fotografie pasu nebo občanského/řidičského průkazu. Problém nastává u ověření místa bydliště, jelikož burzy vyžadují úředně ověřený dokument nejlépe v angličtině se jménem a místem bydliště. [2]

Po přihlášení na burzu nám už jen zbývá si nabít burzovní účet penězi. Zde se opět setkáváme s potížemi v podobě nutnosti nabít účet dolary, eury, či jinou zahraniční měnou a celý proces začátku obchodování na burze se proto natahuje. [2]

Poslední důležitou poznámkou by měl být i fakt, že na světě jsou kvanta podvodných burzovních serverů, které se snaží své účastníky obrat o peníze, a vždy je dobré si před začátkem obchodování na burze o dané burze přečíst recenze uživatelů a vnějších pozorovatelů. Zároveň i u důvěryhodných burzovních systémů hrozí riziko pádu, jak se tomu stalo v případě bitcoinové burzy Mt. Gox, proto se obchodování na burze spíše nedoporučuje. [2, 6]

2.3.2 Face to face obchod

Jak už možná tušíte, face to face (tváří v tvář) obchod je směna mincí mezi 2 stranami tváří v tvář. Svého prodejce, či nákupčího můžeme najít na sociálních sítích nebo pokud jde o Bitcoiny na localbitcoins.com. Zadáme zde jen město, kde chceme prodejce/nákupčího najít a web nám nabídne nabídky a poptávky v okolí. Je to rychlý způsob, jak nakoupit nebo prodat bitcoiny a zároveň se třeba seznámit s dalšími uživateli této měny. [2]

Důležité je dávat si pozor kolik peněz chceme vyměnit, jelikož podle změny zákona 261/2014 Sb. o omezení plateb v hotovosti nesmí částka přesáhnout 270 000 Kč. [10]

2.3.3 Platby

Na závěr se dostáváme k samotným platbám pomocí kryptoměny u obchodníků. Počet obchodníků přijímajících platby v kryptoměnách stále přibývá díky platformám, které zprostředkovávají tyto platby (Bitpay.com, Paybear.io či třeba Coinpayments.net) a zjednodušují tak prodejcům vstup na tento trh. [6]

Každá služba zřídí obchodu webovou peněženku, na kterou (nebo ze které) budou přicházet platby v měně zadané při tvorbě peněženky. Za tyto pohyby v peněžence jsou zákazníkovi účtovány menší poplatky. Jak již bylo zmíněno, měnu si vybíráme při tvorbě peněženky, ale není problém mít takovýchto peněženek více a nabídnout tak zákazníkovi našeho obchodu více alternativ pro platbu. Když chce následně obchodník

peníze z peněženky vybrat, nabízí se mu možnost vybrat buďto mince kryptoměny nebo podle interního kurzu směnit tyto kryptoměny za fiat peníze. [2]

Zároveň je tlačným faktorem i nynější populárnost alternativních forem plateb a spousta obchodníků tak tento trend využívá pro zviditelnění.

Obchodníci přijímající kryptoměny Na trh s kryptoměnou se dostává stále více a více obchodníků, kteří v tomto trhu vidí potenciál. Dříve šlo hlavně o malé obchůdky, ve kterých jsme si mohli koupit pizzu, nebo třeba opravit kolo. S postupem času a se zvyšujícím se počtem uživatelů kryptoměn se však na poli příjemců kryptoplateb objevují i známá jména a velké korporace.

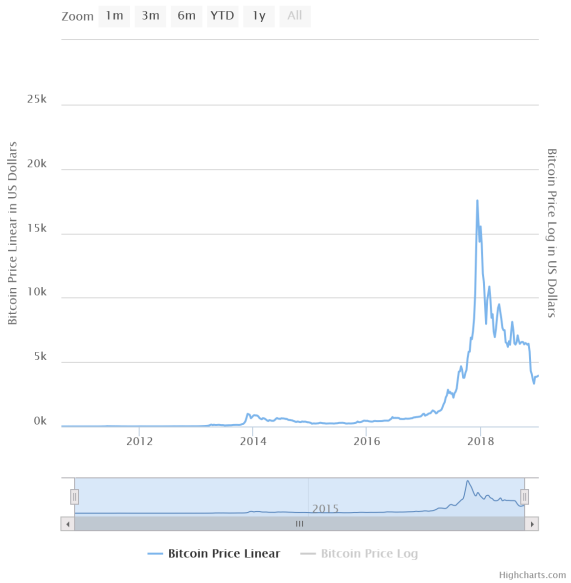
Kanadské KFC, Playboy nebo třeba Subway je jen špička ledovce obchodů přijímajících kryptoměny. Z dalších velikánů nelze nezmínit Microsoft, který zavedl platby pomocí Bitcoinu za hry, aplikace a filmy ve Windows store a Xbox store. Kdo by však chtěl takto platit v Microsoft store bude zklamaný, jelikož do tohoto obchodu platby ještě nebyly zavedeny. Na českém poli by pak jasně vítězil internetový obchod Alza.cz. [11, 12]

Ve výčtu výše zmíněných příjemců kryptoplateb se povětšinou setkáme s platbami pomocí Bitcoinu, díky jeho popularitě. Na trh se ale pomalu dostávají i další měny jako Ethereum, Litecoin a další, které si pomalu ale jistě získávají své uživatele. Rozhodně revolučním velikánem v tomto ohledu je internetový obchod Overstock.com, který podporuje všechny 3 zmíněné měny. [11, 12]

II. PRAKTICKÁ ČÁST

3 Přehled kryptoměn

Tato kapitola je věnována kryptoměnám, které můžeme najít na dnešním trhu. Některé to možná překvapí, ale k 28. únoru 2019 se na světě vyskytuje více než 2100 kryptoměn s tržní kapitalizací okolo 123 591 320 060 $, což jsou závratná čísla. Probrat všechny by zabralo spoustu času, a proto zde bude zmíněno pouze pár vybraných měn, které přišly autorovy zajímavé. Velký nárůst obchodu a vzniku nových měn můžeme zaznamenat od začátku roku 2017, jak je vidět na obrázku (Obr. 3.1) znázorňujícím tržní kapitalizaci kryptoměn. Jelikož se za zakladatele moderních kryptoměn obecně považuje Bitcoin, všechny zbylé měny můžeme nazývat slovem altcoin, které vychází ze spojení slov alternative coin. [13]



Obr. 3.1 Tržní kapitalizace kryptoměn od roku 2013 [13]

Velký boom kryptoměn způsobuje vznik stále nových a nových měn, které jsou buďto odvozeny od Bitcoinu a jeho systém upravují do své podoby nebo se snaží razit novou cestu pomocí svých technologií. Tabulka (Tab. 3.1) reprezentuje kryptoměny, které budou v bakalářské práci dále rozpracovány. Trh s kryptoměnou je doslova živý organizmu, a proto musíme brát čísla v tabulce spíše jako orientační, jelikož se jejich hodnoty mění v řádech sekund.

Tab. 3.1 Přehled kryptoměn k 28. 2. 2019

#	Jméno	Zkratka	Tržní kapitalizace [$]	Cena mince [$]
1.	Bitcoin	BTC	67 953 190 114	3 869,18
2.	Ethereum	ETH	13 539 475 837	128,80
3.	XRP	XRP	12 709 367 032	0,306751
4.	EOS	EOS	3 013 395 820	3,33
5.	Litecoin	LTC	2 804 247 662	46,22
6.	Bitcoin cash	BCH	2 353 910 632	133,39
7.	Tether	USDT	2 040 781 960	1,01
8.	Moner	XMR	831 226 783	49,41
9.	Dash	DASH	697 909 371	80,51
10.	NEO	NEO	546 128 866	8,40
11.	Dogecoin	DOGE	236 429 596	0,001996
12.	Vertcoin	VTC	20 437 149	0,421488

3.1 Známé kryptoměny

Do kategorie známých kryptoměn bychom mohli bez pochyby zařadit minimálně dvě kryptoměny. Začněme tedy rovnou tou nejznámější a snad nejdiskutovanější kryptoměnou dnešní doby a tím je Bitcoin.

3.1.1 Bitcoin (BTC)

Bitcoin začal psát svůj příběh v roce 2009. Vytvořil jej anonymní vývojář pod přezdívkou Satoshi Nakamoto a dodnes se spekuluje, kdo to vlastně byl. Měna je založena na protokolu blockchain, který spolu s již zmíněnou měnou Nakamoto navrhl. Zásoba mincí je fixně omezena na 21 milionů a měla by být kompletně vytěžena do roku 2140, kdy se těžba zastaví. Aby bylo docíleno postupného těžení, je rychlost těžby uměle omezena na 1 blok za zhruba 10 minut. [2, 6]

Díky decentralizaci a anonymitě nepotkal Bitcoin stejný osud jako spoustu dalších kryptoměn, které dále po roce 2010 vznikaly a které byly státem označeny v kontextu nelegální činnosti jako pračky špinavých peněz, pokusy o terorizmus a tak dále.

