Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra ekonomických teorií

Bakalářská práce

Kryptoměny jako investiční příležitost nebo investiční podvod

Martin Čihař

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Čihař

Ekonomika a management

Název práce

Kryptoměny jako investiční příležitost nebo investiční podvod

Název anglicky

Cryptocurrency as an investment opportunity or investment fraud

---

Cíle práce

Hlavním cílem bakalářské práce je vytvoření návrhu jednoduchého, ale účinného investičního portfolia na základě získaných informací o kryptoměnách. Dílčím cílem práce je získání základních znalostí o kryptoměnách, jejich fungování, získávání, držbě a prodeji. Dalšími dílčími cíli práce jsou určení metod odhalení podvodných investic a kroky, jak jim předejít, faktory úspěchu vybraných a populárních kryptoměn, výběr vhodných kryptoměn pro optimistického a pesimistického investora, získání znalostí o směnárenské činnosti a chytré kontrakty. Posledním dílčím cílem je doporučení efektivních způsobů získávání, udržování a prodeje kryptoměn pro účely získání zisku a zhodnocení investic.

Metodika

V bakalářské práci budou na základě znalostí získaných z odborné literatury popsány kryptoměny, a to konkrétně jejich získávání, udržování, prodej, směnárenská činnost, proof of work, proof of stake, blockchain, smart contracts, faktory úspěchu populárních kryptoměn a kryptoměn obecně, historické investiční podvody, Ponziho schéma a pyramidový model. V praktické části bude vytvořeno investiční portfolio, kde na základě aktuálních cen kryptoměn, investičního trojúhelníku, charakteru investora, metod zhodnocení investic a statistických dat z kryptoměnových směnáren bude vytvořen vhodný poměr vybraných investičních produktů pro začínajícího investora s cílem zhodnocení těchto investic.

Doporučený rozsah práce

30 – 40

Klíčová slova

Bitcoin, blockchain, decentralizované finance, Ethereum, investování, investiční portfólio, kryptoměna, Ponziho schéma, proof of work, proof of stake, smart contracts

---

Doporučené zdroje informací

AMMOUS, S. The Bitcoin Standard: The Decentralized Alternative to Central Banking. 1st Edition, Wiley, 2018. ISBN 978-1119473862

BURNISKE, C. & TATAR, J. Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond. 1st Edition, McGraw Hill, 2017. ISBN 978-1260026672

LAU, et al. How to DeFi (Advanced). 1st Edition, 2021. ISBN 979-8530318443

LAU, et al. How to DeFi (Beginner). 1st Edition, 2021. ISBN 979-8530408434

SKALICKÝ, J. & STROUKAL, D. Bitcoin a jiné kryptopeníze budoucnosti. 3. Vydání, Grada Publishing, Praha, 2021. ISBN 978-80-271-1043-8

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. David Křížek, Ph.D.

Garantující pracoviště

Katedra ekonomických teorií

Elektronicky schváleno dne 25. 1. 2023

doc. PhDr. Ing. Lucie Severová, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 22. 2. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 05. 03. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Kryptoměny jako investiční příležitost nebo investiční podvod" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.03.2023 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Davidu Křížkovi, Ph.D. za trpělivost, vstřícnost, cenné rady a věcné připomínky při odborném vedení této bakalářské práce, bez kterých by tato práce stěží dosáhla takové odbornosti, jakou má nyní. Dále bych rád poděkoval své rodině, blízkým a kamarádům za podporu při studiu.

Kryptoměny jako investiční příležitost nebo investiční podvod

Abstrakt

Zpracovaná odborná práce se zabývá tvorbou modelového kryptoměnového investičního portfolia pro začínající investory. Teoretická část práce charakterizuje, co jsou to kryptoměny, jejich způsob fungování a chování, dále jsou popsány kryptografické coiny a tokeny, blockchain a způsob jeho fungování, chytré kontrakty, protokoly Proof-of-Work a Proof-of-Stake, kryptoměnové peněženky, nejpopulárnější kryptoměny současnosti, investování do kryptoměn přes směnárny, P2P obchodování a spotový trh, investiční strategie a podvody s kryptoměnami.

Vlastní práce se zabývá tvorbou kryptoměnového investičního portfolia pro modelového začínajícího investora. Je definován charakter modelového začínajícího investora, způsoby identifikace charakteru investora jako investiční trojúhelník, nebo profil rizika. Dále jsou nastíněny investiční strategie vhodné pro začínající investory, dle jejich investičního charakteru a návazně na to jsou představeny vybrané kryptoměny. Součástí vlastní práce jsou také způsoby odhalení podvodných kryptoměn a konečně portfolia modelového začínajícího investora rozdělená do tří kategorií podle charakteru investora.

Výsledkem práce jsou tři modelová investiční kryptoměnová portfolia, která jsou aplikovatelná pro širokou škálu rozdílných charakterů začínajících investorů. Portfolia mají přesně definované strategie, měny a jejich podíl na celém portfoliu.

