UNIVERZITA PALACKÉHO V OLOMOUCI
PŘÍRODOVĚDECKÁ FAKULTA

BAKALÁŘSKÁ PRÁCE

Kryptoměny jako investiční instrument

Katedra matematické analýzy a aplikací matematiky
Vedoucí bakalářské práce: **RNDr. Ondřej Pavlačka, Ph.D.**
Vypracoval: **Patrik Raška**
Studijní program: B1103 Aplikovaná matematika
Studijní obor: Matematika-ekonomie se zaměřením na bankovnictví/pojišťovnictví
Forma studia: prezenční
Rok odevzdání: 2022

BIBLIOGRAFICKÁ IDENTIFIKACE

Autor: Patrik Raška

Název práce: Kryptoměny jako investiční instrument

Typ práce: Bakalářská

Pracoviště: Katedra matematické analýzy a aplikací matematiky

Vedoucí práce: RNDr. Ondřej Pavlačka, Ph.D.

Rok obhajoby: 2022

Abstrakt: V této bakalářské práci se zabývám novou formou peněz a jejím použitím na poli investic. Cílem této práce je obecné seznámení s problematikou a vysvětlení základních principů jejich fungování, jak tuto novou měnu využít jako investici nebo srovnání s ostatními možnostmi investování. V první části uvádím krátkou historii této formy peněz (kryptoměn) a následné rozšíření po celém světě. Stručně popíšu, na jakých principech kryptoměny fungují a jaké jsou jejich výhody a nevýhody. V druhé části se věnuji zpeněžení kryptoměn a jak se dají považovat za investici, popřípadě jaké existují další způsoby, jak na nich vydělat. Na konci srovnávám investici do kryptoměn s konvenčním způsobem investování, které finanční trh nabízí. Zmínil jsem i zákony, které se kryptoměn týkají.

Klíčová slova: kryptoměny, Bitcoin, investice, hodnocení investic

Počet stran: 42

Počet příloh: 1

Jazyk: český

BIBLIOGRAPHICAL IDENTIFICATION

Author: Patrik Raška

Title: Cryptocurrencies as an investment instrument

Type of thesis: Bachelor's

Department: Department of Mathematical Analysis and Application of Mathematics

Supervisor: RNDr. Ondřej Pavlačka, Ph.D.

The year of presentation: 2022

Abstract: In this bachelor thesis I deal with a new form of money and its use in the field of investment. The aim of this work is a general introduction to the issue and an explanation of the basic principles of their operation, how to use this new currency as an investment or comparison with other investment options. In the first part, I present a brief history of this form of money (cryptocurrency) and its subsequent spread around the world. I will briefly describe the principles on which cryptocurrencies work and what their advantages and disadvantages are. In the second part, I focus on the monetization of cryptocurrencies and how they can be considered as an investment, or what are the other ways to make money on them. In the end, I compare investing in cryptocurrencies with the conventional way of investing that the financial market offers. I also mentioned the laws that apply to cryptocurrencies.

Key words: cryptocurrencies, Bitcoin, investment, investment evaluation

Number of pages: 42

Number of appendices: 1

Language: Czech

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně za vedení a pomoci pana RNDr. Ondřeje Pavlačky Ph.D. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Olomouci dne…….. ……..
podpis

Obsah

Poděkování

Tímto bych rád poděkoval panu RNDr. Ondřeji Pavlačkovi Ph.D. za odborné vedení této bakalářské práce, cenné rady a čas, který mi v průběhu psaní a při konzultacích věnoval. Mé díky směřuje také těm, co mě u studia podporovali a motivovali.

Úvod

V posledních letech jsou kryptoměny diskutovaným tématem nejen na poli teoretické funkčnosti, ale i jako potenciální náhrada státem krytých peněz. Svou popularitu získaly díky propracovanému systému, který využívá nejrůznější poznatky z ekonomie, kryptografie a informatiky. Práce přiblíží základní fungovaní kryptoměn a na jakých principech stojí.

Bakalářská práce je rozdělena do dvou částí, kde bych se v první části rád věnoval krátké historii kryptoměn a vzniku té první, nejslavnější, Bitcoinu. Popíšu motivaci k vzniku autonomního „peněžního“ systému, díky které Bitcoin a další kryptoměny vznikly. V práci nastíním základní principy, na kterých kryptoměny (alespoň většina) stojí z pohledu rakouské ekonomické školy, která kladla důraz na minimální zásah státu do ekonomiky. Kryptoměnám se to povedlo úplně a nejsou závislé na státu ani jiné autoritě a jsou čistě autonomní. Uvedu nejběžnější využití ze strany uživatele, který kryptoměny jen posílá, ale taky který kryptoměny těží (získává za vykonanou práci) nebo potvrzuje transakce, za které dostává odměnu. Díky, nebo spíš bohužel, se kvůli tomu, že kryptoměny nemají žádnou centrální autoritu, často zneužívají. Proto uvedu nejčastější výhody a nevýhody různých kryptoměn.

Druhá část práce je zaměřená na využití kryptoměn jako investiční instrumenty. Díky vzrůstající ceně a zvyšující se popularitě v posledních letech všechny kryptoměny rapidně rostou na ceně. Vydělat se na nich dá různě. Díky kolísavosti cen se přirozeně objevují spekulanti, kteří nakoupí, když je cena nízko a prodají když cena vzroste. Kryptoměny potřebují i svoje těžaře, kteří mají za úkol ověřovat správnost transakcí a za to jsou odměňováni. Kryptoměny srovnám s různými druhy investic v podobě podílových fondů, akcií nebo komodit. Budou představeny základní právní normy, které jsou ještě v plenkách a podle kterých by se měl nebo nemusel případný zisk danit.

1. Počátek a fungování kryptoměn

V této bakalářské práci zaměřené na kryptoměny, se budu v první části věnovat krátké historii a vzniku první a dodnes nejslavnější a nejpoužívanější kryptoměny Bitcoinu, uvedu motivaci k jejich vytvoření, základní principy fungování a způsob použití. Nastíním také jejich výhody, jako třeba náhradu běžných peněž, ale také jak se dají kryptoměny zneužít.

1.1 Stvořitel Bitcoinu a jeho motivace k jeho vytvoření

Barterový obchod byl kdysi naprosto běžným způsobem, jak získat věc, kterou nemám, za věc, kterou mám. Problémové bylo zaplatit jen zlomek věci, které chci, nebo naopak. Hotovostní platební styk tento problém řeší dokonale, jenže potřebuji někoho, kdo mi zaručí, že hotovost, kterou přijmu, přijme i někdo jiný se stejnou důvěrou, se kterou jsem ji přijal já. Jinak by peněžní systém nefungoval. Této role se vždy zhostil někdo z vládnoucí sféry, který na měnu musí dohlížet. S postupem času bylo možné provádět transakce přes internet, kde byly převody peněz ještě jednodušší, a proto je i bezhotovostních peněz více než těch hotovostních. Daň za jednoduchost je anonymita, o kterou přicházíme, a proto jsou všechny transakce lehce vystopovatelné a banky mají přehled, kdo komu poslal i sebemenší částku peněz. Spojit tyto aspekty a vytvořit ideální měnu, která funguje na internetu, je anonymní, která nepodléhá žádné autoritě a je plně autonomní, se zdá být nemožné. Následující část je vypracována podle literatury. [1]

V roce 2009 byl vytvořen Bitcoin anonymním vývojářem pod pseudonymem Satoshi Nakamoto na základě článku, který publikoval již v říjnu roku 2008, na kterém pracoval už od roku 2007. O Nakamotovi se toho moc neví, a tak se ani neví, jestli jde o jednotlivce nebo o skupinu lidí. Kandidátů je hned několik. Patří mezi ně například Michael Clear, který v roce 2008 psal o P2P (počítačová síť ve které spolu komunikují přímo jednotliví uživatelé) a byl nejlepším studentem kryptografie na škole. V březnu 2014 se v časopise Newsweek objevil článek, který psal o japonci žijící v Kalifornii, který se jmenuje Dorian Nakamoto, a který se narodil se jménem Saotshi Nakamoto. Pracoval jako systémový inženýr a podle slov jeho dcery se považoval za libertariána, tedy člověka, který svou ideologii zakládá na osobní svobodě a autonomii. Později pak Dorian popřel, že by byl zakladatelem Bitcoinu. Zatím nejpravděpodobnější adept na tvůrce Bitcoinu je americký programátor Nick Szabo, u kterého si všimli používání podobných slov v textech Szaba a Nakamota. Ukázalo se, že i on psal články pod pseudonymy, jako třeba „bit gold“, ještě před Nakomotem. Navíc mají oba stejné iniciály

a Szabo je bezpochyby génius. Szabo ovšem popřel, že by Bitcoin vytvořil. Důležité je, že znalost tvůrce Bitcoinu pro samotný Bitcoin není vůbec podstatná a proto můžeme hledání s čistým svědomím přeskočit. [1]

1.2 Jak Bitcoin funguje

Představme si, že jsme ve skupině čtyř přátel, kteří mezi sebou uskutečňují různé transakce. Pro lepší představu si je pojmenujme Verča, Lucka, David a Patrik. Těmto kamarádům se nechce platit hotově hned potom, co se vytvoří nějaký dluh vůči druhému, a proto se rozhodli vytvořit jakousi účetní knihu (protokol), kde se budou transakce zapisovat a na konci měsíce se všechno takzvaně vyrovná. Zápis v protokolu může mít podobu „Verča platí Davidovi 10 Kč“, „Lucka platí Patrikovi 20 Kč“. Tento protokol bude veřejný a přístupný všem, aby mohl kdokoli přidat jakýkoli zápis o nové transakci, třeba na internetu. Na konci měsíce se spočítá, kdo kolik půjčil ostatním a kolik si kdo půjčil od ostatních. Pokud si někdo půjčil více peněz od ostatních, něž kolik poskytnul k půjčce, dá rozdíl na financování těm, kteří více peněz poskytli a jsou v deficitu.

Problém nastane, pokud bude někdo chtít zneužít veřejnou podobu protokolu, jelikož každý může přidat zápis, a to i neautorizovaný. Řešením by mohl být podpis, který má každý svůj a v ideálním případě ho nelze nahradit ani zfalšovat. Jelikož jsme v digitálním světě, podpis by měl podobu nějaké sekvence jedniček a nul, které by mohly být v nešifrované podobě lehce okopírovány a vloženy. Proto existují různé takzvané hashovací funkce. Bitcoin těchto funkcí využívá hned několik a různě je kombinuje. Pro účely vysvětlení bude stačit funkce SHA-256, která pracuje s takzvaným *Public key (Veřejný klíč)* a *Secret key (Soukromý klíč)*, které jsou generovány společně a mají podobu řetězce 256 bitů. Na papíře má rukou psaný podpis stejnou podobu, nehledě na to, jaký dokument je s ním podepsán. Digitální podpis je silnější, jelikož mění podobu s měnící se zprávou. Formálně můžeme napsat, že podpis vygenerujeme pomocí funkce

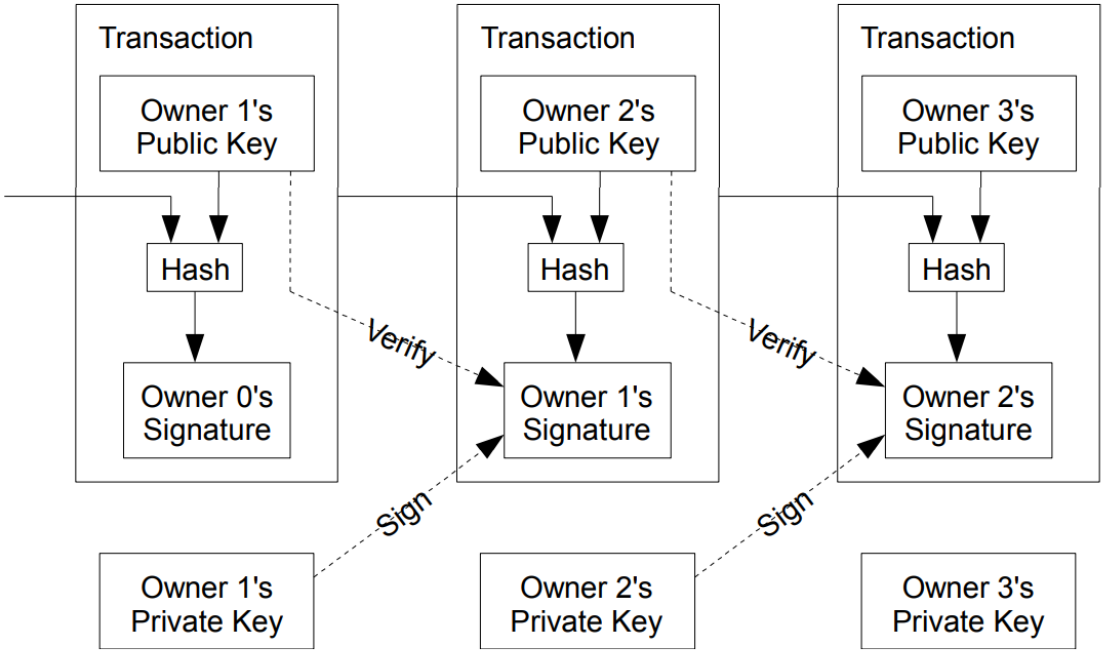
$$podp(zpráva, Sk) = podpis,$$

kde Sk je Secret key. Pro ověření, jestli je podpis platný, je tady druhá funkce, která využívá Public Key. Formálně ji můžeme napsat pomocí funkce

$$ověř(zpráva, podpis, Pk) = T/F,$$

kde Pk je Public Key a výstup funkce je v podobě True or False, který nám indikuje, jestli byl podpis vytvořen z konkrétního soukromého klíče. Neexistuje jiná možnost než zkoušet a ověřovat náhodné podpisy v podobě sekvence 256 bitů k tomu, aby se našel validní Secret key k příslušnému Public key. To je 2^{256} možností, jak může Secret key vypadat. Proto může být uživatel naprosto klidný, pokud by měl obavy, že se někdo pokusí jeho Private key zjistit.