Jednou z nejslavnějších transakcí a dalo by se říci i velkým nakopnutím obchodu s Bitcoinem je obchod uskutečněný mezi Laszlem Hanyeczem a neznámým anglickým programátorem, kdy Laszlo nabídl 10 000 Bitcoinů za 2 pizzy, které mu byly skutečně doručeny. V dnešní době by za pizzy Laszlo utratil neuvěřitelných 38 milionů dolarů, nicméně právě díky němu a dalším odvážlivcům se stal Bitcoin populární a lidé začali kryptoměnu považovat za reálnou možnost plateb. [2, 3]

Bitcoin zažil v průběhu let světlé i stinné stránky při prudkých vzrůstech a pádech, periodicky se opakujících s novými vlnami zájmu o měnu. Tyto výkyvy by se daly

přirovnat k nafukování bubliny, která dříve či později musí prasknout a nastane tak další propad. Prasknutí bubliny mají ve velké oblibě hlavně média, která následně ráda haní kryptoměny a jejich nestabilitu, nicméně je nutno říci, že i když dojde k propadu ceny mincí, cena se ustálí a v budoucnu, až se ustálí i počet uživatelů měny, k nafukování bublin nebude docházet. [2, 6]

Další vlnou skepse a negativního přístupu k Bitcoinu bylo odhalení serveru Silk Road, který byl zaměřený na obchod s drogami, zbraněmi, dětskou pornografií a obecně byl spojován s dalšími nelegálními činnostmi. Tento server se podařilo rozbít, jeho provozovatele vypátrat a odsoudit, ale fakt, že byl Bitcoin používán k nelegální činnosti, nebylo možné popřít a zájem o měnu opět prudce klesl. [2, 6]

Stále větší zájem o kryptoměnu vedl k zahlcení sítě transakcemi a uživatelé volali po změně. Velikost bloku byla 1 MB a rychlost transakcí tak byla zhruba 7 transakcí za vteřinu, což je pro celosvětový trh žalostné číslo. V roce 2015 vývojáři představili segwit[6)], který měl navýšit počet transakcí v bloku zhruba o 80 %. Optimalizace protokolu však některým uživatelům stále nestačila, a tak došlo 1. 8. 2017 k hard forku a Bitcoin se rozdělil na 2 větve sestávající se z Bitcoinu a nově vzniklého Bitcoinu cash. [3]

3.1.2 Bitcoin cash (BCH)

Nově vzniklý Bitcoin cash se tak stal vůbec prvním derivátem Bitcoinu. Rozdělení bylo považováno za krok špatným směrem a analytici nevěřili v budoucnost této měny, během zbytku roku 2017 se však podařilo Bitcoinu cash vyrůst až na 20 % ceny původního Bitcoinu. Dalším důsledkem rozdělení bylo, že majitelé tzv. „starého“ Bitcoinu při vzniku Bitcoinu cash získali stejný obnos i nově vzniklého Bitcoinu. [14]

Jaké jsou ale změny oproti stávajícímu Bitcoinu? Velikost bloku byla zvýšena až na 8 MB, z protokolu byl odstraněn segwit. Dalším logickým krokem bylo zavedení replay protection, aby se zamezilo zaměnitelnosti s BTC. Vývojáři toho docílili díky pozměnění ověřovacího algoritmu validity transakce. Byl také pozměněn algoritmus pro náročnost těžby, jelikož se zděděnou úrovní obtížnosti od BTC by bylo zbytečně těžké vytěžit první bloky, pokud by síť neobsahovala dostatek těžařů. [6, 14]

3.1.3 Litecoin (LTC)

Litecoin byl představen světu 7. 10. 2011 bývalým programátorem Googlu Charliem Lee. Jedná se o jeden z nejznámějších derivátů Bitcoinu. Byl navržen pro mikroplatby

[6)] Segwit, zkrácenina spojení slov segregated witness je označení pro vnitřní reorganizaci bloku tak, že jsou odděleny podpisy transakcí od transakcí. Tím je docílena značná úspora místa za stávající velikosti bloku.

(odtud i název Litecoin) a jeho rozdíl oproti Bitcoinu spočívá v rychlejším generování bloků, a to až čtyřnásobném. Celkový počet mincí je 84 milionů oproti 21 milionům BTC a náročnost těžby je zde optimalizována pro méně výkonný hardware. [15, 16]

Spousta zdrojů souhlasí s přirovnáním, že pokud je Bitcoin zlato, potom je Litecoin stříbro na poli kryptoměn. Tvůrci samotní jej označují jako doplněk k Bitcoinu. V kódu LTC je již zakomponovaný segwit a dá se říci, že všechny všechny změny v LTC jsou předzvěst změn u BTC. Litecoin se tak stal jakýmsi pokusným králíkem pro Bitcoin. [6]

Pokud bychom se rozhodli těžit Litecoin, je zde stále možnost těžby pomocí GPU, nicméně i zde navzdory použití jednoduššího těžebního algoritmu Scrypt již pronikla ASIC těžba a těžba pomocí GPU tak může být ztrátová. Abychom však zakončili na lehčí notu, Litecoin začíná být velice rozšířeným platebním nástrojem, jako příklad by se dala uvést možnost plateb v LTC v obchodě Alza.cz a rozrůstající se počet automatů směňující české koruny na LTC po České republice. [6, 16]

3.2 Perspektivní kryptoměny

Do kapitoly perspektivních kryptoměn by se dal zařadit i BCH nebo Litecoin. V tomto případě bude však pozornost zaměřena spíše na menší projekty, u kterých cena ještě nepřesáhla oněch ikonických 100 dolarů. Zároveň tyto kryptoměny nabízejí nové funkcionality a rozšiřují základní vlastnosti Bitcoinu, ze kterého vycházejí, zase o kus dál.

3.2.1 Dogecoin (DOGE)

Jako první bychom si představili trochu recesistickou měnou s názvem Dogecoin. Dogecoin se objevil na scéně v prosinci 2013 v návaznosti na úspěšný meme obrázek s plemenem psa Shiba-Inu. Na svědomí jej mají Billy Markus z Portlandu a Jackson Palmer ze Sydney. Jedná se o derivát Litecoinu, jež se navzdory své absurditě rychle chytil a rozšířil. Původní záměr obou zakladatelů byl vytvořit tokeny, kterými by bylo možné ohodnocovat kvalitní obsah na serveru Reddit. Oba zakladatelé brali svou kryptoměnu spíše jako vtip než jako skutečnou kryptoměnu pro uskutečňování plateb v obchodech. [13, 17]

Nemožné se však stalo skutečností a měna si rychle vytvořila širokou fanouškovskou a uživatelskou skupinu a nyní je s ní možné platit od hostingových služeb, přes ubytování, umění, hudbu až po jídlo a pití v kavárnách.

Dogecoin je podle oficiálního webu obchodovatelný na 8 burzách příznačně pojmenovaných jako DogeStuff's Store, SuchList, DogEshop a další. V českém prostředí je patrně nevyužitelný, ale může být veselým zpestřením a zajímavou volbou pro experimentování s kryptoměnou.

3.2.2 Dash (DASH)

Dalším zástupcem perspektivních měn je Dash. Dash vznikl v roce 2014 pod názvem XCOIN, poté byl přejmenován na Darkcoin než se jeho název ustálil na finálním Dash formou spojení slov digital cash. [18]

Dash je odvozen tak jako Dogecoin od Litecoinu, ale přináší do světa kryptoměn pár novinek. Hashovací algoritmus SHA-256 byl vyměněn za algoritmus X11 a do sítě byly přidány krom běžných uživatelů a těžařů ještě master uzly. Ty zde slouží k zachování anonymity transakcí v rámci sítě. Ke vzniku master uzlu je potřeba 1 000 mincí, které slouží proti kompromitaci uzlu. Motivací pro založení uzlu je pak 45% podíl na nově vytěžených mincích. Dalších 45 % získávají těžaři a zbylých 10 % je odloženo bokem do tzv. pokladnice pro rozvoj sítě na základě uživatelské zpětné vazby. O schválení uživatelsky navržených změnách opět rozhodují master uzly a celý systém je tak motivován k rozvoji kryptoměny. Díky těmto nástrojům je také komunita okolo měny řazena k nejaktivnějším na poli kryptoměn. [18, 19]

Krom podílu na vytěžených kryptoměnách mohou zajišťovat master uzly také transakce mezi uživateli, aniž by museli čekat, až se tyto transakce zapíší do blockchainu. Díky tomu jsou transakce mezi uživateli prováděny podle oficiálních zdrojů za 1 vteřinu. Krom funkce InstantSend, která byla právě popsána, mají master uzly ještě druhou funkcionalitu s názvem PrivateSend, která zajišťuje anonymitu plateb. Princip fungování je velmi jednoduchý a funguje na spojování menších transakcí do větších. Pokud tedy odesílá uživatel 1 platbu uživateli 2 a uživatel 3 uživateli 4, ve finále pouze zjistíme že uživatelé 1 a 3 odesílají platby uživatelům 2 a 4. Poslední podmínkou pro fungování master uzlu je neustálý přístup k síti, aby bylo zajištěno její správné fungování. [18, 19]

Pokud bychom se rozhodli pro těžbu, i zde se setkáme s těžbou pomocí ASIC čipů. Tento osud nevyhnutelně potkává zatím téměř každou kryptoměnu. Jako nejvhodnější řešení těžby je podle serveru Alza.cz momentálně ASIC hardware pod názvem Antminer D3. [6, 19]

K dnešnímu dni je možné Dash použít u více než 4 800 obchodníků, směnit jej lze zhruba na 90 burzách a směnárnách a denně jej použije přes 48 000 uživatelů. Jedná se tedy o široce rozrostlou síť, která stále nabírá na objemu a s cenou okolo 80 dolarů za minci je ještě přijatelnou a zajímavou variantou pro investici.

