

Univerzita Pardubice
Fakulta ekonomicko-správní

Kryptoměny jako investiční nástroj
Bc. Petr Václavek, MBA

Diplomová práce
2022

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE (projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Petr Václavek**
Osobní číslo: **E20760**
Studijní program: **N0413A050009 Ekonomika a management**
Studijní obor: **Ekonomika a management podniku**
Téma práce: **Kryptoměny jako investiční nástroj**
Zadávací katedra: **Ústav podnikové ekonomiky a managementu**

Zásady pro vypracování

Cílem práce je popsat decentralizované digitální měny, tzv. kryptoměny. Práce bude obsahovat popis vývoje kryptoměn od historie až po jejich dnešní pozici na finančním trhu. Dále se bude zabývat jejich vlastnostmi, technologií blockchainu, právním rámcem a problematikou jejich využití v praxi. Bude provedena komparace různých kryptoměn mezi sebou a s dalšími investičními instrumenty, kde budou sledovány ukazatele výnosnosti, volatility a rizik spojených s investicí. Zároveň bude práce obsahovat doporučení pro investice do kryptoměn pro různé subjekty finančního trhu, včetně podniků.

Osnova:

- Historický vývoj kryptoměn.
- Druhy a vlastnosti kryptoměn, jejich vzájemná komparace.
- Sestavení modelového investičního portfolia.
- Doporučení pro investice do kryptoměn.

Rozsah pracovní zprávy: **cca 50 stran**
Rozsah grafických prací: **=**
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

GUTTMANN, Benjamin. The Bitcoin Bible gold edition. Norderstedt: Books on demand, 2014. 429 s. ISBN 9783732296965.

LÁNSKÝ, Jan. Kryptoměny. V Praze: C.H. Beck, 2018. ISBN 978-807-4007-224.

MARTINÁK, Tomáš, 2015. Bezhotovostní peníze versus elektronické peníze. Olomouc: Iuridicum Olomoucense, s.r.o., ve spolupráci s Právnickou fakultou Univerzity Palackého v Olomouci. ISBN 978-80-87382-74-5.

REJNUŠ, Oldřich. Finanční trhy 4., aktualizované a rozšířené vydání. Praha: Grada Publishing a.s., 2014. 760 s. ISBN 978-80-247-9407-5.

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. 195 stran. ISBN 9788027107421.

Vedoucí diplomové práce: **doc. Ing. Liběna Černožorská, Ph.D.**
Ústav ekonomických věd

Datum zadání diplomové práce: **1. září 2021**
Termín odevzdání diplomové práce: **30. dubna 2022**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

Ing. Michaela Kotková Strítěská, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2021

Prohlašuji:

Práci s názvem „Kryptoměny jako investiční nástroj“ jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 26.04.2022

Bc. Petr Václavek, MBA v. r.

PODĚKOVÁNÍ

Tímto bych osobně rád poděkoval své vedoucí diplomové práce p. doc. Ing. Liběně Černožské, Ph.D. za její odbornou pomoc, za poskytnuté materiály a také za její cenné rady, které mi pomohly při zpracování diplomové práce. Dále mé poděkování směřuje k mé rodině, která se mnou měla veškerou trpělivost při studiu a psaní diplomové práce.

ANOTACE

Tato práce slouží k pochopení kryptoměnové problematiky a investování peněžních prostředků do kryptoměn. Jsou zde popsány druhy a vlastnosti kryptoměn, jejich vzájemná komparace, nadále historický vývoj kryptoměn a konkrétní příklad sestavení modelového investičního portfolia.

KLÍČOVÁ SLOVA

kryptoměny, podnik, investiční portfolio, investiční instrumenty, blockchain, finanční trh

TITLE

Cryptocurrencies as an investment tool

ANNOTATION

This work will serve to understand the problem of cryptocurrencies and investing funds in cryptocurrencies. The types and properties of cryptocurrencies and their mutual comparison are described here, as well as the historical development of cryptocurrencies and a specific example of the compilation of a model investment portfolio.

KEYWORDS

cryptocurrencies, enterprise, investment portfolio, investment instruments, blockchain, financial market

OBSAH

Seznam obrázků	9
Seznam tabulek	10
Seznam zkratk	11
Úvod	12
1 Definice peněz a kryptoměn	13
1.1 Definice a funkce peněz	13
1.2 Formy peněz	15
1.2.1 Hotovostní peníze	15
1.2.2 Bezhotovostní peníze	16
1.3 Definice a vlastnosti kryptoměn	16
1.3.1 Vlastnosti kryptoměn	17
1.4 Porovnání kryptoměn a peněz	18
2 Kryptoměny	20
2.1 Historický vývoj kryptoměn	20
2.2 Dělení kryptoměn	24
2.3 Technologie kryptoměn	25
2.3.1 Kryptografie	26
2.3.2 Peer-To-Peer	26
2.3.3 Adresa	26
2.3.4 Peněženka	27
2.4 Těžba kryptoměn	28
2.5 Hash	30
2.6 Blockchain	31
2.7 Právní rámec kryptoměn na našem území	33
2.8 Využití kryptoměn v reálném životě	35
2.8.1 Kryptoměna jako investice	35
2.8.2 Kryptoměna jako platební prostředek	36
2.8.3 Ostatní využití kryptoměn	36

2.9	Rešerše odborné literatury	37
3	Komparace vybraných kryptoměn	40
3.1	Tržní kapitalizace kryptoměn	40
3.2	Počet mincí a dělitelnost kryptoměn.....	43
3.3	Poplatky za transakci převodu kryptoměn	45
3.4	Rychlost transakce	46
4	Metodika výpočtů investičních kritérií	48
4.1	Metodika výpočtu výnosnosti.....	48
4.2	Metodika výpočtu volatility.....	49
4.3	Sharpe ratio	50
5	Sestavení modelového portfolia	51
5.1	Představení vybraných indexů a komodit.....	51
5.2	Výnosnost	52
5.3	Volatilita	56
5.4	Sharpe Ratio.....	59
5.5	Potencionální investice	60
6	Doporučení pro investice do kryptoměn.....	65
	Závěr	67
	Použitá literatura	69
	Přílohy.....	73

SEZNAM OBRÁZKŮ

Obrázek 1: Merkeleho strom.....	31
Obrázek 2: Tržní kapitalizace kryptoměn vyjádřená v procentech.....	41
Obrázek 3: Srovnání volatility kryptoměn, indexů a komodit.....	58
Obrázek 4: Investice do kryptoměn v roce 2017	60
Obrázek 5: Investice v roce 2018 do 2020 do kryptoměn	61
Obrázek 6: Investice v roce 2017 do 2022 do indexů a komodit.....	62
Obrázek 7: Investice v roce 2018 do 2020 do indexů a komodit.....	63
Obrázek 8: Investice do kryptoměn, indexů a komodit od 2018 do 2020	64

SEZNAM TABULEK

Tabulka 1: Počet vytvořených mincí.....	44
Tabulka 2: Poplatky za převod kryptoměn	45
Tabulka 3: Rychlost transakcí.....	47
Tabulka 4: Výnosnost kryptoměn	53
Tabulka 5: Výnosnost indexů.....	54
Tabulka 6: Výnosnost komodit	55
Tabulka 7: Volatilita kryptoměn	56
Tabulka 8: Volatilita Indexů a Komodit	58
Tabulka 9: Sharpe ratio investičních aktiv.....	59

SEZNAM ZKRATEK

ASIC	Application Specific Integrated Circuit
BTC	Bitcoin
CPU	Central processing unit
ČNB	Česká národní banka
DCA	Dollar cost averaging
DDoS	Distributed Denial of Service
FPGA	Field Programmable Gate Array
GDPR	General Data Protection Regulation
GPU	Graphics processing unit
IT	Informační technologie
MB	Megabyte
MMF	Mezinárodní měnový fond
POS	Proof of Stake
POW	Proof of work
P2P	Peer to peer
QR	Quick Response
TPS	Transactions per second
USB	Universal Serial Bus
USD	United States Dollar

ÚVOD

Moderní doba jedenadvacátého století je úzce spjata s digitalizací. Podstatná část našich životů se odehrává v on-line světě. Ať už se jedná o každodenní konverzace s přáteli či s kolegy v práci pomocí emailové schránky nebo pomocí sociálních sítí. Nejinak tomu je v případě placení peněžními prostředky. V dnešní době významně převažují platby pomocí platební karty nebo formou bankovních převodů. Převod „fiktivních“ jedniček a nul, tedy peněz, které jsme fakticky nikdy neviděli ve fyzické podobě je již běžnou součástí nynějšího života. Přejít do digitalizace tedy postupně ovládá i samotnou ekonomiku. V případě možnosti rozvoje digitálních decentralizovaných měn byl milníkem rok 2009, kdy světlo světa spatřila nová forma peněz a byly jimi konkrétně kryptoměny. I když od tohoto roku uplynula doba delší než dekáda, a protože není v dnešním světě o informace nouze, neboť se nacházíme v online době, tak stále masová část lidí nemá povědomí o tom, co kryptoměny vlastně jsou, kde se vzaly a jak vůbec jako celek fungují. Když už se veřejnost dozví o kryptoměnách, tak je to často z médií a pouze na téma typu „Kolik stojí jeden Bitcoin?“. O komplikovanosti kryptoměnového světa, nebo o tom, jaký raketový start kryptoměny zažily, se ví jen málo. Snad je to zapříčiněno i nedostatkem materiálu v českém jazyce. Právě každé další zpracování tematiky kryptoměn může prohloubit informovanost jak k potenciálním investorům, tak i k běžnému obyvatelstvu.

Má diplomová práce bude zaměřena na kryptoměny jako investiční nástroj, a tedy na možnosti investování do kryptoměnového repertoáru. Budou zde využity dosavadní znalosti zejména z předmětu finanční investování, prohloubené hlavně svým samostudiem.

Cílem diplomové práce je popsat decentralizované digitální měny, tedy kryptoměny. K naplnění tohoto cíle bude sloužit teoretické uvedení do problematiky, tedy nastínění historie a vývoje kryptoměn, jejich charakteristické vlastnosti a popis jejich současné situace na finančním trhu. Nebude opomenuta tematika technologie blockchainu, právní rámec a aplikace kryptoměn do praxe. Podstatnou částí bude modelové sestavení investičního portfolia, kde bude mezi vybranými kryptoměnami a dalšími investičními instrumenty provedena vzájemná komparace a analýza, například výnosnost a volatilita. V závěru diplomové práce bude sepsáno doporučení pro investice do kryptoměn pro různé subjekty finančního trhu, tedy včetně podniků.

1 DEFINICE PENĚZ A KRYPTOMĚN

Na úvod diplomové práce bude po teoretické stránce pro lepší představu a porozumění samotné oblasti kryptoměn vysvětlena problematika peněz, a to včetně definice, charakteristiky peněz a druhů.

1.1 Definice a funkce peněz

Peníze jsou fenoménem nejenom dnešního století, ale i těch předešlých. Hlavním problémem při definici peněz je všeobecný rozpor mezi teoretickým vymezením a praktickou použitelností. Při charakteristice se zpravidla uvádějí dva typy definic.

Teoretická definice peněz vychází z podstaty v nejobecnějším znění, a tedy že lze za peníze považovat jakékoliv aktivum, které je všeobecně přijímáno při placení za služby a zboží nebo při úhradách dluhu. Jak lze z předešlých slov vyčíst, peníze (po teoretické stránce) obsahují aspekt všeobecnosti. Jinými slovy je dané aktivum přijímáno všemi subjekty dané společnosti. Pokud by tomu tak nebylo, tak nejde o peníze, ale o jejich neumělou a často jen časově omezenou náhražku. Dále definice uvádí dva velmi podstatné pojmy z říše peněz, konkrétně důvěryhodnost a kupní sílu. Tyto dva pojmy úzce souvisí se samotnou podstatou peněz. Důvěryhodnost peněz je předpokladem pro jejich všeobecné přijímání. Obchodní subjekty peníze přijímají, protože jim skutečně věří. Věřící v jejich použitelnost, ať už v rámci platby za zboží či služby nebo na úhradu dluhů. Samotné přijímání peněz lze nařídít státem. Kupní síla peněz prezentuje množství zboží a služeb, které při existujících cenách lze peníze za získat.

Druhou definicí, která je v literatuře zmiňována, je empirická definice peněz. V souvislosti s teoretickou definicí v současnosti funkci peněz plní pouze hotovostní peníze (bankovky a mince) a bezhotovostní peníze (vklady v bankách). V některých funkcích peněz účinkují šeky, směnky a další cenné papíry. Při směně lze zaplatit pomocí nástrojů platebního styku, hlavně platebními kartami. Právě tyto skutečnosti limitují využití teoretických definic peněz hlavně při odpovědích na otázky: „*Co to jsou ještě peníze a co již nejsou? Které peníze jsou v oběhu a které jsou mimo běh?*“. Řešením je však definování peněz pomocí empirie. Míru vlivu kvanta peněz na jiné makroekonomické veličiny se lze pokusit posoudit pomocí kvantitativního sledování vývoje jednotlivých „složek peněz“. Za tímto účelem jsou peníze definovány empiricky a výsledkem je sestavení měnových agregátů. Za dokonalé vymezení peněz je pak považován měnový agregát, jehož vývoj nejlépe umožňuje predikovat evoluci jednotlivých makroekonomických veličin.

mických proměnných, a který by měl být objasněn především vývojem množství peněz. Měnové agregáty jsou důsledkem empirických definic peněz. Představují souhrn peněžních prostředků s určitým stupněm likvidity. Jejich stanovení, sledování a ovlivňování má význam především v měnové politice. Samotná náplň měnových agregátů může být v různých ekonomikách rozdílná, především v závislosti na využívání peněžních instrumentů v dané zemi a čas od času se může upravovat. (Revenda, 2012, s. 17-18)

V oblasti funkcí peněz je celosvětová shoda. Definuje je například samotná Evropská centrální banka, případně Federální rezervní systém, který je centrální bankovním systémem Spojených států amerických. Funkcemi peněz se rozumí následující tři.

Peníze slouží především jako prostředek směny. Je základní funkcí, kterou každé aktivum v podobě peněz musí plnit, jak již bylo naznačeno v předchozím odstavci, a tedy, že lidé mohou volně směňovat za zboží a služby všeho druhu a každý musí tyto peníze přijmout. Funkce peněz do značné míry determinuje formu peněz. V minulosti, tedy v dobách barterového obchodu bylo vždy potřeba najít někoho, kdo má statek, který daný člověk potřeboval a zároveň byl ochoten směnít onen statek za nabízený. Nevýhoda barterového obchodu byla taková, že bylo velmi komplikované takovou směnu provést, příp. najít obchodníka, který zrovna poptává to, co druhý nabízí. Jako nejvhodnější pro tuto funkci se v historii ukázaly drahé kovy, především zlato a stříbro. Tyto kovy na sebe následně vzaly podobu mincí. Avšak i stříbro a zlato mají své nevýhody. Pravděpodobněji těmi největšími jsou, že náklady na těžbu jsou vysoké. Dále jsou to kovy, které vyjadřují vysokou hodnotu, což dokládá jejich vzácnost.

Druhou funkcí peněz je tzv. zúčtovací jednotka. Prostřednictvím peněz se vyjadřují konkrétní ceny zboží, služeb, kapitálu a práce. Znamená to, že peníze pomáhají určit hodnotu všech produktů a služeb, které existují. Díky nim lze porovnat, zda je lepší si koupit zboží A nebo zboží B. Jistěže cena není jediný ukazatel, ale pokud je zboží stejné či podobné kvality, pak cena ve výběru zboží velice usnadní volbu. Tato funkce se v dějinách objevila společně s poklesem transakčních nákladů.

Peníze slouží jako uchovatel hodnoty, což je třetí z funkcí, zároveň pravděpodobně nejkomplikovanější. Teorie říká, že vlastní-li osoba například 100 Kč a chce s nimi disponovat po dvaceti letech, peníze by stále měly mít stejnou hodnotu. Pokud by tedy toto pravidlo platilo, tak by peníze fungovaly jako uchovatel hodnoty. Realita je ovšem odlišná. Každoročně peníze ztrácejí na hodnotě kvůli inflaci. Fyzicky jich sice osoba vlastní stále stejné množství, jenže za stejné množství si každý vlivem běhu času koupí menší množství zboží, než roky předtím. Je

samozřejmostí, že peníze jsou v této konkrétní funkci součástí celkového bohatství každé osoby. Kvalita peněz jako uchovatele hodnoty je přímo svázaná hlavně s vývojem jejich kupní síly. Očekává-li jednotlivec vzestup cen služeb a zboží, peníze výrazně slábnou a vyplatí se je vložit do prostředků, které penězům zachovají stejnou hodnotu jako dnes, případně ještě jejich hodnotu posílí.

1.2 Formy peněz

Peníze mají dvě základní formy. Jsou jimi hotovostní peníze a bezhotovostní. Mezi těmito dvěma pojmy existuje velice úzký vztah, nýbrž kvůli snadné přeměny jedné formy peněz na tu druhou. Hotovostní peníze lze vložit na svůj bankovní účet přímo v bance, nebo naopak lze přijít do své banky a požádat o výběr peněžních prostředků, kterými daný jedinec disponuje na bankovním účtu.

1.2.1 Hotovostní peníze

Jakožto hotovostní formy peněz lze pokládat následující

- Mince, jež jsou kus kovu kruhovitěho tvaru a obsahují rysovanou hodnotu a hmotnost daného kovu. Často lze na rubové straně mince najít nominální hodnotu, a na přední straně charakteristickou vlastnost země.
- Obchodní mince je mincovní prostředek vyrobený z drahého kovu. Je určena výhradně pro obchodování s drahými kovy. Není tedy součástí soustavy zákonných peněz a nemá nominální hodnotu stanovenou v peněžní jednotce, není s ní ani v zákonném poměru. Tyto mince jsou nejčastěji vyráběny ze zlata. Například v dnešní době emitent ČNB upřednostňuje vydávání zlatých mincí s nominální hodnotou.
- Státovky lze charakterizovat jako původně cenný papír na určitou peněžní částku, vydávaný státem, neúročitelný, znějící na majitele, a který byl u pokladen státu přijímán na zaplacení státních pohledávek, např. daní.
- Bankovky jsou cennými papíry, na kterých je uvedena nominální hodnota. Tuto bankovku vydává emitent, v případě České republiky se jedná o Českou národní banku. Bankovka je bezúročná a musí být přijímána jako platební prostředek.

Hotovostí (uváděnou pod anglickým slovem cash) se podle Mezinárodních standardů účetního výkaznictví rozumí oběživo a vklady na běžných účtech, neboť tyto vklady jsou likvidní

jako oběživo. Toto pojetí zhruba odpovídá peněžnímu agregátu M1. Někdy se i hotovost chápe v užším pojetí jako oběživo (bankovky a mince), tj. jako peněžní agregát M0. (Jílek, 2013, s. 16)

1.2.2 Bezhotovostní peníze

Společně s hotovostní formou peněz představují základy současných peněz. Spojení mezi bezhotovostními penězi a hotovostními je velice pevné. Velice jednoduše lze hotovostní peníze přeměnit na formu bezhotovostních, stejně jako je možné naopak bezhotovostní peníze přeměnit na hotovost, například vkladem na účet nebo výběrem z běžného účtu. Největším rozdílem mezi těmito dvěma formami peněz je emise. Jelikož jedinou institucí ve státě, která může emitovat hotovostní peníze je centrální banka. Naproti tomu bezhotovostní peníze, tj. peníze v podobě zápisů na bankovních účtech, však mohou emitovat kromě centrální banky i banky komerční. Z tohoto vyplývá, že banky neposkytují úvěry pouze z přijatých depozit, nýbrž i díky emisi bezhotovostních peněz mohou poskytovat úvěry nad rámec přijatých depozit.

A právě přes bezhotovostní peníze se lze dostat k pojmu kryptoměny, respektive k problematice celé této diplomové práce, kterými kryptoměny jsou. Zejména tehdy, když kryptoměny existují pouze v digitální podobě a nelze je nijak jinak popsat než jako bezhotovostní.

Nahrává k tomu i fakt, že dle zákona č. 370/2017 Sb. § 4 o platebním styku elektronickými penězi je peněžní hodnota, která (Zakonyprolidi.cz, 2021):

- představuje pohledávku vůči tomu, kdo ji vydal,
- je uchovávána elektronicky,
- je vydávána proti přijetí peněžních prostředků za účelem provádění platebních transakcí,
- je přijímána jinou osobou, než tím, kdo ji vydal.

1.3 Definice a vlastnosti kryptoměn

Oproti definici k penězům se nedá jistě říct, že existuje celosvětová shoda na jedné definici kryptoměn. Nepanuje ani shoda na tom, zdali je lze považovat za peníze, či nikoliv. V čem se uživatelé kryptoměn shodují s teoretiky je to, že se kryptoměny dají považovat za digitální prostředek směny, který je založen na decentralizovaném platebním systému využívající kryptografii. Nejblíže kryptoměny definuje oblast směrnice 2018/843 Evropské unie, která nazývá

„virtuální měny“ jako digitální aktivum. To není vydáváno ani garantováno jednou centrální bankou nebo jiným veřejným orgánem. Dále nemá status právní měny, která může být přijímána jako prostředek směny a může být uchovávána a obchodována elektronickými prostředky. Jak bylo řečeno, z terminologického hlediska se nejčastěji v definicích objevují pojmy jako virtuální aktivum, jelikož kryptoměny nejsou měnou v běžném slova smyslu. Smyslem vyvinutí virtuálních měn bylo vyvinout prostředek směny mimo stávající peněžní systém s využitím kryptografie a bez účasti třetích stran, tedy bez účasti centrálních a komerčních bank. V tom případě lze jistě říct, že neexistuje jednotná univerzální definice, přesto má nezaměnitelnou podobu v tom, že se obecně uznává, že virtuální měna není fiat měnou a neměla by být ani zaměňována s elektronickými penězi. (СТОЙКА, 2021, s. 7)

1.3.1 Vlastnosti kryptoměn

Kryptoměny mají několik vlastností, kterými se tolik odlišují od běžných měn. Často se ztotožňují s již zmíněnými informacemi sepsanými v předešlých odstavcích. (Ajiboye, 2019, s. 29)

Decentralizovanost. Jedná se o pojem, který představuje fakt, že se v kryptoměnové síti nevyskytuje žádný centrální server, který by platby a převody v síti kontroloval. Potvrzování transakcí mají na starost těžaři jako vedlejší produkt těžby. V případě, že je platební transakce potvrzena, je informace o potvrzení okopírována do veškerých počítačů v síti. Nelze tak transakce zfalšovat a ochraňuje to samotnou síť před potenciálním výpadkem centrálního serveru, který neexistuje. Bezpečnost transakcí je do velké míry založená a závislá na skutečné decentralizaci potvrzování měny, tedy potvrzování z mnoha počítačů s malým výkonem.