Každá nová transakce musí mít navíc svoje ojedinělé ID (třeba pořadové číslo) aby nemohl někdo jiný okopírovat řádek a použít ho znovu v protokolu. Následující schéma transakce bylo použito v originálním článku Nakamota v roce 2008.



Obrázek 1 - Schéma transakce [zdroj 5]

Další problém nastává v situaci, kdy jeden z členů party vytvoří velký dluh, který nedokáže splatit, a na konci měsíce odmítne dát peníze k vyrovnání. Tento problém by se dal vyřešit počátečním vkladem. Například každý dá 100 Kč na začátku. Zápis bude mít podobu „Verča vložila 100 Kč“, „David vložil 100 Kč“, „Lucka vložila 100 Kč“ a „Patrik vložil 100 Kč“. Patrik potom zaplatí 50 Kč Verči a 50 Kč Lucce stejným způsobem zápisu. Poté se pokusí zapsat „Patrik platí Davidovi 20 Kč“, ale zápis nebude validní, jelikož přesáhl počáteční vklad. Je nutné vědět celou historii transakcí k ověření nových. Toto pravidlo a znalost historie transakcí hraje velkou roli v kryptoměnách, jelikož je na něm založené.

Tento krok je zároveň podstatný v cestě za nezávislostí na centrální autoritě, jelikož už nepotřebujeme používat konkrétní měnu. Uvědomme si, že v této fázi může docházet k transferu pouhých čísel. Spojení protokolu a fyzických peněz zaniká. Závislost na systému se v našem příkladu schovává už jen v hypotetické online stránce, kde transakce zaznamenáváme. V tuto chvíli máme centralizovaný systém dobře chráněných a evidovaných transakcí bez nutnosti použití státní měny.

Pro názornost přestaneme používat koruny (Kč) a nahradíme je třeba žetony (Ž). Potom David může dát Verči 10 Kč v reálném světě výměnou za její autorizovaný zápis v protokolu v podobě „Verča platí Davidovi 10 Ž“. Proč ne. Tato směna ovšem nebude zaznamenána v protokolu. Analogicky se dá směnit jakákoli jiná měna nebo i věc nezávisle na výše uvedených principech. Podstatná myšlenka k pochopení kryptoměn je v ekvivalenci protokolu (historii transakcí) a měny (ve které jsou transakce prováděny). Historie transakcí = měna.

Decentralizace byla největší výzvou při tvorbě Bitcoinu, jelikož se zdálo být neproveditelné, aby existoval systém nezávislý na centrální autoritě. Tento problém byl vyřešen pomocí Blockchainu. Nejdříve si ale nasimulujeme, jak by tento problém řešila naše parta přátel. Řekněme, že každý z party bude mít svou vlastní kopii protokolu, aby nemuseli mít protokol online. Poté, co někdo bude chtít vytvořit zápis (transakci), jednoduše dá všem vědět, že má v plánu transakci provést a poprosí, aby si každý transakci zapsal. Problém nastává v tom, že nikdo si nemůže být jistý, že dostává validní transakce a ve stejném pořadí. Na řadu přichází systém, který určuje správnost protokolu podle vykázaného výpočetního výkonu.

Kryptografická hashovací funkce je způsob, jak vytvořit a ověřit elektronický podpis a zajistit integritu dat. Myšlenka stojí na tom, že pokud použijeme výpočetní výkon na to, v co vkládáme důvěru, museli bychom vynaložit neúměrné množství výpočetní síly k tomu, abychom obsah nebo integritu dat změnili. Výstup (Hash) hashovací funkce SHA-256 je řetězec 256 bitů, který vypadá náhodně s měnícím se vstupem (zápisem), ale není. Jeden vstup má jeden konkrétně vypadající výstup, ale i sebemenší změna vstupu, třeba jen o jedno písmeno, kompletně změní řetězec bitů na výstupu. Změna je naprosto nepředvídatelná a nikdo a nic zatím není schopný zjistit původní vstup ze známého výstupu (Hashe). Tato vlastnost se nazývá asymetrie a je charakteristická právě pro kryptografické hashovací funkce.

Jak tedy využít této vlastnosti k ověření správnosti dat. Pokud v protokolu pod transakcemi připíšu nějaké číslo a aplikuji hashovací funkci SHA-256, existuje určitá pravděpodobnost, že prvních 30 čísel Hashe budou nuly. Pravděpodobnost nebude moc velká, konkrétně $\frac{1}{2^{30}}$. Jediný způsob, jak najít Hash, kde je na začátku 30 nul je zkoušet zápisy po

jednom a samostatně, každý s jiným číslem. To znamená, že ten, co by chtěl konkrétní Hash najít, by musel projít 1 073 741 824 možných protokolů a aplikovat hash funkci. Jinými slovy, můžeme ověřit, že někdo prokázal velký výpočetní výkon k nalezení konkrétní podoby Hashe. Tato metoda se nazývá „Proof of work“. Důležité je, že tato práce je spojena s podobou zápisu s transakcemi. Kdyby se protokol (transakce) změnil, kompletně se změní Hash a výpočetní výkon by se musel provést znovu.

Zpět k našim kamarádům, kteří si chtěli posílat stejnou podobu protokolu a kteří chtěli mít jistotu správnosti transakcí. Domluví se, že validní protokol s transakcemi bude jen ten, jehož Hash bude obsahovat na prvním místě nuly. Základem pro určení správnosti je výpočetní práce, která je do protokolu vnesena. Protokoly s jednotlivými transakcemi, u kterých byl prokázán výpočetní výkon, budeme nazývat bloky. Stejně jako u transakcí, které jsou podepsané a jsou validní, tak u bloků, u kterých byl prokázán výpočetní výkon a našli jsme Hash, ve kterém jsou nuly, budeme nazývat validní. Navíc, abychom zachovali pořadí bloků s transakcemi, bude každý následující blok obsahovat Hash předchozího bloku. Proto, kdybychom jen trochu změnili zápis v jakémkoli předchozím bloku v řetězci bloků (Blockchainu), kompletně se změní Hash, bloky nebudou validní a my bychom museli výpočetní výkon prokázat znovu. V této fázi můžeme našim kamarádům dovolit, aby mohli zapsat validní transakce, vytvořit blok, prokázat výpočetní výkon, aby Hash bloku začínal nulami a rozeslat ho ostatním kamarádům, kteří jednoduše ověří, že se jedná o validní blok(y) v řetězci, a přijmou ho.

Nastává problém, jak přinutit ostatní, aby spotřebovávali elektřinu k nalezení konkrétního Hashe. Konkrétně u Bitcoinu je motivací pro hledání určité podoby Hashe bloku odměna (Block reward), v podobě systémové transakce, která přísluší tomu, kdo našel sekvenci nul a tím vytěžil blok. Odměnu následně zahrne do bloku, který vytěžil, uzavře a připojí k předešlým blokům. Odměna od nikoho nepřichází, takže nemusí být podepsaná. Zároveň to znamená, že počet Bitcoinů v systému s každým vytěženým blokem roste. Motivací těžaře těžit a tím ověřovat správnost transakcí je odměna, kterou dostane za poskytnutý výpočetní výkon jeho počítače. Pokud chce někdo pouze uskutečňovat transakce, potom sleduje ostatní těžaře a aktualizuje osobní kopii Blockchainu. V momentu, kdy zaznamená dva řetězce bloků s konfliktními transakcemi, přesune se na ten delší, ve kterém bylo potřeba vykonat více výpočetního výkonu. Pokud nastane remíza v délce řetězců, počká, až někdo objeví validní blok, který řetězec prodlouží. Takže i když zde není centrální autorita, která by správnost řetězce zaručovala, dosáhli jsme decentralizované kontroly, která je v zájmu každého uživatele.

Řekněme, že naše parta přátel začala používat Bitcoin a David bude chtít vydat podvodný blok, ve kterém se píše "Lucka platí Davidovi 10 BTC". Aby mu to vyšlo, musí najít další blok, kterým by uzavřel svůj podvodný, a pokračovat ve své vlastní větvi Blockchainu. A to se může stát, klidně může mít štěstí a blok najít dříve než ostatní těžaři. Problém je v tom, že Lucka dostává informace o nových blocích ostatních těžařů, které vypadají jinak, takže aby ji udržel v nevědomosti o podvodném bloku, musí vynaložit stejné nebo větší úsilí, jako všichni ostatní těžaři na tvorbě delšího řetězce. Po čase se ukáže, že David nedokáže konkurovat všem ostatním těžařům a jeho podvodné větvi přestanou věřit. Těžař nemusí hned věřit řetězci, který je o jeden blok delší, ale s přibývajícím počtem bloků se pravděpodobnost, že pracuje na validním řetězci, zvyšuje.

V této fázi jsme zmínili všechny podstatné náležitosti, které by decentralizovaný měnový systém měl mít. Digitální podpis, Blockchain, decentralizace na základě prokázané práce a dostatečné zabezpečení. V příkladu jsem uváděl, že potřebuji najít konkrétní číslo, které, když společně s transakcemi projdou hashovací funkcí, objeví se na prvním místě 30 nul. Způsob, jakým skutečný Bitcoin funguje, je trochu jiný. Mění se počet nul, který je potřeba nalézt tak, aby byl nový blok vytěžen v průměru za 10 minut. S přibývajícím počtem těžařů se počet potřebných nul k nalezení zvyšuje. U různých kryptoměn se čas však liší. Je určena i odměna za vytěžený blok, která se geometricky zmenšuje a začínala na 50 BTC. Každých 210 000 vytěžených bloků se odměna sníží o polovinu. Tímto způsobem je stanovený i maximální počet nových vytěžených Bitcoinů, označme S,

$$S = 210\,000 \cdot (50 + 25 + 12{,}5 + 6{,}25 + \cdots)$$

$$S = 210\,000 \cdot \frac{a_1}{1-q} = 210\,000 \cdot \frac{50}{1-\frac{1}{2}} \qquad pro\ |q| = \frac{1}{2} < 1$$

$$S = 21\,000\,000.$$

Těžit nové bloky s přibývajícími těžaři a klesajícími odměnami bude stále méně a méně rentabilní, jelikož se zvětšuje množství elektřiny, které se na výpočetní sílu spotřebovává, ale cena za ni zůstává prakticky stejná.

To ovšem neznamená, že těžaři přestanou přijímat Bitcoin. Mohou vybrat volitelný poplatek za transakci někoho cizího, který bude společně s transakcí zapsaný do bloku. Poplatek je motivací pro těžaře, aby transakci do Blockchainu zapsal. Každý blok je limitován na zhruba 2 400 transakcí, což mnoho kritiků považuje za zbytečně omezující. Pro srovnání

VISA v průměru provede 1 700 transakcí za vteřinu a je schopná tento limit zvýšit až na 24 000 za vteřinu. To je spojeno s vyššími transakčními poplatky, které si těžaři nárokují. Navíc zde platí pravidlo, že si těžař vybírá, kterou transakci provede, a transakce s malými poplatky čekají na zápis delší dobu. [1], [5], [13], [22]

1.3 Užití v praxi

Tato podkapitola je vypracována podle zdroje [1]. Stejně jako u běžné měny je potřeba pořídit si peněženku. Možností je hned několik. Peněženku si můžeme představit jako unikátní kód, který můžeme umístit do počítače, externího disku nebo klidně na papír. Jedním z prvních způsobů, jak si peněženku pořídit, byl a je na webu bitcoin.org. Ten je specifický tím, že spolu s klientem se stáhne celý Blockchain Bitcoinu. Vzhledem k relativně dlouhé historii používání je nutné stáhnout transakce o velikosti více než 350 GB. Pro běžné uživatele se zdá být tato metoda zbytečná. Pro běžné uživatele je snadnější vytvořit si virtuální peněženku na některých webech, které tyto služby poskytují. I na nich platí šifrování v určité podobě, proto se uživatel nemusí bát o bezpečnost svých dat. Zároveň ale platí, že pokud svěřuji svůj majetek třetí osobě, fakticky ho nevlastním a jsem odkázaný jí důvěřovat. Proto mít v úschově třetích stran větší množství kapitálu v podobě kryptoměn není zcela ideální.