3.2.3 Monero (XMR)

V pořadí 3. kryptoměnou v této kapitole je Monero. Jeho dřívější název byl BitMonero, ale v krátké době po startu byl zkrácen do nynější podoby. Měna vznikla nedlouho po vzniku Dashe v roce 2014 odvozením od původního Bitcoinu, i když v dnešní době s ním má málo společného. Tak jako Dash i Monero přináší na pole kryptoměn spoustu

novinek a nejhlavnější z nich je úplná finanční anonymita. [6, 20]

Vývojářům Monera se podařil husarský kousek, jelikož dokázali vytvořit blockchain Monera zcela anonymní. Díky této absolutní anonymitě dosáhlo Monero i dalšího významného milníku, a to úplné zaměnitelnosti mincí jako je tomu u běžných fiat peněz. Jelikož u běžných kryptoměn můžeme vypátrat historii mincí a možné propojení s nelegální činností, může zde nastat zmrazení účtu s takovými mincemi. Toto se však u Monera stát nemůže. Pokud je však vše anonymní, může zde lehce dojít právě k nelegální činnosti. I na toto vývojáři mysleli, a tak se krom klasického soukromého a veřejného klíče zavádějí ještě 2 další klíče tzv. klíče k prohlížení. Tyto klíče slouží třetí osobě k nahlížení do stavu účtu či k historii transakcí. Tímto způsobem se dá zajistit transparentnost účtu a pohybů na něm. [6, 20]

Oproti měnám jako BTC či LTC, které mají pevně daný počet mincí, je Monero nekonečně inflační s inflací postupně klesající k nule. Do roku 2022 mají vývojáři v plánu vypustit do oběhu něco okolo 18 milionů mincí, kdy po roce 2022 začne fáze postupně se snižující inflace menší než 1 % ročně. Výhodou tohoto řešení je, že se nemusíme bát, že by po vytěžení poslední mince síť přišla o těžaře, kteří ztratí motivaci zůstávat aktivní a síť by se tak stala náchylnější k útokům. Další nespornou výhodou Monera je pevně daná míra emitování nových mincí, která může vyrovnávat poklesy stavu oběživa z důvodu ztrát mincí. [6, 20]

Oproti Bitcoinu je Monero také snáze dělitelné díky 12 dekadickým řádům (Bitcoin jich má 8). Jejich názvy vycházejí z jednotek SI, a tak se nejmenší jednotka nazývá piconero a největší meganero. [2]

Jak bylo řečeno u Bitcoinu, problém dnešní doby je jeho malá velikost bloku, a to 1 MB. U Monera tento problém byl vyřešen adaptabilní velikostí bloku, která se počítá z aktuální vytíženosti sítě a tím se mění i velikost poplatku za transakci.

Problém těžby pomocí ASIC čipů trápí nejednu kryptoměnu. Monero se však rozhodlo s těmito těžaři bojovat, aby zajistilo decentralizaci těžby a férové podmínky pro všechny těžaře. Aby bylo zamezeno použití ASIC čipů, rozhodli se vývojáři pro razantní krok a každého půl roku tak dochází k forkování kryptoměny a změně těžebního algoritmu. Tento krok, jak se vývojáři i komunita domnívá, odradí výrobce ASIC těžebních přístrojů od tvorby zařízení specializujících se na Monero a těžba tak zůstane v oblasti CPU a GPU těžby. [6, 20]

Malou vadou na kráse Monera je fakt, že díky anonymizačním nástrojům je velmi pracné vytvářet pro Monero peněženkový software a nejjednodušší způsob, jak nyní mince uchovávat je vytvořit si papírovou peněženku nebo vlastní uzel (node), na kterém budou mince uchovány. Světlejší zítřky však slibuje komunita, podle které by do roku 2020 měla být na trhu funkční hardwarová peněženka, obdobná českému Trezoru.

3.2.4 Vertcoin (VTC)

Závěrečnou měnou v této kapitole je měna s názvem Vertcoin. Vznikla v roce 2014 a obdobně jako Monero se snaží být měnou pro obyčejné lidi. Vertcoin nebyl oproti ostatním kryptoměnám zde zmíněných odvozen od jiné kryptoměny, ale vývojáři si dali tu práci a vytvořili si svůj vlastní blockchain. [6]

Velkou předností Vertcoinu jsou jeho nízké transakční poplatky, obrovská uživatelská přívětivost, a tak jako u Monera nemožnost měnu těžit pomocí ASIC zařízení. Jádro kryptoměny tvoří hlavně dobrovolníci a veškeré financování probíhá pomocí veřejných sbírek a darů. Zajímavou implementací Vertcoinu je i ošetření možnosti těžby pomocí botnetů. Aby bylo možné zamezit této těžbě, je u Vertcoinu zakázána těžba pomocí CPU. Někteří těžaři s takovýmto přístupem nebudou souhlasit, ale je to jednoduchý způsob, jak docílit férového boje. [6]

Počet mincí je zde omezen na 84 milionů s intervalem těžení zhruba 2,5 minuty na blok. Nemožnost těžby pomocí ASIC zařízení garantuje možnost ještě stále těžit pomocí vašeho domácího zařízení a technologie One-Click-Miner. Tato technologie vyvinutá právě pro Vertcoin se snaží uživateli zjednodušit těžbu tak, aby jí byl schopný i naprostý laik a měna tak byla dostupná opravdu pro každého. [6]

Dnes je vytěžena zhruba polovina mincí s aktuální cenou okolo poloviny amerického dolaru, další nespornou výhodou je podpora všech počítačových platforem (Windows, Mac, Linux) a podpora softwarových a v brzké době i hardwarových peněženek. [13] Podle mého názoru se jedná o jednu z nejčistších forem kryptoměny, s jakou se dnes můžeme setkat.

3.3 Neperspektivní kryptoměny

Ne všechny kryptoměny, které se tváří jako úžasná investiční příležitost se tak skutečně chovají. Mnoho rádoby kryptoměn se snaží jen potencionální investory „oškubat“ a místo měny budoucnosti jim jen „věší bulíky na nos“. Kapitola neperspektivních kryptoměn se bude takovými měnami zabývat.

3.3.1 OneCoin (ONE)

Krásným příkladem je OneCoin, se kterým měl autor tu smůlu přijít do styku. Jde o klasické pyramidové uspořádání, kde nezískáme vůbec nic a vyhodíme tak jen peníze. Společnost vznikla v Bulharsku a rychle se rozšířila po Evropě. Tato doslova imaginární měna se nikde neobchoduje, její kurz není odvozen podle nabídky a poptávky, ale společnost si ho sama vymýšlí, a i když tvrdí jak sofistikovaný systém a blockchain má, není to pravda, jelikož blockchain nikdy neměla a podvodným způsobem tak od lidí získává peníze.

Pokud se vám podařilo přijít s OneCoinem do styku, přišli jste o své peníze a koupili jste si jen zbytečně předražený výukový balíček. Jak se vyskytuje u kryptoměny slovo balíček, nejedná se o slušnou kryptoměnu, ale jen o podvod, kde na potencionální uživatele nečeká zhola nic.

3.3.2 Tether (USDT)

Zajímavou kryptoměnou je bezesporu Tether založený v roce 2012 společností Tether Limited. A zde je hned první kámen úrazu, jelikož je mince centralizována právě okolo firmy Tether Limited, což porušuje základní myšlenku decentralizovanosti kryptoměn. Přejdeme-li však tento fakt, máme zde měnu, která se od všech ostatních odlišuje. Tether je totiž jako jediný z výše zmíněných měn považován za stable coin. Doslovný překlad by zněl stabilní mince, což není daleko od pravdy, poněvadž se Tether řadí k nejstabilnějším kryptoměnám současnosti. V našem případě má toto dvouslovné spojení význam krytí fiat měnou. [6, 13]

Tether je už od svého založení krytý pomocí amerického dolaru. Později se přidalo i euro a japonský jen. Právě díky tomu, že je každá mince kryta skutečnou bankovkou uloženou ve firemním fondu, dává měně její stabilitu a cenu kolísající okolo jednoho dolaru. Transparentnost celého procesu se snaží firma dokládat pomocí výpisů z bankovních účtů dokládajících skutečný soulad mezi stavy měn. [6, 13]

Jak už bylo řečeno, celá měna je centralizována okolo Tether Limited a vývoj kupředu bude jen pomalý. Zároveň je měna málo uplatnitelná, jelikož o ni nejeví mnoho obchodníků zájem, a tak jej můžeme uplatnit pouze na internetu nebo jako prostředek pro další obchodování na burze.