Anonymita. Úzce souvisí s platebními transakcemi, protože s odesláním či přijetím kryptoměn neodchází žádné osobní údaje o odesílateli, ale ani o příjemci. Propojení mezi účtem a osobou zná pouze vlastník účtu a nikdo jiný.

Transakce. Nemožnost odvolat transakci. Pokud odesílatel odešle potvrzení transakce, splňuje všechny podmínky a je tedy neodvolatelná.

Bezpečnost a transparentnost. Je jednou ze stěžejních vlastností kryptoměn. Jak bylo uvedeno, kryptoměny využívají kryptografii. Několikanásobné šifrování zaručuje bezpečnost proti veškerým výpočetním technikám, ale i hackerům. Nelze tak snadno ukrást kryptoměny například z hardwarové peněženky. Dokonce ani nejrychlejší výpočetní technika světa v aktuální

fázi nedokáže prolomit šifrování bitcoinu. Transparentnost zaručuje fakt, že existuje zápis o potvrzení transakce, tzn. veškeré převody jsou zapsány do sdílené historie transakcí.

Platby za transakce. Obvykle mají být stanoveny velmi nízké nebo žádné poplatky za platby. V případě, že jsou poplatky zavedeny, jedná se o ty z nich, které mají vést k motivaci těžařů k rychlejšímu potvrzování transakcí.

Časově neomezený rozsah. Celý kryptoměnový systém je závislý pouze na připojení k internetu.

1.4 Porovnání kryptoměn a peněz

Z vypsaných vlastností kryptoměn lze zvolit porovnání s klasickými fiat penězi. V případě peněz neplatí decentralizovanost, neboť každá národní měna státu podléhá jeho centrální bance. V případě České republiky se jedná o Českou národní banku. Všeobecně se tak dá povědět, že měny jsou centralizované a všechny transakce jsou regulovány zvláštními subjekty. Dalším rozdílem mezi klasickými penězi a kryptoměnami lze spatřit v šifrování. Tam klasické peníze žádné speciální šifrování nevyužívají, oproti kryptoměnám. Na první pohled navíc ve fyzickém stavu kryptoměny neexistují oproti klasickým penězům, které existují i ve formách bankovek. Je potřeba vnímat, že kryptoměny jsou stále ve své rané fázi a je veliký prostor pro jejich další rozvoj.

Kryptoměny s penězi lze porovnat nejlépe podle funkcí peněz, tedy zdali kryptoměny funkce peněz naplňují, či nikoliv. Funkcemi peněz se rozumí, že jsou: všeobecným prostředkem směny, zúčtovací jednotkou a uchovatelem hodnoty.

V případě prvním, tedy zdali jsou kryptoměny všeobecným prostředkem směny, tak lze polemizovat. V dnešní době se lze doplatit určitých služeb a zboží za kryptoměny, nýbrž ve velice omezeném rozsahu. Proto u kryptoměn neplatí ono všeobecný, kdy drtivá většina obchodníků nepřijímá kryptoměny jako platební prostředek. Je to dáno hlavně povahou kryptoměn, kdy se jedná stále o něco nového a ačkoliv v určitých oblastech kryptoměnami již platit lze, tak všeobecně nikoliv. Zde navíc klasické peníze mají výhodu v tom, že se všeobecně přijímají a to dokonce ze zákona.

Z pozice další, zúčtovací jednotky, lze opět tvrdit, že kryptoměny silně těžce absentují ve formě zúčtovací jednotky. Tedy, že ne zcela snadno usnadňují ekonomickou kalkulaci. To je dáno hlavně vysokou volatilitou kryptoměn a to včetně i těch více známých jako je Ethereum nebo Bitcoin.

V rámci poslední funkce tedy uchovatel jednotky, tak lze potvrdit, že určitá část kryptoměn, jako je Bitcoin, můžou představovat a představují z dlouhodobého hlediska velmi dobrého uchovatele hodnoty. Avšak kryptoměna se nerovná pouze Bitcoin, ale i další stovky až tisíce kryptoměn dalších, které jsou založené vyloženě za účelem spekulace. Na druhou stranu už bylo i uvedeno, že problémem u klasických peněz je právě položka uchovatel hodnoty, že zcela tomu tak není.

2 KRYPTOMĚNY

Kryptoměny jsou v dnešním pojetí stále novou rozvíjející se technologií. K samotnému pochopení pojmu nestačí mít dobrou znalost pouze z jednoho oboru, ale hned z několika oblastí. Využívají totiž několik oborů napříč odvětvími. Konkrétními oblastmi jsou např. ekonomie a finance, softwarový vývoj a inženýrství, případně samotná kryptografie a datové struktury. Samozřejmě, že tímto krátkým výčtem to nekončí. Znázorňuje však rozmanitost ve vývoji jedné kryptoměny. V dnešním pojetí jsou alternativou ke měnám s nuceným oběhem, jinak definovaným také jako fiat měnám, které jsou vydávány a garantované jednotlivými státy. Kryptoměny jsou čistě digitální, decentralizované a využívají kryptografických principů pro potvrzování transakcí. Transakce provedené pomocí kryptoměn jsou nevratné, pseudoanonymní a často levné a rychlé. Dnes lze vypočítat několik tisíců alternativních aktivních kryptoměn, na druhou stranu je ale možné vyjmenovat hned několik stovek kryptoměn zaniklých.

2.1 Historický vývoj kryptoměn

Historie digitálních měn či kryptoměn není zdaleka dlouhá. Obsahuje však již linii důkazů o tom, jak zásadní inovací technologie blockchainu je. Počátek kryptoměn je velice rozpačitý a neexistuje přesný čas, kdy digitální měny či kryptoměny spatřily světlo světa. Zpočátku se digitálním měnám říkalo spíše digitální peníze a jejich čas přišel až s mohutným rozšířením internetu u veřejnosti v devadesátých letech. Jednalo se o první náznaky skutečného řešení problému tradičního a zastaralého bankovníctví.

S první velkou digitální měnou historie přišlo sdružení Digicash, později provozující měnu ecash. Digicash vytvořil kryptograf David Chaum, který je někdy přezdíván jako otec digitálních měn nebo otec anonymní komunikace. Část společnosti dokonce věří, že onen David Chaum je Satoshi Nakamoto, pozdější autor Bitcoinu, o kterém je detailněji psáno v dalších kapitolách. Teorie však nevyvrací ani nepotvrzují, zdali je Chaum skutečně objevitelem Bitcoinu. David Chaum byl velikým inovátorem na poli digitální komunikace. V roce 1982 představil kryptografický systém na poli digitální komunikace pro anonymní transakce a o osm let později ho v roce 1990 uvedl do života pod názvem ecash. Úspěch ecash však netrval nijak dlouho, jelikož David Chaum o několik let později vyhlásil bankrot. Odborníci a pozorovatelé se domnívají, že hlavní příčinou bylo to, že Chaum vyžadoval příliš anonymity pro své uživatele, a nebyl tak schopen do své měny vtáhnout státní peníze. Je však nutné dodat, že Chaum

nechtěl nahradit celý peněžní systém, ale chtěl pouze přijít s alternativou k současným peněžním mikrotransakcím k drobným peněžním převodům, které považoval za příliš složité a málo anonymní, zejména pak pomocí platebních karet nebo šeků. (Stroukal, 2018, s. 28)

Ecash byl mimořádným vynálezem své doby, ale nepředstavoval dostatečnou revoluci. Stejně jako například společnost PayPal, která skutečně zjednodušuje mikroplatby na internetu, ale stále se jedná o dolary, eura, či české koruny, tedy o tradiční měnu, akorát kódovanou v elektronické podobě.

Za dalšího předchůdce Satoshiho Nakamota je označován americký vývojář a počítačový vědec Nick Szabo, který navrhl první formu blockchainu v roce 1998. Konkrétně jeho projekt Bit Gold byl jedním z prvních pokusů decentralizované virtuální měny. Právě Szabův pokus o vytvoření „bitcoinu své doby“ se považuje za předchůdce bitcoinového protokolu. Ve své podstatě totiž Bit Gold a bitcoinové protokoly vytvářejí tak těsné paralely, že se opět spekuluje o anonymním tvůrci Bitcoinu. Bit Gold kombinuje různé prvky kryptografie a těžby k dosažení decentralizace. Tyto prvky zahrnují bloky s časovým razítkem, které jsou uloženy v registru titulů a jsou generovány pomocí řetězců proof-of-work (POW). Bohužel, Bit Gold nikdy nebyl uveden ve skutečnost, tedy nebyl uveden do provozu. (Guttman, 2014, s. 14)

Dalším zajímavým milníkem ve vývoji kryptoměn byla kryptoměna s názvem Hash Cash. Stejně jako například Bit Gold je Hash Cash založený na algoritmu proof-of-work. Tato kryptoměna byla vytvořena kryptografem Adamem Backem, a to konkrétně v roce 1997. Systém Hash Cashu byl vytvořen mimo jiné i proti spammerům (zejména v technologii email) a proti DoS útokům.

Později v dalších letech došlo k objevení dalších měn, jako například CyberCoin, militant, Visa Cash, Mondex, či Liberty Dollar a další. Některé byly slepými uličkami, jiné ukázaly cestu kudy nejít a naznačily směr, kterým se vydat ke chtěné digitální měně. V čase se bohužel ukázal jeden významný fakt, který nás utvrzuje v tom, že nelze vytvořit konkurenci státním penězům, aniž by dříve, či později vývojář neskončil u soudu. Nejlepším ilustrantem tohoto problému je příklad měny E-gold. E-gold byla digitální měna krytá skutečným zlatem, které společnost tvůrců nakupovala a skladovala. Jednoduše řečeno, vláda znala tvůrce E-goldu a sídlo společnosti, a proto tvůrci i zakladatelé skončili u soudu.

Mezníkem v dějinách digitálních měn byl CyberCoin, měna společnosti CyberCash, která se zrodila na konci devadesátých let. Naneštěstí se stala pohledem dnešních očí obětí banálního problému roku 2000 (označovaný jako Y2K problem). Některé počítače nedokázaly na přelomu

tisíciletí přečíst a nastavit datum na 1. ledna 2000, protože jejich číselný rozsah pro rok dosáhl maximální hodnoty a místo toho se vrátili na začátek – do roku 1900. CyberCoin z tohoto důvodu, z důvodu krátkozrakosti počítačových vývojářů byl nucen vyhlásit bankrot, a to proto, že CyberCoin zaznamenal řadu dvojitých transakcí, což znamenalo jeho zkázu.

I přes všechny možné systémové i tržní kolize digitální měny nikdy nepřestaly být populární, paradoxně do segmentu autorů začalo pronikat čím dál větší množství velkých firem. Příkladem lze uvést firmy jako Visa, či Mastercard. Visa přišla se svým konceptem Visa Cash a Mastercard zakoupil od společnosti National Westminster Bank elektronický peněžní systém Mondex. Ve výsledku i tak daly obě společnosti později přednost tradičnímu bankovníctví.

Poslední veliký předchůdce dnešních kryptoměn či přímo Bitcoinu je zmiňovaný Liberty dollar. Liberty dollar byl soukromý měnový systém založený v roce 1998 Bernardem von NotHausem. Předpokladem měny Liberty dollar bylo to, že na rozdíl od amerických dolarů a vůbec světových měn byl každý Liberty dollar kryt specifikou vahou drahého kovu. Například dvacet Liberty dolarů bylo nastaveno na jednu unci stříbra. Na rozdíl od ostatních alternativních měn měl každý Liberty dollar nominální hodnotu. Nominální hodnota vyražená na mincích však byla zpravidla vyšší než hodnota stříbra využitá k její výrobě. Za tímto stála tehdejší vzrůstající cena stříbra na světovém trhu. Americké úřady nezůstaly dlouho sedět v povzdálí. Vzhledem k tomu, že Bernard von NotHaus si pouze všiml toho, že americké dolary již desítky let nejsou ničím kryté a mohou tak podléhat zkáze skrze libovůli států a centrálních bankéřů. Bernard von NotHaus dle americké prokurátorky Anne Tompkins jednal proti zájmu státu a dopustil se dle jejích slov jedinečného případu terorismu. Dále tvrdila, že se von NotHaus snažil zničit měnu své vlastní země. A tak i Liberty dollar nedopadl moc slavně. Podobně dopadl i případ digitální měny Liberty Reserve, kterou využívalo přes jeden milion lidí. Americká vláda zde v tomto případě obvinila tvůrce Arthura Budkovskyho z praní špinavých peněz a společnost mu zabavila. V roce 2013 federální úřady a detektivové dopadly Budkovskyho ve Španělsku a zatkli ho. Do tohoto roku šlo o nejstarší digitální měnu, jelikož vznikla v roce 2001. Princip měny byl vcelku jednoduchý, a to v tom, že společnost převáděla tradiční peníze na Liberty Reserve dolary nebo Liberty Reserve eura, a poté z každého transferu účtovala jednorozhodný poplatek. Pointou bylo opět ukládání peněz do zlata, avšak Liberty Reserve nabízel i možnost ukládání do dolaru či eura. (Stroukal, 2018, s. 30)

Zde lze překlenout dobu až do roku 2008, kdy neznámá osoba nebo skupina lidí známa dnes pod jménem Satoshi Nakamoto vydala technický dokument popisující nový platební systém s názvem Bitcoin. Satoshi Nakamoto si v roce 2008 zaregistroval internetovou doménu

bitcoin.org. V říjnu téhož roku zaslal rozšířenou verzi návrhu bitcoinového systému do kryptografické e-mailové skupiny, kde se však setkal s většinou negativní reakcí. Jediným příznivcem se stal Hal Finney. Za projevenou podporu mu Satoshi Nakamoto zaslal beta verzi softwaru, který měl bitcoinový systém provozovat. Počátkem roku 2009 Satoshi Nakamoto zaslal finální verzi zdrojových kódů v jazyce C++ do kryptografické e-mailové konference a zároveň začal bitcoinový systém provozovat na několika vlastních počítačích. Milníkem se stal první blok (pořadové číslo 0) bitcoinového systému, který se nazývá základní (genesis) blok a je součástí zdrojových kódů. Obsah základního bloku je velice prostý a je v něm odkaz na článek Chancellor on brink of second bailout for banks (Elliot a Duncan, 2009) vydaného v americkém deníku Times právě 3.1. 2009. Odkaz na tento článek má dva účely:

- prokazuje, že základní blok nebyl vytvořen před datem článku,
- upozorňuje, že Bitcoin je konkurentem současného finančního systému.

Jednotlivé bloky si lze prohlédnout například na webových stránkách Blockchain.info, kde je možné spatřit i blok s pořadovým číslem 1. První transakce proběhla dne 12.01.2009, a to v bloku 170, kdy Satoshi Nakamoto zaslal 10 bitcoinů, jejichž příjemcem byl Hal Finney. V následujících měsících systém pouze a jen stagnoval, vzhledem k jeho nevyužívání. Na podzim roku 2009 se Martti Malmi za účelem přilákat nové uživatele rozhodl založit fórum bitocintalk.org. Záměr se vydařil a jeden uživatel pod přezdívkou NewLibertyStandard se zabýval myšlenkou obchodování bitcoinů za americké dolary. NewLibertyStandard a Martti Malmi provedli první transakci bitcoinů za dolary. Dne 12.10.2009 v bloku číslo 24835 Martti Malmi zaslal uživateli NewLibertyStandard 5050 bitcoinů. NewLibertyStandard zaslal na oplátku 5,02 amerických dolarů pomocí služby PayPal. Tehdejší cena bitcoinu byla stanovena podle ceny elektrické energie spotřebované při těžbě bitcoinů, tedy 1 000 bitcoinů za dolar. V roce 2010 přišel další milník, a to ten, když programátor Laszlo Hancz přišel s nápadem na využití grafických karet pro těžbu bitcoinů. Při těžbě pomocí procesoru počítače obvykle získal jeden blok 50 bitcoinů za den. Díky Hanczově vynálezu vytěžil cca 70 000 bitcoinů. Den, který se skloňuje v souvislosti s kryptoměnami a je současně označován za výročí Bitcoinu, je 22. květen. V roce 2010 jistá osoba v bloku číslo 57043 zaplatila celkem 10 000 bitcoinů za dvě pizzy v hodnotě 50 dolarů. (Lánský, 2018, s. 5-6)

I samotná Česká republika má své nenahraditelné místo v historii kryptoměn. V roce 2010 dne 27. listopadu český programátor Marek Palatinus vytvořil první těžební skupinu (označováno jako mining pool), nyní pod názvem SlushPool. Podstatou těžební skupiny je to,

že skupina umožňuje uživatelům spojit svůj výpočetní výkon za účelem vytěžení bloku. Následně se odměna za vytěžení bloku rozděluje mezi uživatele poměrně dle množství výpočetního výkonu, kterým přispěli na těžbu. Zároveň Marek Palatinus o dva roky později vytvořil jednu z neznámějších a nejrozšířenějších kryptopeněženek se jménem Trezor. Jedná se o první hardwarovou peněženku na světě.

S rozšířením do světa v roce 2013 byl zprovozněn v USA v San Diegu první bitcoinový automat umožňující zakoupení bitcoinů za běžné finanční prostředky, konkrétně za fiat měnu. O další dva roky později již došlo k masivnímu rozšíření kryptoměn i do sféry akademické. Kryptoměny se staly součástí výuky na vysokých školách v Nicosii, Princetonu a Praze. V roce 2017 došlo k přidání symbolu pro Bitcoin, který je znázorňován velkým písmenem B, přeškrtnutým dvěma vodorovnými čarami, prakticky stejně jako S u dolaru. K další události došlo v témže roce, kdy v bloku číslo 478 558 došlo k rozštěpení bitcoinového systému na dva systémy: původní Bitcoin a nový Bitcoin Cash. K tomuto rozdělení došlo z důvodu maximální velikosti bloku, kdy Bitcoin Cash umožňoval bloky o maximální velikosti 8 MB, zatímco Bitcoin pouze 1000 kB. (Lánský, 2018, s. 8)

2.2 Dělení kryptoměn

Každou z kryptoměn je možné diferencovat do určité podskupiny kryptoměn. Dělí se do tří skupin podle specifických vlastností. Stejně jako v historii kryptoměn, resp. v celkovém kryptodění hraje tu vůbec nejdůležitější úlohu samotný Bitcoin. Právě podle něho se nejčastěji kryptoměny dělí, a to na základě toho, jak vznikají. Dá se říct, že Bitcoin přinesl základní stavební kámen pro vznik dalších kryptoměn.

Dělení kryptoměn probíhá ve třech skupinách:

- Bitcoin,
- altcoiny,
- tokeny.

Bitcoin z hlediska své důležitosti, z hlediska své historie a svých vlastností zaujímá svoji vlastní skupinu, která se odděluje od ostatních.

Druhou skupinou jsou altcoiny, kde je často základem samotný Bitcoin. Platí to jak pro protokol (resp. specifikaci datových struktur a síťové komunikace), tak pro softwarovou imple-

mentaci, kterou altcoiny postavené nad Bitcoinem odvětvují z volně dostupného softwaru repositáře Bitcoinu a dále upravují. Samotný pojem altocin je odvozen od názvu „alternativní kryptoměna“. Ovšem jak již bylo zmíněno, tak ne všechny altcoiny vycházejí z Bitcoinu. Jiným existujícím protokolem je tzv. CryptoNote, který rozšiřuje anonymizací schopnosti kryptoměny. Také jsou některé kryptoměny řešeny zcela rozdílně oproti Bitcoinu. Dělení některých kryptoměnových zástupců lze provést pomocí toho, jde-li pouze o měnu, nebo o nějakou univerzálnější platformu, která může sloužit jako základ odvozených projektů. Altcoiny stejně jako Bitcoin mají často předem známou monetární strategii, tedy často deterministickou – jednoznačnou a známou dopředu. Lze ji mít jako u Bitcoinu konečně inflační, kde u Bitcoinu se ví kolik mincí kdy existuje, a že maximální počet jich bude jedenadvacet milionů a nikdy více. Podobným příkladem je měna Litecoin, jejíž zdroje uvádí, že by mělo být v konečné fázi maximálně čtyřiaosmdesát milionů. Naopak může být i nekonečně inflační se známým tempem uvolňování mincí nových, jako například u měny Monero. Důležitou součástí altcoinů je také těžba, tedy distribuce mincí. Může vycházet z klasické těžby, nebo těžba nemusí existovat vůbec a při uveřejnění měny je vydáno i určité množství jejich mincí, jako například u měny Ripple. Velmi významnou je odlišnost kryptoměn ve strategii konsensu (shody) na stavu, resp. zápisu do ledgeru (blockchainu). Zápisem do ledgeru se potvrzují transakce, což má vliv i na jejich rychlost. Je potřeba vědět všeobecně, kdo a kdy může zapisovat (vytvářet nový blok). O to se stará klasická těžba pomocí proof-of-work, kdy je v procesu tvorby dalšího bloku zvýhodněn ten, kdo vykoná víc práce za jednotku času. (Stroukal, 2018, s. 142)

Třetí specifickou skupinou kryptoměn jsou tokeny. Ty se liší tím, že obvykle nemají vlastní síť a leží na Blockchainu jiné kryptoměny. Právě k tomu je nutné mít platformu – blockchainovou síť. V podstatě mohou tokeny představovat jakékoliv aktivum, které je zaměnitelné a obchodovatelné. Vytvoření takového tokenu je tak z hlediska náročnosti oproti altcoinům o mnoho snazší. Nejznámější a nejčastější platformou je Ethereum. Nejoblíbenějším standardem je ERC-20, kde je mnoho známých kryptoměn, například: Golem, Augur, či Omisego.