Klíčová slova: Bitcoin, blockchain, decentralizované finance, Ethereum, investování, investiční portfolio, kryptoměna, Ponziho schéma, proof of work, proof of stake, smart contracts

Cryptocurrency as an investment opportunity or investment fraud

Abstract

This elaborated bachelor thesis focuses on creating a model cryptocurrency investing portfolio for beginner investors. Theoretical part of this thesis explains what are cryptocurrencies and how they work, what are tokens and coins, blockchain and how it works, smart contracts, Proof-of-Work and Proof-of-Stake protocols, cryptocurrency wallets, most popular cryptocurrencies today, investing in cryptocurrency through exchanges, P2P trading and spot trading, investment strategies and crypto scams.

Analytical part of this thesis focuses on creating a cryptocurrency investing portfolio for model beginner investor. This part of the work also focuses on investing triangle, risk profile, investment strategies appropriate for beginner investors, according to their investment character and then are chosen appropriate cryptocurrencies. Next part also shows methods to prevent investing in crypto scams and finally portfolios of model beginner investors categorized into three categories depending on investor character.

Result of this bachelor thesis are three model investing cryptocurrency portfolios, all of which are applicable on different types of beginner investors. Shown portfolios have accurately defined strategies, currencies and their share in the portfolios.

Keywords: Bitcoin, blockchain, decentralized finance, Ethereum, investing, investing portfolio, cryptocurrency, Ponzi scheme, proof of work, proof of stake, smart contracts

Obsah

1 Úvod

Svět digitálních měn se za posledních deset let vyvinul neskutečným tempem. Satoshi Nakamoto, možná člověk, skupina, nebo korporace (pro přehlednost budeme předpokládat že jde o jednu osobu, muže), vytvořil Bitcoin – první digitální měnu, která umožňovala provádět decentralizované transakce bez závislosti na třetí straně.

Bitcoin spustil lavinu vytváření nových coinů a tokenů, které se ho snažili napodobit a vylepšit. Mezi nimi se objevil jeden coin, který všem duplikátům a imitátorům kraloval. Jde o Ethereum, které se na trhu kryptoměn prosadilo svojí, dnes velice rozsáhlou, sítí digitálních aplikací a finančních služeb, které v současnosti umožňují statisícům uživatelů provádět transakce na jeho blockchainu s pomocí Ethereum peněženky. Od té doby vznikla spousta dalších imitátorů a duplikátů, které se snaží prosadit svými službami na obří kryptoměnové síti, ale zatím žádná z nich neměla takový dopad jako Bitcoin a Ethereum.

Tato odborná práce má za účel Vás o těchto kryptoměnách, a mnoha dalších, poučit, předat vám základní informace o jejich způsobu fungování, ukládání, těžbě, validování, obchodování, a dalších metodách, které jsou s kryptoměnami spojené. Zároveň má tato odborná práce za účel vytvořit jednoduché modelové kryptoměnové investiční portfolio pro začínajícího investora a nastínit metody prevence před podvodnými kryptoměnami a jak je zavčasu rozpoznat.

Lze předpokládat, že kryptoměny, nebo aspoň jejich budoucí forma, nahradí konvenční centralizované měny, což by mohlo být skutečnou budoucností finančnictví, která změní celý svět, tak jak ho známe dnes. Kryptoměny se neustále vyvíjí a s nimi i všechno ostatní – je jen na nás, jak se této příležitosti chopíme.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem této odborné práce je vytvoření správného, smysluplného a výdělečného modelového kryptoměnového portfolia, které bude sloužit jako základ pro investování do kryptoměn se zaměřením na začínající investory. Dílčími cíli této odborné práce jsou odhalení podvodných kryptoměn, předání základních vědomostí o vybraných populárních kryptoměnách a fiat měnách, základních technologiích s nimi spojenými a způsoby jejich fungování.

2.2 Metodika

V teoretické části této odborné práce jsou na základě znalostí získaných z odborné literatury rozpracována různorodá témata týkající se kryptoměn, a to konkrétně jejich získávání, ať už formou nákupu na centralizované, nebo decentralizované směnárně a způsoby jejich fungování, dále je popsán blockchain, jeho prvky a způsob jeho fungování. Následně jsou vysvětleny a popsány chytré kontrakty, populární kryptoměny dnešní doby, protokoly proof-of-work a proof-of-stake, historické investiční podvody jako například Ponziho schéma a podvody spojené s investováním do kryptoměn, kde byla jako příklad uvedena kryptoměna CoinOne. Všechna tato témata byla důkladně prozkoumána a popsána pro účely obeznámení se s tématem a pro vypracování praktické části.

V praktické části jsou na základě informací získaných z teoretické části práce a z alternativních odborných tištěných zdrojů, anebo spolehlivých webových zdrojů vytvořena tři modelová investiční kryptoměnová portfolia pro začínajícího investora. Tato portfolia jsou vytvořena na základě několika kroků, mezi které patří zkoumání investičního chování investora, dále vypracovaný profil rizika, který určuje schopnost přijímat rizika. Další vybraná kritéria jsou výběr investiční strategie a kryptoměn do portfolia, kde se počítá s diverzifikací portfolia, v konkrétním případě dle tržní kapitalizace.