3.3.3 XRP (XRP)

Kapitolu uzavřeme posledním zástupcem a tím je XRP dříve též známý pod názvem Ripple. Hned v úvodu si musíme říci, že XRP není typickou kryptoměnou, jaké známe z předchozích stránek. [2]

Ripple totiž nemá blockchain. Nejsou zde vytvářeny žádné bloky, nýbrž tzv. Ledger neboli účetní kniha. Ledger obsahuje veškeré informace o Ripple účtech a o počtu mincí na nich a k jeho aktualizaci dochází průměrně jednou za 5 sekund. Ledgerů může být nekonečně mnoho, je však potřeba, aby se na jeho finální podobě shodlo minimálně 80 % všech uzlů, což nás přivádí k další odlišnosti tohoto systému, a to je Proof-of-correctness. [2, 6]

Tento způsob ověřování transakcí se liší tím, že transakce zde potvrzují důvěryhodné uzly. Aby se mohl uživatel takovým ověřovatelem stát, musí podat žádost a ostatní ověřovatelé ho musí mezi sebe přijmout. [2]

Poslední abnormalitou oproti ostatním kryptoměnám je absence pobídky či motivace pro těžaře. Zatímco Bitcoin a další měny pobízí těžaře k těžení formou odměn jako jsou například transakční poplatky, u XRP se tomu tak neděje. Transakční poplatek zde sice je, ale nikomu se nepřiděluje, nýbrž je spálen a toto malé množství měny již nebude nikdy použito. Provozování uzlu je tak čistě dobrovolná věc, motivací pro některé uživatele může být možnost navrhovat změny v systému. [2, 6]

Dále se zaměříme na problémy, které tato síť má. První problém, který některým vadí, je centralizace okolo firmy Ripple Labs. Došlo tak sice k vysoké rychlosti transakcí (cca 1500 za vteřinu), je to ale na úkor dohledu nad naším účtem a možnosti účet zmrazit. Do oběhu by mělo být vypuštěno 110 miliard jednotek XRP, přičemž valnou většinu nyní vypuštěných mincí vlastní zaměstnanci firmy a její majitelé. [2, 6]

Jaký je tedy význam této kryptoměny? Budoucnost, které by chtěli vývojáři dosáhnout, se točí okolo systému RippleNet. Vize zakladatelů je totiž vytvořit systém, který by mohly používat banky k urychlení převodů peněz po světě, což by zároveň vedlo ke snížení nákladů bank. Token ve formě XRP, který byl k tomuto systému vytvořen, je tak spíše takovým bonusem a vedlejším produktem, který by v budoucnu (pokud tedy banky skutečně začnou protokol firmy Ripple používat) mohl fungovat jako platidlo pro mezibankovní transakce a jeho cena by mohla růst.

3.4 Další kryptoplatformy

Kryptoměna, to není vždy jen alternativa dnešním bankovkám, ale najdeme zde i spoustu zajímavých projektů zakládajících se právě na pilířích moderních kryptoměn jako je blockchain, decentralizovaná síť a dalších. Těmto zajímavým projektům bude věnováno také pár řádků a v rychlosti budou představeny jejich hlavní přednosti.

3.4.1 Ethereum (ETH)

O projektu jménem Ethereum slyšel snad každý. V roce 2013 jej představil programátor Vitalik Buterin a pro všechny pohybující se ve světě počítačů a kryptoměn to byla naprostá senzace. Jak píše server Kryptomagazin [6]: *„Dr. Gavin Wood, přední vývojář Etherea, na jedné ze svých přednášek řekl, že když postavili základní verzi Etherea, tak najednou vyvstala otázka, co to vlastně postavili a co všechno to bude umět.“* Je vidět že ani sami vývojáři pořádně nevěděli, co vlastně stvořili. Dnes už můžeme 100% říci, že se jim podařilo vytvořit virtuální počítač. Decentralizovaný výpočetní stroj pro obecné výpočty.

Jeho rychlost není díky decentralizovanosti nijak závratná, ale to je daň za vysokou míru zabezpečení výpočtů. Oproti tomu jsou tu ale výhody jako nemožnost zaseknutí, vypnutí, cenzury a dostupnost po celém světě (nebo alespoň tam kde je internet). [6, 21]

Výchozím programovacím jazykem je Solidity, který je turingovsky ekvivalentní[7]. Aplikace napsané pro Ethereum běží nad jeho blockchainem, který jim slouží jako uložiště dat a kódu programu. Všechny tyto vlastnosti pak umožňují tvorbu tzv. smart kontraktů, jež jsou jednou z hlavních předností Etherea. [2]

Smart kontrakt vzniká mezi 2 a více stranami a jde o automatizovaný kód, který se dá upravit dle potřeb obou stran. Díky open-source technologii se nekladou meze modulovatelnosti kontraktů a jelikož se kontrakty ukládají do blockchainu je zde zaručena transparentnost operací. Abychom však lépe pochopili použití v praxi, uveďme zde velmi pěkný příklad ze serveru Kryptomagazin [6]: *„Představte si, že chcete prodat auto. Už nebudete muset sepisovat složitě smlouvy, ale budete moci využít vytvořený smart kontrakt, nastavit cenu automobilu a ve chvíli, kdy na adresu smart kontraktu jiný uživatel nahraje požadovaný počet Etheru, tak se kontrakt automaticky provede a na Ethereum blockchain se zapíše, že již auto patří novému majiteli a vám připadá požadovaná částka Etheru.“*

Nyní se dostáváme k samotné měně, kterou Ethereum využívá. Její jméno je Ether a dělí se na 11 řádů. Zajímavostí je jejich pojmenování po známých osobnostech ze světa kryptoměn a vědních oborů. Microether se tak jmenuje po Nicku Szabo, kiloether po Albertu Einsteinovi atd. Ethery můžeme využít dvojím způsobem. Buďto s nimi můžeme platit těžařům za provoz naší aplikace běžící cloudově na síti nebo je můžeme utratit za zboží a služby. Měna je nekonečně inflační a funguje na bázi PoW, kterou chce do budoucna zkombinovat i s PoS pomocí algoritmu Casper. [2, 6]

Zbývá už jen osvětlit poslední pojmy ze světa Etherea a to jsou ICO (Initial Coin Offering) a ERC20 tokeny. První si vysvětleme pojem ERC20 token. Ethereum totiž nabízí možnost vytvořit na svém blockchainu tokeny chováním velmi podobné měně Ether. Vytvořením tohoto standardu odstartovalo ICO šílenství. ICO staví právě na standardu ERC20. Spousta start-upů začala tvořit své vlastní tokeny (mince chcete-li) a začala je nabízet veřejnosti za Ether. To vedlo k usnadnění zisku financí pro nastartování projektů a v některých případech i k vysokým ziskům na straně uživatelů nakoupených tokenů. [21]

Jako příklad můžeme uvést EOS, který také začínal jako ERC20 token a do dnešního dne narostl do takové velikosti, že přechází na vlastní blockchain. [13]

Shrnutí by bylo tedy následující, Ethereum přináší do (nejen) počítačového světa spoustu nových poznatků a jde bezesporu o zajímavý projekt, který stojí za povšimnutí. Možnosti platit Etherem nejen za provoz cloudových aplikací by mohla měnu

[7] Tuto vlastnost má stroj, počítač, programovací jazyk, který má stejnou výpočetní sílu jako Turingův stroj. To značí, že stroj je natolik univerzální, jak je jen možné. V našem případě programovací jazyk má tedy stejné možnosti v programování, jako u běžně používaných programovacích jazyků jako je Java, C, C++ apod.

Ether řadit do perspektivních kryptoměn a s tímto názorem nelze nesouhlasit. Nicméně Ethereum autora zaujalo hlavně po stránce právě onoho virtuálního počítače, a proto se řadí právě až do dalších kryptoplatforem.

3.4.2 NEO (NEO)

Obdobnou platformou pro Ethereum je i čínská platforma NEO, která je ve světě kryptoměn nazývána čínské Ethereum právě díky použití smart kontraktů. Krom smart kontraktů platforma přináší i další funkce a to [6]:

- NeoX – systém propojující různé blockchainy
- NeoFS – služba pro decentralizované skladování dat (podobný systém jako peer-to-peer Dropbox)
- NeoQS – kryptografický mechanizmus tvořící umělou překážku pro kvantové počítače, které by mohly svět kryptoměn ohrozit

Platforma NEO tak v sobě ukrývá celý ekosystém funkcí. V ekosystému figurují krom běžných uživatelů také účetní. Při tvorbě bloku se na jeho podobě musí shodnout 2/3 účetních uzlů, pokud se tak stane, vybere se účetní uzel, který blok vytvoří, a následně se nemůže podílet na hlasovaní o příštím bloku. Toto řešení by podle tvůrců mělo urychlit zpracování transakcí až na 1000 transakcí za sekundu a v budoucnu by mohlo vyrůst až na 10 000 transakcí za sekundu. [6]

NEO také obsahuje tokeny jménem GAS, tyto tokeny dostává pravidelně na svůj účet každý majitel mincí a bylo by možné obnos tokenů chápat jako dividendu za držení měny. Není tomu však úplně tak. Tokeny se používají k platbám poplatků za použití smart kontraktů a automaticky se přičítají na účet účetního uzlu. Pokud tedy provozujeme účetní uzel, získáváme tak i pasivní příjem v podobě tokenů GAS. [6]

Jako každá kryptoměna i NEO se snaží do světa kryptoměn přinést inovace, jak samotný název může napovídat (z řečtiny nový, mladý). Otázkou bude, jestli se tento systém uchytí a jak se bude jeho ekosystém vyvíjet dále.

4 Porovnání těžby

Abychom měli přehled o tom, které měny je pro nás výhodné těžit, představíme si v této kapitole shrnutí všech pro a proti těžby výše zmíněných měn. Jak již bylo zmíněno u těžby, abychom mohli jednotlivé měny těžit, potřebujeme těžební software. Pro každou měnu používáme jiný software, pokud se tedy nerozhodneme pro Merged Mining[8)]. Do výčtu měn nebudou zahrnuty pouze neperspektivní měny.

Pokud bychom se rozhodli pro těžbu, musíme zvážit jednotlivé aspekty těžby. Do valné většiny zmíněných měn se již propracovala technika těžby pomocí ASIC čipů, což ztěžuje vstup na pole těžby ať už vysokými pořizovacími náklady ASIC hardwaru, nebo samotnou vysokou spotřebou elektrické energie těžebních stanic.