2.3 Technologie kryptoměn

Každé aktivum či prvek má svoji definici, základní prvky, vlastnosti a také problematiku toho, jak funguje. Nejinak tomu je se samotnými kryptoměnami. Následující kapitola se této

problematicke bude věnovat. Budou popsány vlastnosti kryptoměn, kryptografie, těžba kryptoměn až po samotné transakce kryptoměn a software, kde jsou kryptoměny uchovávány, tedy peněženky.

2.3.1 Kryptografie

Kódování je dnes nejdůležitější formou tajného zpravodajství na světě. Formy tajného zpravodajství, ačkoliv to může znít zvláště, jsou propojené i s kryptoměnami. Jak se tedy definuje kryptografie? Dle několika autorů počátky vycházejí resp. sahají až do období Mezopotámie a antického Řecka. V případě druhé jmenované říše se jedná o rok 460 před naším letopočtem. Od té doby se samozřejmě kryptografie silně vyvinula. Prošla několika milníky, hlavně v období válek až po dnešní moderní dobu. V jedenadvacátém století se s kryptografií lidé setkávají hlavně v oblasti IT technologií, skrze problematiku ochrany osobních údajů (například nedávno přijaté hledisko GDPR; zdali jsou citlivé osobní údaje dostatečně zabezpečené nebo nikoliv apod.).

Kryptografie je dnes definována jako soubor vědních poznání, která se zaměřují na šifrování a převádění prostého běžného textu na text, který lze rozluštit pouze s naučenou znalostí. Využívá matematických algoritmů, které využívají i kryptoměny, tzn. hashovacích funkcí, k převodu běžného textu, který je pro běžného jednotlivce čitelný, do textu, kde jsou takové kombinace čísel a písmen, které donutí nabýt osobu dojmu, že nedávají absolutně žádný smysl. Tomuto se říká „hash“. (Kahn, 1996. s. 22)

2.3.2 Peer-To-Peer

Pojem, který se často označuje jednoduchou zkratkou P2P. Peer-to-peer se využívá pro označení typu počítačové sítě, kde jsou všechny uzly navzájem rovnocenné a jednotliví uživatelé spolu komunikují napřímo a nikoliv prostřednictvím centrálního uzlu (serveru). Od asymetrického modelu klient-server v peer-to-peer s rostoucím množstvím klientů roste i přenosová kapacita sítě. Velkou nevýhodou symetrie P2P je však obtížnost počátečního navázání komunikace mezi určitými uživateli. (Stroukal, 2018, s. 24)

2.3.3 Adresa

Je další součástí mozaiky kryptoměn, kdy se jedná o unikátní číslo vygenerované odesílatelovi nebo příjemci. Obdobně lze uvést adresu i u bankovních účtů, kdy příjemce či odesílatel

musí peníze odesílat na unikátní adresu složenou z osobního čísla účtu a unikátního kódu banky. V případě kryptoměn se toto složené číslo skládá ze zakódovaného řetězce alfanumerických znaků, které mají následující vlastnosti (Stroukal, 2018, s. 38):

- rozlišují se malá a velká písmena, neplatí pro adresu Bech32,
- délka adresy je 27-34 znaků (podle škálování typu BIP 174 je počet 14-74 znaků),
- začíná označením verze – číslicemi 1 nebo 3 pro formát PS2SH nebo bc1 pro formát Bech32,
- neobsahuje znaky, které jsou typograficky zaměnitelné jako 0 a O, či 1 a I.
- poslední znaky obsahují kontrolní součet (zabezpečení proti špatnému opsání, či vykopírování)

Příkladem adresy pro P2SH je *3P14159f73E4gFr7JterCCQh9QjiTjiZrG*, příkladem adresy typu Bech32 je *bc1qar0srrr7xfkvy5l643lydnw9re59gtzwwf5mdq*.

Jak bylo uvedeno u kapitoly rozdělení kryptoměn, valná většina kryptoměn je odvozena od Bitcoinu. Mají tedy svá určitá pravidla. Pravidla uvedená výše jsou příkladem právě pro kryptoměnu Bitcoin. Například pro kryptoměnu Litecoin platí určité odlišnosti, avšak samotný princip zůstává absolutně neměnný.

Otázkou zůstává, v čem spočívá samotný rozdíl mezi výše uvedeným bankovním účtem a kryptoměnovou adresou. Odpověď je jednoduchá – v tom, že každý jedinec má přiřazený pouze jeden typ jednoho čísla účtu (jedinečné). Naproti tomu v případě drtivé většiny kryptoměn si každý může vygenerovat novou adresu pro každou novou transakci. Uživatelsky tato schopnost není nikterak obtížná, například prostřednictvím peněženky Trezor. Tento princip systém využívá hlavně z důvodu ochrany uživatele, kdy poskytuje každá nová vygenerovaná adresa uživateli určitou pseudoanonymitu.

2.3.4 Peněženka

Pro bezpečné uchování kryptoměn jako je Bitcoin, Monero, či Ethereum atd. se velmi doporučuje jejich vložení do kryptoměnových peněženek. Těch je značné množství. V zásadě se dělí na dva typy: na softwarové peněženky a hardwarové peněženky. Oba tyto typy mají svá určitá specifika a zásadnosti. Liší se v typu zabezpečení a v uživatelském rozhraní. Největším rozdílem je princip uchování kryptoměny. Na hardwarovou peněženku se vloží kryptoměna se

a umístí mimo „online“ sféru. Zjednodušeně řečeno, vloží se na USB disk, ke kterému má přístup jen uživatel, který USB disk vlastní. Naopak softwarová peněženka je umístěna v online prostředí, tedy kryptoměny jsou umístěny „na internetu“, a zde samozřejmě existuje větší šance možného odcizení kryptoměn z účtu.

Jak bylo v textu výše uvedeno, tak tyto peněženky generují jedinečné adresy pro každou novou platbu. Kryptoměny tedy obecně přinášejí v této sféře lepší finanční soukromí jedinečných adres, které patří stejné bitcoinové peněžence. (Ajiboye, 2019, s. 98)

2.4 Těžba kryptoměn

Významným prvkem ke správnému fungování kryptoměn je těžba. Ta slouží k uchování transakcí do blockchainu, kdy těžaři ověřují transakce, které byly zadány odesílateli či příjemci platby. V momentu, kdy shledají transakce jako platné, je shlukují do bloků, které následně zanesou do účetní knihy. Může se zdát, že těžba kryptoměn působí na laika zcela složitě, že se jedná o řešení různých složitých rovnic, napříč propojenými mezi sebou. Opak je však pravdou. Princip těžby zcela souvisí s náhodou. Samozřejmě si tato hra na náhodu žádá spotřebování určité elektrické energie.

Těžba, pro kterou se používá i jiný termín, tzv. mining, je proces, při kterém se pomocí strojově náročného výpočtu hledá další blok pro napojení do blockchainu. Pokud je validní blok nalezen, znamená to, že je splněna základní podmínka, a to ta, že hash je nižší než určitý cíl (tzv. parametr target). Tento cíl se odvozuje z aktuální obtížnosti, která se mění každých 2016 bloků v závislosti na rychlosti jejich nalezení tak, aby průměrná rychlost generování nových bloků činila 1 blok za 10 min. Pakliže by blok nesplnil podmínku na nízký hash, je nutné ho jeho sterilizací pozměnit a zkusit hash přepočítat. Na úplných začátcích se těžba kryptoměn (hlavně Bitcoinu) prováděla na procesorech samostatných osobních počítačových soustav, kdy tak její obtížnost stoupala, a to konkrétně z důvodu vyššího zapojení počítačů při stejné rychlosti generování bloků. Postupně se přesouvala od CPU (mezi lety 2009 a 2010) k paralelním výpočetním architekturám, tedy od GPU (grafické karty, rok 2011 až 2015) přes FPGA (programovatelná hradlová pole, rok 2011 a 2012) až k ASIC (zákaznické hardwarové obvody, navrženy speciálně k počítání jednoho typu výpočtu). (Stroukal, 2018, s. 82)

Předpokladem pro správné zacházení s kryptoměnami je decentralizovaná těžba. To znamená, že pro uživatele je velmi žádoucí, aby se těžba nesoustředila do jednoho centrálního místa, nýbrž naopak do celého světa. Je to dáno zejména z důvodu možné vysoké kontroly nad

kryptoměnami. Existuje tu možnost, že by jeden těžař získal více než 51 % na trhu s těžbami kryptoměn, tudíž by reálně získal moc spravovat technologii blockchain do vlastní vůle, což by popíralo základní vlastnost kryptoměny, onu decentralizovanost. Nejinak tomu je s fungováním samotné sítě na těžení kryptoměn, která musí zůstat v neustálém provozu, aby nedošlo k výpadkům potvrzování transakcí a zpomalení celého systému. Je tak zcela žádoucí, aby těžaři svoji aktivitu neomezovali a těžili kryptoměny nepřetržitě v jedné líně.

Odměny za těžbu kryptoměn získává vždy pouze jen jeden těžař, který vyhrál v soutěži o náhodu. Nic takového, jako je částečná odměna pro všechny těžaře, neexistuje. Další možnosti odměn pro těžaře jsou poplatky za vykonání transakce, které se pohybují ve velmi nízkých úrovních. Tyto poplatky mají být motivací pro těžaře, proč vybranou zaslanou transakci zahrnout do svého bloku. Poslední možnou odměnou za vytěžení kryptoměn je generující transakce, a ta je již součástí vytěženého bloku. V počátcích těžby Bitcoinu bylo za vytěžení prvních 210 000 bloků odměna 50 Bitcoinů. S postupem času však tento proces klesá vždy s odměnou na polovinu.

Jedná se o pojem půlení, neboli halving. Zakladatelé Bitcoinu nechtěli, aby zásoba mincí rostla do nekonečna. Místo toho stanovili časový plán vydávání bitcoinů, který měl raketový start s 50 Bitcoinů za odměnu, nicméně postupně spěje k tomu, že se žádné nové mince vydávat nebudou. V základním kódu Bitcoinu je zabudováno půlení blokové odměny, které odměnu přibližně každé čtyři roky o polovinu snižuje. Zhruba za deset let dojde k dalším třem půlením odměny, což bude mít za následek, že 99 % Bitcoinů bude vytěženo a jeden blok vytvoří méně než 1 Bitcoin. Konec těžby je určen kolem roku 2140. (Pritzker, 2020, s. 44)

Identický proces je nastaven pro silnou většinu kryptoměn. Například kryptoměna Ethereum má odměnu za vytěžení nového bloku v blockchainu více než 3 ETH.

Aby byla těžba kryptoměn efektivní, z většiny těží v dnešní době pouze úzce specializovaní těžaři, kteří každoročně investují statisíce či miliony korun do extrémně výkonných počítačových strojů. Sdružení jsou v několika velkých skupinách, tedy poolech. Mezi největší těžební pooly patří BTC.com, AntPool, ViaBTC a BTC.TOP. Těžaři tak těží společně a generují transakce včetně poplatků, jež jsou odváděny poolu, který je následně rozděluje. Eliminuje se tak riziko, že těžaři nedostanou žádnou odměnu. Motivace je pak velice jednoduše vysvětlena na následujícím příkladu. V rámci těžení se zdá být 50 BTC jako velmi zajímavý výdělek, avšak aby tuto odměnu těžař obdržel, je zapotřebí mít obrovský výpočetní výkon. Je tedy velmi nepravděpodobné, že k takové odměně dospěje. Pokud se však jednatel přidá do poolu, který

má podíl na trhu 20 % výpočetní kapacity sítě, získá tak dvacetiprocentní šanci, že tento blok vytěží a z vytěžených bitcoinů získá následně svou poměrnou část (0,1 % celého výkonu v poolu sdružujícím 20 % kapacity je 0,5 % výkonu v rámci poolu), tedy 0,125 BTC. (Stroukal, 2018, s. 86)

2.5 Hash

Důležitým pojmem spojeným s kryptoměny je hash. Ten je součástí jak protokolu, tak i uchování bezpečnosti informací v internetovém prostředí. Hashovací funkce v obecné rovině vyjadřuje matematický proces, který přijímá vstupní data libovolné velikosti a vykonává na nich přesné operace a následně vrací výstupní data s jasně danou velikostí. V různých situacích se hashovací funkce využívá jako sekvence písmen a čísel libovolné délky jako vstupu a následně vrátí řetězec písmen a čísel s pevně danou délkou kombinace. Jestli budou vstupní data různé délky nemá na hashovací funkci žádný vliv. Můžou mít délku jednoho písmena, ale i jedné knihy.

Běžný uživatel nespojený s kryptoměny hashovací funkce také využívá, ačkoliv si to v mnoha případech jednotlivci ne zcela uvědomují. Využívají se totiž při přidělení a ukládání hesel, např. u jednotlivců, kteří se rozhodli vytvořit si heslo například na určité webové stránce. Uživatel si vymyslí heslo, které projde hashovací funkcí a následně se výsledný hash, který hashovací funkce vyprodukovala, uloží k přihlašovacímu menu. Vždy, když se uživatel rozhodne přihlásit na webový portál, zadá heslo složené z písmen a čísel, a to projde hashovací funkcí, kde server zkontroluje, zdali se výsledek shoduje s uloženým záznamem.

Příkladem využití hashovacích funkcí v kryptoměnách bude opětovně Bitcoin. V Bitcoinu je hashovací funkce součástí zabudovaného algoritmu hashovacího bloku. Tento algoritmus se využívá na zápis nových transakcí v blockchainu prostřednictvím těžby.

Vzhledem k tomu, že účast v systému jako je Bitcoin je čistě dobrovolná a nevyžaduje povolení a lidé se mohou připojit podle své vůle, aniž by je někdo řídil, tak se počet těžářů každým okamžikem mění. Hash má tedy přímý vliv na samotnou těžbu Bitcoinu, kdy jakmile je potřeba zvýšit obtížnost platných hashů, když se k loterii připojí víc hráčů, a jak ji naopak snížit, když hráči loterii těžby opouští, tak aby rychlost vytváření bloků zůstala stabilní. Zásadní otázka. Vysoká rychlost hashování vypovídá o tom, že velké množství lidí se účastní těžby a tím pádem systém funguje hladce. Naopak, klesne-li hashovací rychlost, tak se cíl přehodnotí a náročnost hashování se zjednodušuje. V praxi to znamená, že je-li rychlost příliš velká, tak

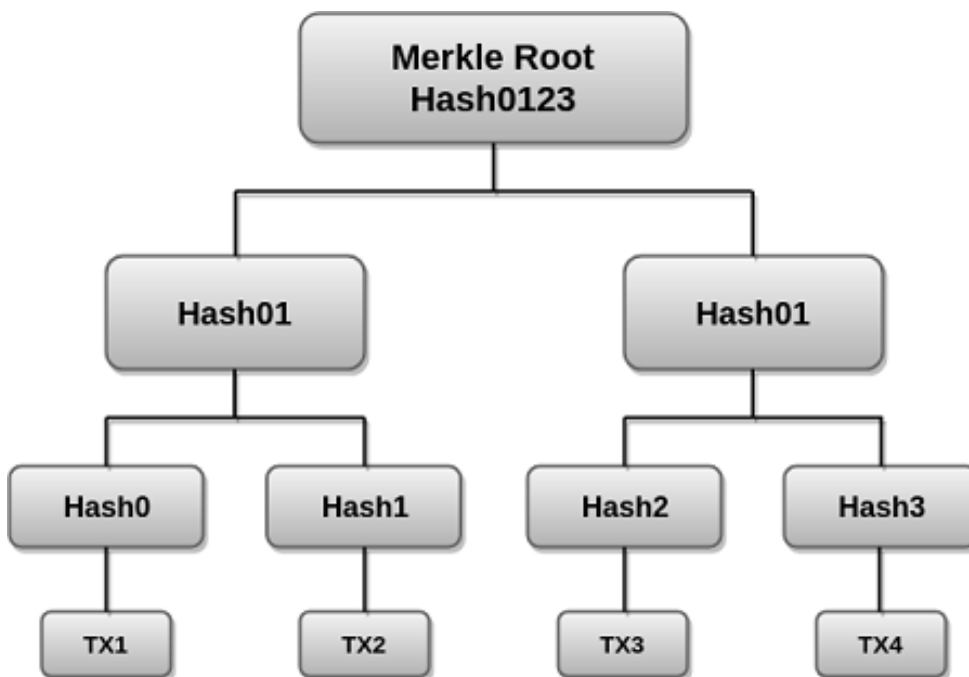
při dalším přepočtu náročnosti cíle se přidá další nula na začátek řetězce. Je-li tomu naopak, že hashovací rychlost je příliš nízká, tak se počet nul potřebných k hashu sníží. (Pritzker, 2020, s. 48)

2.6 Blockchain

Pojem blockchain byl již několikrát zmíněn, avšak ne zcela vysvětlen. Vzhledem k tomu, že se pravděpodobně jedná o absolutně nejdůležitější součást kryptoměn, tak technologii blockchain bude věnována speciální pozornost.

Blockchain jsou v zásadě databáze, které nejsou uloženy na centrálním serveru, ke kterému přistupují všichni uživatelé. Odborně se též využívá pojmu řetězce bloků, který vychází ze spojového seznamu bloků. Spojení seznamu vznikne tak, že je dosaženo hashe předchozího bloku v datech bloku následujícího. Blockchainové záznamy jsou ukládány do počítačů uživatelů celého světa.

Na počátku blockchainu byl založen úplně první blok, který je známý pod názvem genesis blok. Ten nemá vyloženě předka, nýbrž za předka je považováno číselné vyjádření nula. Každý následující nově vzniklý blok má tak svého předka.



Obrázek 1: Merkeleho strom

Zdroj: javatpoint.com

Merkelův strom není spjatý od počátku věku pouze s kryptoměnami. Právě naopak. Principem Merkeleho stromu bylo vyřešit proplánované zabezpečení a ověřování údajů. S tím právě přišel Merkeleho strom. Ověřování dopomohlo k tomu, aby nebyly zasílané falešné údaje. Diagram v obrázku 1 znázorňuje, jak Merkeleho strom vypadá. Každý hash vyšší úrovně je tvořen hashem nižší úrovně, tak jak již bylo zmíněno v odstavci předchozím. Na nejnižší úrovni, zde označené TX3, jsou vložená data. Na nejvyšší úrovni je uzel, který obsahuje informaci o všech těchto datech. Merkeleho strom, resp. následující struktura umožňuje velmi jednoduché vyhledávání dat ve stromě a jejich následující zpracování, kdy v jednom hashu může být uložených několik tisíc dat. Pro využití v samotném blockchainu byl využitý Merkeleho strom později. Několik řad Merkeleho stromů za sebou bylo vložených do bloků, kde každý následující blok obsahuje informace o tom předcházejícím. A právě v tom posledním se nachází celá historie celého řetězce. (Lafaille, 2018)

Základní datovou jednotkou blockchainu je předmět nazývaný „blok“. To jsou soubory, ve kterých jsou donekonečna uchovávané údaje týkající se veškerých kryptoměn. V každém nově vytvořeném bloku jsou zahrnuty všechny transakce týkající se určité odesílané měny. Jak bylo definováno, tak blockchain je v podstatě kniha, kam se zapisují ony bloky místo stránek. Tyto bloky následně již nikdy nemohou být ani přejmenované, ani změněné nebo odstraněné. Z hlediska výhodnosti si tak lze povšimnout, že k uskutečnění plateb v rámci kryptoměn není třeba žádného zprostředkovatele neboli institucí jako jsou banky, příp. nebankovních institucí, které mají na starost převody peněz.

Blockchainový protokol

V zásadě existuje hned několik blockchainových protokolů, ale těmi dvěma nejdiskutovanějšími jsou Proof of Work a Proof of Stake.

Proof of Work je nejstarším typem algoritmů tvorby bloků. Nazývá se také jako „důkaz prací“. Je to matematický algoritmus, který byl vybudován ještě před první kryptoměnou, pro ochranu před útoky známé jako DDoS. Principem důkazu o práci je hledání řešení matematického problému, kdy se těžař snaží najít část hash bloku, které nesou informace o bloku předchozím. Výpočty by měly být snadné a rychle ověřitelné. V případě, že hash nalezne jako první, je odměněn. První kryptoměnou, která používala důkaz prací je Bitcoin. (Lánský, 2018, s. 24)

Proof of Stake je alternativním přístupem k dosažení konsenzu na cílené rozšíření kryptoměnového systému. Je nazýván buď jako důkaz podílem, nebo důkaz o sázce. V PoS získávají

právo vytvořit nový blok vlastníci jednotek dané kryptoměny. Čím více jednotek dané kryptoměny vlastní, tím mají vyšší pravděpodobnost, že budou moci vytvořit nový blok. Zde se na rozdíl od protokolu Proof of Work nepoužívá pro tvorbu nového bloku pojem těžba bloku, nýbrž slévání bloku a ražení bloku. Výhodou Proof of Stake je, že na rozdíl od protokolu Proof of Work nepotřebuje zdaleka takový vysoký výpočetní výkon. Tím klesá spotřeba energie a i celkové náklady. PoS funguje na principu, kdy každý, kdo má zájem se podílet na ověření transakcí, musí vsadit určitou část peněz. Sázka je vyhodnocována tak, že postupně náhodně vyřazuje vsazené peníze a vybírá náhodně jednoho, kterému přiřkne odměnu. Peníze jsou mezi vyhodnocením sázky uloženy do peněženky, kde jsou lidově řečeno zmrazené. (Lánský, 2018, s. 38)

2.7 Právní rámec kryptoměn na našem území

Kryptoměny v dnešní době a vůbec všeobecně v epoše nového milénia zažívají velice dynamický a progresivní vývoj. Důležité je však to, jak si stojí kryptoměny v otázce posouzení právního aspektu na území České republiky. Je zřejmé, že by stát měl v národní legislativě progresivně reagovat a tento moderní trend zařadit i do svých právních aspektů.