3 Teoretická východiska

3.1 Co jsou to kryptoměny

Kryptoměny jsou kryptografická digitální měna, která oproti svým hmotným alternativám umožňuje provádět transakce prostřednictvím internetu, bez nutnosti ověření třetí stranou, tedy například finanční institucí jako je banka nebo státem. Provádění transakcí centralizovanými metodami má mnoho nevýhod, a to například zmíněná účast třetí strany, která jednak zvyšuje riziko selhání systému nebo krádeži, a zároveň umožňuje třetí straně kontrolovat celý průběh transakce a kdykoliv zasáhnout, jak uzná za vhodné (Ammous, 2018), a s řešením přichází právě digitální měna ve formě *smart contracts*.

Naopak peníze, které běžně užíváme ve formě hotovosti a prostředků na debetních kartách, se kategorizují jako měny fiat – jde o latinské slovo, které lze volně přeložit jako „nechť se stane“ a jde typicky o peníze pod kontrolou státu. Jak uvádí Ammous (2018), měny fiat jsou ve své podstatě veškeré finanční prostředky, nad kterými dohlíží nějaká centralizovaná organizace, jako je banka nebo stát.

3.1.1 Centralizace financí

Kryptoměny jsou semi-decentralizovaná měna. Decentralizovaná měna je charakteristická tím, že není závislá na centralizované moci, tedy například bance či státu, a poskytuje tak větší uživatelskou svobodu v provádění transakcí. Kryptoměny prozatím nejsou kompletně decentralizované, ale i přesto jsou podstatně více decentralizované než měny fiat. Níže si popíšeme druhy centralizace a způsob jejich fungování.

Decentralizované finance

Jak uvádí Lau a kolektiv (2020), decentralizované finance, v současnosti známé především pod zkratkou *DeFi (Decentralized Finance)*, představují soubor finančních služeb, které se nespoléhají na centralizovaných institucích pro jejich fungování. Tyto finanční služby fungují díky decentralizovaným aplikacím *(Dapps – Decentralized applications)*. Dapps jsou ve své podstatě balíček software, který umožňuje provádět transakce na základě chytrých kontraktů. Dapps nejsou omezeny jen na jednoduché transakce, ale poskytují také finanční služby jako například pojištění, půjčky, spoření a mnoho dalších. Decentralizovaným aplikacím se někdy říká LEGO finančnictví, jelikož je

díky jejich unikátnímu způsobu fungování možné různé finanční služby poskládat dohromady.

Centralizované finance

Opakem DeFi jsou finance centralizované. Charakteristickými vlastnostmi centralizovaných financí je používání centralizovaných cenových zdrojů, centrálně určované úrokové sazby, centrálně poskytovaná likvidita a obecně kontrola a moc nad množstvím a oběhem takové měny (Lau, et al., 2020). Příkladem centralizované měny je třeba americký dolar (USD), nebo japonský yen (JPY) – takové měny jsou plně pod kontrolou vlády, a to z nich dělá měnu centralizovanou. Příkladem digitálních centralizovaných měn mohou být například *Salt, BlockFi, Nexo* a *Celsius* (Lau, et al., 2020).

Semi-decentralizované finance

Finance, které jsou semi-decentralizované leží někde mezi financemi centralizovanými a decentralizovanými, s tím, že mají typicky více prvků centralizovaných. Taková měna je například na decentralizované vývojové platformě, ale úroková míra je určená centralizovaně. Příkladem takových měn jsou například *Compound*, *MakerDAO*, *dYdX*, *bZx* a další (Lau, et al., 2020).

3.2 Coin vs. Token

Coin

Kryptoměnový coin *(crypto coin)* je přirozeným produktem svého blockchainu. To znamená, že je jeho neoddělitelnou součástí a funguje jako médium pro transakce. Coiny lze získat na základě Proof-of-Work *(PoW)*, Proof-of-Stake *(PoS)*, nebo nákupem. Typickým příkladem kryptoměnových coinů jsou Bitcoin (BTC), Ethereum (ETH), nebo třeba Cosmos (ATOM), které jsou všechny produktem své sítě (Crypto.com, 2022).

Token

Kryptoměnový token *(crypto token)* je vytvořen pro provoz decentralizovaných projektů na už existujících blockchainech. Nejznámějším blockchainem pro takové projekty je síť Ethereum. Tokeny jsou velice často prostředkem pro uskutečnění chytrých kontraktů. Tokeny mají specifické využití a ve své podstatě nejsou samostatnou kryptoměnou – jde o uměle vytvořené, účelové moduly pro jiné kryptoměny. Příkladem tokenu mohou být SAI a DAI, nebo Maker, které běží na Ethereum síti a jsou závislé na ETH coinu pro své fungování (Crypto.com, 2022).

3.3 Blockchain

Blockchain zaznamenává veškeré informace o transakci, tedy adresu příjemce a odesílatele, dále datum, čas, a množství peněz v transakci (Quest, 2018).

Ve své elementární podobě je blockchain rozsáhlá účetní kniha, která vede záznam o všech transakcích, které kdy na dané kryptoměnové síti proběhly. Blockchain funguje díky obrovské síti vzájemně propojených bodů a bloků.