Pokud bychom se rozhodli nepořizovat si speciální těžební hardware a chtěli bychom těžit na domácím zařízení nebo pomocí externích grafických karet, budeme muset sáhnout po měnách, do kterých se ASIC ještě neprobojoval anebo má jen velmi malé zastoupení.

Pro usnadnění porovnání těžby a návratnosti vložených investic bude použita webová kalkulačka na serveru Cryptocompare. Tento jednoduchý nástroj nabízí po zadání výpočetních parametrů stanice snadnou kalkulaci výnosů a ztrát od denních až po roční. Jelikož kalkulačka nenabízí českou mutaci a výsledná čísla jsou v dolarech, je zde použit aktuální kurs 22,94 Kč. Zároveň je použita průměrná cena elektřiny na rok 2019, která činí 4,28 Kč, kdy po přepočtu na dolar a zaokrouhlení na 2 desetinná místa dojdeme k výsledku 0,19 $/KWh.

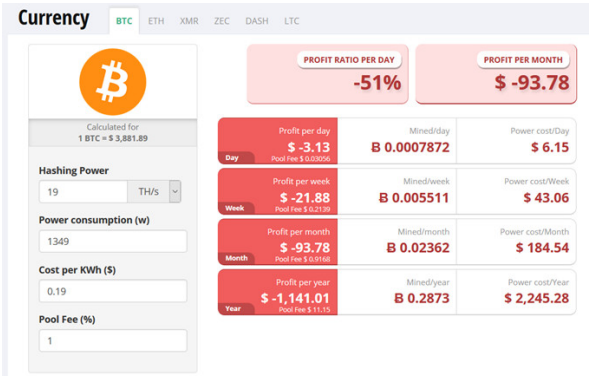
4.1 Bitcoin a Bitcoin cash

Tyto dvě měny můžeme z pohledu porovnání těžby sloučit do jedné kategorie, jelikož obě mají podobnou obtížnost. Hned na začátku musíme vyloučit možnost těžby na GPU. U Bitcoinu si už s grafickými kartami „neškrtneme“ a pokud se rozhodneme těžit, budeme si muset pořídit ASIC hardware.

Jeden z velkých prodejců zařízení uzpůsobených pro těžbu Bitcoinu je společnost Bitmain se svými produkty řady AntMiner. Na trhu existuje i řada dalších výrobců, jako například Baikal nebo DragonMint. Všechna zařízení nabízejí více či méně stejný výkon a prodejci je nabízejí za podobné ceny. Při výběru bychom se měli zaměřit na výkon, spotřebu elektrické energie a cenu zařízení. Ceny přístrojů začínají na 7 000 Kč, ale mohou se vyšplhat až ke 20 000 Kč.

[8)] Jde o techniku těžby, kdy těžíme 2 měny (blockchainy chcete-li) zároveň. Primárně těžený blockchain obsahuje kód i sekundárního blockchainu a při vytěžení primárního bloku je to dostatečný důkaz o vynaložené práci i pro blockchain sekundární. Tuto techniku musí podporovat pouze sekundární blockchain. [2]

Pro ilustraci použijm zařízení AntMiner s výkonem 11-19 TH/s v ceně zhruba 500 dolarů. Jednotka TH/s nám vyjadřuje rychlost řešení jednotlivých hash hodnot, jeden TH/s tedy vyjadřuje 1 bilion hash hodnot za sekundu. Po zadání všech hodnot do kalkulačky nám vyjde zajímavý výsledek, a to že prodělláváme.



Obr. 4.1 Kalkulace těžby BTC [32]

I když se nám podaří za rok vytěžit Bitcoin v hodnotě okolo 1 115 dolarů, naše náklady jsou dvojnásobně vyšší a tratíme přes 50 %. Naši situaci nezlepší ani nákup dalšího stroje, neboť úměrně s výkonem nám poroste i spotřeba elektrické energie. Řešením by bylo najít si v dražbě elektrické energie lepšího dodavatele, nebo použít alternativní zdroj energie, jakou jsou solární panely či větrná elektrárna, pak bychom se mohli dostat ze ztráty, ale pořizovací náklady oněch alternativních zdrojů také nejsou malé. Otázkou také je, zda by byly výnosy dostatečně velké na to, aby nám dokázaly vrátit investice vložené do nákupu těchto zařízení.

V případě druhé odnože BCH dojdeme k velmi podobnému výsledku, který se od BTC liší jen v desetinách. Závěr tedy zní BTC i BCH jsou pro obyčejného těžaře již nedostupné. Velkou zásluhu na tom mají hlavně enormní kryptoměnové doly v Číně, které produkují každý okolo 1-3 % výkonu celé sítě.

4.2 Litecoin a Dash

Další porovnávanou dvojicí je Litecoin a Dash. Tak jako u BTC a BCH je i zde nejvýhodnější těžit pomocí ASIC zařízení, jelikož jejich podíl na těžbě je již tak vysoký, že těžba pomocí CPU a GPU je nerentabilní.

Kdybychom se rozhodli těžit Litecoin, máme na výběr z několika zařízení. Litecoin používá jednoduchý algoritmus scrypt a tím bychom se měli také řídit při výběru zařízení. Asi nejrozšířenějším zařízením na tomto poli je AntMiner L3+. Jeho cena se pohybuje okolo 8 000 Kč a s parametry 600 MH/s a příkonem 850 W jde pro začátek o rozumný přístroj.

Dalším velmi oblíbeným zařízením s poněkud vyšší cenovkou okolo 20 000 Kč Innosilicon A4+ LTCMaster. Vyšší pořizovací náklady mohou od nákupu odradit, po technické stránce je však přístroj se svými parametry 620 MH/s a příkonem 750 W výhodnější koupí.

Jak je to však s renatabilitou těžby? Opět jsme se dostali do konfliktu s cenou elektřiny v České republice. Abychom totiž dokázali na těžbě vydělávat, museli bychom srazit cenu elektřiny na necelých 2,5 Kč, což jsou dvě třetiny dnešní ceny.

Druhý v pořadí je Dash s hashovacím algoritmem X11. Opět se zde setkáváme se zařízeními řady AntMiner, Innosilicon a nově také se známými zařízeními Baikal. Z řady AntMiner bychom nyní volili typ D3 s výkonem 19,3 GH/s, příkonem 1200 W a cenou pohybující se okolo 10 000 Kč. Zástupce od společnosti Innosilicon s označením A5+ se pyšní takřka desetkrát vyšší cenovkou a výkonem 60 GH/s za požadovaného příkonu 1500 W. Za stejnou cenu si můžete také pořídit Baikal Giant X5, ten však nabízí jen 10 GH/s při 800 W.

Absolutní špičkou je zde ale Spondoolies Tech SPx36. Disponuje výkonem neuvěřitelných 540 GH/s s příkonem 4 400 W. Daní za jeho vysoký výpočetní výkon je doslova astronomická pořizovací cena 300 000 Kč.

Když porovnáme výsledky z kalkulačky, vidíme postupný trend snižování ztráty. Nyní se pohybujeme jen v řádech několika procent a těžba by se nám mohla po malých částkách vracet. Samozřejmostí je, že nejvyšší výdělek by nám přineslo zařízení od Spondoolies (i za stávajících cen elektřiny bychom ročně vydělali přes 20 000 Kč), ale jeho pořizovací náklady jsou tak vysoké, že investovat do koupi tohoto zařízení by bylo velice riskantní.

4.3 Monero a Vertcoin

Nyní se dostáváme asi k té nejzajímavější části. Monero i Vertcoin totiž zatím nelze těžit pomocí ASIC zařízení. I když kolovaly éterem zprávy o tom, že Monero bylo pokořeno a výrobci přišli na řešení, jak jej těžit pomocí ASICů, nic z toho nebylo potvrzeno a Monero tak stále zůstává těžitelné pouze za pomoci GPU či CPU.

Díky této možnosti můžeme provozovat těžbu v podstatě na domácím počítači. Abychom si vybrali správné těžební náčiní, je dobré využít benchmarků provedených na jednotlivých CPU a GPU. Těchto testů naleznete na internetu opravdu mnoho a po bedlivějším prostudování lze vybrat nejvhodnější grafickou kartu či procesor.

Kvůli nižší ceně mince nemůžeme očekávat astronomické výdělky. Kupříkladu pokud bychom se rozhodli těžit pomocí CPU a využili procesoru INTEL CORE I7-4980HQ 2.8 GHZ, vydělali bychom okolo 120 Kč. Částka je to sice malá, ale jako důkaz možnosti využití domácího počítače postačující.

Právě zmíněná těžba přes CPU je i kámen úrazu Monera. U Monera se totiž rozmohl nešvar zneužívání těžby pomocí CPU nic netušících uživatelů internetu. Za využití Botnetu[9)] se útočníci nabourávají do počítačů obyčejných lidí a využívají jejich výpočetní výkon k těžbě ať už Monera nebo i další kryptoměn. Podobný způsob je praktikován i na některých webových stránkách, které potajmu využívají výkon návštěvníkova počítače, zatímco si prohlíží obsah stránky. Na druhou stranu se můžeme setkat i se stránkami, které této techniky využívají, ale vždy se návštěvníka zeptají, zda mohou jeho sestavy k tomuto účelu využít. Jaký je tedy závěr u Monera? Těžit se dá, dá se na něm i profitovat, ale výdělky budou spíše symbolické.