Právní forma bude v následující kapitole probírána s důrazem na Českou republiku, nikoliv na státy sousedící. Z hlediska obecného pohledu českého práva na kryptoměny je právní řád velmi kusý.

Veřejné právo se zabývá kryptoměnami prakticky pouze tam, kde je to z hlediska zákonodárců nejdůležitější, tedy v oblasti praní špinavých peněz a legalizace výnosů z trestných výnosů. Přesně řečeno, zákon č. 253/2008 Sb, o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Uvedený zákon v § 4 odst. 9 popisuje virtuální aktivum těmito slovy „*Virtuálním aktivem se pro účely tohoto zákona rozumí elektronicky uchovatelná nebo převoditelná jednotka, která je způsobilá plnit platební, směnnou nebo investiční funkci, bez ohledu na to, zda má nebo nemá emitenta* ". V minulosti se namísto virtuálního aktiva hovořilo o virtuální měně. Tento pojem již právo zaměnil za nový pojem, a tedy za virtuální aktivum. Tato změna nabyla účinnosti ke dni 1.1.2021.

Jakákoliv jiná zmínka o kryptoměnách však v soukromém právu chybí, a proto je potřeba se na kryptoměny podívat pohledem občanského zákoníku. Několik právních názorů na Bitcoin a obecně kryptoměny nahlíží z hlediska ustanovení § 489, kde dle právní definice je věcí vše, co je rozdílné od osoby a slouží k potřebě lidí. Toto kryptoměny bezesporu splňují. Zejména

pro obyvatelstvo splňuje dvě základní roviny, a to jednak jako směnitelná hodnota, ale také představují formu investic. Obecně lze tedy říct, že Bitcoin je možné označit za věc v právním smyslu. Právní vztah mezi kupujícím a prodávajícím je další částí z českého práva, na kterou se vyplatí detailněji podívat. Standardně za poskytnuté zboží a službu platí klasickými fiat penězi a vzniká tak standardní kupní smlouva. Ačkoliv se může zdát, že v případě kryptoměn je tomu stejně, tak nikoliv. Aby se mohlo jednat o závazkový vztah ve formě kupní smlouvy, tak by kupující musel zaplatit kupní cenu v uznávané měně, avšak Česká národní banka kryptoměny jako platební prostředek neuznává, a tudíž se o kupní smlouvu optikou českého práva jednat nemůže. Jedná se tak o vztah čistě závazkový ve formě směny. Při směně nedochází k výměně zboží za peněžní ekvivalent, ale pouze se převádí vlastnická práva k věcem nabitým v právním smyslu. Jak již bylo zmíněné výše, tak na Bitcoin české právo nahlíží jako na věc, proto vztah vymezený mezi osobou platící Bitcoinem a osobou poskytující zboží či službu bude směnou. (epravo.cz, 2022)

Stanovisko České národní banky se během let prakticky nemění. Od začátku představitelé ČNB a guvernér říkají, že kryptoměny nejsou peníze, a to z důvodu toho, že se nejedná o peněžní prostředky ve smyslu zákona o platebním styku, tedy ani o bezhotovostní peníze, ani o tzv. peníze elektronické, nýbrž naplňují znaky klasických komodit. Zároveň ke kryptoměnám nepřístupují negativním, ale ani pozitivním názorem. Spíše se uvádí velmi neutrální postoj. Česká národní banka se nesnaží vytvářet nějaká preskriptivní detailní pravidla pro regulaci kryptoměn, protože by to mohlo být v konečné fázi kontraproduktivní. Všeobecně se i dá říct, že ČNB nezajímá, kam bitcoiny zařadit, nýbrž zdali obchodování s nimi dopadá na právní předpisy, na jejichž dodržování ČNB dohlíží. (ČNB, 2022, online)

Vzhledem k tomu, že se Česká republika nachází v uskupení Evropské unie, tak na Česko dopadají i právní aspekty Evropské unie. V rámci Evropské unie byl zaveden pojem digitální měna. Tento pojem definovala Evropská centrální banka, která jej označila za typ neregulovaných digitálních peněz, které jsou při platbách akceptovány členy online komunit, kterých jsou součástí a kontrola obvykle spadá do působnosti jejich vydavatelů. (Martinák, 2015, str. 49)

Poslední částí z hlediska právního aspektu České republiky bude nahlíženo z hlediska daňového systému. V České republice fyzické osoby zdaňují příjmy dle zákona č. 586/1992 Sb, zákon o daních z příjmu, všechny příjmy, při kterých dochází ke zvýšení majetku. Od daně jsou zpravidla osvobozeny osoby s příjmy do výše 30 000 Kč, pokud se jedná o příležitostný příjem a nikoliv o hlavní předmět podnikání dané osoby. Zároveň jsou osvobozeny i dary v rámci ro-

diny v přímé linii do výše až 5 000 000 Kč. V rámci státu je zajímavý posudek na zdanění kryptoměn v oblasti investic. Příkladem jsou příjmy z prodeje cenných papírů, které jsou od daně osvobozené v případě, kdy doba mezi nákupem a prodejem stejných cenných papírů dosáhla alespoň tří let. Zároveň mohou být od daně osvobozeny v případě, kdy příjmy z prodeje všech cenných papírů v daném kalendářním roce nepřesáhly 100 tisíc korun. Kryptoměny na rozdíl od cenných papírů nic jako tříletý časový test neznají, ani neexistuje žádná výjimka v podobě 100 000 Kč. V případě investic do kryptoměn rozdíl mezi jejich prodejní a nákupní hodnotou podléhá patnáctiprocentní sazbě daně z příjmu fyzických osob.

2.8 Využití kryptoměn v reálném životě

Obecně kryptoměny či digitální aktiva mají v dnešním moderním světě velmi široké pojetí. V následující kapitole dojde k představení hned několika možností, jak potencionálně kryptoměny využívat, a kde se s nimi v této době kratší či delší dobu pracuje.

2.8.1 Kryptoměna jako investice

Kryptoměna jako investiční instrument. Převážná část osob, nebo podniků využívá segment kryptoměn jako investic. Ne všechny kryptoměny se ale dají pokládat za investici v podobě získání budoucího zisku. Existují určité části kryptoměn, které se nevyužívají pro investice. Jsou jimi typicky nazývané „stable coin“y. Zde se jedná o kryptoměny, které uchovávají svoji hodnotu vůči americkému dolaru v poměru 1:1, příkladem takové kryptoměny je Tether a USD Coin.

Zbytek kryptoměn je však využíván hlavně pro investice. Z pozice uživatele není nikterak obtížné si je zakoupit na jedné z kryptoměnových burz jako jsou coinbase.com, nebo binance.com. Zde za směnu lidé zaplatí v určitém kurzu vůči své měně, nejčastěji za USD nebo Euro, kdy si připsí virtuální kryptoměnu, kterou si nejčastěji odešlou na kryptoměnovou peněženku, o kterých již byla řeč. Předpokladem investice je budoucí zhodnocení daného aktiva v průběhu měsíců nebo let. Nejčastěji obchodovatelné kryptoměny se řadí dle tržní kapitalizace, o které bude zmíněno později.

Obecně v platnosti ve světě investic se za nejúčinnější investiční strategii považuje dollar-cost-averaging, ve zkratce známou jako DCA. Jedná se zároveň o nejvíce využívanou strategii v oblasti kryptoměn. Zjednodušeně vysvětleno se jedná o strategii, který má za cíl pravidelné a dlouhodobé investování stejné částky do jednoho investičního nástroje, zde v tomto případě

kryptoměny. Samotným principem je fakt, že investor investuje stejnou částku bez ohledu na to, zdali je kurz investičního nástroje vysoký či nízký. Investorovi tak odpadá otázka – tzv. načasování trhu, tedy nakoupit pouze tam, kdy je kryptoměna na nízkém kurzu a prodat na vysokém. Jedná se tak o průměrování nákladů ke snížení potencionální ztráty a zvýšení potencionálního výnosu.

2.8.2 Kryptoměna jako platební prostředek

V roce 2022 se kryptoměny více a více využívají pro každodenní platby. Kryptoměnamí lze zaplatit za produkty nebo služby, které poskytují podnikatelé. Je následně na podniku, které kryptoměny za platby přijme. Obecně se však využívají hlavně nejznámější kryptoměny určené k platbám, tedy Bitcoin, Litecoin, případně Ethereum. Každá z těchto kryptoměn má své unikátní vlastnosti. Příkladem v České republice mohou být internetové portály využívající platby prostřednictvím kryptoměn. V případě největšího internetového prodejce společnosti Alza.cz se jedná o průkopníka v placení kryptoměnamí. Prakticky cokoliv, co si uživatel chce na tomto portále zakoupit, může uhradit i prostřednictvím kryptoměn, aniž by je potřeboval zasílat na kryptoměnové burzy, tam je směnit na peníze, které by následně uživatel zaslal na svůj bankovní účet a až posléze zaplatil. Toto již není potřeba. Nyní uživateli postačí jeho kryptoměnová peněženka, prostřednictvím které dokáže zaplatit. Navíc v posledních letech zažila velké rozšíření funkce Lightning Network. Tu mnozí příznivci považují za nejlepší cestu v oblasti placení. Ve zkratce se o platbách přes Lightning Network dá říct, že probíhají nejčastěji pomocí QR kódů, a platby jsou tedy jak rychlé, tak i velmi levné. Kryptoměnamí se tak nemusí platit pouze přes internetové prodejce jako je Alza, avšak například i v restauracích, kavárnách a obdobných zařízeních.

2.8.3 Ostatní využití kryptoměn

Kromě využití kryptoměn jako nástroje platby či investice existují i další způsoby jejich využití. Jedním z nich je postavení kryptoměny na stejnou rovinu jako například americký dolar, tedy coby oficiální platidlo. Středoamerický stát Salvador se rozhodl prostřednictvím svého prezidenta Nayiba Bukeleho zavést oficiální platidlo Bitcoin. Právní rámec je ošetřen prostřednictvím vydaných zákonů. Ten dále předpokládá, že na směnu Bitcoinu nebude v žádném případě vybírána daň z kapitálového zisku a pouze trh určí kurz vůči americkému dolaru, který se v této zemi normálně využívá. Toto vše je podpořeno národním IT systémem a aplikací digitální

peněženky, kam se bude moci přihlásit každý občan Salvadoru. Toto vše má být doplněné rekonstruováním soustavy bitcoinových automatů na výběr či vklad a směnu peněz za Bitcoin. Stát se tak stal oficiálně první zemí, která zpřístupnila kryptoměnu coby stejnou formu placení. Na toto však zareagovala i ratingová agentura Moody's, která hodnotí úvěrovou spolehlivost země. Ta snížila konečné ohodnocení. Zároveň v roce 2022 vyzval Mezinárodní měnový fond Salvador k tomu, aby upustil od Bitcoinu. MMF považuje rizika spojená s Bitcoinem za příliš vysoká pro finanční stabilitu, integritu a ochranu spotřebitele. Salvador zareagoval tak, že přikoupil další množství Bitcoinu a nedal tak na doporučení MMF. Bude konkrétně velmi zajímavé z hlediska právního i fiskálního vývoje sledovat, jak se v tomto ohledu bude tato středoamerická země vyvíjet.

Dále je potřeba zmínit, že to není pouze Salvador, který prosazuje ve velké míře kryptoměny jako běžný platební prostředek. S rozvojem finančnictví souvisí i vysoký rozvoj IT technologií, dopravy a cestovního ruchu, ve kterém by bylo rovněž možné využít kryptoměny jako platební prostředek. Po vzoru Salvadoru zavedly do svého platebního systému kryptoměny hlavně státy Blízkého východu, které se považují za jedny z nejmodernějších celků světa.

2.9 Rešerše odborné literatury

Řada autorů v minulosti zkoumala možnosti investic do kryptoměn jako celků, případně do části segmentu kryptoměn. Derks, Gordijn a Siegmann zkoumají možnosti těžby kryptoměn a výnosnosti na jejich denních bázích. K tomu využívají počty, které jsou prakticky stejné s těmi, které se využívají k výpočtům ziskovosti kryptoměn v delších intervalech. Jejich publikace zkoumala výzkum peněžních toků a ziskovosti mezi roky 2012 až 2016.

Stejnou problematikou spojenou s kryptoměnami se zabývali turečtí autoři Nurgun Komusoglu Yilmaz a Hulya Boydas Hazar (2018). Ti analyzovali budoucnost investičních trendů podle Conjoint analýzy, což je metoda statistické analýzy, pomocí které výzkumníci určují hodnotu atributů, jež jsou v daném výrobku nebo vlastnosti pro spotřebitele částečně využívány i v marketingu. Jako hlavní složku svého výzkumu si vybrali a analyzovali atribut ziskovosti, neboť dle jejich názoru investora primárně zajímá částka, kterou vydělá, což vyplývá i z jejich závěru, že pro investora se jedná o nejdůležitější kritérium. To představuje rozdíl mezi aktuální tržní cenou a nákupní cenou investora v dané investici. Dalšími atributy, které autoři vybrali ve své publikaci, jsou anonymita, riziko a bezpečnost.

Obdobně zkoumá ziskovost kryptoměn na bázi optimalizace kryptoměnového portfolia z hlediska rizik ve své publikované knize autor Viktor Boiko (2021) z Kyjevské národní ekonomické univerzity. Ve své studii uvádí, že pro investora je důležitá ziskovost v průběhu určitého období dle investora, avšak přidává k tomu, že důležitou součástí se stává i rizikovost. Zde předkládá, že ji lze ovlivnit dvěma způsoby. Konkrétně diverzifikací portfolia finančních aktiv, případně pouze kryptoměn a výpočtu Sharpe ratia. Pro své zkoumané portfolio vybral šest kryptoměn dle tržní kapitalizace podle coinmarketcap.com a akcie Amazonu. Na tomto příkladu analyzoval ziskovost kryptoměn po dobu pěti čtvrtletí od 19. 7. 2018 do 12. 10. 2019. Ve výsledcích zjistil, že kryptoměna Bitcoin způsobuje dostatečně vysoké zhodnocení a představuje nízké riziko v portfoliu kryptoměn pro investora.

Podobně se zabývají možnostmi investic do kryptoměn v moderním finančním trhu autorky Saksonova a Kuzmino-Merlinova (2019), které analyzují investice do kryptoměn z hlediska tří hlavních aspektů pro investora. Data a publikace pocházejí z roku 2019. Ziskovost počítající mezi určenými obdobími představuje i zde pro investora hlavní složku investic. Pro eliminaci rizika spočívající v investování do kryptoměn doporučují rozdělit potencionální investice do investičního portfolia obsahující více než jednu kryptoměnu. Zároveň se autorky zabývají korelacemi mezi kryptoměnami navzájem, tedy sledují, jaký vliv má vzrůstající trend, případně klesající trend kurzu jedné kryptoměny ke druhé. Pro toto porovnání autorky analyzují zejména kryptoměnu Bitcoin jakožto nejdůležitější kryptoměnu z hlediska tržní kapitalizace s kryptoměnami dalšími jako například Ethereum a Litecoin. Ve svém závěru upozorňují také na důležitost posouzení volatility, která v případě kryptoměn hraje velikou roli. Ve svém závěru uvádějí, že kryptoměny z hlediska vývoje posledních let lze považovat za legitimní investiční nástroj, nicméně je potřeba dbát na rizika spojená s onou volatilitou.

Dalšími autory analyzující investice do kryptoměn jsou Alexander Brauneis a Roland Mestel (2019). Ti zkoumají přínosy kryptoměnových portfolií z hlediska rizik a výnosů. Využívají Markowitzův rámec střední hodnoty a rozptylu. Konkrétně na základě údajů o pěti stech nejvíce kapitalizovaných kryptoměnách za období od 1. 1 2015 do 31. 12. 2017 vztahují riziko a výnos kryptoměn k různým investičním indexům. Ve svých dílech hojně využívají ukazatel Sharpe-ratio. Ze závěrů posuzují, že Markowitzovo optimální portfolium vykazuje vyšší poměr než jednotlivé kryptoměny. Výsledky poukazují na to, stejně jako u předešlých autorů, že kryptoměny je dobré pro investora kombinovat a nespolehat se pouze na výnos kryptoměny jedné.

Kombinace faktorů volatility, ziskovosti a výpočtu Sharpe-ratia analyzují autoři David Kuo Chuen Lee, Li Guo a Yu Wang (2018). Ti ve své práci z roku 2018 zkoumají faktory a

k tomu Information Ratio a Maximum Drawdown, kdy na základě tržní kapitalizace kryptoměn vybrali ty s nejvyšší hodnotou. Navíc tyto kryptoměny porovnávají se ziskovostí, volatilitou a Sharpe Ratio index S&P 500 a komodity jako je zlato a ropa. Data, ze kterých čerpají, pocházejí z rozmezí let 2014 až 2017. Na základě svých výsledků ze své práce popisují, že průměrné denní výnosy kryptoměn s tradičními aktivy jsou vyšší, avšak upozorňují na současně vyšší riziko, jehož hodnoty dosáhli výpočtem Sharpe-Ratia, spojeného zároveň s vyšší volatilitou kryptoměn. Tak jako předešlí autoři k eliminaci rizika doporučují, mít investiční portfolio založené na více investičních instrumentech než pouze na jednom. Ve svém úplném závěru se zaměřili taktéž na korelaci kryptoměn a další investiční instrumenty. V těchto letech se ukázalo, že korelace mezi kryptoměnami a tradičními aktivy jsou trvale nízké.

3 KOMPARACE VYBRANÝCH KRYPTOMĚN

Následující část diplomové práce se věnuje komparaci vybraných kryptoměn na základě specifických, ekonomických a unikátních vlastností. Kryptoměny byly zároveň vybrány na základě důležitosti a oblíbenosti v obchodování na dnešních kryptoměnových trzích. Reprezentační vzorek je složen z těch nejvyužívanějších (a historicky nejvýznamnějších) zástupců. Výběr byl zúžen z toho důvodu, že by jinak celkový počet zástupců znamenal hodnotu v řádech tisíců.

Výběr kryptoměn byl řízen na základě tržní kapitalizace (z dat společnosti CoinMarketCap.com), data v příloze DP. V úvahu byly vzaty poznatky, že kryptoměny, které budou porovnávány a představeny navzájem, by měly přesáhnout alespoň tržní kapitalizaci přes pět milionů dolarů, aby se zachovala relevance daných kryptoměn a jednalo se tak o kryptoměny využívané pro obchodování a investování. Zároveň kryptoměny budou vybrány tak, aby se od sebe navzájem v určitých aspektech lišily, a to ať už matematickým algoritmem, celkovým vydáním počtu mincí či fungování těžby.

Vzhledem k těmto podmínkám budou vybrány kryptoměny: Bitcoin, Litecoin, Ethereum, Tether, Cardano, BNB, Solana a USD Coin. Tyto vybrané kryptoměny pokrývají značnou část celkové tržní kapitalizace, a to až ze 75 %.

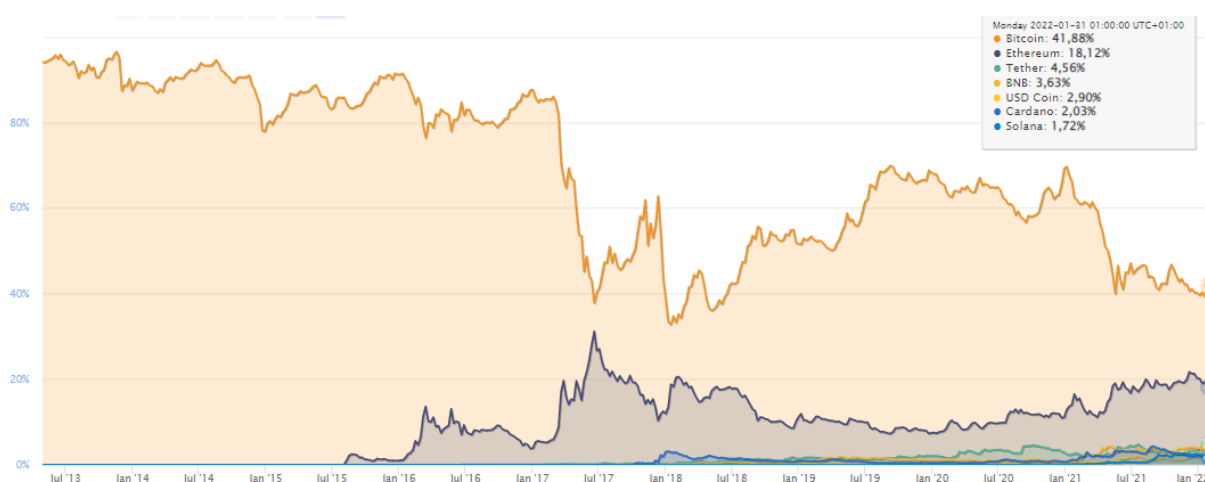
3.1 Tržní kapitalizace kryptoměn

Tržní kapitalizace jako jedna z nejdůležitějších vlastností kryptoměn ukazuje, jak je daná kryptoměna stabilní a silná. Případně jakou může mít i likviditu. Kapitalizace dokáže i znázorňovat, jakou pozici kryptoměna má na trhu, a to hlavně z dlouhodobého hlediska, zdali má dostatečnou šanci se udržet na trhu.