Nodes

Jak uvádí Quest (2018), tyto vzájemně propojené síťové body se nazývají *nodes*, obdobně jako v síťové architektuře. Každý *node* představuje počítač, který je součástí sítě. Zároveň je každý uživatel napojen na několik jiných bodů naráz. Pokud chce uživatel poslat zprávu (informaci o transakci) do celé sítě, stačí ji odeslat na své bezprostředně sousedící body a ty je pošlou svým sousedícím bodům a tak dále. Tím se dostane informace po celé síti za velice krátký čas.

Transakce

Quest (2018) dále vysvětluje, jakým způsobem probíhají transakce na síti. Transakce musí obsahovat dvě základní informace, aby byla dokázána jejich pravdivost. Jako první podmínku uvádí existenci nějakého svědka a zadruhé je potřeba nějaký důvod, proč transakce probíhá. Svědka transakce si síť zajišťuje formou *nodes*, které informaci o transakci sdílejí po celé síti, a je proto nemožné, aby byla existence transakce promlčena. Zmíněný důvod, proč transakce probíhá, je ve většině případů samotný pohyb peněz.

To si lze vysvětlit v situaci, kdy jeden uživatel provádí transakci s druhým uživatelem o přesunu měny mezi jejich účty. Informace je zachycena na síti a v transakci je uvedené, že dochází k nějaké formě obchodu. Tím jsou splněny obě podmínky, které Quest uvádí ve své odborné publikaci.

Blocks

Transakce je ve formě dat následně vložena do bloku. Jak ve své knize zmiňuje Quest (2018), tento blok vyjadřuje souhrn informací o proběhlé transakci. Jakmile je blok vytvořen, obdrží unikátní hashovací číslo, které je samo sobě originálem. Dojde-li k jakékoliv změně v transakci, hashovací číslo bloku se okamžitě změní na jiné unikátní číslo, a tím vznikne

úplně nový blok a originál ochráněn, čímž je zajištěna pravost informací na síti. Jakmile je blok vytvořen – obsahuje informace o transakci a má svůj unikátní hashovací kód, je umístěn v blockchainu. Poté obdrží informaci od předešlého bloku v blockchainu, o jeho hashovacím kódu. Výsledkem je tedy blok, který má informace o transakci, svůj unikátní hashovací kód a hashovací kód předešlého bloku. Bloky jsou spojené jako řetěz a vnímají jeden druhého jako článek. Proto pojem blockchain – řetěz bloků informací, který se může spolehnout sám na sebe.

Historie vzniku blockchainu

S metodou dávat data do bloků a následně do blockchainu přišli vědci už v roce 1991 jako způsob, jak nenávratně, a tedy unikátně, časově označit vědecké dokumenty. Bohužel v té době nebyl o tento způsob moc zájem a po blockchainu se slehla zem (Bhalla, 2021). Velký návrat zažil blockchain v roce 2007, kdy Satoshi Nakamoto začal poprvé psát kód Bitcoinu a využil metodu blockchainu jako páteř celé sítě (Satoshi, 2007). Dnes je blockchain nedílnou součástí digitálních měn, a zdá se, že tomu tak bude i nadále.

3.4 Smart Contracts

Chytré kontrakty představují souhrn podmínek, které je nutné splnit pro úspěšné provedení transakce. Jak uvádí Lau a kolektiv (2020), takové kontrakty dovolují dvěma stranám nastavit podmínky splnění transakce, bez závislosti na třetí straně, jako prostředníka pro schválení transakce. Jednoduchým příkladem chytrého kontraktu může být dohoda, kdy jeden uživatel chce pravidelně každý měsíc platit peníze druhému uživateli. Uživatelé se dohodnou na podmínkách chytrého kontraktu, který bude kontrolovat a plnit následující podmínky:

1 Zkontroluje dnešní datum (tím vyhodnotí, zdali je čas peníze odeslat)
2 Na začátku měsíce odešle pravidelnou částku z účtu prvního uživatele uživateli druhému
3 Opakuje proces, dokud není kontrakt naplněn

Tím jsme efektivně vytěsnili potřebu třetí osoby, která by náš kontrakt musela kontrolovat a provést. Jednoduše řečeno, chytré kontrakty mají za úkol zkontrolovat splnění podmínek a následně provést cílovou operaci, a to vše bez potřeby třetí strany. Celou tuto operaci provádí počítač, který je nestranný a nemůže ovlivnit průběh kontraktu, a tím je efektivně férovým prostředníkem. Samozřejmě vše je odvislé od kvality samotného kódu chytrého kontraktu – může se stát, že dojde k chybám nebo že kontrakt nebude funkční, ale to už je jen běžná lidská chyba, nikoliv chyba systému.

3.5 Získávání kryptoměn těžbou a validací transakcí

Pokud chceme kryptoměnu získat přímo z blockchainu, musíme ji buďto vytěžit *(mine)*, nebo validovat transakci *(mint/forge)*.