Aby u Vertcoinu nedošlo ke stejné situaci jako u Monera, rozhodli se vývojáři omezit možnost těžby pouze na GPU. Tento impuls nám tak dává velkou naději vytěžit ze svého počítače více než u Monera.

Další nespornou výhodou, která byla představena už při popisu měny, je one-click-miner, který velmi usnadňuje těžbu i pro úplného laika. Zde však veškeré výhody končí. Uveďme si příklad, pokud se rozhodneme těžit na grafické kartě Nvidia GeForce GTX 1050ti, která stojí 5 000 Kč, po po prvním roce jsme ve ztrátě stejně velké, jako je pořizovací cena grafické karty. Vše je opět způsobeno cenou elektrické energie, která znemožňuje na těžbě profitovat.

4.4 Ethereum

Posledních několik řádků této kapitoly bude věnováno Ethereu. Jeho potenciál je vysoký a v budoucnu by se mohlo vyplatit vlastnit alespoň pár mincí této platformy. Pokud bychom se rozhodli investovat do grafické karty částku do 20 000 Kč, pak je podle nezávislých výkonnostních testů nejlepším řešením grafická karta Nvidia GeForce GTX1080Ti 11 GB s výkonem 31,3 MH/s a spotřebou okolo 350 W.

Levnější variantou jsou grafické karty od společnosti AMD. Karty nabízí obdobný výkon s polovičními pořizovacími náklady. Kupříkladu grafická karta AMD Radeon R9 390 disponuje výkonem 28,5 MH/s, spotřebou 275 W a pořizovacími náklady něco přes 10 000 Kč. Nicméně v obou variantách opět prodělváme.

Asi 9 měsíců nazpět se objevila nová ASIC zařízení AntMiner E3 a Innosilicon A10 ETHMaster vhodná pro těžbu Etherea. Může se to jevit jako špatná zpráva pro všechny malé těžaře, předběžné odhady však hovoří o tom, že na síť by tento vpád neměl mít vliv větší než 3 %, což by běžný těžař neměl ani pocítit. Otázka je, zda jsou tyto odhady správné a výsledky ukáže až čas. Jak AntMiner, tak Innosilicon jsou zde výrazně kratší dobu než například u BTC, a tak ještě nemůžeme říci, zda byla síť nástupem ASIC zařízení výrazněji ovlivněna.

[9)] Síť počítačů infikovaných malwarem řízeným útočníkem z jednoho místa.

Zároveň zařízení Innosilicon A10 ETHMaster s výkonem 480 GH/s a spotřebou jen 800 W by nám dokázalo i přes vyšší pořizovací náklady činící přes 100 000 Kč vydělat slušnou částku a vrátit nám naši investici do doby okolo 4,5 roku.

4.5 Tabulkové porovnání

Pro lepší orientaci ve výše uvedených možnostech těžby naleznete v příloze tabulkové porovnání obsahující veškeré relevantní informace. Tabulka je doplněna i o zařízení, která nebyla zmíněna v textu a rozšiřují portfolio výběru.

5 Platby u obchodníků

K čemu by byly kryptoměny, kdyby se jimi nedalo platit. Obyčejné bankovky můžeme v případě nouze použít jako obyčejný papír, ale kryptoměny, které jsou uloženy jako soubor čísel a znaků jen těžko zužitkujeme podobným způsobem.

5.1 Bitcoin

Co se týče možnosti využití kryptoměny při platbách ať už v obchodech nebo na internetu, suverénně dominuje tomuto odvětví, jak asi všichni očekávají, Bitcoin. I přes jeho vysokou cenu ho přijímá nejvíce obchodníků na světě.

Chceme-li zjistit, zda obchodníci v našem okolí přijímají Bitcoin, jednoduše stačí najít naši polohu na webu coinmap.org, kde uvidíme obchody okolo nás a jejich zaměření. Obchodů je vážně mnoho a kompletní seznam zatím neexistuje. Odhady mluví o číslech převyšujících 6000 obchodníků. Vypisovat je zde všechny by zabralo více času a stránek, než se autorovi dostává, a proto budou zmíněny jen ty nejzajímavější.

Některé to možná překvapí, ale už i automobilky přijímají Bitcoiny a nejedná se o žádná neznámá jména, ale o koncerny jako BMW či Tesla. K přijímání kryptoměn se staví banky většinou negativně, objevily se ale i první vlaštovky v oblasti bankovnictví, co přijímají Bitcoiny. Jsou to Royal Bank of Canada, německá Fidor Bank nebo WorldCore s kořeny v České republice. Mezi další známá jména patří:

- Subway
- Domino's Pizza
- Burger King
- LOT Polish Airlines
- Microsoft
- PayPal
- eGifter
- Old Fitzroy, Sydney
- Coca-Cola automaty
- BTCTrip
- ExpressVPN
- Reddit
- Badoo.com
- Playboy
- Xbox
- PlayStation
- Overstock

Seznam by tímto způsobem mohl pokračovat dál a dál. Možnosti jsou takřka neomezené, jelikož se obchodníci řadí snad do všech kategorií od webového hostingu přes nábytek, casina, rychlá občerstvení, hotelové služby, až po univerzity. [22]

Aby toho nebylo málo, seznam se stále rozrůstá a v roce 2019 by jej měli doplnit giganti jako McDonald's, Google, Amazon, Starbucks a mnozí další. Proč bychom však měli zůstávat jen u obchodníků? Na masové přijímání Bitcoinu se chystají celé země. Japonsko, Kanada, USA a i celá Evropa pracuje na zákonech začleňujcích kryptoměny do finančních sektorů. Následující roky by tak mohly pro Bitcoin znamenat velký krok vpřed v oblasti využitelnosti. [22]

5.2 Bitcoin cash a Litecoin

Když dva dělají totéž, není to totéž. To by se dalo říci i o BTC a BCH. Bitcoin cash totiž oproti svému předchůdci není na poli obchodníků tak rozšířený. K dnešnímu dni ho akceptuje do 1 000 obchodníků. Největší společností je zde Microsoft, následován webovou encyklopedií Wikipedia, dále Amazon a Overstock. Tím však známá jména končí a na scénu přicházejí menší obchodníci.

Návštěvníci nebo obyvatelé Evropy určitě ocení možnost platit pomocí BCH u řetězce s rychlým občerstvením Takeaway disponující 31 000 pobočkami. Doufejme, že postupem času počet obchodníků poroste a uživatelé tak budou mít větší šanci využít svých ať už naspořených nebo vytěžených mincí.

Velmi podobně je na tom i Litecoin. Obchodů není mnoho, jejich zaměření je však široké. Tak jako u BTC, i zde se objevuje cestovní kancelář BTCTrip nebo společnost Overstock. Užitečným nástrojem pro zjištění, co si za své mince můžeme koupit, je web uselitecoin.info, který nabízí třídění podle jednotlivých kategorií a nabízí i krátký popis s možností prokliku do obchodu. Těžaře určitě zaujme možnost nakupovat těžební hardware od firmy KnCMiner a dále tak rozšiřovat své těžební impérium. Velmi diskutovaným je i kalifornský automobilový dealer Benz and Beamer nabízející automobily luxusních značek.

Vývojáři vědomi si malého zastoupení na trhu se proto rozhodli spojit se se společností SPEND. Ta poskytuje svým uživatelům debetní karty, pomocí kterých je možné platit v kterémkoli obchodě přijímající karty Visa. Otevírá se tak brána ke vstupu na téměř jakýkoliv trh, jelikož karty Visa podporuje ohromných 40 milionů obchodníků.

5.3 Dogecoin a Dash

Dogecoin nemá moc velké zastoupení na poli obchodů a varianty, jak ho utratit jsou dosti omezené. Pro příklad jídlo a pití si můžeme celosvětově pořídit jen v 6 kavárnách, což je malé číslo, i kdyby šlo jen o jeden stát či město. V dalších oblastech Dogecoin také pokulhává. Některé potěší možnost zaplatit si pomocí Dogecoinů cestu po Milánu ve stylovém cyklotaxi. Dále však Dogecoin zatím nešel a stále tak jde spíše o recesi a příklad toho, že aktivní kryptoměnu si dnes může založit úplně každý zručnější člověk.

Pomineme-li Dogecoin a přesuneme se k měně Dash máme na výběr z více než 4 900 obchodníků. I Dash nám nabídne vlastní webovou stránku discoverdash.com, kde můžeme jednotlivé obchodníky procházet podle kategorií. Velmi užitečnou funkcí je i rozdělení podle zemí, takže nemusíme hledat odkud daný obchod pochází, ale jednoduše si zvolíme například Českou republiku a web nám vypíše veškeré prodejce akceptující Dash.

Kdybychom se zaměřili na největší firmy akceptující Dash, opět se nám jako první na seznamu objeví Overstock. Pomocí BitCart můžeme také nakupovat na Amazonu, a to s 15% slevou. Rok 2017 byl pro Dash přelomový. Vývojáři totiž uzavřeli dohodu o zakomponování také jejich kryptoměny s provozovatelem Bitcoinových debetních karet. Výsledkem tohoto kontraktu bylo, že Dash je nyní akceptován kdekoliv, kde je možné platit kartou Visa, obdobně jako Litecoin. Kryptoměny se tak tímto způsobem dostávají více a více ke svému cíli stát se měnou každodenního života.