V případě tržní kapitalizace data vychází z prostředí CoinMarketCap webu, který je v kryptokomunitě považován za celosvětově nejcitovanější web pro sledování cen a ukazatelů kryptoměn na světě.

V průběhu vytváření této diplomové práce z hlediska tržní kapitalizace zcela dominuje kryptoměna Bitcoin. Ta se na pomyslné první příčce drží již od svého počátku až dodnes. I tak ale jistá změna během existence Bitcoinu nastala. V minulosti, což znázorňuje i obrázek č. 2, zaujímal Bitcoin v tržní kapitalizaci svoji dominancí až 90 %. V průběhu let se tento ukazatel silně mění. Na začátku roku 2022 Bitcoin držel svoji dominancí „pouze“ 41,8 %. To znamená

takřka padesátiprocentní ztráty oproti roku 2016. V roce 2017 nastal hlavní pokles dominance Bitcoinu, kdy kryptoměny zažívaly svůj přerod, neboť světlo světa spatřila velká část nových zástupců. Na popularitě navíc získala hlavně kryptoměna Ethereum, která dokonce v jednom momentě kryptoměnu Bitcoin v jejím prvenství téměř dostihla. Od první příčky kryptoměnu Ethereum dělilo pouze sedm procentních bodů. V roce 2022 tyto dvě nejsilnější kryptoměny opět dělí širší pole, a to konkrétně 23,76 %, což značí to, jak je Bitcoin i po takové dlouhé době silnou kryptoměnou. V průběhu let si Ethereum drží stabilní pozici dvojky na trhu. Co se týče tržní kapitalizace, dnes si zde obstojně stojí se svými 18 %. Další kryptoměny pokrývají již menší část kryptoměnového trhu. Jedná se o takřka stabilní coin Tetherem (4,56 %) a ještě novou kryptoměnu BNB (3,63 %). Ostatní kryptoměny na tržní kapitalizaci zajímají menší část než jsou 3 %. Konkrétně USD Coin zaujímá 2,9 %, Cardano 2,03 %, Solana 1,72 % a Litecoin 0,3 %. Dohromady tak zaujímají celkovou tržní kapitalizaci přesahující 75 %.



Obrázek 2: Tržní kapitalizace kryptoměn vyjádřená v procentech

Zdroj: <https://coinmarketcap.com/charts/>

V porovnání s ostatními komoditami či indexy mají dohromady kryptoměny celkovou tržní kapitalizaci 1 540 miliard dolarů (během procesu psaní diplomové práce). V roce 2021 se dostaly kryptoměny až na hodnotu 3 000 miliard dolarů. Pro porovnání s jinými aktivy poslouží například Amazon. Jeho celková tržní kapitalizace v době psaní diplomové práce činí 1 510 miliard USD. Kdyby se tedy kryptoměny přenesly do indexu S&P 500, zaujmuly by v tomto žebříčku 3. místo.

Bitcoin byl vytvořen v roce 2009 anonymní osobou nebo lidmi pod jménem Satoshi Nakamoto. Má maximální limit 21 milionů a k únor 2022 je v oběhu takřka 19 milionů bitcoinů. Je široce přijímána jako nejoblíbenější kryptoměna a má největší trh kapitalizace.

Ethereum je open-source platforma založená na blockchainu, na které běží chytré kontrakty v Turingově systému. Hodnotový token blockchainu Ethereum se nazývá ether. Vymyslel ho Vitalik Buterin v roce 2013 a později byl vyvinut s využitím fondu bitcoinů v hodnotě 18 milionů USD, získaných prostřednictvím veřejného online crowdového prodeje etheru v roce 2014.

Litecoin byl vynalezen v říjnu 2011 Charlesem Leem a využívá technologii podobnou Bitcoinu. Hlavními rozdíly oproti Bitcoinu jsou doba generování bloků, která se zkrátila z deseti minut na 2,5 minuty na blok; maximální limit je 84 milionů pro Litecoin, který je čtyřikrát vyšší než u Bitcoinu. Obsahuje odlišný hashovací algoritmus oproti Bitcoinu.

Tether vznikl v roce 2017 a je největší "stabilní mincí" v ekosystému kryptoměn a v současné době má dohromady tržní hodnotu přibližně 82 miliard USD. Stabilní mince využívají online kryptografické burzy, protože jim umožňují oceňovat kryptoměny v USD, aniž by si musely zřizovat bankovní účet v USD. Tether se řadí ke stablecoinům, protože byl původně navržen tak, aby měl vždy hodnotu 1,00 USD za jeden tether.

BNB, ze své zkratky známá jako Binance Coin je digitální kryptoměna založená v roce 2017 kryptoměnovou burzou Binance. BNB bylo dříve vynalezeno hlavně z důvodu tzv. utility tokenu na blockchainu Etherea a sloužilo primárně pro placení levnějších poplatků na kryptoměnové burze Binance. Svoji známost získal hlavně díky spojení Binance Chain a Binance Smart Chain, kdy spojením těchto dvou blockchainu vznikl nativní token BNB.

USD Coin je velmi podobnou kryptoměnou jako Tether. Je to také digitální stablecoin, který je navázán na jeden americký dolar. USD Coin založila společnost Circle v roce 2018.

Cardano je kryptoměna uvedená na trh v roce 2017. Kryptoměna je pojmenována po italském matematikovi. Hlavním cílem Cardana není vytvořit pouze jednu kryptoměnu, avšak celou platformu, na které se dají vyvíjet a tvořit nejrůznější další tokeny, podobně jako u Etherea.

Solana je kryptoměna založená na bázi veřejného blockchainu. Byla uvedena v roce 2017. Její tvůrci tvrdí, že nabízí daleko rychlejší časy a nižší náklady než její konkurent Ethereum. Kryptoměna slouží primárně k placení transakčních poplatků a jako odměna pro validátory na blockchainu. Využívá se také ve sféře NFT.

3.2 Počet mincí a dělitelnost kryptoměn

Dalším faktorem pro investování do kryptoměn je nutnost vzít v potaz, kolik mincí dané kryptoměny bude vydáno a kolik jich již vydáno bylo. Různé kryptoměny k tomuto faktoru přistupují odlišně. Některé se zaměřují na finální počet mincí, jiné naopak počet mincí neřeší.

V první řadě lze vzít za příklad Bitcoin, který v úplném prvopočátku definoval, kolik bude mincí celkem vytvořeno. Limit v případě Bitcoinu je nastaven na 21 000 000 oběžných mincí. Tento limit by měl být dle všech předpokladů dosažen v roce 2140. Není to však pouze Bitcoin, který má předem daný počet mincí. Většina dalších kryptoměn má navíc cílový počet mincí zcela rozdílný, hlavně tedy vyšší. V případě komparace uvedených kryptoměn se jedná například o BNB, který je tokenem založený na platformě Ethereum. Maximální počet mincí je stanoven na 200 milionů BNB. Binance Coin je navržen jako deflační kryptoměna. Její cílový konečný počet mincí činí 100 milionů BNB, přesně polovinu z maximálního počtu. V případě Cardana je celkový počet vydaných mincí v budoucnu vyčíslen na 45 000 000 000. Poslední kryptoměna, která zná svůj budoucí celkový stav vytěžených mincí, je Litecoin. Toho se vytěží celkem 84 000 000 mincí, což je v konečném součtu čtyřnásobek mincí Bitcoinu, jelikož Litecoin byl stvořen jako derivát Bitcoinu a měl tak vzniknout „lehčí“ a rychlejší Bitcoin.

Dalším důležitým aspektem, co se týče vydaných mincí, je dělitelnost mincí. Vzhledem k tomu, že tyto kryptoměny mají působit „deflačně“, byla zavedena kryptoměnová dělitelnost. Důvod je relativně prostý. Aby se v budoucnu zamezilo tomu, že hodnota jedné vydané mince kryptoměny nenaroste do obřích rozměrů a stane se tak zcela nepoužitelnou v běžném životě. Nejznámější kryptoměna Bitcoin je dělitelná až na osm desetinných míst, přičemž nejmenší jednotce dělitelnosti Bitcoinu se říká podle zakladatele Satoshi. Litecoin je dělitelný zcela stejně jako Bitcoin, tedy na osm desetinných míst. Oproti konkurenci je nejlépe dělitelný jeden Ether, který se dokázal rozčlenit až na jednu triliontinu.

Ne všechny kryptoměny mají celkový počet vydaných mincí. Již zmíněné Ethereum zcela záměrně nemá stanovený žádný limit budoucích vytvořených mincí. Má jediné omezení, a to pouze na vytěžení určitého počtu mincí za jeden rok. U Solany taktéž celkový počet není určen. V případě Tetheru a USD Coinu se jedná o stabilní mince, které kopírují cenu jednoho dolaru a není stanovený budoucí počet těchto kryptoměn.

Tabulka 1: Počet vytvořených mincí

Kryptoměna	Aktuální počet mincí	Konečný počet mincí	Procentuální vyjádření vytvořených mincí na počtu celkovém
Bitcoin	18 947 681	21 000 000	90,23%
Ethereum	119 427 265	Není určeno	X
Tether	77 949 705 184	Není určeno	X
BNB	165 116 761	100 000 000	165,12%
USD Coin	50 564 623 181	Není určen	X
Cardano	33 571 064 327	45 000 000 000	74,60%
Solana	314 884 190	Není určen	X
Litecoin	69 557 644	84 000 000	82,81%

Zdroj: vlastní zpracování podle coinmarketcap.com

Právě v tabulce 1 lze postřehnout rozdíly mezi různými kryptoměnami. Bitcoin, Litecoin a Cardano mají jasně stanovená maxima, kde všechny tři kryptoměny již překonaly poměr na celkovém počtu vytvořených mincí, a to 70 % oproti specifické kryptoměně BNB, která své vytvořené mince postupně pálí až na celkový počet 100 000 000 z počtu 200 000 000. Nyní se nachází ve 35 % postupu a zbývá tak vypálit ještě 65 % mincí. Ethereum, Solana a Stable coinny nemají určený celkový počet vytvořených mincí.

3.3 Poplatky za transakci převodu kryptoměn

Jak bylo zmíněno v části o blockchainu, každá kryptoměnová transakce se zapisuje do hlavní účetní knihy, tedy blockchainu. Aby transakce byly dostatečně motivující pro těžáře, kteří je potvrzují, částečně za ně vybírají poplatky, a to za každou provedenou transakci. V Tabulka 2: Poplatky za převod kryptoměn budou porovnány data dle společnosti Coinmarket.com, jaký poplatek dané kryptoměny za transakci vyžadují. Časový horizont je stanoven na posledních šest let. Poplatky jsou uváděné v českých korunách po přepočtu dle aktuálního kurzu ke dni 03.02.2022.

Tabulka 2: Poplatky za převod kryptoměn

Kryptoměna	2017	2018	2019	2020	2021	2022
Bitcoin	10,56 Kč	217,67 Kč	3,59 Kč	11,72 Kč	299,75 Kč	35,83 Kč
Ethereum	0,22 Kč	24,37 Kč	1,46 Kč	2,11 Kč	325,34 Kč	760,59 Kč
Tether	X	X	X	X	X	X
BNB	X	X	0,28 Kč	0,75 Kč	2,80 Kč	7,44 Kč
USD Coin	X	X	X	X	X	X
Cardano	X	1,50 Kč	0,21 Kč	0,21 Kč	3,21 Kč	7,91 Kč
Solana	X	X	X	0,01 Kč	0,01 Kč	0,01 Kč
Litecoin	0,54 Kč	4,38 Kč	0,47 Kč	0,44 Kč	0,65 Kč	0,34 Kč

Zdroj: vlastní zpracování

Z tabulky číslo 2 se lze dozvědět několik zajímavých informací. Za zdůraznění stojí zejména poplatky v době největšího boomu kryptoměn, tedy v roce 2018 a v roce 2021. Speciálně Bitcoin je zajímavý skrze poplatky, neboť v únoru činil sankce za převod až 218 Kč. Na vyšší metu dospěl i v roce 2021, kdy se blížil hodnotě 300 Kč. Pro kryptoměnové investice i pro kryptoměny samotné jsou tak vysoké poplatky zcela nepřijatelné. V posledních letech se s vysokými poplatky, ba dokonce i vyššími potýká druhá nejpopulárnější kryptoměna Ethereum. Za posláni části této kryptoměny na počátku roku 2022 uživatel zaplatil poplatek 760 Kč, rok před tím 325 Kč, přičemž roky před tím se poplatky pohybovaly v řádech korun. Odlišná situace panuje u tzv. „stable coinů“, tedy Tetheru a USD Coinu, které představují kryptoměny navázané na dolar, tedy jejich hodnota koreluje s touto měnou a poplatky za převod či transakci tam žádné nejsou. U ostatních populárních kryptoměn činily poplatky částky maximálně v řádech korun,

ba dokonce nižší, v hodnotě desetiny koruny. Uživatele posláni např. kryptoměny Litecoin stálo pouze 0,34 Kč, oproti Etheru, kdy poplatek činil 760 Kč.

3.4 Rychlost transakce

K ceně transakce neodmyslitelně patří i samotná rychlost převodu. Ta v celkovém pojetí kryptoměn hraje opravdu podstatnou roli. Na rychlosti je závislý prakticky celý kryptoměnový systém, a to hlavně z důvodu poskytnutého komfortu pro uživatele kryptoměn. Není totiž vůbec žádoucí, aby zaslání vybrané kryptoměny do peněženky trvalo příliš dlouhou dobu. Zároveň s tím souvisí potvrzení o přijetí kryptoměny. Konkrétně jde o čas, během kterého se odešle kryptoměna (nebo její část) z daného souboru do kryptoměnové peněženky příjemce. Dalším způsobem, jak lze vnímat rychlost kryptoměn je, kolik transakcí zvládne kompletně celý systém potvrdit za určitý čas. Tento údaj se udává v transakcích za vteřinu, označováno zkratkou tps, z anglického transactions per second.

Rychlost odeslání kryptoměny je znakem modernizace nejen v oblasti kryptoměn. Tak, jak se vyvíjí nové technologické postupy v odvětví IT, tak i tyto inovace dopadají do segmentu kryptoměn. Tyto nové prostředky využívají nejčastěji tvůrci a zakladatelé kryptoměn k dosažení vyšších rychlostí. Ovšem ne u všech kryptoměn to je takto snadné, jelikož je vyšší rychlost ovlivněna hned několika faktory, například přílišný příliv uživatelů do sítě, což může vést až k přetížení sítě. S tím je spojený vyšší poplatek za zprostředkování transakce uživatelů.

V případě komparace pro tuto diplomovou práci vybraných kryptoměn se jejich každá rychlost lehce liší. Nejčastěji je to dáno velikostí bloků, na kterých je rychlost závislá. Platí jednoduchá rovnice, že čím větší blok, tím je rychlost transakce vyšší. V případě nejznámější kryptoměny Bitcoin se jedná o velikost bloku velikého okolo 1 MB. To znamená, že maximální počet transakcí, který Bitcoin zvládne zpracovat za sekundu, je 7. Oproti tomu například Litecoin dokáže zpracovat až 56 transakcí za sekundu. Z hlediska kryptoměny, druhově jako např. Ethereum, se jedná o velice progresivní postup v oblasti rychlosti, neboť chce razantně zvyšovat její hodnotu a tedy i inovovat své vnitřní prostředí. V předešlých řádcích bylo zmíněno, že u Bitcoinu je maximální počet transakcí za vteřinu na hodnotě sedm. To ale neznamena, že 7 tps musí být finální počet, avšak pro samotnou změnu je potřeba najít velice složitý konsenzus u vývojářů. (O'Keeffe, 2018)

Tabulka 3: Rychlost transakcí

Kryptoměna	Čas potvrzení transakce	Počet transakcí za sekundu
Bitcoin	60 min	7 tps
Ethereum	6 min	25 tps
Tether	60 min	42 tps
BNB	15 min	200 tps
USD Coin	45 min	40 tps
Cardano	10 min	250 tps
Solana	2,5 s	29 000 tps
Litecoin	30 min	56 tps

Zdroj: vlastní zpracování podle Aleph Zero

V tabulce 3 jsou shrnuty veškeré rychlosti potvrzení transakcí kryptoměn. Byly zpracovány časy potvrzení a počty transakcí za sekundu u vybraných kryptoměn. Již v dříve probírané komparaci dochází k častým rozchodům v rychlosti, nyní i v počtu transakcí za sekundu. Kryptoměny Bitcoin a Litecoin, které mají rychlosti předem dány a jen velmi těžce je lze měnit, již byly diskutovány. K vůbec nejrychlejší kryptoměně ze zmíněného výčtu patří Solana, u které její zakladatelé uvádějí rychlost pro potvrzení 2,5 sekundy, prakticky tedy ihned. V počtu transakcí dochází k vysokému číslu 29 000 tps, navíc některé zdroje uvádějí i možnou rychlost blízkou až k 50 000 tps. Naproti tomu Stable Coiny, USD Coin a Tether svoji rychlost relativně korelují a jsou si velmi podobné. Rychlé jsou i kryptoměny Cardano a Ethereum, které dokáží měnit i rychlost v průběhu let a stávat se tak rychlejšími. V době psaní diplomové práce dosahují rychlosti k času potvrzení transakce pod 10 minut.

4 METODIKA VÝPOČTŮ INVESTIČNÍCH KRITÉRIÍ

Pro analýzu a komparaci vybraných kryptoměn je nejprve nutno si charakterizovat samotnou metodiku výpočtů různých ukazatelů a představit si, co znázorňují. V určitých vlastnostech se dají porovnat kryptoměny navzájem, jdou však porovnat nejenom sami s sebou, avšak i s jinými investičními instrumenty a měnami. Bude zde představena problematika nejznámějších a nejrelevantnějších indexů doplněných o určité aspekty.

4.1 Metodika výpočtu výnosnosti

Na základě rešerše odborné literatury byla zvolena metodika výpočtu výnosnosti. Tuto metodiku využívali prakticky všichni představení autoři, jelikož ji pokládali všichni za zcela srozumitelnou. Konkrétně Derks Gordijn a Siegmann, tak i Chuen, David Lee, Wang a Yilmaz a Hazar.

Ukazatelé výnosnosti jsou obecně pro investory a akcionáře, jedním z nejvíce sledovaných poměrových ukazatelů. Vyplývá to z toho, že informují o efektu, jehož bylo dosaženo vložením vlastního kapitálu, čili měří jistou „úspěšnost“. (Rejnuš, 2014, s. 271)

Prvním výpočtem, který je potřeba si představit, je metoda výpočtu výnosnosti. Tím nejjednodušším na porovnání aktiv je bezesporu cena. Cena aktiva je základní informace, se kterou investor či podnik pracuje. Metoda teorie výpočtů výnosnosti nebude počítat s další cashflow v podobě dividend, které navíc ani u kryptoměn jako takových nevznikají. Protože není možné zjistit výnosnost pouze z prosté tržní ceny, je nutné využít vzorec jednoduché výnosnosti. Ta se definuje jako odměna vyjádřená v procentech. V případě jednoduché výnosnosti zní vzorec následovně:

$$R_T = \frac{P_t}{P_{t-1}} - 1 = \frac{P_t - P_{t-1}}{P_{t-1}} \quad (1)$$

kde:

- R_T je míra výnosnosti za období mezi časem t-1 a t,
- P_t je cena aktiva v čase t,
- P_{t-1} je cena aktiva v čase t-1.

Pro všeobecnou představu a základní přehled je výpočet jednoduché výnosnosti zcela dostačující, avšak při detailním pohledu může být kontraproduktivní. Proto se navíc sleduje vola-

tilita, které se využívá v přesnějších výpočtech. Pro eliminování manipulace a výnosnosti pomocí geometrického a aritmetického průměru se využívá logaritmická výnosnost. Ta je chápána jako přirozený logaritmus jednoduché hrubé výnosnosti a vypočítá se podle následujícího vzorce (Linnertova, 2017):

$$r_t = \ln(1 + R_t) = \ln \frac{P_t}{P_{t-1}} \quad (2)$$

Pro získání denního přehledu výnosnosti se využije vzorec pro průměrnou denní výnosnost, který se spočítá dle následujícího vzorce (Linnertova, 2017):

$$\bar{r} = \frac{1}{n} \sum_{t=1}^n r_t \quad (3)$$

kde:

- r_t je ona logaritmická výnosnost za období t , tedy za jeden den,
- n je počet období t , tedy dní,
- \bar{r} je průměrná denní výnosnost.

4.2 Metodika výpočtu volatility

V rámci metodiky výpočtu volatility se rozhodli autoři Viktor Boiko a Chuen, David Lee, Wang a Saksonova s Kuzmino-Merlinovou počítat právě s volatilitou, jakožto s rizikem, které pro potencionální investice v kryptoměny představuje.

Dalším výpočtem, který bude hrát svoji roli v komparaci kryptoměn mezi sebou, bude volatilita. Tento ukazatel vypovídá o tom, jak se určitá hodnota aktiva, případně výnosnost odlišuje od svého průměru. V případě kryptoměn se jedná o velice zásadní ukazatel. Navíc dokazuje, jaké riziko musí podstoupit investor, který se rozhodne investovat do segmentu aktiv. V matematice je volatilita definována jako směrodatná odchylka, která se označuje řeckým malým písmenem sigma a vypočítá se jako odmocnina z rozptylu. Výsledný vzorec tak dostane následující podobu (Macroption, 2019):

$$\sigma = \sqrt{\frac{1}{n} \sum_{t=1}^n (r_t - \bar{r})^2} \quad (4)$$

kde:

- σ je směrodatná odchylka, která znázorňuje volatilitu,
- n je počet období, nejčastěji dnů,
- r_t znázorňuje logaritmicickou výnosnost,
- \bar{r} představuje již zmíněnou průměrnou denní výnosnost.