Řekněme, že jsme si vybrali jeden z mnoha způsobů, jak si peněženku pořídit. Chceme tedy výměnou za reálné peníze nakoupit třeba Bitcoiny. Nutno dodat, že touto situací se zaobírala ČNB a Ministerstvo financí, které vyjádřilo souhlas, a Bitcoin za legální považují. V metodickém pokynu MF-86583/2013/24 k Bitcoinu pouze konstatuje, že je třeba považovat transakce nad 1000 euro za rizikové a transakce nad 1500 euro ohlašovat. Prvním, nejjednodušším způsobem, jak získat Bitcoiny, je koupit je od někoho, kdo je má. Třeba je vytěžil nebo opět získal od někoho jiného. Dalším způsobem, jak Bitcoiny koupit, jsou bankomaty. Stačí si pořídit peněženku, která je součástí volně stažitelné aplikace, a pak jen přiložit QR kód k bankomatu, který vám obratem v daném kurzu a s marží pošle Bitcoiny na vaši peněženku. Další způsob je online směnárna (zhruba 3% poplatek) nebo burza (okolo 0,25 %). Každý způsob je vhodný pro jinou velikost nákupu a trvá různě dlouho společně s různými poplatky. Při větších nákupech je nutné ověření identity nebo doložení původu prostředků.

Další způsob, jak získat Bitcoiny, je již zmíněná těžba. Proces těžby Bitcoinu se podobá těžbě zlata. Víme, že zlata je omezené množství. Pokud se omezíme na naši planetu, nejde ničím nahradit, je vzácné a množství vytěženého zlata se pořád zmenšuje. Proto stejně jako u Bitcoinu je méně a méně rentabilní ho těžit. V počátcích 19. století na Aljašce během zlaté horečky stačil

(obrazně) krumpáč a šťastná ruka. Stejně tak u Bitcoinu na začátku stačil běžný počítač s průměrným výpočetním výkonem. S postupem času a množstvím vytěženého Bitcoinu/zlata se obtížnost těžby zvyšuje. V dnešní době je těžení Bitcoinu pro obyčejného smrtelníka naprosto nereálné, proto se vytvořily takzvané Pooly, v nichž se spojí výpočetní výkon více těžařů, a případnou odměnu za vytěžený blok si následně rozdělí.

Když už Bitcoiny mám, chci je ochránit. Samy o sobě jsou prvky Bitcoinu skoro neprolomitelné. Problém nastává v úschově peněženky a dat, které mohou být třeba v osobním PC nebo v aplikaci. Pro tyto účely se používají různé způsoby ochrany jako šifrování nebo fyzické úschovny v podobě hardwaru, který data uschová. Jeden z nich nabízí český startup SatoshiLabs, který nabízí malé zařízení v podobě flashky, ve kterém je váš soukromý klíč, který se nikdy nedostane do vašeho počítače nebo mobilu, kde by mohl být zneužitý. Útočník proto nemá možnost se k vaší peněžence dostat.

1.4 Základní principy ostatních kryptoměn

Tato podkapitola je vypracovaná podle zdroje [1]. Ke konci roku 2017 existovalo více než tisíc různých kryptoměn. Některé se ve fungovaní vzhledem k Bitcoinu dost liší a některé jsou jen trochu přeparametrizované klony Bitcoinu. První z nich se začaly objevovat od roku 2011 a popularitu si získaly v letech 2013 a 2014. Některé z nich měly obrovskou volatilitu, a tak se na nich přiživovali spekulanti, kteří se ve větším počtu domlouvali a pořádali akce typu pump&dump, kdy ve velkém nakoupili, navýšili cenu a pak ve velkém prodali. Ti, co nastoupili do rozjetého vlaku pozdě, odešli s masivní ztrátou, a jejich vložený majetek se redistribuoval mezi málo vyvolených. Proto je potřeba dobře si rozmyslet a chápat základní principy celé problematiky, než se člověk rozhodne využít kryptoměny jako investiční instrument.

Zpět k našim alternativám k Bitcoinu, zvané také Altcoiny. Základní strukturu fungování má většina altcoinů stejnou jako Bitcoin, zejména protokol a softwarovou implementaci. Jsou zde ovšem i jiné protokoly jako například CryptoNote, který rozšiřuje anonymizační schopnosti. Jiné mohou zakládat svou monetární strategii jinak než Bitcoin, která je deterministická a známá dopředu. Třeba může být nekonečně inflační s předem známou rychlostí „emise“ tokenů, jako například Monero. Důležitá je i prvotní distribuce tokenů, která v případě Bitcoinu začala od chvíle spuštění, a od té doby nebyla závislá na nikom jiném než na uživatelích.

V případě kryptoměny XRP (Ripple) těžba vůbec neprobíhá a bylo vydáno určité množství tokenů, konkrétně 100 miliard. Ilustrujme si fungovaní kryptoměny na příkladě. Já

chci poslat Davidovi 100 Kč, proto zajdu ke svému zprostředkovateli plateb A nechám mu svou stokorunu s instrukcí, komu má peníze dát. Zprostředkovatel A pošle zprávu zprostředkovateli B, který má vydat stokorunu Davidovi. David přijde a od B si peníze vezme. Tento způsob platby se až moc podobá cenným papírům (elektronické směnky), které musí být evidované, proto podle Komise pro cenné papíry (SEC) jsou XRP tokeny považovány za cenné papíry a autory čekaly soudní spory kvůli jejich obchodování. Dodnes neexistuje jednotné stanovisko. Transakce se nepotvrzují těžbou, ale je založen na 80% shodě všech uzlů. Systém je rychlejší, ale založený na důvěryhodnosti uzlů mezi sebou. To se líbí finančním institucím, které Ripple využívají. Je to decentralizovaný systém, ale vývoj a určování pravidel se řídí kolem společnosti Ripple.

Pravděpodobně nejznámějším derivátem Bitcoinu je Litecoin (LTC), který byl představen v roce 2011 a jeho autor je programátor Googlu Charlie Lee. Je to odlehčená verze Bitcoinu, v tom smyslu, že generuje bloky rychleji, a to čtyři krát, a původně byl navržen pro mikroplatby. To znamená, že každý nový blok je nalezen za zhruba 2,5 minuty oproti Bitcoinu, který má periodu cca 10 minut. Litecoin má i čtyři krát více mincí (84 000 000). Kvůli vysokým transakčním poplatkům v roce 2017 bitcoinoví uživatelé začali používat Litecoin, který díky čtyřikrát větší rychlosti transakcí ukojil poptávku po kryptoměnách lépe. Říká se, že Litecoin je k Bitcoinu jako stříbro ke zlatu.

V neposlední řadě je tady třeba ještě Peercoin (PPC), který vznikl v roce 2012 a jeho autory jsou Scott Nadal a Sunny King. Tato měna je nekonečně inflační s inflací 1% za rok a zároveň deflační za fixní transakční poplatek 0,01 PPC/kB, které se zničí. Jeho nevýhoda je centralizující prvek, který spočívá v potřebě zásahu autora do Blockchainu.

Obrovským přínosem do světa kryptoměn a celkově decentralizovaných systémů bylo Ethereum. Kryptoměna, se kterou přišel tehdy 19 letý programátor z Ruska Vitalik Buterein. Spolu s Gavinem Woodem přišli na to, že by kromě virtuálních mincí mohly fungovat i decentralizované aplikace. Oproti centralizovaným aplikacím jako třeba Facebook, Uber, internetové bankovnictví nebo jakákoli jiná aplikace, která zajišťuje chod a druh určité komunikace mezi uživateli, nabízí Ethereum decentralizovaný systém tohoto střetu nabídky a poptávky po službě, která může mít více podob, než jenom transakce tokenů. Na základě smart contractů, což jsou konkrétní podoby služby, jsou těžaři odměňováni za jejich provedení a zapsáni do Blockchainu, stejně jako u ostatních kryptoměn. Celý koncept je v počátcích, a proto je tady hodně problémů jako rychlost schvalování nebo velká náročnost na výpočetní výkon. Proto tvůrci navrhují používat místo Proof of Work (PoW) jinou záruku pravosti zápisů, a to Proof of Stake (PoS). Ten funguje na principu zálohy, kdy se validátor zaručí určitým

množstvím tokenů a po správném zapsání se mu záloha vrátí i s odměnou. Tento systém se využívá u více kryptoměn, protože je rychlejší, ale má také nevýhody, protože zvýhodňuje bohatší a je částečně narušena decentralizace.

Kryptoměn je spousta a od Bitcoinu se svět kryptoměn vyvíjí rychlým tempem. Nakamoto položil surový základní kámen fungování decentralizovaného systému a teď se tvůrci nových kryptoměn předhánějí v tom, kdo vytvoří lepší, rychlejší, uživatelsky přívětivější a bezpečnější verzi. Díky jednoduchosti, robustnosti, bezpečnosti a popularitě nejspíš zůstane na předních příčkách Bitcoin ještě dlouho. Nutno dodat, že některé kryptoměny svým provedením a adaptacím na globální poptávku silně dýchají Bitcoinu na záda.

1.5 Výhody a nevýhody

Tato podkapitola je vypracována podle zdrojů [4] a [16]. Jako každý vynález má i tento klady a zápory. Mezi největší výhody a vlastně důvod k vytvoření kryptoměn je již zmíněná decentralizace. Z povahy systému a šifrování zde není důvod kontroly ani dohledu nad chodem kryptoměn. Nikdo nemůže ovlivnit počet vydaných mincí, nikdo nemůže padělat mince, blokovat účty a podobně. Také nepodléhá inflaci právě díky omezenému počtu mincí. Další výhodou je anonymita, kterou kryptoměny poskytují. Některé více, některé méně. To záleží na podobě softwaru a preferenci uživatele, který podle toho druh kryptoměny volí. To se pojí i s podobou Blockchainu, který nabízí úplnou historii transakcí, plně transparentně a se všemi adresami peněženek, které ovšem nenesou jméno majitele ani adresáta. Adresa má totiž podobu 34 náhodných znaků a zná ji jen ten, který si nechal adresu a k ní příslušnou peněženku vygenerovat. Celé fungování je založeno na kryptografickém šifrování, které je (zatím) neprolomitelné a dává kryptoměnám punc nejvyššího zabezpečení. Nakonec bych rád zmínil robustnost celého systému, který právě díky decentralizaci zajišťuje jeho nesmrtelnost. Aby zkolaboval Blockchain, a tím pádem celá měna, musely by zkolabovat všechny počítače, které jsou do systému nějakým způsobem zapojené. Stačí, aby přežil jediný počítač s kopií Blockchainu a měna může být vzkříšena.

Nemohou být ovšem opominuty ani velké nevýhody decentralizovaných sítí a měn. Jednou z nich je obrovská volatilita, která může kolísat i v desítkách procent za den. Ani zkušení tradeři nejsou schopni přesně určit budoucí vývoj ceny. Poplatky za transakce a prodleva mezi zadáním a uskutečněním transakce rostou s počtem uživatelů. V roce 2017 trvala jedna transakce na zapsání v průměru 91 minut kvůli obří vytíženosti. Od té doby se ustálila na 10 minut, což odpovídá délce těžby jednoho bloku. Další nevýhodou jsou hackerské útoky,

které útočí na burzy, soukromé počítače nebo mají podobu různých známých metod a virů na prolomení hesel a krádeže dat. Největší a zároveň nejnebezpečnější nevýhodou je kriminalita, se kterou jsou některé kryptoměny spojovány. Poskytují anonymitu, která je živnou půdou pro prodej drog, dětskou pornografii a vlastně všeho, co lze ilegálně financovat. To je i hlavním motivem vlád pro jejich regulaci. Konkrétně u Bitcoinů je pak velký problém alokace všech mincí, které vlastní jen hrstka uživatelů. Tento problém by mohl být pro Bitcoin v budoucnu zásadní.

1.6 Budoucnost kryptoměn

Tato podkapitola je vypracována podle zdroje [1]. Vyvstává otázka, jestli není Bitcoinu nebo obecně kryptoměn málo (myšleno množství mincí). Pro tenhle případ se dá dělit Bitcoin na osm desetinných míst a nejmenší jednotka je jeden Satoshi (pojmenovaný po tvůrci). Ovšem ani v případě, že by nastala nutnost ho dál dělit, není nutné měnit celý systém. Pouze by se poupravilo fungování peněženek a uživatelé by pouze museli vymyslet nějaký pěkný název pro nejmenší jednotku. Co by ovšem problémy dělat mohlo je již zmíněná alokace.

Jako jeden z největších problémů se zdá být státní regulace. Je přirozené, že v zájmu monetárních orgánů, např. ČNB, určitě není vznik a fungování nějaké měny, kterou nemohou kontrolovat, případně řídit. Není příliš ideální k výběru daní a vysoká anonymita taky nehraje Bitcoinu, coby alternativy peněz, do karet. Už ze samotné podstaty nelze Bitcoin a všechny kryptoměny založené na decentralizovaném Blockchainu nijak regulovat. Situaci krásně vystihuje příklad s jistým americkým regulátorem, který zjistil, že Bitcoin se považuje za měnu, což je v rozporu s tamními zákony, které říkají, že jediná měna je americký dolar. Následně pak sepsal dopis s žádostí o ukončení činnosti s podmínkou, že pokud činnosti nezanechají, sáhne k trestu. Jelikož Bitcoin nemá centrální autoritu a tím pádem nemá ani adresu, na kterou by se mohly stížnosti a připomínky posílat, poslal onen regulátor dopis neziskové organizaci, která měla Bitcoin ve jméně. Po přečtení dopisu v neziskové organizaci příběh končí. Co ovšem stát regulovat může, jsou státní peníze, za které se kryptoměny směňují. Monetární systém dovoluje nakupovat cizí měnu a tím ovlivňovat kurz mezi státní měnou a třeba Bitcoinem. Což by ale vedlo k legitimizaci a posílení kryptoměn. Zbývá už jen regulovat příjemce a nějakou formou je sankcionovat. Vzhledem k problémům spojovaným s trestnou činností k tomu mají dobrý důvod, proto by mohly státní orgány systematicky znevýhodňovat příjemce kryptoměn a pro ty by se s dodatečnými náklady zmenšovala motivace kryptoměny používat.