5.4 Monero a Vertcoin

Poslední dvojicí jsou měny, které k sobě mají velice blízko. Začněme Monerem, to nabízí přímo na svých oficiálních webových stránkách seznam služeb a obchodů, kde můžeme měnu uplatnit. Seznam není nejkratší, postrádá však větší jména nadnárodních společností. Větší expanze se zde tedy nekoná a pro Evropana se tak může zdát Monero téměř nevyužitelné, pomineme-li internetové obchody.

Nezoufejme však, neboť pomocí webu XMR.to můžeme naše mince snadno převést (za menší poplatek samozřejmě) na Bitcoiny a pole použitelnosti se tak mnohonásobně rozrůstá. Web slibuje rychlé a bezpečné platby, vystačíme si tak s připojením k internetu a mobilním telefonem. Nevýhodou Monera je jeho složitost, ta znatelně brzdí jeho rozmach.

Vertcoin je na tom se složitostí v podstatě nastejno. Zde se ale tvůrci rozhodli jít jinou cestou než všichni ostatní. Vertcoin podle všech dostupných informací není možné utratit u žádného obchodníka. Místo toho přišli vývojáři s nástrojem VertVerser. Tak jako XMR.to řeší převod Monera na Bitcoiny a následnou platbu, tak řeší VertVerser převod Vertcoinu na Bitcoin. Tvůrci si tak usnadnili vstup na trh a svezli se na vlně zájmu o Bitcoin, aniž by museli pracně hledat obchodníky, kteří by se rozhodli Vertcoin přijímat. Od tvůrců je to chytrý tah, jelikož trh je dnes takřka přesycen kryptoměnami a nutit obchodům další by se stěží setkalo s úspěchem.

5.5 Platforma SPEND

O platformě jsme mluvili v souvislosti s měnami Dash a Litecoin a nebylo by od věci o ní trochu pohovořit. Ve stručnosti se jedná o webovou peněženku a k ní náležící platební

kartu. SPEND funguje velmi podobně jako banka s tím rozdílem, že nám navíc dovoluje vlastnit 16 kryptoměn a převádět je mezi až 27 fiat měnami. [23]

Veškeré tyto operace jsou zpoplatněny malými poplatky v řádech desetin procenta, ale nejzajímavější na celém konceptu je karta. Jde totiž o Visa kartu a uživateli se tak otevírá v podstatě celý tržní svět. [23]

Díky podpoře všech známých kryptoměn od Bitcoinu, přes Ethereum, Litecoin až po XRP a podpoře 27 měn, které zahrnují i českou korunu, tak máme možnost svými vytěženými mincemi platit takřka za cokoliv a kdekoliv.

5.6 Kryptoměnové bankomaty

Už i v České republice jsou samozřejmostí bankomaty zaměřené přímo na kryptoměny. Dříve se tyto bankomaty zaměřovaly hlavně na Bitcoin, s rostoucí popularitou dalších kryptoměn se portfolio bankomatů stále rozrůstá, a tak můžeme vybírat z měn jako Dash, Litecoin, BCH nebo dokonce Ethereum. Kde se bankomaty nacházejí a jaké měny podporují můžeme nalézt na webu coinatmradar.com, kde můžeme filtrovat jednotlivé bankomaty i podle námi upřednostňované měny. Pokud bychom nahlédli do mapy, zjistíme, že v České republice se momentálně vyskytuje 63 bankomatů. Největší koncentrace se nachází v Praze, nalezneme zde nadpoloviční většinu. Zbytek republiky je vybaven bankomaty spíše poskrovnu.

ZÁVĚR

Cílem této bakalářské práce bylo představit problematiku spojenou s kryptoměnami, jejich pořízením, držením a útratou.

Teoretická část je zaměřena na obecné vysvětlení pojmu kryptoměna, její historii, principy fungování a ekonomickou stránku. Historie je věnována hlavním předchůdcům dnes známých kryptoměn a představuje principy, na kterých stavěly pozdější kryptoměny. V rámci principů fungování práce seznamuje čtenáře s technologií blockchain a pojmy souvisejícími s touto technologií. Ekonomická část je následně rozdělena do dvou celků z pohledu světa a České republiky. Nutno říci, že ani v jednom z obou případů nedochází k ucelenému řešení problematiky zařazení kryptoměn do finančních rámců, což v některých případech vede k zákazům užívání či držení kryptoměn na území některých států.

Dalším bodem je otázka těžby a směny. Zde se setkáváme s širokou škálou možností, jak kryptoměnu uchovávat a jakými nástroji kryptoměny těžit. Na tuto otázku neexistuje jednoznačná odpověď, nicméně v oblasti uchovávání kryptoměn i těžby se představují jasné trendy ve směru těžby pomocí ASIC hardwarových prvků a následném ukládání do hardwarových peněženek.

Kapitola si také všímá možnosti burzovních spekulací a směny mezi uživateli. Burzovní spekulace nabízí lepší kurzy, jsou však náročnější na orientaci a jsou koncipované spíše pro zkušené obchodníky, svědčí o tom i poměrně náročný vstup do tohoto odvětví. Proto je zde raději zvolena cesta směny mezi uživateli, či na k tomuto účelu provozovaných serverech.

V praktické části se poté autor zaměřuje již na konkrétní kryptoměny, jež pro něj byly z pohledu použitých technologií nebo rentability zajímavé. První kapitola se věnuje obecně známým kryptoměnám jako jsou například Bitcoin nebo Litecoin. Seznamuje čtenáře s jejich vývojem a nynějším stavem. Jsou zde rozebrány použité technologie a jejich přínosy v daném odvětví.

Další podkapitolou jsou perspektivní kryptoměny následovány podkapitolou neperspektivních kryptoměn. Z podkapitoly perspektivních kryptoměn by si zasloužily zmínit alespoň Monero nebo Vertcoin, jelikož se snaží kryptoměny zjednodušit a co nejvíce přiblížit obyčejnému smrtelníkovi. Naopak v neperspektivních kryptoměnách se objevují měny jako Tether či XRP vinou centralizovanosti dohledu nad celou sítí nebo rozdělováním velkého objemu mincí mezi činovníky společnosti.

Poslední podkapitolu tvoří další kryptoplatformy, jelikož kryptoměna není pouze o penězích. Typickým příkladem je projekt Ethereum, který posouvá technologie kryptoměn o krok dále a za jejich pomoci projektový tým vytvořil virtuální počítač. Mimo

jiné Ethereum skončilo i jako nejvýdělečnější platforma co se týče porovnání výnosů a vložených investic.

Předposlední kapitolou je porovnání náročnosti těžby. Návratnost vložených investic zde byla porovnávána v horizontu od jednoho dne do jednoho roku. Jak se však ukázalo, většina porovnávaných kryptoměn za dnešních cen elektřiny a náročnosti těžby není těžitelná se ziskem. Nejvyšších výdělků za dnešních cen elektřiny bylo dosaženo u Etherea, které dokázalo investice vložené do pořízení těžebního vybavení splatit během jednoho roku a následně vydělávalo poměrně slušné částky.

Závěrečná kapitola dotváří ucelený obraz o kryptoměnách a představuje jednotlivé možnosti jak a kde utrženou kryptoměnu utratit. Zlomovým momentem je zde možnost pořízení platebních karet Visa převádějících kryptoměny na běžné peníze, díky kterým se kryptoměnám otevírá v podstatě celý svět.

Jak již bylo řečeno v úvodu, tato práce je vhodná pro všechny, kteří by si rádi rozšířili znalosti na poli kryptoměn, mají v úmyslu si vyzkoušet těžbu nebo jen hledají pár informací z tohoto odvětví.

SEZNAM POUŽITÉ LITERATURY

[1] *Kryptoměny | KOMPLETNÍ průvodce investováním - Finex.cz. Finex.cz* [online]. Lázně Bělohrad: Finex.cz, 2018 [cit. 2018-12-02]. Dostupné z: `https://finex.cz/rubrika/kryptomeny/`

[2] *STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky.* 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN 978-802-7107-421.

[3] *NARAYANAN, Arvind. Bitcoin and cryptocurrency technologies: a comprehensive introduction.* Princeton: Princeton University Press, 2016. ISBN 978-069-1171-692.

[4] *Untraceable Electronic Cash. CHAUM, David, Amos FIAT a Moni NAOR. Advances in Cryptology - CRYPTO '88 Proceedings.* První. New York: Springer, 1990, s. 319-327. ISBN 978-0-387-97196-4.

[5] *DigiCash - An introduction to ecash. Internet Archive* [online]. San Francisco: Internet Archive, 2018 [cit. 2018-11-28]. Dostupné z: `https://web.archive.org/web/19970605025721/http://www.digicash.com:80/publish/ecash_intro/ecash_intro.html`

[6] *Bitcoin, Blockchain, zpravodajský portál o kryptoměnách* [online]. Praha: MEDIA BASE, 2018 [cit. 2019-01-11]. Dostupné z: `https://kryptomagazin.cz/`

[7] *Čím je kryta měna? - Česká národní banka. Česká národní banka* [online]. Praha: Česká národní banka, 2003-2018 [cit. 2018-12-15]. Dostupné z: `https://www.cnb.cz/cs/faq/cim_je_kryta_mena.html`

[8] *HEISSLER, Herbert. Ekonomie bitcoinu: analýza a modelování bitcoinu v rozvinutém stadiu.* Vydání první. Praha: Vysoká škola finanční a správní, 2014. Eupress. ISBN 978-80-7408-104-0.