4.3 Sharpe ratio

Pro výpočet Sharpe ratia, tedy zohledňující jak výnosnost, tak ziskovost se rozhodli autoři Alexander Brauneis a Roland Mestel a Chuen, Lee, Wang. I proto byl právě zvolen ukazatel Sharpe ratio.

Posledním vzorcem představeným pro komparaci kryptoměn bude Sharpe ratio, které se snaží vyřešit vztah mezi výnosem a rizikem. Ukazatel Sharpe ratio vypomáhá investorovi pochopit výhodnost investice, jelikož zohledňuje, jak výnosnost, tak i riziko dané investice. Obecně se udává, že čím vyšší je výsledná hodnota, tím lépe. Za zakladatele tohoto ukazatele je udáván laureát Nobelovy ceny za ekonomii William F. Sharpe. Vzorec zní následovně (Hargrave, 2019):

$$\text{Sharpe ratio} = \frac{R_t - R_f}{\sigma} \quad (5)$$

kde:

- R_t představuje výnos daného aktiva za určité období,
- R_f znázorňuje bezrizikovou úrokovou míru,
- σ představuje volatilitu sledovaného aktiva.

5 SESTAVENÍ MODELOVÉHO PORTFOLIA

V předchozích kapitolách byly popsány hlavně specifické vlastnosti kryptoměn, jak si ve světle světa kryptoměn jednotliví zástupci stojí. Následující kapitola se bude věnovat z podstatné většiny ekonomickým aspektům vybraných kryptoměn, a to z pohledu potencionálního investora v podobě fyzické osoby, případně osoby právnické. Data, ze kterých výpočty výnosnosti, volatility a Sharpe-ratio vychází, pochází z dostupných dat ze společnosti CoinMarket-Cap, která představuje jednu z nejnavštěvovanějších stránek z oblasti kryptoměnové problematiky. Dále data ohledně indexů a komodit, ze kterých vychází výpočty pochází z veřejně dostupných prostředků, konkrétně z platformy Tradingview.com. Tato data byla následně převedena do jednoho formátu. Konkrétně data jsou uvedeny v příloze diplomové práce, ze kterých výpočty vychází.

V úvodu bude popsána výnosnost, která byla vysvětlena teoreticky v podkapitole 3.1, následně budou kryptoměny srovnány z hlediska komparací s vybranými indexy světových trhů a zástupci výnosnosti také budou vybrány ze světa komodit. V případě investic se kapitola 5 bude následně zabývat i složkou volatility kryptoměn a Sharpe ratia. Tyto dvě složky byly opět teoreticky popsány v kapitole 4.2, resp. 4.3.

5.1 Představení vybraných indexů a komodit

Pro sestavení modelového portfolia a pro porovnání výnosnosti, volatility a Sharpe ratia s kryptoměnami byly vybrány čtyři zástupci investičních indexů a tři zástupci komodit.

S&P 500, známý pod dlouhým názvem Standard & Poor's je jeden z nejznámějších akciových indexů. Konkrétně se jedná o přední americký index složený z pěti set největších akcií kapitalizovaného trhu amerických podniků. Celosvětově se jedná o nejdůležitější index a v podobě, ve které se nachází dnes, se objevil již v roce 1957. Absolutní kořeny tohoto indexu ale sahají až do roku 1923. K největším společnostem obsaženým v tomto indexu patří Apple, Microsoft, Amazon nebo Tesla.

FTSE100 je cenový index londýnské akciové burzy London Stock Exchange. Obsahuje sto společností s největší kapitalizací, které mají své sídlo ve Velké Británii. Index je oproti S&P 500 mnohem mladší. Vznikl v roce 1984. Patří mezi jedny z nejvíce požívaných a oblíbených indexů světa. Spadají pod něj společnosti jako například Barclays, Tesco, Vodafone Group a TUI.

DAX je třetím indexem, který bude sloužit pro porovnání investic. Index, dlouze Detscher Aktienindex, vznikl v roce 1987 a jedná se o německý burzovní index Frankfurtské burzy. Do roku 2021 byl známý pro svůj široký repertoár třiceti největších německých vlastnických společností. Zmíněný repertoár se posléze rozšířil na číslovku čtyřicet, z nichž nejznámější jsou Allianz, Bayer, Adidas a Volkswagen.

NASDAQ je posledním akciovým americkým indexem, který bude sloužit k porovnání s kryptoměny. Jedná se o index, který byl založen v roce 1985. V rámci diplomové práce bude využit index NASDAQ-100, který zahrnuje průmyslové, technologické, maloobchodní, telekomunikační, zdravotnické, dopravní a mediální podniky. Z toho vyplývá, že tento index nezahrnuje společnosti z finančního sektoru. Do tohoto indexu patří společnosti jako PayPal, NVIDIA, Apple nebo META.

Ropa je první z komodit. Jedná se o jednu z nejznámějších a nejžádanějších komodit na trhu. Ropa je základní surovinou prakticky pro celé průmyslové odvětví. Obchoduje se s ní za cenu jednoho barelu. Konkrétně se obchoduje se dvěma nejznámějšími typy ropy. Ropa Brent, zahrnující ropy z nalezišť v Severním moři a ropu WTI, jež se prodává jako severoamerická ropa. Pro účely diplomové práce bude vyprána ropa Brent.

Stříbro je prvním ze vzácných kovů, který se využívá pro stříbrné šperky a průmyslově využitelný kov. Jako komodita je obchodováno na několika světových burzách, například v New Yorku.

Zlato je druhou komoditou z prvku vzácných kovů, které se také využívá k výrobě šperků, příp. v průmyslu. Zároveň se jedná o jednu z nejtradičnějších investic ve světě.

5.2 Výnosnost

V podstatě věcí je výnosnost hlavní složka, která potencionálního investora zaujme. Jedná se o složku, která v drtivé většině rozhoduje, zdali je investor ochoten investovat do instrumentů, které mají pozitivní výnos a nikoliv záporný. Investorovi tedy přináší určitý zisk, v horším případě ztrátu.

Z hlediska porovnávaných instrumentů bylo vybráno období od roku 2017 do dnešního roku 2022, konkrétně do 7.2.2022. Z hlediska delšího intervalu by data mohla být velice zkreslená vzhledem k tomu, že hlavní fáze popularity kryptoměn odstartovala právě v roce 2017 a udržuje se v neměnném stavu dodnes. V čem se mohou výsledky lehce lišit, je založení určité kryptoměny. Ne všechny do jedné vznikly před rokem 2017. V porovnání výnosnosti, ale i v

dalších složkách existují kryptoměny, které jsou mnohem mladší, je jí například velmi populární kryptoměna (i co se týče tržní kapitalizace) Solana, v jejímž případě se tak budou brát v potaz výsledky od roku 2020 a nikoliv od roku 2017. V případě porovnání tvrdých dat výnosnosti, volatility a Sharpe ratia se neberou v potaz případné poplatky za nákup, prodej nebo převod kryptoměny na peněženku a jiné poplatky, stejně tak v případě indexů a komodit.

Data pro výpočty jsou uvedeny v příloze diplomové práce, která obsahuje veškeré kurzy za roky srovnávané v diplomové práci.

Tabulka 4: Výnosnost kryptoměn

Kryptoměna	Průměrná denní výnosnost za rok 2017	Průměrná denní výnosnost za rok 2018	Průměrná denní výnosnost za rok 2019	Průměrná denní výnosnost za rok 2020	Průměrná denní výnosnost za rok 2021	Průměrná denní výnosnost do 7.2. 2022	Celková výnosnost
Bitcoin	0,730	-0,363	0,182	0,383	0,135	-0,367	4190 %
Ethereum	1,241	-0,477	0,002	0,473	0,443	-0,473	38875 %
Tether	0,000	0,000	0,000	0,000	0,000	0,000	0 %
BNB	1,199	-0,916	2,242	2,803	6,979	-0,443	410708 %
USD Coin	X	0,000	0,000	0,000	0,000	0,000	0 %
Cardano	0,978	-0,778	-0,066	0,454	0,553	-0,258	5759 %
Solana	X	X	X	0,237	1,245	-0,974	15452 %
Litecoin	1,068	-0,539	0,075	0,301	0,048	-0,319	2772 %

Zdroj: vlastní zpracování

V porovnání, které je zdokumentováno v tabulce číslo 4, si lze povšimnout několika zajímavých událostí z hlediska kryptoměn ve smyslu obecném. V globálu se dá říct, že kryptoměny v průběhu celých let kontinuálně rostou. Za posledních šest let, které jsou porovnávány v tabulce číslo 4, hned roky 2017, 2019, 2020 a 2021 vyšly velmi pozitivně, avšak jako varovný signál pro investory může vyznívat rok 2018, kdy kryptoměny zažily velice tvrdou realitu v podobě záporné výnosnosti, kdy některé kryptoměny zažily pád v podobě kurzu až o 90 %, příp. více, nebo i méně, ale jako celek skutečně propadly. Zároveň se i část roku 2022 u všech kryptoměn odráží negativně, kdy zatím nedokáží navázat na roky předešlé, co se výnosnosti týče.

Konkrétně se nejvyšší výnosnost ukázala v podobě kryptoměny BNB, která rostla až extrémně, a to hlavně v roce 2021, kdy se denní výnosnost ukázala jako nejvyšší z celého spektra

kryptoměn. V případě investora tak celková výnosnost činila těžko uvěřitelných 410 708 %. Jak bylo ale zmíněno, z hlediska roku 2017, od kterého lze brát relevantnější data, kdy se kryptoměny dostaly více mezi veřejnost, se některé, jako např. Bitcoin či Litecoin, dokázaly více dostat do povědomí, ale některé zase méně. V roce 2017 byla BNB jednou z nejmladších, nyní se ale v roce 2022 dá říct, že se jedná o relevantní perspektivní kryptoměnu. Zajímavý růst však zažily prakticky všechny kryptoměny. Za zmínku stojí ještě popsat situaci kryptoměn Tether a USD Coin, které se z podstaty věci nesnaží o růst v podobě kurzu, nýbrž se jedná o kryptoměny, které mají jako svůj stanovený cíl držet stejný kurz s americkým dolarem USD v poměru 1:1. Některé dny a roky vykazovaly tyto kryptoměny kurz v podobě 0,99968, některé dny zase lehce přes jeden dolar, např. 1,000036, avšak v globálu se jedná o zanedbatelné číslovky a svůj cíl perfektně drží, kdy platí 1 \$ = 1 Tether.

Tabulka 5: Výnosnost indexů

Index	Průměrná denní výnosnost za rok 2017	Průměrná denní výnosnost za rok 2018	Průměrná denní výnosnost za rok 2019	Průměrná denní výnosnost za rok 2020	Průměrná denní výnosnost za rok 2021	Průměrná denní výnosnost do 7.2. 2022	Celková výnosnost
S&P 500	0,058	-0,015	0,057	0,041	0,048	-0,031	97 %
FTSE100	0,016	-0,027	0,023	-0,035	0,033	0,023	5 %
DAX	0,034	-0,047	0,050	0,009	0,032	-0,059	31 %
Nasdaq	0,073	0,010	0,038	0,119	0,019	-0,026	155 %

Zdroj: vlastní zpracování

Pro porovnání výnosnosti kryptoměn jsou vybrány čtyři zastupující indexy, konkrétně jimi jsou S&P 500, FTSE100, DAX a Nasdaq, jak je vidět v tabulce 5. Tabulku 4 a 5 lze tak velmi dobře porovnat navzájem. Opět se vychází z období za posledních 6 let, od roku 2017. Indexy mají jednu velkou výhodu oproti kryptoměnám. Jedná se o již zavedené a velmi prověřené investorské instrumenty, oproti kryptoměnám se jedná také o index mnohem staršího data založení. V případě investice do indexů a do kryptoměn si lze povšimnout, že z části tyto instrumenty společně korelují. Indexy zažily velmi dobré roky 2017, 2019, 2020 a 2021. Oproti tomu rok 2018 byl stejně jako v případě kryptoměn zasažen negativní výnosností. Pouze index Nasdaq si udržel po celých pět let stabilní výnos, kdy každý rok překonal pozitivní výnosnost. Pouze v letošním roce ztrácí, ale jak bylo již jednou zmíněno, je to dáno tím, že rok 2022 je zatím na svém začátku, a nelze tedy říct, jaký bude kurz na konci roku, resp. jak se bude index po celý rok vyvíjet.

V čem lze hledat rozdíl je celková výnosnost od roku 2017. Oproti kryptoměnám se zde jedná o výnos, který může být z pohledu investora zajímavý, avšak oproti kryptoměnám se jedná o výnosy o několik řádů níže. Je to hlavně z toho důvodu, že kryptoměny jsou daleko mladšího data. Nejhuře si ze zmíněných čtyř indexů vedl index FTSE100, který zahrnuje sto společností s nejvyšší tržní kapitalizací, sídlící ve Velké Británii. Následuje index DAX s celkovou výnosností 31 %. Index DAX je německý burzovní index Frankfurtské burzy, který zahrnuje třicet nejvýznamnějších německých společností, od roku 2021 jich je čtyřicet. Velmi dobře si vedl index S&P 500, který se pohybuje těsně pod stoprocentní výnosnosti. Tento index zahrnuje akcie pěti set největších obchodovaných podniků sídlících v USA. Posledním indexem, o kterém již byla řeč, je index Nasdaq, který s celkovou výnosností 155 % porazil ostatní zmíněné. Jedná se o index ryze elektronický, nacházející se na burzovním trhu ve Spojených státech amerických.

Tabulka 6: Výnosnost komodit

Komodita	Průměrná denní výnosnost za rok 2017	Průměrná denní výnosnost za rok 2018	Průměrná denní výnosnost za rok 2019	Průměrná denní výnosnost za rok 2020	Průměrná denní výnosnost za rok 2021	Průměrná denní výnosnost do 7.2. 2022	Celková výnosnost
Zlato	0,023	-0,008	0,042	0,039	-0,025	0,046	31 %
Ropa	0,049	-0,056	0,051	-0,074	0,118	0,478	65 %
Stříbro	0,012	-0,028	0,039	0,115	-0,043	-0,035	39 %

Zdroj: vlastní zpracování

Posledním finančním investičním instrumentem srovnávaným s kryptoměnami jsou komodity. Za zástupce komodit byly vybrány zlato, ropa a stříbro. Jak je tabulky 6 již patrné, tak ze všech ostatních investičních instrumentů mají nižší výnosy od roku 2017. Nejvyšší výnos zaznamenala ropa, následovaly drahé kovy, jejichž celková výnosnost činila 39 % v případě stříbra a 31 % v případě zlata. Komodity se, poměrně vzato, na investičních trzích považují za nejtradičnější investiční instrumenty. Obecně vzato všechny instrumenty zaznamenaly nejvyšší denní výnosnost v roce 2019, oproti tomu v r. 2018 zaznamenaly nejhorší rok za posledních šest let. V roce 2022 má vysoké vyhlídky zejména ropa Brent.

V konečném hodnocení je výnosnost pro investora velmi klíčovým ukazatelem, na který z pozice investujícího nahlíží jako první. Celková výnosnost však nevyovídá prakticky nic

o riziku, jelikož platí, že čím vyšší je výnosnost, tím vyšší je i riziko spojené s investicí do instrumentu. Proto je velmi důležité porovnat i další investiční ukazatele.

5.3 Volatilita

V následující kapitole bude představena volatilita aktiv. Konkrétně se volatilita kryptoměn považuje za jeden z hlavních problémů. Jak bude představeno v následujících tabulkách, volatilita u kryptoměn dosahuje daleko vyšších hodnot než u klasických investičních instrumentů, jak jsou indexy, případně komodity. Data, ze kterých volatilita vychází jsou uvedena v příloze diplomové práce.

Tabulka 7: Volatilita kryptoměn

Kryptoměna	Volatilita za sledované období
Bitcoin	0,060574
Ethereum	0,088400
Tether	0,000000
BNB	0,084088
USD Coin	0,000000
Cardano	0,092374
Solana	0,113291
Litecoin	0,067642

Zdroj: vlastní zpracování

V tabulce 7 si lze povšimnout, že celková volatilita u kryptoměn dosahuje vysokých hodnot. Pouze v případě Tetheru a USD Coinu, které jsou brány za „stable coin“, nevykazuje volatilita žádné hodnoty. Nejvyšší zaznamenaná volatilita je spojena s kryptoměnou Solana, která je z výčtu kryptoměn nejmladší. V případě Cardana, Etheru a BNB dosahuje velmi podobných hodnot. Naopak nejmenší volatilitu vykazuje Litecoin a Bitcoin.

Investující jedinec či podnik do kryptoměn by si měl uvědomit, že volatilita kryptoměn je zkrátka daná. Má to hned několik opodstatňujících důvodů. Za prvé, jak už bylo několikrát

zmíněno, se kryptoměny těší relativně mladé historii, kdy oproti indexům a komoditám za sebou nemají tak dlouhou historii. Mladý trh má nevýhodu v tom, že každá malá změna může trh silně ovlivnit, a to jak s cenou dolu, tak i nahoru.

Hlavním problémem vysoké volatility však není pouze mladý věk, ale hlavní podstata kryptoměn obecně. Kryptoměny jako celek nemají žádnou vnitřní hodnotu a nejsou kryté. To znamená fakt, že za kryptoměnami nestojí žádné společnosti, případně celé státy, které by mohly regulovat samotné využívání kryptoměn. V dnešním moderním světě tak kryptoměny fungují pouze z hlediska zájmu investorů o nákup kryptoměn, případně nezájmu.

Dalším faktorem vysoké volatility je i složka médií. Ty dokážou silně pozitivně zapříčinit vysoké objemy nákupů investorů do svého portfolia, což vede k pozdějšímu zvýšení cen kryptoměn. Ovšem média působí i opačným směrem, kdy dokáží negativně ovlivnit trh tím, že smějí usměrnit prodeje investorů a potom celý trh „zhroutit“. To následně vede k poklesu kurzu až o 90 % v případě Bitcoinu na přelomu let 2018/2019. Navázaným problémem na média je absence chybějících dlouhodobých investic v kryptoměnách, kdy na trhu působí veliké množství vysoce spekulativních obchodníků, kteří dokáží s cenou dlouhodobě manipulovat jak nahoru, tak i směrem dolů.

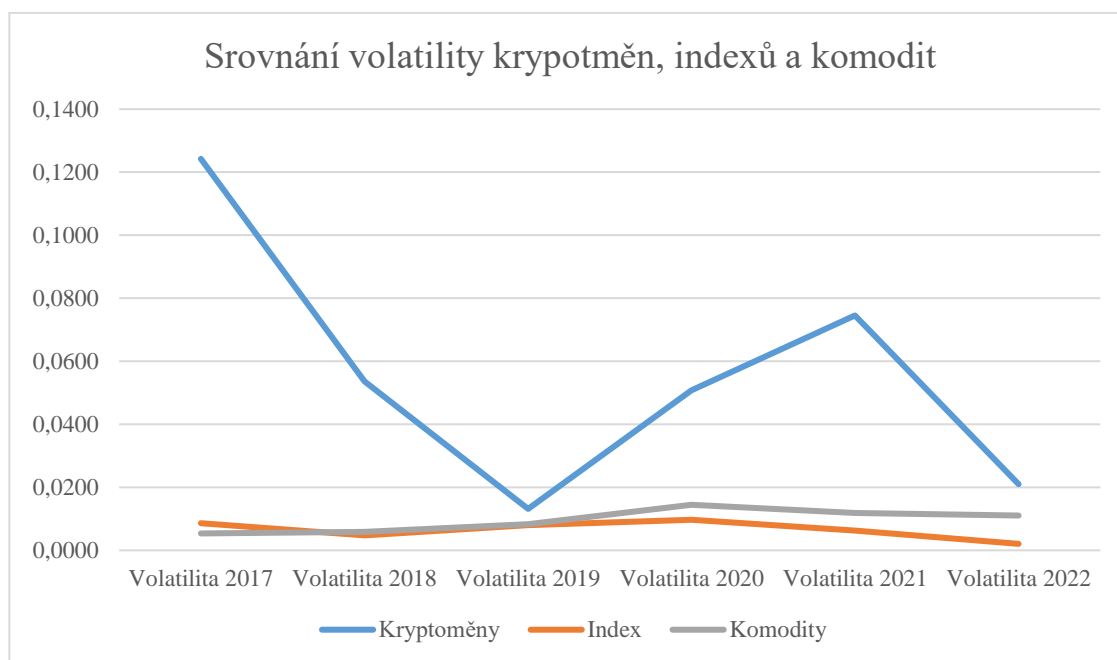
Dalším problémem souvisejícím s volatilitou jsou bariéry vstupu na trh pro jednotlivce. Ty prakticky oproti jiným trhům, jako je akciový trh, neexistují. Každý jedinec či podnik si může dovolit vstoupit na kryptoměnový trh. To následně vede k tomu, že existují milióny amatérských investorů. Tito amatérští investoři jsou následně více náchylní k davové psychóze, kdy nezkušený investor dokáže z pocitu strachu nevhodně prodat a nevhodně kryptoměnu nakoupit. Problémem je i z části to, že se veliké podniky nebo společnosti do kryptoměnového trhu příliš nehrnou, případně pouze v malých částkách. Potvrzující výjimkou je rok 2021, kdy se našly firmy ochotné investovat do kryptoměn. Ukázkovými zástupci jsou společnosti Tesla nebo Microstrategy. Je několik dalších faktorů, které ovlivňují celkovou volatilitu, například nedostatečná právní regulace, jak bylo ukázáno na českém právu, či různé obchodní burzy s nejednotnými pravidly.