Stejně jako vynález knihtisku, který se už dnes nepoužívá jen pro tisk biblí, nebo vynález internetu, který dnes nefunguje jen pro vojenské účely v časech studené války v Americe, jsou i kryptoměny v počátcích, a tak jako se dá zneužít internet, se dá zneužít jakýkoli jiný velký vynález. Lidská společnost se vyvíjí a kryptoměny potřebují svůj čas a místo k vývinu také.

2. Kryptoměny jako investiční instrument

Gavin Andersen, který je pokládán za pokračovatele práce Nakamota řekl: “Bitcoin je experiment. Chovejte se k němu tak, jak byste se chovali ke slibnému internetovému startupu. Možná změní svět, ale uvědomte si, že investice peněz či času do nového nápadu je vždy riskantní.“ [1]

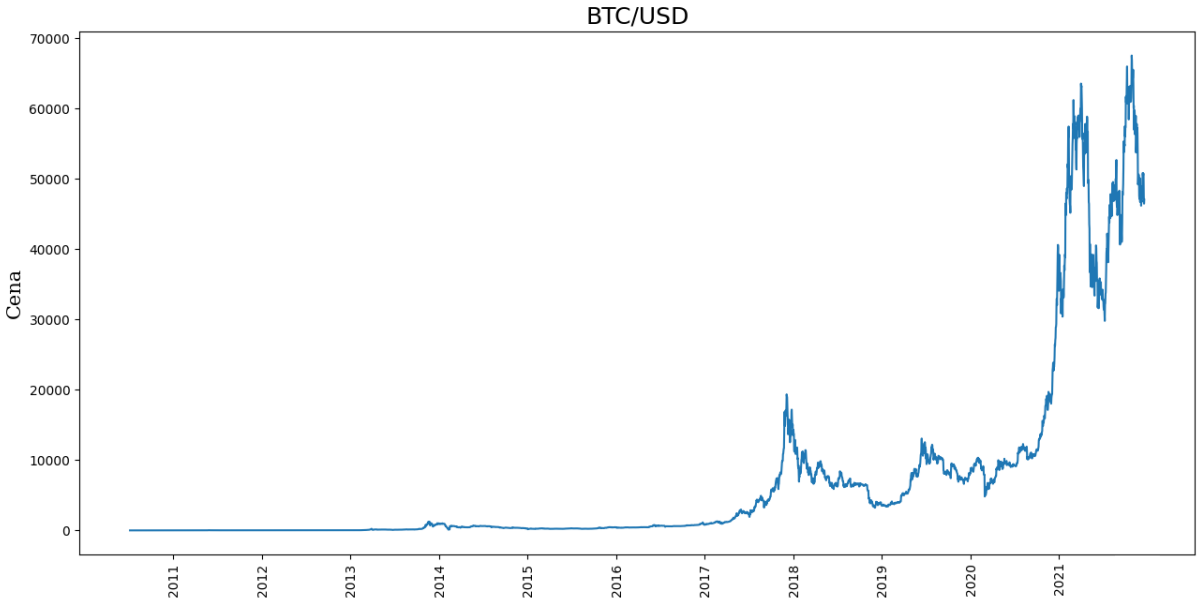
Pohlížet na měnu jako na investici není úplně běžné. Z podstaty věci k tomu běžné státní měny ani nejsou uzpůsobené, mají funkci prostředku směny, zúčtovací jednotky, popřípadě uchovatele hodnoty. Málokdo ve velkém nakupuje určitou měnu a čeká, až se cena těchto peněz vyšplhá výš, a následně prodá. Centrální banky, které měny spravují, ani neumožní takové kolísání. V některých případech se spíše jedná o obrovskou inflaci měny vlivem vnějších vlivů jako jsou války nebo hospodářské a finanční krize. V těchto situacích se o investici ani mluvit nedá, jelikož celá měna kolabuje a nepomůže jim ani podpora skrze centrální banky. Rozdíl mezi státem vydanou měnou s nuceným oběhem a kryptoměnami je v jejich (ne)závislosti na centrální autoritě. Státní měnu spravuje centrální banka a ta je odpovědná za její fungovaní a chod. Kdežto kryptoměny (alespoň většina) nejsou závislé na ničem, pokud nepočítáme uživatele, internet a elektřinu, které potřebují i státní peníze. Proč však cena kryptoměn vzhledem k ostatním měnám roste vysvětlím v následující části.

2.1 Růst ceny díky davové psychologii

Hlavní cenotvorný faktor kryptoměn je poptávka. Pokud se zvýší poptávka, kupující začnou nabízet více vlivem nedostatku komodity na trhu. Je to základní ekonomické chování všech komodit na trhu, které má například i zlato, se kterým se Bitcoin srovnává. Na rozdíl od zlata, u kterého můžeme hypoteticky nalézt nové naleziště, je Bitcoin absolutně omezený co se týče jeho množství. Nikdy ho nebude více než 21 miliard díky mechanismu, který postupně uvolňuje mince do systému. Podobně jako u zlata je pak uvolňování/těžení stále náročnější. Tímto způsobem je navíc eliminována inflace, která by mohla cenu oslabovat.

Od založení do března roku 2010 neměl Bitcoin prakticky žádnou cenu. Byl v povědomí malé skupiny lidí a fanoušků, kteří byli nadšení z nové technologie. V květnu 2010 nabídnul programátor z Floridy 10 000 BTC tomu, kdo mu objedná a nechá dovézt dvě pizzy. O pár dní později mu jistý dobrovolník z Anglie pizzy objednal a první transakce za zboží byla na světě. 13.4. 2021 by tyto dvě pizzy v hodnotě 25 dolarů stály více než 13,5 miliardy Kč. V únoru 2011

dosáhl Bitcoin parity s americkým dolarem. Postupem času se konaly mezinárodní konference, z nichž jedna také v Praze. O Bitcoin se začali zajímat vývojáři, ekonomové a také média. V červnu 2011 měl Bitcoin cenu 31,91 dolarů a během čtyř dnů se propadl na pouhých 10 dolarů. Události se později začalo přezdívat Velká bublina roku 2011. V roce 2012-2013 rostla cena Bitcoinu velmi pomalu, vývojáři pracovali na předešlých chybách v zdrojovém kódu a snažili se o konkurenceschopnost s ostatními měnami. Bitcoin není jen sofistikovaná hračka pro počítačové nadšence a ukázalo se, že může opravdu sloužit jako platidlo. Jedna z prvních firem, která začala přijímat Bitcoin byla WordPress (redakční publikační systém), která byla následovaná dalšíma. Objevily se první restaurace, lékaři, právníci a dokonce i taxi služby, kde bylo možné Bitcoiny platit. V neposlední řadě bylo nabízeno elektronické zboží, zejména software nebo online předplatné. Po rekordní ceně z roku 2013 ve výši 1163 dolarů se cena stabilizovala mezi 800 a 900 dolary. V únoru 2014 však přišla velká krize spojená s burzou Mt.Gox, která zprostředkovávala skoro tři čtvrtiny všech obchodů s bitcoiny a stala se synonymem k Bitcoinu. Burza přestala vyplácet peníze a zbankrotovala. Cena Bitcoinu postupně klesala až k 340 dolarům. Ve stejném roce prohlásil britský úřad pro výběr daní a cel Bitcoiny za soukromé aktivum, ze kterého není nutné platit daň z přidané hodnoty, zatímco v Americe přišly první návrhy na skutečné regulace virtuálních měn. [1] Rok 2015 byl rok klidu, kdy se cena neměnila tak dramaticky a kdy měli Bitcoin a jeho vývojáři a uživatelé možnost vybudovat potřebnou infrastrukturu. Mezitím přibyly další firmy jako Dell, T-Mobile nebo Twitch (streamovací služba), které začaly Bitcoin používat. Cena se pohybovala od 150 do 450 dolarů. V následujících dvou letech 2016-2017 Bitcoin rostl cenou i popularitou. Další firmy začaly Bitcoin přijímat, a to i české. V česku byla jako první Alza. Japonská vláda kryptoměny uznala za aktivum, norské banky poskytly uživatelům bitcoinové účty a o spolupráci s kryptoměnami začala uvažovat i ruská vláda. Na konci roku 2017 byla cena jednoho bitcoinu 19 783 dolarů, kdy se mluvilo o další cenové bublině jako v roce 2011. Během následujícího roku 2018 (po 19 dnech od rekordu) spadla cena na 6 200 dolarů. V roce 2020 Bitcoin posílila i aktuální pandemická situace, kdy lidé investovali také do zlata, které svou cenu také zvýšilo. Ostatně jako vždy, když nastane krize. Další prudký nárůst byl zapříčiněn zprávou Elona Muska, ve které oznámil investici skrz firmu Tesla ve výši 1,5 miliardy dolarů, což zapříčinilo růst až k 44 200 dolarům. Poté oznámil, že těžba Bitcoinu je neekologická a část odprodal, což mělo za následek pokles ceny Bitcoinu až o třetinu. Dodnes byla nejvyšší cena Bitcoinu zaznamenána 8.11.2021 a činila 67 527 dolarů. Následující graf zachycuje cenu Bitcoinu vzhledem k americkému dolaru od konce roku 2010.



Obrázek 2 - Cena Bitcoinu

Co se týče ostatních kryptoměn a jejich růstu, jsou na tom velmi podobně a křivky mají skoro stejný tvar se stejnou amplitudou na přelomu roku 2017 a 2018. To s největší pravděpodobností vypovídá o davovém šílenství ohledně cenové bubliny samotného Bitcoinu, kdy si v té době každý myslel, že Bitcoin a tím pádem i ostatní kryptoměny jsou jakýsi investiční zázrak. Postupem času byla cena neudržitelná a některé z kryptoměn se dostaly prakticky na nulu což mělo za následek masivní ztrátu vložených peněz.

2.2 Trh s kryptoměnami

V úvodu práce jsme si řekli, jak si kryptoměny pořídit. Mezi nejjednodušší způsoby patří již zmíněné směnárny, online platformy, fyzický nákup nebo kryptoměnové bankomaty. Nevýhodou těchto způsobů nákupu je čas uskutečnění transakce, vysoké poplatky nebo potřeba být fyzicky jinde, než u svého počítače. Kryptoměnové burzy tento problém řeší nejlépe ze všech zmiňovaných způsobů a pro jejich obchodování jsou nejvhodnější. Trader (člověk, který obchoduje na burze) potřebuje uskutečnit transakci ideálně ihned po zadání obchodu kvůli kolísání ceny a za co nejmenší poplatky. K tomu slouží právě kryptoměnové burzy, kterých je na světě již více něž 300. [24]

Burzy kryptoměn fungují stejně jako komoditní burzy, kdy se nabídka a poptávka střetnou a vzniká kurz. Kurz má navíc tendenci se ustálit i mezi ostatními burzami díky arbitráži (obchodování napříč burzami). Pokud je tedy člověk přesvědčen, že celé problematice

kryptoměn dostatečně rozumí a chce je využít jako investiční nástroj, zbývá mu už jen otevřít si účet na jedné z mnoha burz, které obchodují s kryptoměnami.

Před samotným výběrem burzy je vhodné zjistit si základní informace o burze. Některé burzy nepodporují evropský trh, proto je nutné ověřit, zda je Česká republika mezi podporovanými zeměmi. Výhodou také je, když burza podporuje převod z Korun českých na Bitcoin nebo jinou kryptoměnu, společně s možností volby platebního styku. Vždy je pohodlnější zaplatit kartou, popřípadě převodem nebo rovnou kryptoměnou, se kterou chci obchodovat. Důležitým faktorem jsou poplatky, které jsou většinou v rozmezí 0,1 - 0,5 % za obchod, ale mohou být i vyšší. Dalším relevantním faktorem je to, jak moc je burza používaná mezi ostatními uživateli. Čím více uživatelů burzu využívá, tím je důvěryhodnější a strávíte méně času při uskutečnění jednotlivých obchodů. Samotný obchod je pak založený na kryptoměnách, které burza obchoduje, proto není od věci, aby burza obchodovala s co nejvíce kryptoměnami pro větší volnost při výběru oné konkrétní. V neposlední řadě hraje obří roli zabezpečení, které se dá jednoduše ověřit v prohlížeči, a to tak, že je web na zabezpečeném protokolu HTTPS. Signalizuje ho logo uzavřeného zámku vedle vyhledávací adresy. Vhodná je také Dvoufaktorová autentizace (2FA), která kromě uživatelského jména a hesla vyžaduje také ověření přes SMS nebo e-mail. Všechny tyto informace je možné si zjistit v jakémkoli online srovnávači a finálně vybrat individuálně nejlepší možnost. Pro lepší přehled přikládám nejpoužívanější burzy s kryptoměnami a jejich parametry roku 2021.