[9] *Regulation of Cryptocurrency Around the World. The Library of Congress* [online]. Washington: The Library of Congress, 2018 [cit. 2018-12-21]. Dostupné z: `https://www.loc.gov/law/help/cryptocurrency/world-survey.php`

[10] *261/2014 Sb. Zákon, kterým se mění některé zákony v oblasti finančního trhu. Zákony pro lidi* [online]. Zlín: AION CS, s.r.o., c2010-2019 [cit. 2019-02-02]. Dostupné z: `https://www.zakonyprolidi.cz/cs/2014-261`

[11] *A List of Merchants Accepting Ethereum In 2019. CoinSutra - Bitcoin Community* [online]. CoinSutra - Bitcoin Community, c2017-2019 [cit. 2019-02-18]. Dostupné z: https://coinsutra.com/who-accepts-ethereum/

[12] *Who Accepts Bitcoins As Payment? List of Companies. 99 Bitcoins* [online]. 99 Coins ltd, 2018 [cit. 2019-02-18]. Dostupné z: https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/

[13] *Cryptocurrency Market Capitalizations | CoinMarketCap* [online]. USA: CoinMarketCap, 2019 [cit. 2019-01-11]. Dostupné z: coinmarketcap.com

[14] *Bitcoin vs. Bitcoin Cash. Jaký je mezi nimi rozdíl? | Alza.cz. Alza.cz* [online]. Praha: Alza a.s., c1994-2019 [cit. 2019-03-04]. Dostupné z: https://www.alza.cz/bitcoin-vs-bitcoin-cash

[15] *Litecoin - Open source P2P digitální měna* [online]. Litecoin Project, c2011-2019 [cit. 2019-03-04]. Dostupné z: https://litecoin.org/cs/

[16] *Litecoin (VŠE, CO CHCETE VĚDĚT) | Alza.cz. Alza.cz* [online]. Praha: Alza a.s., c1994-2019 [cit. 2019-03-04]. Dostupné z: https://www.alza.cz/litecoin

[17] *Dogecoin* [online]. USA: The Ðogecoin Project, b.r. [cit. 2019-03-18]. Dostupné z: https://dogecoin.com/

[18] *Homepage - Dash* [online]. Dash, 2019 [cit. 2019-03-06]. Dostupné z: https://www.dash.org/

[19] *Dash (VŠE, CO CHCETE VĚDĚT) | Alza.cz. Alza.cz* [online]. Praha: Alza a.s., c1994-2019 [cit. 2019-03-06]. Dostupné z: https://www.alza.cz/dash

[20] *Monero (VŠE, CO CHCETE VĚDĚT) | Alza.cz. Alza.cz* [online]. Praha: Alza a.s., c1994-2019 [cit. 2019-03-06]. Dostupné z: https://www.alza.cz/monero

[21] *Ethereum Project* [online]. Zug (Švýcarsko): Ethereum Foundation, 2019 [cit. 2019-03-18]. Dostupné z: ://www.ethereum.org/

[22] *250+ Places That Accept Bitcoin Payment (Online Physical Companies). ICOholder* [online]. ICOholder, 2019 [cit. 2019-03-18]. Dostupné z: https://icoholder.com/blog/places-accept-bitcoin/

[23] *Spend Wallet Spend Visa® Card - Spend.com* [online]. Spend, 2019 [cit. 2019-03-22]. Dostupné z: https://www.spend.com/

[24] *Legal Status of Cryptocurrencies - map1.pdf. The Library of Congress* [online]. Washington: The Library of Congress, 2018 [cit. 2018-12-21]. Dostupné z: https://www.loc.gov/law/help/cryptocurrency/map1.pdf

[25] *Regulatory Framework for Cryptocurrencies - map2.pdf. The Library of Congress* [online]. Washington: The Library of Congress, 2018 [cit. 2018-12-21]. Dostupné z: https://www.loc.gov/law/help/cryptocurrency/map2.pdf

[26] *Countries that Have or Are Issuing National or Regional Cryptocurrencies - map3.pdf. Library of Congress* [online]. Washington: The Library of Congress, 2018 [cit. 2018-12-21]. Dostupné z: https://www.loc.gov/law/help/cryptocurrency/map3.pdf

[27] *The Evolution of the Internet: Centralized, Decentralized and Distributed Networks – Digital Communications with Bill Greider. Digital Communications with Bill Greider* [online]. Digital Communications with Bill Greider, 2019 [cit. 2019-01-11]. Dostupné z: https://billgreider.blog/2016/10/19/the-evolution-of-the-internet-centralized-decentralized-and-distributed-networks/

[28] *TREZOR One White - Hardware peněženka | Alza.cz. Alza.cz* [online]. Praha: Alza.cz a.s, c1994-2019 [cit. 2019-01-24]. Dostupné z: https://www.alza.cz/trezor-white-d4684680.htm?o=2

[29] *Ledger Nano X - Hardware peněženka | Alza.cz. Alza.cz* [online]. Praha: Alza.cz a.s., c1994-2019 [cit. 2019-01-24]. Dostupné z: ://www.alza.cz/ledger-nano-x-d5527473.htm?o=4

[30] *How blockchain and serverless processing fit together to impact the next wave. A Cloud Guru — How blockchain and serverless processing fit together to impact the next wave as application patterns evolve to event-driven architectures.* [online]. A Cloud Guru, 2017 [cit. 2019-02-18]. Dostupné z: https://read.acloud.guru/blockchain-and-serverless-processing-similarities-differences-and-how-they-fit-together-c12142373287

[31] *Blockchain - Explainations about chaining of transactions - Bitcoin Stack Exchange. Bitcoin Stack Exchange* [online]. New York: Stack Exchange Inc, 2019 [cit. 2019-02-18]. Dostupné z: https://bitcoin.stackexchange.com/questions/10279/explainations-about-chaining-of-transactions

[32] *Bitcoin Mining Profitability Calculator. CryptoCompare* [online]. Londýn: Crypto Coin Comparison Ltd, 2019 [cit. 2019-03-18]. Dostupné z: https://www.cryptocompare.com/mining/calculator/btc

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ALU	Arithmetic Logic Unit
ASIC	Application Specific Integrated Circuit
BCH	Bitcoin cash
BTC	Bitcoin
CPU	Central Processing Unit
DOGE	Dogecoin
ETH	Ethereum
FPGA	Field Programmable Gate Array
GPU	Graphics Processing Unit
ICO	Initial Coin Offering
LTC	Litecoin
PoS	Proof-of-Stake
PoW	Proof-of-Stake
USB	Universal Serial Bus
USDT	Tether
VTC	Vertcoin
XMR	Monero
Y2K	Year 2000 Problem

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I. TABULKOVÉ POROVNÁNÍ

Název kryptoměny	Druh těžby	Těžební HW	Cena [Kč]	Výkon [H/s]	Spotřeba [W]	Náročnost těžby	Výdělek za rok[Kč]	Návratnost investic
Bitcoin	ASIC	AntMiner S11-19 TH/s	11 515	19 000 000 000 000	1 350	63792654511411.05	-2 109,32	Nikdy
Bitcoin	ASIC	AntMiner S9j	6 205	14 500 000 000 000	1 350	63792654511411.05	-2 611,28	Nikdy
Bitcoin	ASIC	AntMiner T15-23 TH/s	16 534	23 000 000 000 000	1 541	63792654511411.05	-2 261,83	Nikdy
Bitcoin cash	ASIC	AntMiner S11-19 TH/s	11 515	19 000 000 000 000	1 350	255971518945.87	-1 846,42	Nikdy
Bitcoin cash	ASIC	Avalon 7	20 152	6 000 000 000 000	850	255971518945.87	-23 178,01	Nikdy
Dash	ASIC	Spondoolies Tech SPx36	300 000	540 000 000 000	4 400	76670837.4889333	24 000	12,5 let
Dash	ASIC	Baikal Giant X5	20 335	10 000 000 000	800	76670837.4889333	-2 235,95	Nikdy
Dash	ASIC	Innosilicon A5+	100 000	60 000 000 000	1 500	76670837.4889333	-3 058,29	Nikdy
Dash	ASIC	AntMiner D3	10 000	19 300 000 000	1 200	76670837.4889333	-3 213,10	Nikdy
Ethereum	GPU	AMD Radeon R9 390	12 887	28 500 000	275	1,77145E+14	-6 515,52	Nikdy
Ethereum	GPU	Nvidia GeForce GTX1080Ti 11 GB	19 896	31 300 000	350	1,77145E+14	-9 618,00	Nikdy
Ethereum	ASIC	Antminer E3	41 220	200 000 000	800	1,77145E+14	-6 703,57	Nikdy
Ethereum	ASIC	Innosilicon A10 ETHMaster	114 500	480 000 000	850	1,77145E+14	24 694,22	4,5 roku
Litecoin	ASIC	Innosilicon A4+ LTCMaster	20 000	620 000 000	750	9814639.91002089	-1 101,10	Nikdy
Litecoin	ASIC	AntMiner L3+	8 000	600 000 000	850	9814639.91002089	-1 451,61	Nikdy
Monero	CPU	INTEL CORE I7-4980HQ 2.8 GHZ	14 000	550	47	36463243728	120,00	116 let
Monero	GPU	RADEON VII	19 386	3 125	240	36463243728	542,73	27,8 let
Vertcoin	GPU	Nvidia GeForce GTX 1050ti	5 000	80 000 000	260	39355,10904	-5 293,56	Nikdy