Tabulka 8: Volatilita Indexů a Komodit

Investiční instrument	Celková volatilita
S&P 500	0,0073
FTSE100	0,0045
DAX	0,0061
Nasdaq	0,0085
Zlato	0,0048
Ropa	0,0158
Stříbro	0,0078

Zdroj: vlastní zpracování

Pro lepší pochopení problematiky slouží tabulka 8, ve které lze porovnat hodnoty volatility indexů a komodit. Ty jsou o několik řádů nižší. Z výčtů nejnižší volatilitou disponuje komodita zlato. Nejvýše je ropa, ovšem i tak ani zcela nedosahuje takových hodnot, jakou má volatilita u kryptoměn.



Zdroj: vlastní zpracování

Celková volatilita byla srovnána napříč celým spektrem kryptoměn, indexů a komodit. Tak jak již byly výsledky nastíněny v tabulkách předchozích, veškerá data byla i převedena do obrázku 3. Konkrétně do vyobrazeného grafu, který zcela jasně nastiňuje, že se volatilita indexů a komodit drží v rámci normálních hodnot, tedy ani závratně nestoupá, ani neklesá. Naopak

u kryptoměn volatilita představuje vysoce rozdílné hodnoty, kdy klesá a stoupá daleko ve vyšších rádech.

5.4 Sharpe Ratio

V posledním spočítaném ukazateli budou představeny výsledné hodnoty Sharpe ratio. Tento ukazatel bere v potaz výnosnost, ale i případné riziko v podobě volatility určitého aktiva. Sharpe ratio tak jako celek dává zcela větší představu o ideálnosti investice určitého aktiva. Pro výpočet Sharpe ratia je zapotřebí určit bezrizikovou úrokovou míru. Ta bude vycházet ze státních amerických pokladničních poukázek, konkrétně z varianty tříletých, která činí dlouhodobě 3 %. Tyto poukázky byly určeny vzhledem k tomu, že všechny výpočty se vztahují k americkému dolaru.

Tabulka 9: Sharpe ratio investičních aktiv

Investiční instrument	Sharpe Ratio
Bitcoin	13,8839
Ethereum	18,9219
Tether	-20,0000
BNB	35,3436
USD Coin	-19,9556
Cardano	10,1847
Solana	11,3777
Litecoin	10,6433
S&P 500	12,4010
FTSE100	-4,9699
DAX	2,5603
Nasdaq	16,3692
Zlato	3,4320
Ropa	3,6110
Stříbro	3,4453

Zdroj: vlastní zpracování

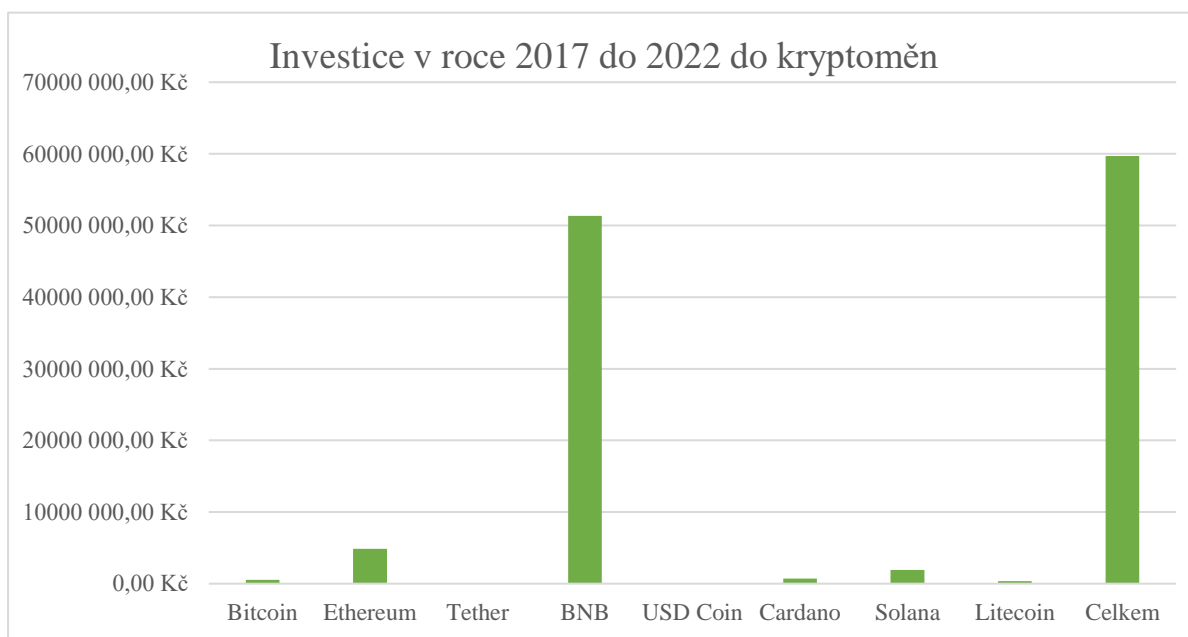
Tabulka č. 9 znázorňuje Sharpe ratio, resp. jeho výsledné hodnoty. V případě kryptoměn se jedná o hodnoty daleko nad výsledky jak Indexů, tak hlavně komodit. Nejvyššího Sharpe ratia dosáhla kryptoměna BNB, následovaná Ethereum. Konkrétně BNB překonalo dvojnásobně

právě i kryptoměnu Ethereum. Všeobecně však neplatí, že Sharpe ratio má nejlepší výpovědní pozici a i tento ukazatel je potřeba brát s určitou rezervou. Pro BNB byly skvělé roky 2017 a hlavně 2021, kdy se v těchto letech ukázala tato kryptoměna jako jedna z vůbec nejziskovějších. V případě Tetheru a USD Coinu je záporná hodnota dána z podstaty těchto kryptoměn, tedy že jsou stablecoiny. Jak však u kryptoměn bylo několikrát znázorněno, je nutné brát je s určitou rezervou, vzhledem k tomu, že zcela závisí na důvěře nakupujících či prodávajících.

5.5 Potencionální investice

V následující kapitole bude znázorněná potencionální investice v souhrnné hodnotě 100 000 Kč. Původní data, ze kterých tato kapitola vychází se nachází v příloze diplomové práce. Jak znázorňuje obrázek, investování do segmentu kryptoměn včetně porovnání samotné investice proběhne od roku 2017 do roku 2022, dále od roku 2018 do roku 2020. Pro srovnání bude využito výpočtů hodnot u indexů a komodit. V závěrečném srovnání dojde k nakombinování všech těchto potencionálních investic.

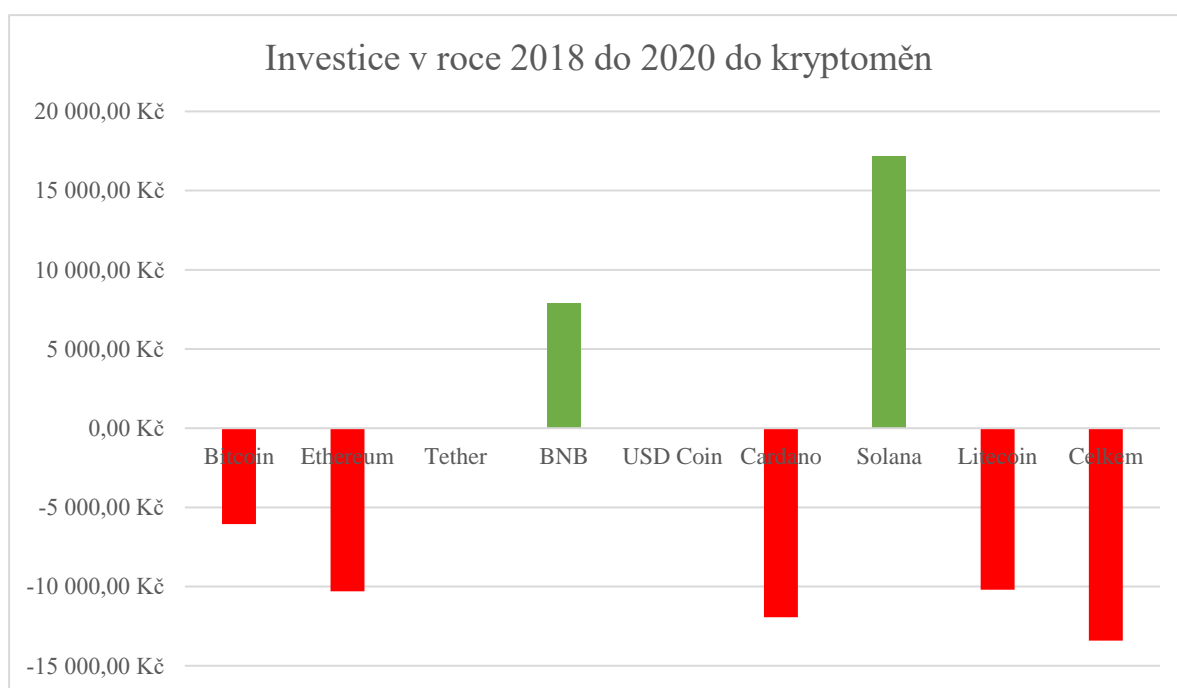
V případě, že by se investor rozhodl investovat celý svůj budget v roce 2017 a rozdělil částku 100 000 Kč zcela rovnoměrně do výběru kryptoměn, který byl určen svojí tržní kapitalizací, tak by investor získal zhodnocení do roku 2022 v následujícím grafu. Veškeré výpočty ke grafům se nachází v příloze diplomové práce.



Zdroj: vlastní zpracování

Z obrázku 4 vyplývá, že největší zhodnocení přinesla kryptoměna BNB. To bylo z části vysvětleno v kapitole výnosnosti. Je to dáno zejména historií kryptoměny BNB, která byla uvedena na trh teprve v roce 2017 a jedná se tak o jednu z nejmladších kryptoměn. Částka, kterou investor vložil do každé kryptoměny čítala hodnotu 12 500 Kč. V případě BNB by tak teoreticky investor obdržel přes 50 000 000 Kč. U dalších kryptoměn by to bylo již podstatně méně, avšak z pozice investora by se jednalo stále o velice zajímavou investici. Ethereum by vyneslo částku takřka 5 000 000 Kč, Cardano přes 700 000 Kč, Bitcoin těsně nad 500 000 Kč a Litecoin 346 000 Kč. Nejméně by vynesly stablecoiny, které však nemají za úkol zhodnotit investorovi investici, nýbrž držet kurz vůči americkému dolaru jedna ku jedné.

Kryptoměny se často setkávají s výkyvy své volatility, tedy nadměrným klesáním, případně stoupáním kurzu kryptoměn za jednotku dané měny. Proto došlo i k porovnání situace, kdyby investor investoval stejnou částku 100 000 Kč, rozmělněnou do osmi vybraných kryptoměn, tedy na každou 12 500 Kč. Tuto investici by ukončil v roce 2020.

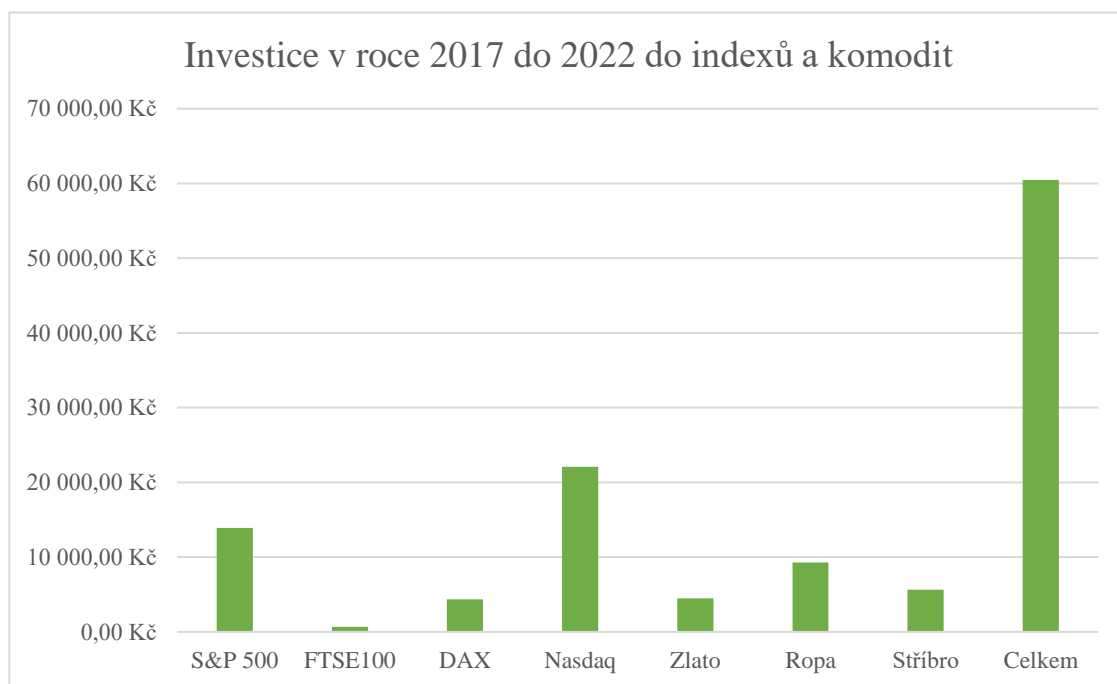


Zdroj: vlastní zpracování

V případě investice do kryptoměn v roce 2018 a s odprodejem v roce 2020 se již investice nejeví tak příznivě jako v případě předchozím, to lze vidět v obrázku 5. V případě Tetheru a USD Coinu zůstává výnosnost stejná, tedy 0 %. Avšak v případě dalších kryptoměn je to zcela odlišné. Výnos z investice si odnáší pouze kryptoměna BNB a Solana, které jsou ale oproti dalším kryptoměnám na trhu nejkratší možnou dobu, tudíž za nimi není žádná dlouhá historie. V případě dalších kryptoměn Bitcoin, Ethereum, Cardano a Litecoin investor realizuje

ztrátu, která se celkově vyšplhala až na částku 13 414 Kč. I proto se velmi silně doporučuje své investice rozdělit do více kryptoměn a nedržet se investice pouze do jedné. Kdyby totiž investor realizoval investici pouze například do Cardana, tak by se ztráta prohloubila do daleko vyšší částky.

Pro srovnání investic poslouží situace, kdy investor investoval své peněžní prostředky pouze do indexů a komodit v roce 2017 do roku 2022 a v roce 2018 do roku 2020.

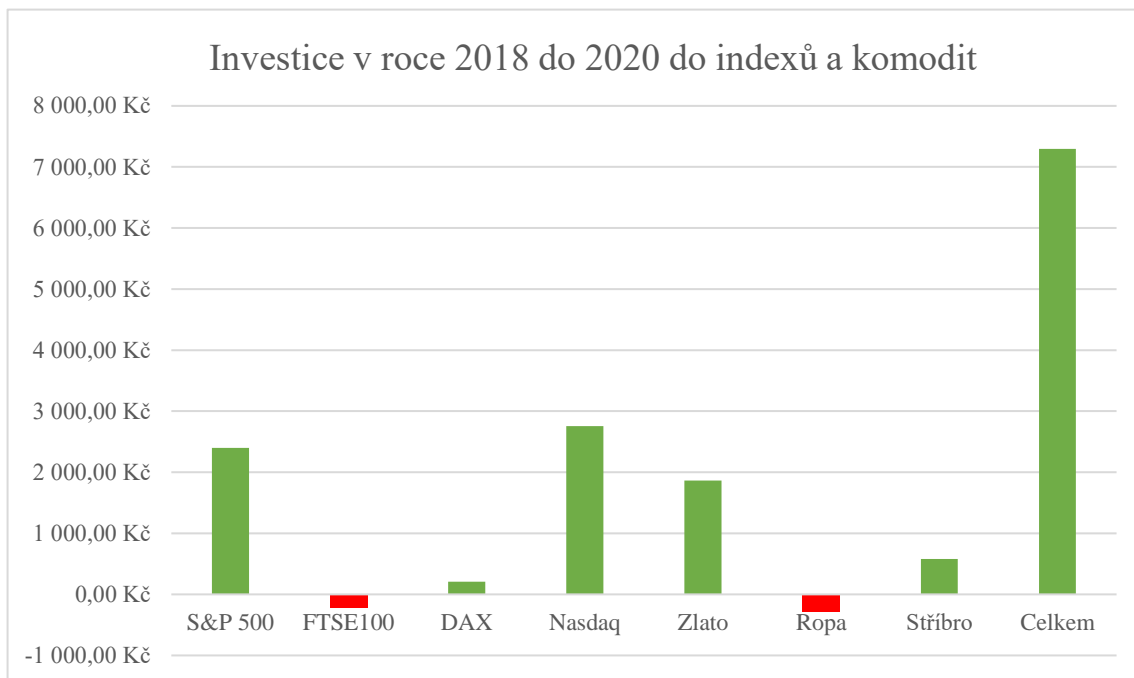


Zdroj: vlastní zpracování

V případě investic do indexů a komodit, jak vyplývá z obrázku 6, investor realizuje zisk. Opět došlo k investici částky 100 000 Kč, úměrně rozdělené do vybraných investičních instrumentů. Závěry jsou velmi pozitivní, a to takové, že všechny položky realizují zisk a žádná ztrátu. Nejmenšího zisku dosahuje index FTSE100, konkrétně 674 Kč, největší zisk index Nasdaq, a to 22 103 Kč. Celkově by investice vynesla 60 456 Kč.

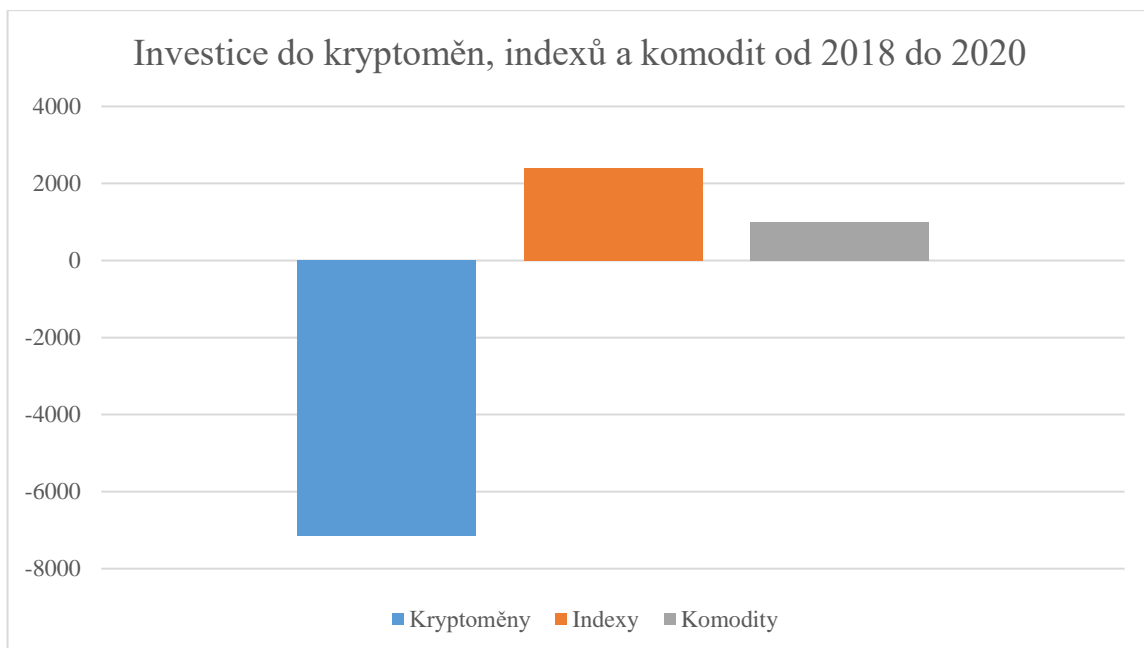
Při srovnání s investicí do kryptoměn v r. 2018 dochází k atraktivnímu srovnání, neb na řadu přicházejí velmi zajímavé závěry. V obrázku 7 se situace naprosto obrací oproti investici pouze do kryptoměn. V případě investice v kryptoměny investor realizuje ztrátu přesahující 13 000 Kč, což je dáno hlavně mladou historií kryptoměn a vysokou volatilitou. V případě, kdy se investor rozhodl investovat své svěřené peněžní prostředky pouze do indexů a komodit v roce 2018 s ukončenou pozicí v roce 2020, realizuje zisk převyšující 7 000 Kč. Je to dáno nízkou volatilitou indexů a komoditami. Ztrátu produkuje pouze index FTSE100 a komodita ropa,

nutno říct, že zcela zanedbatelnou, protože oba tyto investiční instrumenty realizovaly ztrátu pouze přes 200 Kč. Naopak si vedly velmi dobře další indexy, stejně tak i zlato a stříbro.



Zdroj: vlastní zpracování

Pro rozmělnění rizika investování se doporučuje investovat do více investičních instrumentů navzájem. Proto došlo ke spojení investice jak do kryptoměn, tak i do indexů a komodit. Jako příkladné období bylo zvolené to od roku 2018 do roku 2020. Data, ze kterých všechny grafy vychází, jsou umístěná v příloze diplomové práce. Opět došlo k investování souhrnné částky 100 000 Kč, která se rozdělila na 15 dílů, tedy na jeden investiční instrument připadla částka 6 666 Kč.



Zdroj: vlastní zpracování

Z obrázku 8 jasně plyne, že investice do komodit a indexů byly v kladném čísle, oproti tomu zastoupení kryptoměn zcela propadlo. Celková ztráta však nepřevyšovala nijak veliké číslo, nýbrž pouze přes 3 000 Kč. To hlavně z důvodu toho, že investor neinvestoval všechny své peněžní prostředky pouze do kryptoměn, ale zároveň i do indexů a do komodit.