	BINANCE		POLONIEX	coinbase	CEX.IO
	1. Místo	**Sdílené 2. Místo**	**Sdílené 2. Místo**	**Finalista**	**Finalista**
Finální hodnocení	**8.7**	**7.4**	**7.4**	**7**	**6.8**
Poplatky					
Poplatky za obchodování Maker/Taker	0,1%/0,1%	0,025%/0,075%	0,125%/0,125%	Neuvádí	0,16%/0,25%
Poplatek za vklad	Neplatí se	Neplatí se	Neplatí se	Neplatí se	Neplatí se
Poplatek za výběr	Platí se	Neplatí se	Platí se	Neplatí se	Platí se
Podporované kryptoměny					
Bitcoin	✓	✓	✓	✓	✓
Ethereum	✓	✓	✓	✓	✓
Litecoin	✓	✓	✓	✓	✓
Monero	✓	✓	✓	✓	✗
Ripple	✓	✓	✓	✗	✓
IOTA (MIOTA)	✓	✗	✗	✓	✗
Dash	✓	✓	✓	✗	✓
Platební možnosti					
Bankovní převod	✗	✗	✗	✓	✓
Platební karta	✓	✗	✗	✓	✓
Hotovost	✓	✗	✗	✗	✗
Bitcoin	✓	✓	✓	✓	✓
Litecoin	✓	✗	✓	✓	✓
Ethereum	✓	✗	✓	✓	✓
Zabezpečení					
HTTPS	✓	✓	✓	✓	✓
Dvoufaktorová autentizace	✓	✓	✓	✓	✓
Speciální parametry					
Short sell	✓	✓	✓	✓	✓
Swap	✓	✓	✗	✗	✗
Future contracts	✓	✓	✓	✗	✓

Obrázek 3 - Burzy kryptoměn [zdroj 18]

2.3 Algoritmus na štěstí

Tato pod kapitola je vypracovaná podle zdroje [1]. Vývoj ceny kryptoměn se zdá být nepředvídatelný, ale jsou zde lidé, kteří věří, že tomu tak není, a věnují se tzv. algoritmickému obchodování. Je to další způsob, jak pohlížet na kryptoměny jako na investiční instrument. Tito lidé se snaží vyzrát nad kolísáním ceny díky počítačovému programu, který za ně obchoduje. Jedná se o plně automatizovaný nákup a prodej využívaný i na ostatních burzách. Algoritmus predikuje budoucí cenu a následně prodává nebo kupuje. V praxi se algoritmy různí v závislosti

na krátkodobých, střednědobých a dlouhodobých predikcích, kdy každý z nich se zaměřuje na jiná data a jinak je hodnotí.

Pro laika je tento způsob výdělku náročnější varianta, jelikož se algoritmus (program) nedá jednoduše stáhnout. Zájemce o algoritmické programování musí ovládat alespoň základní znalosti IT světa nebo znát člověka, který je kvalifikovaný. Existuje pomůcka zvaná XChange, která umožňuje po zadání požadovaných parametrů automatické obchodování. Další možnost je služba cryptotrader.org, která za měsíční poplatky nabízí své know-how na poli algoritmického obchodování a slibuje velké výdělky. Ani tato možnost ovšem není bez rizika, důkazem je například firma Knight Capital, která díky malé chybě v programu přišla přes noc o tři čtvrtě svého miliardového majetku.

2.4 Hodnota kryptoměn a predikce ceny

Existují dva základní přístupy, jak analyzovat cenné papíry, jejich deriváty nebo komodity. Buďto pomocí fundamentální analýzy nebo technické analýzy. Základem fundamentální analýzy je stanovení vnitřní hodnoty cenného papíru, např. akcie. Akcie nebo jiný cenný papír může mít rozdílnou hodnotu a cenu, za kterou se obchoduje. To znamená, že cenný papír může být nadhodnocený, podhodnocený nebo správně oceněný. Vnitřní hodnota může být definována jako imaginární hodnota, která je nezávislá na tržním kurzu cenného papíru. Představuje jakousi správnou cenu, za jakou by se měla na trhu obchodovat. Vnitřní hodnota, např. akcie, je závislá na kvalitě vedení a managementu firmy, technickými a psychologickými faktory, ale také stupněm efektivnosti trhu. Výpočet vnitřní hodnoty lze provádět pomocí mnoha výpočetních modelů, které mají různou přesnost v závislosti na zadaných datech. Kupříkladu *Dividendový diskontní model* pracuje s výší dividend a požadovanou mírou výnosnosti v jednotlivých letech

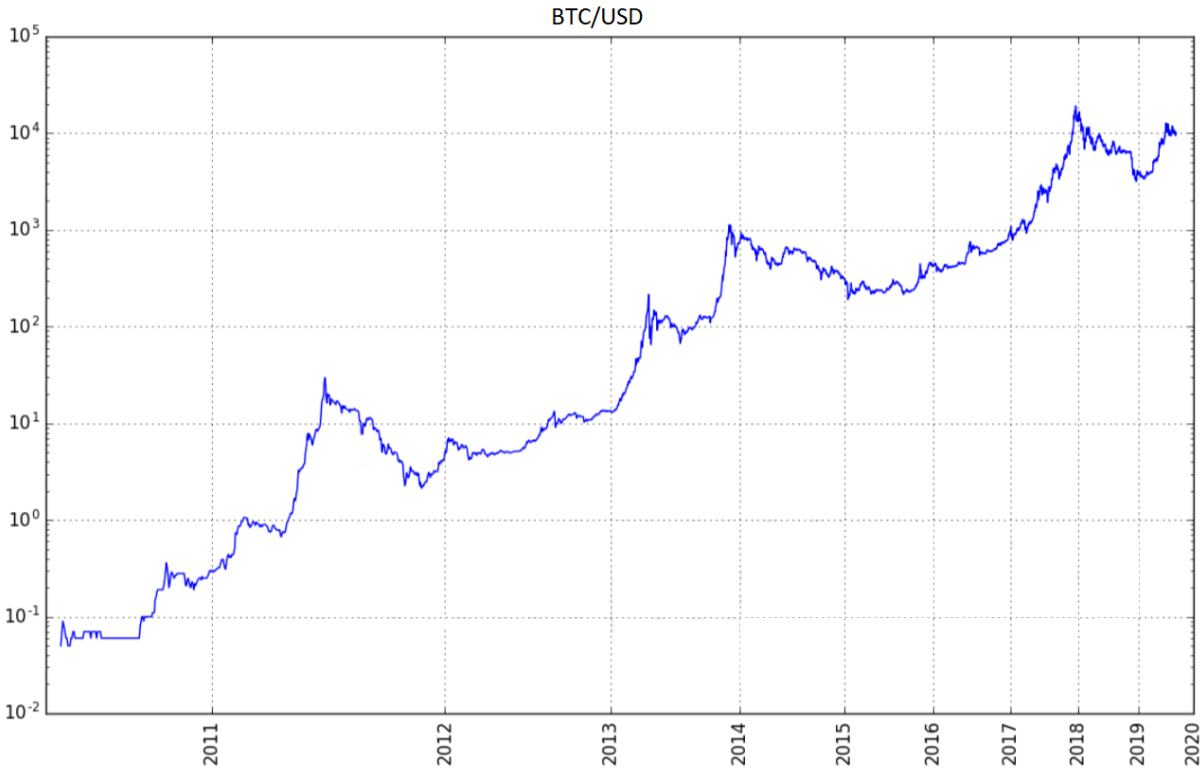
$$VH = \frac{D_1}{1+i} + \frac{D_2}{(1+i)^2} + \cdots + \frac{D_n + P_n}{(1+i)^n},$$

kde D_n jsou vyplacené dividendy diskontované o požadovanou míru výnosnosti a P_n je prodejní cena akcie rovněž diskontovaná stejným způsobem. Ziskové modely zase pracují s čistými zisky připadající na jednu akcii, *Cash flow model* s hotovostními toky a *Bilanční model* s rozvahami akciových společností. Podobně se měří výkonnosti investičních fondů apod. Kryptoměny takto ovšem nefungují a zmíněné údaje bychom hledali těžko. Proto jsme odkázáni

na technickou analýzu, která využívá časové řady a do jisté míry odhad na základě předešlých zkušeností.

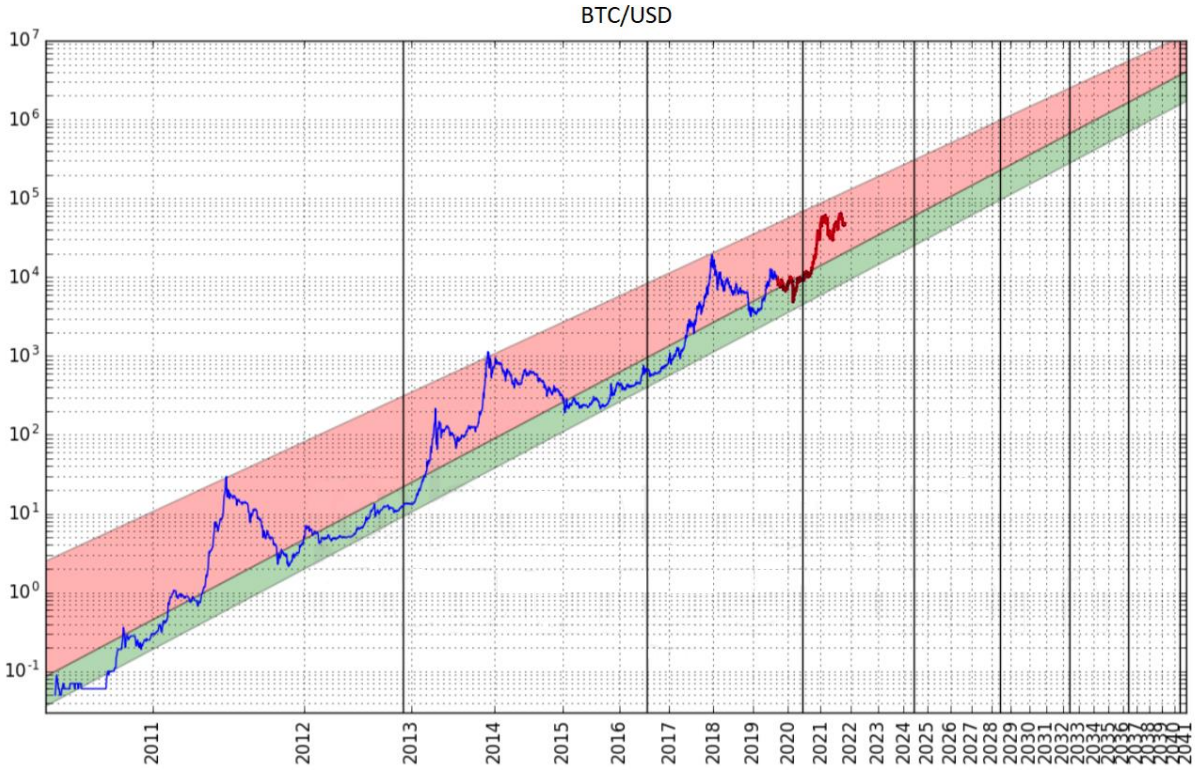
Technická analýza je způsob vyhodnocování a předpovídání cenových pohybů, který se opírá čistě o údaje vytvořené trhem. Na rozdíl od fundamentální analýzy, která se zaměřuje na analýzu finančních výkazů, makroekonomických dat, politických událostí apod., se technická analýza soustředí pouze na to, co je vidět v grafu. Tedy historický růst ceny, obchodované objemy, příchozí objednávky, tržní korelace nebo průběhy různých indikátorů atd. Technický analytik tedy vychází z předpokladu, že všechny kurzotvorné informace jsou již nějakým způsobem odraženy v ceně a nezabývá se dalšími faktory, které mohou, ale taky nemusí mít vliv na její budoucí vývoj.

Následující dlouhodobá predikce je sestavena doktorem Harold Christopher Burgerem, který se v roce 2019 zabýval vývojem ceny Bitcoinu. [6] Tuto predikci jsem vybral, protože pracuje pouze s daty, které zobrazují cenu Bitcoinu a ignoruje vnější vlivy. Jeho predikce počítá s teoreticky nekonečným růstem, což není možné, ale od zveřejnění mu predikce vychází a zdá se, že jeho surová predikce může fungovat ještě nějakou dobu (na obrázku č. 5 vyznačené červeně). Predikce s názvem *Bitcoin's natural long-term power-law corridor of growth* je založena na zlogaritmování os, což má za následek linearizaci grafu, a tím pádem pohodlnější technickou analýzu. Predikce vychází z následujícího grafu (obrázek 4), který pracuje pouze s cenou Bitcoinu v dolarech na zlogaritmovaných osách.



Obrázek 4 - Výboj ceny BTC do září 2019 (log. osy) [zdroj 6]

K predikci použije dva pásy, které odděluje trendová přímka získaná lineární regresí dat od poloviny roku 2010 po září 2019. První hranici pásu získal posunutím lineárního trendu dolů beze změny sklonu, a tím našel podpůrnou přímku, která se opírá o hodnoty v roce 2015. V roce 2010 je cena pod touto přímkou, ale v té době byl celý trh v plenkách a tento nedostatek ignoroval. Další hranici získal pomocí lineární regrese pouze tří amplitud v letech 2011, 2013 a 2017, které leží v těsné blízkosti jejich trendové přímky. Sklon tohoto trendu je nepatrně nižší, než sklon samotného trendu. To může naznačovat slábnutí cenových bublin. Poté osy prodloužil a dostal následující graf.