3.5.1 Těžba kryptoměn (Proof-of-Work)

Jak ve své knize popisuje Ammous (2018), při připojení ke kryptoměnové síti obdrží nový uživatel svojí veřejnou adresu *(public adress)* a privátní klíč *(private key)*, které umožňují posílat a přijímat měnu na síti. V situaci, kdy vznikne transakce, je potřeba vytvořit k ní nový blok, který se přidá k blockchainu. Uživatelé, kteří chtějí blok vytvořit, se nazývají těžaři *(miners)*. Tito lidé spolu navzájem svádějí souboj o to, kdo nový blok vytvoří a obdrží tak odměnu za odvedenou práci. Tento proces se nazývá *Proof-of-Work*. V situaci, kdy uživatel úspěšně nový blok vytvoří, je mu na účet přičtena tzv. *block reward*, neboli odměna za práci, která se skládá ze sumy poplatku za transakci a odměny za tvorbu nového bloku.

Zásadní problém, který zatěžuje PoW systém těžby kryptoměn je vysoká energetická náročnost. Jak uvádí *Cambridge Bitcoin Energy Consumption Index* (Cambridgeský index spotřeby energie Bitcoin sítě) Cambridgeské univerzity (2022), průměrná roční spotřeba energie z provozu sítě Bitcoin činí v průměru 97,47 TWh jednotek energie, což je srovnatelné se spotřebou energie malých států jako je například Lucembursko.

Dalším problémem je vznik *mining pools*. Jak uvádí Jemison (2021), mining pooly vznikly jako reakce na rostoucí obtížnost při těžbě kryptoměn, kdy vytvoření každého zhruba 2016. bloku způsobí nárůst obtížnosti těžby a snížení efektivity těžby pro jedince. Mining pool je skupina minerů, kteří společně soupeří o možnost vytvořit nejnovější blok a výslednou odměnu si rozdělí mezi své členy.

Největší mining pooly sítě Bitcoin jsou podle webu 99bitcoins.com (2022) v současnosti *F2Pool*, *Poolin*, *AntPool*, *BTC.com*. Tyto pooly by po spojení tvořili více jak 51 % celkového objemu trhu, na což navazuje problém většinového podílu.

51% útok z pohledu PoW

Dalším podstatným problémem PoW algoritmu je problém většinového podílu, kterému se věnuje Ammous (2018) ve své knize. Tento problém spočívá v tom, že v situaci, kdy by se jeden miner nebo organizace dostala k jednapadesáti procentům veškerých kryptoměn na blockchainu, efektivně by tak mohli kontrolovat zbylých 49 %, což by z dané

organizace nebo jedince vytvořilo centralizovanou entitu. Jedním z řešení tohoto problému je mít na síti co největší množství počítačů, aby se co nejvíce snížila šance, že jedna osoba získá více rovno 51% kontrolu. Druhé řešení nabízí algoritmus *Proof-of-Stake* (Burniske, a další, 2017).

3.5.2 Validace kryptoměn (Proof-of-Stake)

Jak uvádí web Ethereum.org (2022), alternativní způsob, jak kryptoměnu získat přímo z blockchainu je přes algoritmus zvaný Proof-of-Stake *(PoS)*, který efektivně nahrazuje těžbu kryptoměn přes PoW, kde docházelo k centralizaci moci a k obrovské spotřebě energie. Algoritmus PoS přistupuje k tomuto problému velice elegantně. Celá podstata tkví v tom, že PoS namísto souboje síťových bodů vyžaduje jejich spolupráci. To se projevuje v práci validátorů. Validátoři jsou osoby, které validují transakce přes PoS. Jak už z názvu vyplývá, jejich úkolem je validovat transakce v nově vytvořených blocích. Ale aby mohli bloky validovat, musí nejprve do kryptoměnové sítě vložit vklad jako jistinu.

Čím více kryptoměn validátoři do sítě vloží jako jistinu, tím větší šanci mají na to, že úspěšně validují blok a dostanou tak odměnu. Tento systém tak zvýhodňuje osoby, které vloží větší vklad, ale i přesto je tento systém méně centralizovaný než u minerů, protože u validátorů roste šance na úspěch lineárně s výší jejich vkladu, zatímco při těžbě jde o nelineární růst šance na úspěch, jelikož čím více koupí mineři hardware pro těžbu a spotřebovávají větší a větší množství energie, dostávají větší a větší slevu na spotřebu energie od jejich dodavatelů energie. Je to stejné jako vztah odběratele a dodavatele v podnikové ekonomice, čím více zboží objednám jako odběratel, tím větší dostanu slevu od dodavatele.

Zároveň je blockchain díky PoS více chráněný proti podvodným transakcím. Pokud validátor validuje podvodnou transakci jako správnou, blockchain mu efektivně spálí část jeho vkladu. Díky tomu si validátoři dávají větší pozor na to, jaké transakce validují a do blockchainu se tak dostane mnohem menší množství podvodných nebo nesprávných transakcí. Zároveň je díky tomu počet validátorů mnohem menší, než počet minerů, a to prospívá zmíněné nadměrné spotřebě energie.

Přechod sítě Ethereum z PoW na PoS

Jak uvádí web Ethereum.com (2022), 15. října 2022 došlo k procesu jménem *The Merge*, kdy byla celá Ethereum sít přesunuta z algoritmu Proof-of-Work na algoritmus

Proof-of-Stake. Jde o největší softwarové vylepšení v oblasti kryptoměn od doby jejich vzniku roku 2008. Tento přechod měl proběhnout už v roce 2018, ale kvůli obrovskému počtu výzev a příprav spojených s *The Merge,* se projekt opozdil.