6 DOPORUČENÍ PRO INVESTICE DO KRYPTOMĚN

Závěrečná kapitola se bude věnovat konečnému ohodnocení a doporučení v oblasti investic do kryptoměn, které mohou jednotlivci i podniky učinit.

Jak bylo teoreticky vysvětleno, možnost investovat do kryptoměn, například do Bitcoinu, není potenciaálně nic složitého. Prostřednictvím jedné z burz, nejlépe jedné z celosvětových lze velmi snadno zakoupit kryptoměny. Pro potřebu založení účtu na těchto burzách není potřeba podnikat žádné složité kroky, nýbrž základní verifikaci podle svých osobních údajů uvedených ve svém občanském průkaze. Po zakoupení kryptoměn je důrazně doporučeno vlastnit jednu z některých hardwarových peněženek, například od české známé značky Trezor. Na tu lze následně své investice zasílat. V případě, že by podnik či jedinec nechával investice do kryptoměn ladem ležet na burzách, hrozí jejich znehodnocení, příp. úplná ztráta.

Jako investiční strategii v oblasti kryptoměn je dobré zvolit typ DCA, která eliminuje riziko vysoké a nízké ceny v podobě kurzu za jednu jednotku kryptoměny. Například Ethereum celkovou cenu následně průměruje, a tak nehrozí riziko, že investor nakoupí draze, nebo, že se zrovna treffi do ceny tak, že nakoupí levně. Pravidelné odkládání určité částky v podobě investice v kryptoměny je velmi dobrým způsobem dlouhodobého investování. Vzhledem k tomu, že kryptoměnový svět je stále ještě velmi mladý, existuje zde možnost potenciaálního vysokého růst za účelem své stabilizace a rozvojem IT technologií, které se následně mohou odrazit právě v ocenění investic do kryptoměn.

Tomu nahrává i stále zcela chybějící legislativa České republiky, která o kryptoměnách hovoří velmi okrajově. Pro Bitcoin a další kryptoměny by bezesporu bylo dobré, kdyby čeští zákonodárci postavili kryptoměny alespoň na stejnou rovinu, na jaké se nyní nacházejí akcie, například i pro časový test, kdy by jednotlivec nemusel zisk z investic během průběhu testování danit. Vzhledem k chybějící legislativě v oblasti kryptoměn, tak není ani zcela omezující investování z pozice podniků, či jednotlivců. Proto se rozdíl mezi institucemi investující do Bitcoinu oproti jednotlivcům nevyskytují.

Po teoretickém zvážení všech těchto aspektů je dobře, když si podnik nebo jedinec potenciaální investování do kryptoměn zanalyzuje v rámci jednotlivých cílů, které mají přinést výhody, např. dosažení zisku. Pokud by se investor rozhodoval pouze na základě výsledků výnosnosti, pak lze uvážit, že by pro jednotlivce byla investice správná, hlavně vzhledem k tomu, že jak z dlouhodobého hlediska, tak i krátkodobého hlediska dokáží kryptoměny vý-

razně porážet klasické investiční instrumenty jako jsou indexy S&P 500, FTSE, případně komodity jako jsou zlato nebo stříbro. Klasický investor by se ale neměl rozhodovat pouze na základě jednoho ukazatele, nýbrž na základě vícero ukazatelů, kteří dokáží více zohlednit potenciální riziko investic do kryptoměn. To bezesporu zcela existuje. Vyjadřuje se zčásti například volatilitou investičních aktiv, která dokáží ukázat, jak a o kolik dokáží kryptoměny stoupnout na ceně, případně ztratit. Bylo již zmíněno, že kryptoměnový svět, jmenovitě pak Bitcoin, dokáže ztratit na své hodnotě až 90 %. Je však nutné zdůraznit, že kryptoměny spolu navzájem často korelují, a to nejvíce s Bitcoinem. Klasicky řečeno, klesne-li Bitcoin, klesnou i další kryptoměny. Co je však pro altcoiny o mnoho horší je, že jsou schopné odepsat i celých 95 % své hodnoty, případně i více. Samozřejmě dokáží narůst o stovky procent, avšak stále se jedná o vysoce rizikovou investici v porovnání s jinými indexy, jako je např. Nasdaq, případně investice do zlata nebo stříbra.

Sloučí-li se ukazatelé volatility a výnosnosti, dostane investor komplexní obrázek o vhodnosti investice, neboli ukazatel Sharpe ratio. Podle něj vychází opět nejlépe investice do kryptoměn, zejména Bitcoinu, případně do mladých kryptoměn BNB a Solany.

Závěrem lze říci, že pokud investor zhodnotí i ta rizika, která ucházející jeho pohledu, jeví se kryptoměny jako velmi dobré investiční aktivum, které dokáže přinést v budoucnu zajímavé zisky. V případě, že podnik či jednotlivec nehodlá podstoupit riziko spojené s investicí do kryptoměn, je vhodnější zvolit investice do méně rizikových aktiv, tedy do indexů nebo do komodit, jako jsou zlato nebo stříbro.

ZÁVĚR

V rámci diplomové práce byla rozebrána problematika kryptoměn, hlavně možnosti investování do tohoto investičního instrumentu. Primárním cílem a smyslem celé diplomové práce bylo představení možnosti investice do kryptoměn, sestavení modelového portfolia a pomocí komparace poskytnout potencionálnímu investorovi ucelené informace o investicích do kryptoměn, investičních indexů, případně do komodit, aby následně investor chápal rizika spojená s investicemi do kryptoměn, oproti rizikům spojenými např. s investicemi do zlata.

V diplomové práci byl nejprve charakterizován svět peněz, a tedy jak se peníze definují, jaké jsou jejich vlastnosti a jaké jsou vlastně vůbec základní rozdíly mezi klasickými penězi a kryptoměnami, u kterých byla představená i definice a samotné vlastnosti kryptoměn. Pozornost byla věnována samotné problematice kryptoměn. Nejprve byla na počátku probrána historie samotných kryptoměn, jejich začátky, které se datují do starší historie věku, než je všeobecně známo. Dále došlo k představení dělení kryptoměn, které se diferencují do tří segmentů. Byla představena samotná technologie kryptoměn a vlastnosti, které determinují celý tento segment. V další části byly představeny možnosti, jak se kryptoměny získávají, kde se berou, a tedy samotná těžba. Technologie, která velmi úzce souvisí s tímto tématem, je problematika blockchainu a hashe. Na tomto místě došlo k popisu obou těchto pojmů, bylo vysvětleno využití a charakteristika této moderní technologie. Dále došlo ve druhé části k představení právního rámce na území České republiky, který bohužel stále není zcela rozvinut. Bylo tak nastíněno, že právní rámec našeho státu ne tak zcela pamatuje na segment digitálních aktiv. Zároveň byly popsány možnosti využití kryptoměn v reálném životě a byla představena literární rešerše.

V rámci vzájemné komparace byly vybrány kryptoměny s největší tržní kapitalizací. Byla provedena komparace v počtu mincí a dělitelnost všech uvedených aktiv. Dále byly charakterizovány poplatky za transakci kryptoměn a v neposlední řadě i to, co dělá kryptoměny tolik úspěšnými, jejich rychlost. Její porovnání bylo provedeno s ohledem na to, jak dokáží být jednotlivé kryptoměny rychlé, příp. co zvýšení rychlosti brání.

Pro potřeby diplomové práce a splnění cíle byly popsány metodiky výpočtů, které jsou posléze využity v poslední části práce. Byla představena nejprve výnosnost, podle které se většina investorů rozhoduje. Dále byla popsána metodika výpočtů volatility, tedy jak často se mění a o kolik kurz daného aktiva roste, příp. klesá. Tyto dva výpočty posléze dohromady fungují pro využití ve výpočtech posledního ukazatele, tzv. Sharpe-ratio, který počítá jak s výnosností aktiva, tak i s jeho volatilitou.

K naplnění cíle dopomohla aplikace teoretických znalostí z metodiky výpočtů, čehož bylo dosaženo pomocí softwaru Excel, jehož data jsou uvedena v příloze diplomové práce, ze kterého po zadání jednotlivých dat vzešly hodnoty výnosnosti, volatility a Sharpe ratia. Následně byly všechny tyto hodnoty kryptoměn porovnány se stejnými výpočty z hlediska indexů a komodit. V úplném závěru přišla chvíle pro doporučení spojená s investicemi do kryptoměn ve formě důkladného zvážení veškerých rizik, hlavně jejich volatility. Investice v kryptoměny se jeví v dlouhodobém hledisku jako zisková a porážející klasické instrumenty v podobě vyšších zisků. Kryptoměny jsou i dnes stále něčím novým, ne zcela širokou veřejností probádaným územím. Celý vývoj kryptoměn se nachází stále v rané fázi. Proto bude zajímavé sledovat kryptoměny z hlediska vývoje v dalších letech, případně desetiletích, jestli se dokáží zařadit mezi stabilní investiční instrumenty. Cílem práce bylo popsat decentralizované kryptoměny, to bylo splněno za pomoci popisu jejich vlastností, technologie blockchainu, právního rámce a jejich využitím, tedy všeho uvedeného v předchozích odstavcích. Tento cíl byl splněn i z hlediska komparace kryptoměn navzájem s dalšími investičními instrumenty jako je zlato nebo index Nasdaq, kdy bylo sepsáno zároveň i doporučení pro jednotlivce a podniky. Na závěr je potřeba dodat, že důležité je brát kryptoměny jako novou technologii, která se rozvíjí jak ve veřejné sféře, tak i ve firmách, případně u jednotlivců.

POUŽITÁ LITERATURA

AJIBOYE, Timi, Luis BUENAVENTURA, Alex GLADSTEIN, Lili LIU, Alexander LLOYD, Alejandro MACHADO, Jimmy SONG a Alena VRÁNOVÁ. *The little bitcoin book: why bitcoin matters for your freedom, finances, and future*. Redwood City 2019. ISBN 978-1-64199-050-9.

ALEPH ZERO. *Alephanalysis of 43 Blockchains*. Aleph Zero: Enterprise-grade Public Blockchain [online]. Copyright © 2019 [cit. 04.02.2022]. Dostupné z: <https://alephzero.org/blog/what-is-the-fastest-blockchain-and-why-analysis-of-43-blockchains/>

BOIKO, Viktor, et al. *The optimization of the cryptocurrency portfolio in view of the risks*. Journal of Management Information and Decision Sciences. 2021, s. 1-9.

BRAUNEIS, Alexander; MESTEL, Roland. *Cryptocurrency-portfolios in a mean-variance framework*. Finance Research Letters, 2019, s. 259-264.

COINMARKETCAP: *Cryptocurrencies by market capitalization* [online]. Copyright © 2022 [cit. 01.02.2022]. Dostupné z: <https://coinmarketcap.com>

СТОЙКА, Маріана. *Cryptocurrency–definition, functions, advantages and risks*. Підприємництво і торгівля, 2021, s. 5-10.

CROSBY Michael, NACHIAPPAN, PATTANAYAK Pradhan, VERMA Sanjeev, KALYANARAMAN Vignesh *Blockchain Technology* [online] Copyright © 2015 [cit. 2022-01-23]. Dostupné z <https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>

ČNB. *Náš postoj ke kryptoměnám? Nepomáhat, nechránit, neškodit, nevodit za ruku* [online]. Copyright © ČNB 2022 [cit. 29.01.2022]. Dostupné z: <https://www.cnb.cz/cs/verejnost/servis-pro-media/autorske-clanky-rozhovory-s-predstaviteli-cnb/Nas-postoj-ke-kryptomenam-Nepomahat-nechranit-neskodit-nevodit-za-ruku/>

DERKS, Jona; GORDIJN, Jaap; SIEGMANN, Arjen. *From chaining blocks to breaking even: A study on the profitability of bitcoin mining from 2012 to 2016. Electronic Markets*, 2018, s. 321-338.

EPRAVO.CZ, *Právní (ne)regulace placení kryptoměny*. Sbírka zákonů, judikatura, právo [online]. Copyright © 2021 [cit. 29.01.2022]. Dostupné z: <https://www.epravo.cz/top/clanky/pravni-neregulace-placeni-kryptomenami-113894.html>

HARGRAVE, MARSHALL: *Sharpe ratio definition* [online] 2019 [cit. 31.01.2022] dostupné z: <https://www.investopedia.com/terms/s/sharperatio.asp>

CHUEN, David LEE Kuo; GUO, Li; WANG, Yu. *Cryptocurrency: A new investment opportunity?* The journal of alternative investments, 2017, s. 16-40.

GUTTMANN, Benjamin. *The Bitcoin Bible gold edition*. Norderstedt: Books on demand, 2014. s. 429. ISBN 9783732296965.

JAVATPOINT - *Blockchain Merkle Tree*. Tutorials List [online]. Copyright © 2011 [cit. 27.01.2022]. Dostupné z: <https://www.javatpoint.com/blockchain-merkle-tree>

JÍLEK, Josef. *Finance v globální ekonomice*. Praha: Grada, 2013. ISBN 978-80-247-3893-2.

KAHN, David. *The codebreakers: the story of secret writing*. New York: Scribner, 1996. ISBN 978-0684831305.

KRIPTOMAT.IO. *Blockchain*. [online] Copyright © 2022 [cit. 27.01.2022]. Dostupné z: <https://kriptomat.io/cs/blockchain/co-je-to-blockchain-technologie/>

LÁNSKÝ, Jan. *Kryptoměny*. Praha: C.H. Beck, 2018. ISBN 978-807-4007-224.

LAFAILLE, CHANTELE: *What is blockchain technology? A beginners guide* [online] 2018 [cit. 29.01.2022]. Dostupné z: <https://www.investinblockchain.com/what-isblockchain-technology/>

LINNERTOVÁ, DAGMAR: *Analýza cenných papírů: teoretická východiska a aplikace termínu Bloomberg* [online] 2017 [cit. 30.01.2022] dostupné z:

https://is.muni.cz/el/1456/podzim2017/MPF_ACP1/ACP_1_nove.pdf

MACROOPTION: *Historical volatility calculation* [online] 2018 [cit. 31.01.2022]. Dostupné z: <https://www.macrooption.com/historical-volatility-calculation/>

MARTINÁK, Tomáš. *Bezhotovostní peníze versus elektronické peníze 1. vydání.*

Olomouc: Iuridicum Olomoucense, s.r.o., ve spolupráci s Právnickou fakultou Univerzity Palackého. Olomouc, 2015. ISBN 978-80-87382-74-5

O'KEEFFE, DANIEL: *Understanding cryptocurrency Transaction speed* [online] 2018 [cit. 04.02.2022]. Dostupné z: <https://medium.com/coinmonks/understanding-cryptocurrency-transaction-speeds-f9731fd93cb3>

PRITZKER, Yan. *Vynález jménem bitcoin.* Praha: Braiins Publishing, 2020. ISBN 978-80-907975-0-5.

REJNUŠ, Oldřich. *Finanční trhy 4., aktualizované a rozšířené vydání.* Praha: Grada Publishing a.s., 2014. ISBN 978-80-247-9407-5.

REVENDA, Zbyněk. *Peněžní ekonomie a bankovníctví. 5., aktualiz. vyd.* Praha: Management Press, 2012. ISBN 978-80-7261-240-6.

SAKSONOVA, Svetlana; KUZMINA-MERLINO, Irina. *Cryptocurrency as an investment instrument in a modern financial market.* Вестник Санкт-Петербургского университета. Экономика, 2019, s. 269-282.

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. ISBN 9788027107421.

YILMAZ, Nurgun Komsuoglu; HAZAR, Hulya Boydas. *Predicting future cryptocurrency investment trends by conjoint analysis*. Journal of Economics Finance and Accounting, 2018, s. 321-330.

253/2008 Sb. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu*. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 29.01.2022]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2008-253>

370/2017 Sb. *Zákon o platebním styku*. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 04.11.2021]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2017-370>

PŘÍLOHY

Příloha A – Kurzy kryptoměn ve sledovaném období.....	74
Příloha B – Kurzy indexů a komodit ve sledovaném období.....	75
Příloha C – Potencionální investice v roce 2017.....	76
Příloha D – Potencionální investice v roce 2018.....	77

PŘÍLOHA A – KURZY KRYPTOMĚN VE SLEDOVANÉM OBDOBÍ

BTC	Rok	V USD
07.II	2022	41441
01.I	2022	47476
01.I	2021	28984
01.I	2020	7167
01.I	2019	3687
01.I	2018	13 880
01.I	2017	966

ETH	Rok	V USD
07.II	2022	3118
01.I	2022	3715
01.I	2021	737
01.I	2020	131
01.I	2019	130
01.I	2018	742
01.I	2017	8

Tether	Rok	V USD
07.II	2022	1
01.I	2022	1
01.I	2021	1
01.I	2020	0,996584
01.I	2019	0,99797
01.I	2018	1
01.I	2017	X

BNB	Rok	V USD
07.II	2022	437,1
01.I	2022	515
01.I	2021	38,93
01.I	2020	13,8
01.I	2019	6,02
01.I	2018	8
01.I	2017	0,1064

USD Coin	Rok	V USD
07.II	2022	1,0004
01.I	2022	1
01.I	2021	0,9998
01.I	2020	1,005
01.I	2019	1,0136
01.I	2018	1
01.I	2017	X

Cardano	Rok	V USD
07.II	2022	1,2
01.I	2022	1,32
01.I	2021	0,1753
01.I	2020	0,03346
01.I	2019	0,04255
01.I	2018	1
01.I	2017	0,02048

Solana	Rok	V USD
07.II	2022	120,81
01.I	2022	173,21
01.I	2021	1,8421
01.I	2020	0,7768
01.I	2019	X
01.I	2018	X
01.I	2017	X

LTC	Rok	V USD
07.II	2022	133,5
01.I	2022	150,24
01.I	2021	126,23
01.I	2020	42,02
01.I	2019	31,98
01.I	2018	229
01.I	2017	4,6489

PŘÍLOHA B – KURZY INDEXŮ A KOMODIT VE SLEDOVA- NÉM OBDOBÍ

S&P 500	Rok	V USD
07.II	2022	4483
01.I	2022	4534
01.I	2021	3807
01.I	2020	3278
01.I	2019	2659
01.I	2018	2 807
01.I	2017	2271

FTSE100	Rok	V USD
07.II	2022	7564
01.I	2022	7500
01.I	2021	6640
01.I	2020	7533
01.I	2019	6928
01.I	2018	7 654
01.I	2017	7223

DAX	Rok	V USD
07.II	2022	15233
01.I	2022	15570
01.I	2021	13840
01.I	2020	13392
01.I	2019	11138
01.I	2018	13 201
01.I	2017	11664

Nasdaq	Rok	V USD
07.II	2022	14191
01.I	2022	14326
01.I	2021	13377
01.I	2020	8664
01.I	2019	7540
01.I	2018	7 262
01.I	2017	5571

Zlato	Rok	V USD
07.II	2022	1827
01.I	2022	1796
01.I	2021	1971
01.I	2020	1708
01.I	2019	1465
01.I	2018	1 511
01.I	2017	1390

Ropa BRENT	Rok	V USD
07.II	2022	92,98
01.I	2022	77,915
01.I	2021	50,62
01.I	2020	66,23
01.I	2019	55,06
01.I	2018	68
01.I	2017	56,395

Stříbro	Rok	V USD
07.II	2022	23,01
01.I	2022	23,312
01.I	2021	27,248
01.I	2020	17,93
01.I	2019	15,57
01.I	2018	17
01.I	2017	16,5

PŘÍLOHA C – POTENCIONÁLNÍ INVESTICE V ROCE 2017

Investice v roce 2017	Celková výnosnost
Bitcoin	523 744,82 Kč
Ethereum	4 859 375,00 Kč
Tether	0,00 Kč
BNB	51 338 533,83 Kč
USD Coin	0,00 Kč
Cardano	719 921,88 Kč
Solana	1 931 533,21 Kč
Litecoin	346 455,88 Kč
Celkem	59 719 564,63 Kč

Investice v roce 2017 do indexů a komodit	
S&P 500	13 913,88 Kč
FTSE100	674,40 Kč
DAX	4 370,98 Kč
Nasdaq	22 103,16 Kč
Zlato	4 491,04 Kč
Ropa	9 267,08 Kč
Stříbro	5 636,08 Kč
Celkem	60 456,62 Kč

PŘÍLOHA D – POTENCIONÁLNÍ INVESTICE V ROCE 2018

Investice v roce 2018 do 2020	Celková výnosnost
Bitcoin	-6 045,57 Kč
Ethereum	-10 293,13 Kč
Tether	0,00 Kč
BNB	7 914,20 Kč
USD Coin	0,00 Kč
Cardano	-11 925,48 Kč
Solana	17 142,44 Kč
Litecoin	-10 206,63 Kč
Celkem	-13 414,16 Kč

Investice v roce 2018 do 2020 do indexů a komodit	Celková výnosnost
S&P 500	2 396,95 Kč
FTSE100	-225,83 Kč
DAX	206,68 Kč
Nasdaq	2 757,86 Kč
Zlato	1 862,44 Kč
Ropa	-279,14 Kč
Stříbro	577,77 Kč
Celkem	7 296,72 Kč

Investice v roce 2018 do 2020 do kryptoměn, indexů a komodit	Celková výnosnost
Bitcoin	-3 223,98 Kč
Ethereum	-5 489,12 Kč
Tether	0,00 Kč
BNB	4 220,49 Kč
USD Coin	0,00 Kč
Cardano	-6 359,62 Kč
Solana	9 141,72 Kč
Litecoin	-5 442,99 Kč
S&P 500	1 118,52 Kč
FTSE100	-105,38 Kč
DAX	96,45 Kč
Nasdaq	1 286,94 Kč
Zlato	869,09 Kč
Ropa	-130,26 Kč
Stříbro	269,61 Kč
Celkem	-3 748,54 Kč