Obrázek 5 - Pásy pro predikci ceny BTC [zdroj 6]

Graf můžeme rozdělit do dvou pásem, jedno odpovídá „normálnímu“ režimu (zelenému) a druhé odpovídá režimu cenových bublin (červené). Cena strávila polovinu času v dolním pásmu „normálního režimu“ a polovinu času v cenových bublinách. Predikce pracuje pouze s cenami Bitcoinu do září 2019, kdy ji autor zveřejnil. Data od září 2019 (vyznačené červeně na obrázku 5) jsem doplnil pro srovnání.

Vzhledem k šířce pásem budou intervaly, ve kterých se budeme snažit ceny predikovat, relativně velké. Model ovšem předpokládá pokračující, ale zpomalující růst ceny a zároveň sníženou, ale stále velkou volatilitu v budoucnu. Předpovídá, že cena nedosáhne 100 000 $ do roku 2021, ale také předpovídá, že cena nebude nižší než 100 000 $ od roku 2028. Předpovídá, že cena nedosáhne 1 000 000 $ před rokem 2028, ale také, že pod tuto hranici neklesne po roce 2037. Nutno dodat, že model nepočítá s žádnými vnějšími zásahy jako třeba snahy států o regulaci, zákaz používání kryptoměn nebo budoucí vývoj samotné poptávky. Tato predikce je pouze orientační.

Při studiu fundamentální analýzy Bitcoinu jsem se setkal s obrovským množstvím nejrůznějších predikcí a modelů. Rozhodl jsem se zde zmínit pouze jednu výše uvedenou predikci, jelikož dobře odpovídá budoucím cenám Bitcoinu. Vzhledem k širokým pásmům, ve kterých autor předpokládá, že se ceny budou pohybovat, bych odhad označil za přijatelný.

Faktem ale je, že cenu Bitcoinu a všech kryptoměn ovlivňuje příliš mnoho faktorů od monetární politiky států, přes regulace, až po výroky slavných osobností na sociálních sítích. Vytvořit přesnou predikci na déle než měsíc, je velmi obtížné.

2.5 Srovnání s ostatními možnostmi investic

Pokud se rozhodneme investovat své volné finanční prostředky, je vhodné důkladně si promyslet, kam peníze vložit a jakou investiční strategii použít. Ať už se rozhodneme pro banku, podílový fond nebo se rozhodneme koupit si zlatou cihlu, je důležité zvážit, jak dané investici rozumím a jaká nese rizika. K takovému posouzení slouží tzv. magický trojúhelník, který zohledňuje očekávaný výnos investice, očekáváné riziko investice a očekávanou likviditu. Cílem investora je najít takovou investici, která maximalizuje výnos, má nízké riziko a je vysoce likvidní. Jelikož jdou tyto faktory proti sobě, musí investor některý z nich preferovat. Podle toho, který preferuje, se pak řadí do některého z typů investičních strategií. Mezi ně patří *Strategie maximalizace ročních výnosů, Strategie růstu ceny investice, Agresivní strategie investic, Konzervativní strategie* apod. Proto je na místě, aby si investor rozmyslel, jak velké riziko je ochoten podstoupit v závislosti na výnosu a jak dlouho je ochoten peníze zhodnocovat. [2]

V následujícím textu srovnám konvenční možnosti investic s kryptoměnami. Všechna data jsem čerpal z internetu na stránkách jednotlivých podílových fondů. Zdroje jsou uvedené pod každým srovnáním.

Jak jsem již zmínil, porovnání provedu na základě průměrné roční výnosnosti, rizikovosti a likvidity. První zmíněné kritérium pro volbu investice je roční výnosnost. U podílových fondů jsem jako roční zhodnocení použil vzorec

$$V = \frac{\check{C}HA_t - \check{C}HA_{t-1}}{\check{C}HA_{t-1}},$$

kde V značí výkonnost portfolia fondu, $\check{C}HA_t$ je čistá hodnota aktiv fondu na konci t-tého období a $\check{C}HA_{t-1}$ je čistá hodnota aktiv na začátku t-tého období. O něco komplikovanější je samotná investice do akcií. Tady jsem se rozhodl použít jako ukazatel výnosnosti index S&P 500, který zahrnuje 500 největších podniků obchodovaných na burze v USA. Akcie obsažené v indexu jsou váženy podle tržní kapitalizace na trhu, a tím pádem mají akcie větších firem i

větší vliv na hodnotu samotného indexu. Pro představu, kdybychom koupili všech 500 akcií obsažených v indexu S&P 500 v poměrném zastoupení jejich tržní kapitalizace na trhu, přesně bychom kopírovali tento index, a tím i zhodnocení vloženého kapitálu. Tento index patří mezi hlavní ukazatele vývoje akcií a je jedním z nejdůležitějších akciových indexů na světě. Stejně budu postupovat i u indexu NASDAQ 100, který je složený ze 102 největších nefinančních společnostní obchodovaných v USA (není podmínkou). Výnosnost u komodit a kryptoměn budu měřit na základě jejich tržní ceny, tedy stejně jako u portfolia fondů, ale místo čisté hodnoty aktiv použiji jejich tržní cenu.

Rizikovost investice vyjádřím volatilitou jednotlivých výnosností investic v čase. Tedy jejich směrodatnou odchylkou. Ke každému typu investice se pojí trochu jiné riziko. Podílové fondy jsou náchylné na kreditní riziko. Rozumí se jím riziko zhoršení finanční situace firem, které mají v portfoliu. Záleží pak na typu fondu. Většinou jsou fondy akciové, dluhopisové nebo kombinace těchto dvou. U akcií převládá tržní riziko a u komodit riziko komoditní. Kryptoměny jsou ohroženy zejména velkou kolísavostí ceny, volatilitou. Vzhledem ke komplexnosti problematiky si dovolím použít pouze vzorec pro výběrovou (neznám střední hodnotu) směrodatnou odchylku výnosností jednotlivých investic

$$s = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2},$$

kde s je výběrová směrodatná odchylka, N je počet let a x_i je výnosnost v i-tém roce referenčního data.

Posledním kritériem je likvidita. Udává, jak rychle mohu z investičního instrumentu získat hotovost. U podílových fondů je likvidita v ČR ze zákona 30 dní. Často však bývá vyplacení rychlejší díky velikosti trhu a ochoty podílový list odkoupit jiným investorem. Akcie jsou vázány na burzy, kde se obchodují. Burzy jsou omezené svou provozní dobou, která je většinou jen ve všední dny a v určitý čas. Obchody mimo provozní dobu jsou zpoplatněny. Připsaný kapitál z prodeje je umístěn na investiční účet, který je navíc nutné převést na účet běžný (likvidní). Řádově tak může proces trvat i několik dní (záleží na okolnostech). Likvidita u komodit a kryptoměn závisí na aktivitě trhu, kde se obchodují. Pokud je na trhu vysoká nabídka a poptávka, je trh likvidní a převod komodit nebo kryptoměn může být otázkou pár hodin až minut. V praktické části uvedu orientační počet dní, které jsou potřeba k převedení investičního instrumentu na peníze.

Celkové srovnání provedu na základě průběžného investování na měsíční bázi za posledních 10 let. Fiktivně budu tedy ukládat a zhodnocovat každý měsíc 1000 Kč ve fondech, které považuji za nejvýkonnější, úročit procentem růstu akciových indexů a procentem růstu tržní ceny komodit a kryptoměn. K výpočtu použiji vzorec

$$PV = d \cdot \sum_{k=1}^{n} \prod_{j=k}^{n} (1 + i_j),$$

kde PV znázorňuje celkovou naspořenou částku, d je vklad v každém období snížený o poplatek a i_j bude výkonnost u fondů, procentní nárůst akciových indexů a procentní nárůst tržní ceny komodit a kryptoměn v j-tém měsíci. Počet měsíců v 10 letech je $n = 10 \cdot 12 = 120$, ale poslední měsíc jsem vynechal, jelikož průzkum dělám v prosinci 2021. Jako $j = 1$, tedy první měsíc, označím leden roku 2012. Postupně půjdu až k $j = n$, kde $n = 119$, tedy listopad 2021.

Oblíbenou formou investice jsou podílové fondy díky vyšší výnosnosti a nenáročnosti. Princip spočívá v tom, že si investor zvolí fond, do kterého vloží své peníze a o více se nestará. Podílové fondy, kde ostatní vkládají své peníze, pak řídí zkušení investoři (investiční společnosti), kteří peníze zhodnocují na finančním trhu. Volba fondu je na vás a vy si tak můžete vybrat mezi akciovými, dluhopisovými, nemovitostními, komoditními fondy nebo jejich kombinací, a dokonce si můžete vybrat i fondy fondů, které investují do dalších fondů.

Každý je charakteristický právě tím, s čím obchoduje, proto je důležité se neřídit jen výnosem. Podle strategie se pak fondy dělí na konzervativní, vyvážené a dynamické. Konzervativní fondy působí spíše na peněžním trhu a jejich portfolio je složené ze státních pokladničních poukázek, krátkodobých dluhopisů apod. Vhodné jsou pro uložení peněz za účelem ochrany kapitálu proti znehodnocení vlivem inflace. Vyvážené podílové fondy nabízejí smíšené investice do dluhopisů, akcií nebo nemovitostí, což je o něco rizikovější volba, ale výnos je zpravidla vyšší. Zhodnocení závisí na velkém množství faktorů jako volba konkrétního fondu, situací na trhu a schopnostech investorů, které fond zhodnocují. Dynamické investiční fondy pak investují ve větší míře do akcií a rizikovějších volatilních cenných papírů, kde je dlouhodobý investiční horizont a zároveň větší riziko. Pokud je člověk ochoten přijmout větší riziko a svých peněz se vzdát na delší dobu, může dosáhnout výrazně vyšších výnosů, něž u předchozích dvou typů fondů. Nastat může ovšem i situace, kdy je zhodnocení i několikanásobně vyšší nebo nižší, než jsou naše předpoklady.

Nedílnou součástí fondů jsou poplatky, které je potřeba platit, jelikož se jedná o službu v podobě správy a zhodnocení majetku. Poplatky můžeme rozdělit na vstupní (popřípadě i výstupní), které přímo ovlivňují výši zhodnocení, a správcovské, které jsou již započítány v cenách podílových listů a tím pádem i ve výkonnosti fondu. Vstupní poplatek je určen procentem, které inkasuje správce fondu, obchodník s cennými papíry nebo banka. Tento poplatek motivuje investora k dlouhodobějšímu setrvání (investování) ve fondu a zároveň slouží jako odměna distributorovi. Výstupní poplatek je dnes spíše raritou, ale může se vyskytovat třeba u nemovitostních fondů, aby investora odradili od předčasného výběru prostředků. Správcovský poplatek (někdy také manažerský) je odečten průběžně z majetku fondu a neplatí ho tak přímo investor. Je určen procentem z objemu spravovaného kapitálu za rok. Dalšími náklady mohou být náklady na depozitáře, auditora nebo transakční poplatky a daně. V součtu pak tyto poplatky tvoří koeficient TER (total expense ratio), který je rozhodující pro investora, jelikož se snižujícími se celkovými náklady je výkonnost fondu zpravidla vyšší a vypovídá o jakémsi hospodaření jednotlivých fondů. TER je zahrnut v cenách podílových listů, a proto není potřeba ho zahrnout do výpočtu pro zhodnocení. TER nezahrnuje vstupní poplatek. Český název pro TER je *Celková roční nákladovost fondu* a ze zákona je fond povinen jej zveřejňovat v dokumentu s názvem *Klíčové informace pro investory (KIID)*. Můžeme ho označit jako ekvivalent k RPSN u půjček. Za zmínku stojí i fakt, že u rizikovějších fondů je TER vyšší kvůli nutnosti časté alokace aktiv v portfoliu.