51% útok z pohledu PoS a Slashing

Lau a kolektiv (2021) uvádí, že se algoritmus PoS chrání před problémem většinového podílu jednak systémem validátorů a zároveň takzvaným slashováním *(slashing)*. To znamená, že v situaci, kdy je odhalen podvodný účet na blockchainu, nebo validátor neprovádí svojí práci správně, je mu okamžitě smazána veškerá kryptoměna na peněžence spojená s jeho účtem, včetně kryptoměn ve vkladech na síti.

Ve výsledku je PoS podstatně lépe chráněné proti útokům, má menší energetickou náročnost a díky validátorům má menší potencionální šanci na centralizaci moci.

3.6 Kryptoměnové peněženky

Existuje několik druhů kryptoměnových peněženek *(cryptocurrency wallets)*, kdy každý nabízí jiné možnosti, jak svou digitální měnu uložit a dále s ní manipulovat

3.6.1 Custodial a Non-custodial peněženky

Základnímu rozdělení kryptoměnových peněženek se věnují Lau a kolektiv (2020). Základní rozdíl v krypto peněženkách je skutečnost, jestli jsou vaše měny kryté třetí stranou nebo ne. Z toho vychází termíny *custodial*, tedy kryté, a *non-custodial*, tedy nekryté třetí stranou. V případě custodial peněženky jde hlavně o online peněženky na centralizovaných směnárnách, kde vám směnárna v případě krádeže nebo ztráty nahradí vaše digitální peníze v plné výši. Pokud jde o non-custodial peněženky, tak jde především o webové peněženky na DEXs, které kvůli decentralizaci nemají přístup do vaší peněženky, a proto ale zároveň nemohou ručit za její obsah. Další možností jsou hardware peněženky, které jsou fyzicky u vás doma a kryptoměny na nich uložené jsou kryté privátním klíčem, který je uložen přímo na vaší peněžence, ke kterému nemají třetí strany žádný přístup a peníze jsou u vás v bezpečí.

3.6.2 Hot a Cold peněženky

Dále můžeme krypto peněženky dělit na *hot* a *cold*. Jak uvádí Burniske a Tatar (2017), hot peněženky jsou připojené k internetu, a jsou tedy většinou custodial, zatímco cold peněženky, také známe jako *cold storage*, jsou od internetu odpojeny anebo ani nejsou nainstalované na vašem počítači. Většinou, když se bavíme o cold storage, myslíme hlavně hardware peněženky, které představují jednu z nejbezpečnějších metod, jak zabezpečit krypto peníze. Bezpečnější je už pouze papírová peněženka, která je ovšem velice nepraktická.

3.6.3 Online peněženky

Do této kategorie můžeme zařadit peněženky webové, mobilní (ve smyslu aplikace na chytrém telefonu), desktopové (software na počítači), a papírové.

Webové peněženky

Webové peněženky jsou nejčastěji ve formě peněženek na CEXs a DEXs. Mezi takové patří například peněženka Binance, která nabízí jednou manipulaci s financemi a kryje za vás peníze proti zneužití a krádeži (Binance.com). Alternativou může být třeba webová peněženka Coinbase, která se také těší veliké popularitě (Burniske, a další, 2017).

Mobilní peněženky

Další možností jsou mobilní krypto peněženky na vašich chytrých telefonech. Tyto peněženky jsou ve formě aplikace, kde je zabezpečen váš privátní klíč. Je potřeba se připravit na malé poplatky za transakce. Tyto peněženky jsou kompromisem mezi bezpečností a mobilitou a nejsou pro každého. Příkladem mohou být peněženky custodial peněženky Binance nebo Coinbase v mobilní verzi, nebo třeba non-custodial peněženka Exodus a Atomic (Burniske, a další, 2017).

Desktopové peněženky

Desktopové peněženky jsou ve formě software na vašem počítači. Takové peněženky můžou být zároveň hot nebo cold, v závislosti na připojení k internetu. Tyto peněženky jsou většinou zdarma a jsou bezpečnější než webové a mobilní peněženky, protože je privátní klíč na vašem počítači, ke kterému by musel útočník získat přístup, což je například těžší než se dostat k vašemu chytrému telefonu (Burniske, a další, 2017).

3.6.4 Offline peněženky

Papírové peněženky

Jak dále uvádí Burniske a Tatar (2017), podstata těchto peněženek je zřejmá už z jejich názvu. Místo toho, abychom se spoléhali na počítačový software nebo webovou aplikaci, aby uložili náš privátní klíč, vezmeme situaci do vlastních rukou a privátní klíč si napíšeme na papír. V dnešní době je ve velké míře nahradily peněženky hardwarové, které mitigují většinu nevýhod peněženek papírových.