Všechny hodnoty jsou vybrány z desetiletého průměru výkonnosti fondů, o kterých si myslím, že jsou na trhu stabilní a zastupují je kvalitní banky nebo investiční společnosti. Prvotní srovnání je pouze na roční bázi, abych vyřadil méně výkonné fondy a celkové srovnání prováděl pouze na fondech s vyšším potenciálem. Konkrétně jsem vybral osm podílových fondů. Dva konzervativní, dva vyvážené a čtyři dynamické. První z nich je KBC Master Fund ČSOB Konzervativní, který má ve svém portfoliu 10,34 % akcií, 65,75 % dluhopisů a zbytek má v depozitech a peněžním trhu. Za posledních 10 let je průměrná roční výkonnost fondu 1,77 % s výběrovu směrodatnou odchylkou 2,55 procentního bodu. Druhý konzervativní fond je Fond konzervativní, Generali Investments CEE. Fond investuje převážně do termínovaných vkladů u důvěryhodných bank, státních dluhopisů a do bonitních firemních dluhopisů. Očekávaná míra zhodnocení by se měla pohybovat nad úrovní běžných bankovních spořicích produktů. Výkonnost tomu odpovídá a průměrná roční výkonnost za 10 let se rovná 1,22 % s výběrovou směrodatnou odchylkou 1,23 procentního bodu. Jelikož se výkonnost konzervativních fondů nemůže rovnat výkonnosti ostatních fondů, ve finálním srovnání fondy vynechám. Je ovšem dobré zmínit, že jsou vhodné pro investora s averzí k riziku, a tímto způsobem alespoň trochu

minimalizuje ztráty způsobené vlivem inflace. Osobně si myslím, že je tato možnost lepší, než mít peníze v bance na spořícím účtu, termínovaných vkladech apod. [9],[11]

O něco zajímavější jsou vyvážené fondy, které jsou tažené převážně dluhopisy a akciemi. Jako první z těchto fondů jsem zvolil KBC Master Fund ČSOB Vyvážený, zde je průměrná roční výkonnost 3,76 % s výběrovou směrodatnou odchylkou 4,88 procentního bodu. Premium Balanced Fund, Generali Invest CEE je druhý vyvážený fond s průměrnou roční výkonností 2,06 % za 7 let s výběrovou směrodatnou odchylkou 4,1 procentního bodu. Tyto dvě varianty jsou o něco rizikovější díky svému složení portfolia, ve kterém sice převládají dluhopisy, ale velkou část zastupují akcie. Ani tyto fondy ale nezahrnu do srovnání kvůli malé výkonnosti a relativně vysoké volatilitě. [10],[12]

Dynamickým fondům jsem dal největší prostor a porovnával jsem mezi čtyřmi fondy. První z nich je KBC Master Fund ČSOB Dynamický, který je z 80 % tvořen akciemi. Jeho průměrná roční výkonnost je 7,07 % za 10 let s výběrovou směrodatnou odchylkou 9,54 procentního bodu. Další je Amundi CR All Star Selection s průměrnou roční výkonností 4,74 % za 6 let s výběrovou směrodatnou odchylkou 9,55 procentního bodu. Jako nejlepší fond bych označil J&T OPPORTUNITY CZK OPF, který investuje do akcií a jeho průměrná výkonnost je 9,02 % s výběrovou směrodatnou odchylkou 7,2 procentního bodu. Zde je průměrná výkonnost větší než směrodatná odchylka, a může se tak zdát jako výnosnější a méně rizikový. To může svědčit dobrému řízení portfolia, a tedy větší jistotě. Průměrná měsíční výkonnost za sledované období (průměr z 119 měsíců) je 0,81 %, přičemž před covidovou krizí (do února 2020 včetně) byla průměrná měsíční výkonnost 0,48 % (průměr z 99 měsíců) a poté (od března 2020 včetně) byla průměrná měsíční výkonnost 2,33 % (průměr z 20 měsíců).

Tento skoro pětinásobný nárůst výkonnosti si vysvětluji náhlým poklesem globálního trhu a následnou stimulací ekonomiky v podobě nízkých úrokových sazeb centrálních bank, které zapříčinily zvýšení celkového oběhu peněz v ekonomice. Vzhledem k většímu objemu peněz lidé investují přebytečné peníze právě do cenných papírů, a tím pádem roste jejich cena. Ve výsledku se pak fondům zvyšuje čistá hodnota aktiv, a s ní i cena podílových listů. Dle mého budeme brzy svědky opačné situace, kdy nedostatek peněz v ekonomice napříč státy (vlivem zvyšování úrokových sazeb) donutí investory prodávat cenné papíry, a dojde k snížení cen těchto cenných papírů spolu s cenami podílových listů jednotlivých fondů.

Poslední zmíněný fond vyberu pro výsledné srovnání. Vzhledem k povaze výpočtu naspořené částky, kterou budu porovnávat, jsem se rozhodl doplnit srovnání ještě o jeden dynamický fond, a to kvůli vyšší výkonnosti v prvních letech pozorování. Je to fond NN (L) Global Equity Impact Opportunit, který má průměrnou roční výkonnost 8,69 % s výběrovou

směrodatnou odchylkou 10,63 procentního bodu. Průměrná měsíční výkonnost za sledované období je 1,21 % (průměr ze 119 měsíců), přičemž před covidovou krizí (do února 2020 včetně) byla průměrná měsíční výkonnost 0,99 % (průměr z 99 měsíců) a poté (od března 2020 včetně) byla průměrná měsíční výkonnost 2,22 % (průměr z 20 měsíců). I tento nárůst byl zřejmě zapříčiněn ze stejného důvodu jako fond předchozí. Všechna data jsou v Excelovém souboru s názvem *Srovnání investic.xlsx* umístěné na listu s názvem *Podílové fondy* v tabulce *Výkonnost v letech* a v tabulkách s měsíční výkonností dvou srovnávaných fondů. [3],[8],[15],[19]

Výsledné srovnání je tedy následující. Fond J&T OPPORTUNITY CZK OPF zhodnotil vklad 119 000 Kč na 208 281,42 Kč za necelých 10 letech (o 75,03 %). Tento fond účtuje investorům 5% vstupní poplatek, který se strhne z vkladu. Celková roční nákladovost (TER) je 2,36 % (tento náklad je již zahrnut v ceně podílového listu a nemá vliv na zhodnocení vložené částky). Fond NN (L) Global Equity Impact Opportunit zhodnotil vklad 119 000 Kč na 253 288,40 Kč za necelých 10 let (o 112,85%). Tento fond účtuje opět 5% vstupní poplatek a jeho celková roční nákladovost (TER) je 2,31 %. Všechna data jsou v Excelovém souboru s názvem *Srovnání investic.xlsx* umístěné na listu s názvem *Podílové fondy* v tabulkách *Průběžné investování*.

Pro náročnější investory je zde možnost investice do akcií. Pro tuto možnost se může rozhodnout v ideálním případě jen člověk dostatečně obeznámený s celou problematikou a vůlí studovat firmy, které akcie vydaly a aktuální stav ekonomiky, se kterou firmy interagují. Jako vlastník akcií pak sami nesete rizika související s poklesem jejich tržní hodnoty, ale také můžete inkasovat nemalé zisky. S některými akciemi je spojeno právo na dividendy, což je nárok na určitý podíl ze zisku firmy.

Ani u akcií se nevyhneme poplatkům, které náleží zprostředkovateli obchodů s akciemi neboli brookerovi. Služby brookerů jsou o poznání levnější něž u podílových fondů, jelikož jejich práce je pouze zprostředkování obchodu mezi investorem a burzou. Někteří z nich zprostředkovávají obchod s více cennými papíry, které jsou nákladovější a konkrétně u akcií jsou poplatky malé. Poplatky se pohybují řádově v desetinách procenta. Z internetového srovnávače jsem vybral brookera, který byl vyhodnocen jako nejlepší brooker v roce 2021 s poplatkem 0,08 % z objemu každé transakce (nákupu). [23]

Jak ale vybrat akcie, do kterých investovat? Pomoct by mohly akciové indexy, které ukazují, jakým směrem se určité akcie pohybují. Pro své srovnání jsem použil index S&P 500, který dosahuje ročního průměrného růstu 13,84 % za 10 let s výběrvou směrodatnou odchylkou 9,95 procentního bodu a index NASDAQ 100, který za stejné období dosahuje průměrného růstu 21,19 % s výběrovou směrodatnou odchylkou 14,11 procentního bodu. Všechna data jsou

v Excelovém souboru s názvem *Srovnání investic.xlsx* umístěné na listu s názvem *Akciové indexy* v tabulce *Nárůst indexu v konkrétních letech*. [14]

Uvedené hodnoty neznamenají zhodnocení, ale jen jakýsi obecný růst trhu v konkrétních oblastech. Investorovi dává pouze přehled nad aktuální situací, kdy může a nemusí se jím řídit. Ve výsledku si musí vybrat mezi velkým množstvím akcií, které nabízejí, a každá z nich může nabízet růst odlišný od indexového růstu. Vzhledem k povaze problematiky bych začínajícímu investorovi doporučil svěřit svůj kapitál profesionálovi a to v podobě fondů popsaných výše, které mohou být zaměřeny právě na akcie obsažené v indexu. I zde můžeme pozorovat vliv covidové krize. Před začátkem covidové krize byl průměrný měsíční růst indexu S&P 500 0,79 % (průměr z 99 měsíců), od té doby je 2,9 % (průměr za 20 měsíců) a 1,13 % za celé sledované období (průměr za 119 měsíců). Průměrný měsíční růst indexu NASDAQ 100 před začátkem krize byl 1,27 % (průměr z 99 měsíců), poté 3,57 % (průměr za 20 měsíců) a 1,67 % za celé sledované období (průměr za 119 měsíců). Orientačně pak bude srovnání vypadat takto. Index S&P 500 by v poměrném zastoupení všech akcií podle tržní kapitalizace zhodnotil vklad 119 000 Kč na 245 128,7 Kč za necelých 10 let (o 105,99 %). Index NASDAQ 100 by stejný vklad zhodnotil za stejnou dobu na 380 447,33 Kč (o 219,7 %). U obou indexů jsem použil poplatek 0,08 % z transakce. Všechna data jsou v Excelovém souboru s názvem *Srovnání investic.xlsx* umístěné na listu s názvem *Akciové indexy* v tabulkách *Průběžné investování*.

V neposlední řadě je zde možnost investice do komodit, jako je zlato, stříbro, ropa atd. Cena zlata zaznamenala poměrně strmý růst v době pandemie. To je běžný úkaz během krizí, jelikož se zlato považuje jako dobrý uchovatel hodnoty. Na druhou stranu se ale ukazuje, že se ekonomika zotavuje a nasvědčuje to i pokles ceny zlata na původní hodnotu před pandemií. Zlato se považuje za dobrý uchovatel hodnoty, a proto průměrný roční nárůst ceny je jen 1,15 % s výběrovou směrodatnou odchylkou 14,33 procentního bodu. U stříbra je to podobné a průměrný roční růst je -1,65 % s výběrovou směrodatnou odchylkou 24,16 procentního bodu. Ropa je na tom skoro stejně jako zlato a její průměrný roční růst ceny je 1,23 % s výběrovou směrodatnou odchylkou 31,09 procentního bodu. I zde mohu pozorovat vliv koronavirové krize, kdy před krizí byl průměrný růst ceny zlata 0 % za měsíc (průměr z 99 měsíců), po začátku krize 0,56 % (průměr z 20 měsíců) a 0,1 % za celé období (průměr z 119 měsíců). U stříbra je průměrný růst ceny před krizí -0,62 % za měsíc (průměr z 99 měsíců) a po začátku krize 2,56 % (průměr z 20 měsíců) a -0,06 % za celé období (průměr z 119 měsíců). U ropy je průměrný růst ceny před krizí -0,97 % za měsíc (průměr z 99 měsíců) a po začátku krize 7,61 % (průměr z 20 měsíců) a 0,54 % za celé období (průměr z 119 měsíců). Komodity jsou

náročnější investiční instrument, kdy je potřeba sledovat dění ve světě a podle toho volit investiční strategii. Komodity bych doporučil jen zkušeným investorům, kteří umí využít situace na trhu. Při nákupu komodit strhávám stejný poplatek 0,08 %, jelikož používám stejného poskytovatele. Průběžně investovaná tisícikoruna tak bude zhodnocena takto. U zlata by se vklad 119 000 Kč za necelých 10 let zhodnotil na 146 044,37 Kč (o 22,73%). Stříbro na 134 154,53 Kč (o 12,73%) a ropa na 142 639,87 Kč (o 19,87%). Všechna data jsou v Excelovém souboru s názvem *Srovnání investic.xlsx* umístěné na listu s názvem *Komodity* v tabulkách *Nárůst ceny* a *Průběžné investování*. [14]

Konečně se dostáváme ke kryptoměnám. V porovnání nesmí chybět Bitcoin, který je nejstarší a nejobchodovanější. Druhou kryptoměnu k porovnání jsem vybral Ethereum, které je po Bitcoinu z mého pohledu druhá nejvyužívanější kryptoměna na světě s vyšším potenciálem díky větší praktické použitelnosti. Průměrný roční nárůst ceny Bitcoinu za necelých 10 let je 629,7 % s výběrovou směrodatnou odchylkou 1 392,08 procentního bodu. Ethereum je na tom o něco lépe. Průměrný roční růst ceny je 2 230 % s výběrovou směrodatnou odchylkou 4 541,08 procentního bodu. Nutno dodat, že Ethereum existuje kratší dobu a tento průměr je spočten za posledních 5 let. Zajímavostí je, že za poslední necelé čtyři roky se jejich průměrný růst cen srovnal na 101,84% u BTC a 203,05% u ETH. Nasvědčuje to o mírné stabilizaci trhu. Zde je zajímavé, že průměrný měsíční nárůst cen Bitcoinu a Etherea před a po začátku covidové krize jsou skoro stejné. U Bitcoinu je tento měsíční průměr před krizí roven 13 % (průměr z 99 měsíců) a 12 % po začátku krize (průměr z 20 měsíců). U Etherea je tento průměr dokonce stejný a to 15 % před i po začátku krize. Poplatky za transakce se mohou lišit v závislosti na vytíženosti a počtu uživatelů, kteří chtějí uskutečňovat transakce. Vzhledem k obřím sumám si však dovolím aplikovat stejný poplatek, jaký jsem zaplatil naposled v roce 2017, a to 3 % z transakce. Výše poplatků nijak zásadně nekolísá a nejspíš k tomu nebude důvod ani v budoucnu. Poslední srovnání v zastoupení Bitcoinu a Etherea je pak následující. Bitcoin by zhodnotil vklad 119 000 (1000 Kč za měsíc) na 68 376 312,89 Kč (o 57 359,09% nebo 573,5 krát). Ethereum by pak zhodnotilo vklad 68 000 Kč ukládaný měsíčně od dubna 2016 (5 let a 8 měsíců kvůli kratší existenci) na 2 901 780,616 Kč (o 4 167,32% nebo 41,67 krát). Tak obrovskou sumu by bylo ovšem velmi obtížné vybrat. Pokud najdu kupce, který je ochoten Bitcoiny nebo Ethereum koupit, mám vyhráno. Pokud nikoho takového nenajdu, jsem odkázaný na to prodávat kryptoměny postupně. Buďto přes burzy nebo bitcoinové automaty Bit.plus. Bit.plus jsou automaty provozované českou firmou, která nabízí prodej a nákup Bitcoinu. Denní limit u Bit.plus je 2 500 000 Kč, ale je zde nutné doložit původ prostředků. Zároveň je potřeba ověření účtu na základě občanského průkazu. U vyšších částek je možnost

individuálního přístupu a poplatků. Se zvyšující se částkou pro výběr roste i doba připsání na účet. [7] Všechna data jsou v Excelovém souboru s názvem *Srovnání investic.xlsx* umístěné na listu s názvem *BTC a ETH* v tabulkách *Nárůst ceny v letech* a *Průběžné investování*. [14]