Hardware peněženky

Jak uvádí Burniske a Tatar (2017), jako poslední a definitivně nejlepší možnost, jak zabezpečit své krypto peníze je hardware peněženka. Tyto peněženky jsou dedikovaný kus hardware, na kterém je nainstalovaný jednoduchý software na ukládání privátního klíče a krypto peněženek. Tento systém má několik vrstev ochrany ve formě náhodných slov, až 20místného pinu, hesla apod. Některé fungují sami o sobě a některé je potřeba připojit přes USB kabel k počítači. Mezi nejznámější peněženky tohoto typu patří:

1. **Trezor** – nejpopulárnější hardware peněženka na trhu. Vygenerované privátní klíče nikdy neopustí peněženku, chrání data proti virům a malware, a navíc jde o český výrobek, takže má v České republice velice dobrou dostupnost. Cenově jde o jednu z nejdražších hardware peněženek, ale pokud je vaším cílem kvalitně zabezpečit své kryptoměny, tak tato peněženka je právě pro vás.

2. **Ledger –** peněženky Ledger jsou velice přehledné, jednoduše se ovládají a pro práci s nimi je potřeba je připojit k počítači USB kabelem. Tento kus hardware je velice uživatelsky přívětivý díky integrovanému displeji a intuitivnímu ovládání.

3. **KeepKey –** I u této peněženky najdeme kvalitní zabezpečení ve formě několika vrstev ochrany a intuitivní design s OLED displejem, který peněžence umožňuje konkurovat Ledger a Trezor peněženkám jako rovnocenný soupeř.

3.7 Nejpopulárnější kryptoměny současnosti

Bitcoin (BTC)

První kryptoměnou na světě je Bitcoin (BTC). Bitcoin White Paper byl zveřejněn Satoshi Nakamotem v roce 2007, a je základním kamenem pro další kryptoměny, které vznikly později. Díky Bitcoinu dnes existují stovky kryptoměn, které se pokoušejí obsadit co největší kousek z kryptoměnového trhu. To nám jako investorům dává příležitost si vybírat z obrovského množství kryptoměn a zkoušet různé Dapps, které na svých sítích kryptoměny poskytují.

V současnosti má jeden Bitcoin hodnotu zhruba 19 000 USD (17.10.2022), tedy okolo 479 674 Kč, s tím, že se hodnota v průběhu let mění astronomickým tempem. Nejvyšší hodnota, které Bitcoin dosáhl, byla 08.11.2021, kdy cena jednoho BTC dosáhla neskutečných 67 567 USD, tedy 1 705 999 Kč a market cap byl v té době 1.291 trilionů dolarů (99bitcoins.com).

Ethereum (ETH)

Druhou nejvýznamnější měnou je jednoznačně Ether, který běží na síti Etherea. Hlavním důvodem, proč je tato kryptoměna zajímavá, je množství Dapps, které na její síti běží. Jak uvádí Lau a kolektiv (2020), na Ethereum síti najdeme široké portfolio finančních služeb; pojištění, půjčky, úrokování, spoření, a další. Jelikož je síť Ethereum *open-source*, tedy je veřejně k nahlédnutí, mají developeři možnost vytvářet chytré kontrakty různého druhu, pro různé finanční aplikace.

Ether je hlavní měnou Etherea a lze díky němu nakupovat na internetu i osobně na vybraných místech. Zároveň umožňuje provádět transakce mezi uživateli, je obchodovatelný na směnárně, nebo s ním lze platit poplatky u chytrých kontraktů. Chytré kontrakty na Ethereum síti vyžadují pro svůj provoz *Gas* (jednotka, která vyjadřuje potřebné množství komputační síly pro provoz aplikací na Ethereum síti), která funguje obdobně jako při provozu motorového vozidla. Abyste mohli jezdit, potřebujete palivo. Gas funguje obdobně, ve formě poplatku za provoz. Cena Ethereum paliva může fluktuovat v závislosti na požadavku sítě. Při vysoké zátěži sítě je cena Gas vysoká a při malé zátěži je naopak nízká. V případě velké zátěže algoritmus upřednostňuje transakce s vyšším poplatkem za provoz.

Další způsob, jak lze Ethereum síť využít, který uvádí Lau a kolektiv (2020), je vytvoření *DAO (Decentralized Autonomous Organizations)*, tedy decentralizovaných autonomních organizací, které nejsou vedeny člověkem, ale počítačovým kódem. Tento algoritmus je založen na funkci chytrých kontraktů. DAO jsou transparentní díky jejich veřejnému kódu a není možné je ovlivnit člověkem. Důležitá rozhodnutí jsou prováděna DAO token hlasováním *(DAO token voting)* v rámci chytrého kontraktu.

Dále nám Ethereum síť nabízí možnost vytvořit své vlastní kryptoměnové tokeny. Tvorba tokenů se řídí několika protokoly, podle jejich cíleného využití. Protokol ERC-20 popisuje základní pravidla a standardy pro tvorbu tokenů na síti Etherea. Tokeny vytvořené přes protokol ERC-20 jsou navzájem zaměnitelné a mají stejnou hodnotu. Oproti tomu protokol ERC-721 tokeny jsou nezaměnitelné a jde tak o unikáty s vlastní hodnotou.

Cena Etheru v současnosti (17.10.2022) činí 1 320 USD, tedy okolo 33 000 Kč. Historicky cena dosáhla svého maxima 8. listopadu 2021, kdy dosahoval jeden Ether hodnoty 4 692 USD, tedy zhruba 118 744 Kč (Ethereumprice.org).