Může se zdát, že máme jasného vítěze. Ovšem musíme si uvědomit obrovské riziko spojené s kryptoměnami. Vzhledem ke zpomalujícímu růstu cen Bitcoinu i Etherea je zřejmé, že se v následujících letech růst cen nebude zvyšovat tak obrovským tempem jako v letech předešlých. Růst cen navíc zpomaluje exponenciálně a je možné, že se úplně zastaví. Některé predikce mluví o hranici 100 000 USD, některé naznačují, že půjde k nule kvůli nízké využitelnosti a alokaci všech Bitcoinů (většinu Bitcoinů vlastní pár majitelů). Dle mého názoru by mohl Bitcoin plnit roli investičního instrumentu ještě pár let. Pak bude jeho potenciál (co se týče investice) upadat. Každá nová kryptoměna má vyšší potenciál zhodnotit kapitál na začátku, kdy je volatilita největší. Stejně tak je tomu i u Etherea a dalších kryptoměn. Je ovšem fakt, že tento vynález změnil svět. Jeho původním účelem nebylo vytvoření nového investičního instrumentu, ale zcela nového, bezpečného a nezávislého platidla. A to se novým kryptoměnám daří víc a víc. Věřím, že Bitcoin bude jednou obsažen v učebnicích ekonomie a s ním i celá ekonomika, která díky němu může fungovat na zcela odlišných principech než teď.

Poprvé jsem investoval do Bitcoinu 30.11.2017. Směnil jsem 2 000 Kč a po necelých dvou týdnech jsem všechny směněné Bitcoiny prodal. 11.12.2017 byla cena Bitcoinu o 54,42 % vyšší a já tak dosáhl zhodnocení něco málo přes 1000 Kč. Od té doby investuji pokaždé, kdy mám volné prostředky a v drtivé většině se investice podaří. Kvůli vyššímu riziku ovšem investice nejsou nikdy moc velké. Mám i pár kamarádů, kteří kryptoměnám důvěřují mnohem více a dali do nich nemalé částky, které se většinou vrátily i s tučným výnosem. Ovšem znám i případ, kdy si kamarád vypěstoval nezdravou závislost na obchodování na burze a přišel o celé stavební spoření.

2.6 Zákon a daně

Tato pod kapitola je vypracovaná podle zdroje [20] a [25]. Z pohledu českých státních orgánů se na kryptoměny pohlíží jako na nehmotný movitý majetek. Česká národní banka je neuznává jako peněžní prostředek, a tím pádem ani jako platební službu. Kryptoměny nejsou z pohledu ČNB virtuálními penězi, cizí měnou a ani je nelze považovat za obdobu cenného papíru. Z tohoto důvodu nelze zařadit příjmy z prodeje kryptoměn do kapitálových příjmů. Veškeré obchody, které na burzách probíhají, spadají pod *§10 Zákona o daních z příjmů – Ostatní příjmy.*

Obdobně se podle výše uvedeného zákona postupuje i při zdanění příjmů plynoucích ze směny kryptoměn za jinou kryptoměnu, zboží nebo službu. Spekulanti, kteří s Bitcoiny a jinými virtuálními měnami obchodují a směňují je za standardní peníze, by měli odvést 15 procent ze zisku. Tedy z rozdílu pořizovací a prodejní hodnoty. Od 1.1.2021 je částka nad 1,7 milionu ze základu daně (příjmy ze zaměstnání, výnosy z kryptoinvestic apod.) zdaněna 23 procenty.

V říjnu roku 2015 rozhodl Evropský soudní dvůr (ESD) ve věci Služby za úplatu – Směna virtuální měny „Bitcoin“ za tradiční měny – Osvobození od daně, na základě sporu švédské daňové správy Skatteverket proti Davidu Hedqvistovi, že v případě kryptoměn se jedná o oběživo. Kryptoměny ESD tímto rozhodnutím de facto legitimizoval jako každou jinou měnu a osvobodil je tak od DPH. Ovšem ani tato nejvyšší soudní autorita EU dosud nic na názoru českého státu na kryptoměny nezměnila. Úprava DPH je na celoevropské úrovni a mnohdy bývá odlišná od úpravy zákona o dani z příjmu, jehož znění je zcela v kompetenci každého jednotlivého státu. Každý stát si tak tento zákon spravuje sám.

Co se týče těžby kryptoměn se v tomto případě postupuje jako při získávání věci vlastní činností. Těžba se již netýká pouze správy vlastního majetku, ale jde o poskytovanou službu a jedná se o podnikání. Mimo zřízení živnostenského oprávnění tak také vyplývá povinnost přihlásit se k sociálnímu a zdravotnímu pojištění. Příjem z tohoto podnikání se zdaňuje podle *§7 Zákona o dani z příjmu*. Zdanit jako příjem nelze kryptoměnu jako takovou, ale až její směnu, tedy směnu za fiat měnu nebo něco jiného. Dosáhnete-li jako fyzická osoba při těžbě kryptoměn zisku, daní se 15 %. Ve hře jsou však také návrhy na navýšení této daně z 15 % na 24 %.

Jelikož daň z kryptoměn patří pod ostatní příjmy, základ daně bude rozdílem mezi cenou při pořízení a cenou při prodeji kryptoměny. Pro představu, když koupím jeden Bitcoin za 100 000 Kč a následně prodám za 200 000 Kč, dílčí základ daně bude rozdíl 100 000 Kč.

Závěr

Tématem mé bakalářské práce bylo vyhodnotit kryptoměny jako možný investiční instrument. V první části je popsán princip, na kterém jsou kryptoměny založeny. Popsal jsem jejich funkčnost a stručný návod pro potenciální uživatele. Nastínil jsem fungování ostatních kryptoměn, které konkurují Bitcoinu a které by mohly mít v budoucnu potenciál. Shrnul jsem podstatné výhody a nevýhody, které kryptoměny přinášejí a s ním i možný budoucí vývoj do budoucna.

Cílem druhé části bylo ukázat, že na kryptoměny se dá dívat i jako na investiční instrument. Srovnal jsem kryptoměny s konvenčními způsoby investování jako jsou podílové fondy, akcie a komodity. Jelikož jsou způsoby investování velmi rozmanité, bylo srovnání velmi obecné, ale s jednoznačností zde dominovaly právě kryptoměny, které oproti ostatním způsobům investování nabízely řádově vyšší zhodnocení. Všechny investice jsem porovnával v intervalu 119 měsíců, až na Ethereum a některé fondy, kde jsem musel vklady zhodnocovat jen po dobu jeho existence. Konkrétně Bitcoin zhodnotil vklad o 57 359,09 % a Ethereum o 4 167,32 %. Vzhledem k velké volatilitě je ovšem tato investice vhodná jen pro otrlé investory s tolerancí k riziku. Zároveň hrozí, že cena kryptoměn bude růst menším tempem a s ní i výdělky. Nejlépe kryptoměnám konkurovaly akcie, u kterých bylo zhodnocení 105,99 % (S&P 500) a 219,7 % (NASDAQ 100) z průběžně vloženého kapitálu. U podílových fondů bylo zhodnocení o něco menší. Fond J&T OPPORTUNITY CZK OPF dosáhl zhodnocení 75,03 % a fond NN (L) Global Equity Impact Opportunit 112,85 %. Komodity na tom byly o poznání hůř a zhodnocení bylo mnohem menší. Zlato zhodnotilo vklad o 22,73 %, stříbro o 12,73 % a ropa o 19,87 %. Osobně bych začínajícímu investorovi doporučil vybrat si nějaký podílový fond. Fondy jsou nenáročné, relativně levné a vložený kapitál zhodnocují profesionální investoři. Pro pokročilejší investory mohou být dobrou volbou akcie. Portfolio může být diverzifikované buďto o komodity nebo právě o kryptoměny. Podíl kryptoměn v portfoliu by ale neměl být moc velký.

Ze zjištěných dat a povahy celé problematiky by se kryptoměny daly doporučit jen zkušeným investorům a traderům, kteří hodlají do investování vložit dostatek času a úsilí. Osobně bych kryptoměny jako investiční instrument doporučil, ale jen v menším zastoupení v investičním portfoliu.

Literatura

[1.] Skalický, Jan, Stroukal, Dominik: Bitcoin a jiné kryptopeníze budoucnosti. Grada. Praha 2018.

[2.] Valach, Josef a kolektiv: Investiční rozhodování a dlouhodobé financování. Praha, 2010.

[3.] Amundi CR All Star Selection [online], dostupné na https://www.amundi-kb.cz/fondy/detail/CZ0008474517

[4.] Average time it takes to mine a Bitcoin [online], dostupné na https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/

[5.] Bitcoin: A Peer-to-Peer Electronic Cash System [online], strana 2, dostupné na https://bitcoin.org/bitcoin.pdf

[6.] Bitcoin's natural long-term power-law corridor of growth [online], dostupné na https://medium.com/quantodian-publications/bitcoins-natural-long-term-power-law-corridor-of-growth-649d0e9b3c94

[7.] Bit.plus – Časté dotazy [online], dostupné na https://bit.plus/cs-cz/faq

[8.] ČSOB Dynamický [online], dostupné na https://www.csob.cz/portal/lide/investicni-produkty/podilove-fondy/smisene-fondy/detail-fondu/-/isin/BE0174397886/4

[9.] ČSOB Konzervativní [online], dostupné na https://www.csob.cz/portal/lide/investicni-produkty/podilove-fondy/smisene-fondy/detail-fondu/-/isin/BE0174399908/4

[10.] ČSOB Vyvážený [online], dostupné na https://www.csob.cz/portal/lide/investicni-produkty/podilove-fondy/smisene-fondy/detail-fondu/-/isin/BE0174401928/4

[11.] Generali Fond konzervativní [online], dostupné na https://www.generali-investments.cz/produkty/investice-v-czk/fondy/generali-fond-konzervativni.html

[12.] Generali Prémiový vyvážený fond [online], dostupné na https://www.generali-investments.cz/produkty/investice-v-czk/fondy/generali-premiovy-vyvazeny-fond.html?redirected=1

[13.] How the Bitcoin protocol actually works [online], dostupné na https://michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

[14.] Investing [online], dostupné na https://www.investing.com

[15.] J&T OPPORTUNITY CZK OPF [online], dostupné na https://www.jtis.cz/fond/OCZ

[16.] Kryptoměna Bitcoin: Výhody a nevýhody [online]. Dostupné na https://finex.cz/kryptomena-bitcoin-vyhody-nevyhody/

[17.] Kurzy měn, akcie, komodity, online zprávy [online], dostupné na www.kurzy.cz

[18.] Nejlepší Bitcoin burzy 2021 [online], dostupné na https://www.5nej.cz/srovnani-bitcoin-burz/
[19.] NN (L) Global Equity Impact Opportunit [online], dostupné na https://www.conseq.cz/investice/prehled-fondu/nn-l-global-equity-impact-opportunit-x-hgd-czk
[20.] Obchodování s tzv. převodními tokeny [online], dostupné na https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/stanoviska_a_odpovedi/pdf/k_obchodovani_s_prevodnimi_tokeny.pdf
[21.] Poplatky u investičních fondů [online], dostupné na https://www.finez.cz/blog/jak-investovat/poplatky-u-investicnich-fondu-na-co-si-dat-pozor/
[22.] Přemýšleli jste někdy, jak funguje Bitcoin (a další kryptoměny)? [online]. Dostupné na https://www.youtube.com/watch?v=bBC-nXj3Ng4
[23.] Srovnání brokerů pro obchodování akcií [online], dostupné na https://finex.cz/rubrika/akcie/akciovi-brokeri/
[24.] Top Cryptocurrency Spot Exchanges [online], dostupné na https://coinmarketcap.com/rankings/exchanges/
[25.] Zdanění kryptoměn – Kompletní návod pro rok 2021 [online], dostupné na https://finex.cz/zdaneni-kryptomen-kompletni-navod/

Seznam obrázků

Seznam příloh

Na přiloženém CD lze najít soubor:

Srovnání investic.xlsx