3.8 Investování do kryptoměn

Investování do kryptoměn začíná jejich nákupem a končí jejich prodejem – v různých časových měřítkách a ideálně za vyšší hodnotu, než za kterou jsme je zakoupili. Jak zmiňují Burniske a Tatar (2017), většina lidí získá kryptoměny především skrze kryptoměnové směnárny.

3.8.1 Centralizované směnárny (CEXs)

Centralizované směnárny, známé pod zkratkou CEXs *(Centralized Exchanges)* jsou, jak uvádí George (2022), jednoznačně nejbezpečnějším způsobem, jak zainvestovat do kryptoměn. Nabízí širokou paletu služeb a ve většině případů jistí vaše peníze. Kdyby se směnárnu pokusil někdo hacknout a uspěl, velice pravděpodobně by vám vrátili vaše peníze a měnu zpátky na váš účet. Tato vlastnost decentralizovaným směnárnám chybí. Zároveň mají centralizované směnárny velkou výhodu – rozvinuté a kvalitní služby. Centralizované směnárny jako *Binance*, *Kraken*, nebo *Coinbase* nabízí velké portfolio služeb a možností, jak vydělat, a jsou dostupné jak pro začínající, tak i pro pokročilé investory.

3.8.2 Decentralizované směnárny (DEXs)

Pokud se člověk chce vyhnout centralizovaným směnárnám, obrátí se ke směnárnám decentralizovaným. Decentralizované směnárny jsou známé pod zkratkou DEXs *(Decentralized Exchanges)*. Jak uvádí Lau a kolektiv (2020), narozdíl od centralizovaných směnáren jsou DEX více svobodné a jejich uživatelé mají kompletní kontrolu nad svými měnami. Bohužel mají decentralizované směnárny jednu zásadní nevýhodu, a to že pokud dojde ke kybernetickému útoku na směnárnu, kdy se útočníkům podaří ukrást vaše digitální peníze, už je pravděpodobně nikdy neuvidíte, protože decentralizované směnárny většinou neručí za měnu na vašem účtu. Nehledě na to jsou DEXs populární a zájem o jejich služby stále roste. Mezi nejpopulárnější decentralizované směnárny patří *dYdX*, *Futureswap, MCDEX a Injective Protocol* (Lau, a další, 2021).

3.8.3 Peer-to-peer obchodování (P2P)

Alternativní metodou oproti obchodování na směnárně je, podle Jemisona (2021), skrze P2P *(Peer-to-Peer,* nebo *Peer-2-Peer)* obchodování. Uživatel, který chce kryptoměnu koupit, zkontaktuje uživatele, který chce kryptoměnu prodat a udělají jednoduchý obchod.

To probíhá buďto online, nebo osobně. Výměna kryptoměn mezi uživateli není složitá – problém nastává, když se mění kryptoměna za fiat měnu. V takovém případě došlo k několika incidentům, kdy kupci obdrželi nelegální peníze, nebo byli jinak podvedeni.

3.8.4 Spotový trh

Většina obchodů spojených s kryptoměnami probíhá na směnárnách prostřednictvím spotového trhu. Jak uvádí Smith, (2021), spotový trh je místo, kde lze obchodovat kryptoměny, cenné papíry a jiné komodity. Nákup a prodej probíhá téměř okamžitě. Obchodovatelné položky mají svou spotovou cenu a budoucí cenu. Spotová cena vyjadřuje současnou cenu položky, se kterou je možné okamžitě obchodovat.

Nejznámějším spotovým trhem světa je *New York Stock Exchange (NYSE)*, kde se prodává a nakupuje za spotové ceny (Smith, 2021).

3.8.5 Short-term a Long-term obchodování

Jak uvádí Quest (2018), obchodování z časového hlediska lze rozdělit na *short-term* (krátkodobé) obchodování a *long-term* (dlouhodobé) obchodování. Short-term obchodování probíhá v krátkém časovém měřítku, typicky v rámci hodin, nebo týdnů.

Long-term obchodování probíhá v delších časových intervalech, s investičním horizontem jednoho, dvou, nebo více let.

3.8.6 HODLing

HODLing, neboli *buy-and-hold*, je long-term strategie, která je hojně využívána při obchodování s kryptoměnami. Quest (2018) uvádí, že *HODLing*, neboli lidově HODLování, znamená nákup a dlouhodobou držbu kryptoměn, po dobu delší než jeden rok, s cílem jejich zhodnocení.

HODLování je časově a finančně výhodnější, oproti krátkodobým investičním strategiím v případě obchodování s kryptoměnami. Investor, který HODLuje, nemusí být neustále aktivní na spotovém trhu a sledovat aktuální cenu každý den a zároveň ušetří velké množství peněz na poplatcích z nákupu a prodeje, díky malému celkovému množství uskutečněných transakcí.

3.9 Podvody s kryptoměnami

3.9.1 Ponziho schéma a CoinOne podvod

Jak uvádí Lewis (2016), Ponziho schéma je velice jednoduchý a efektivní peněžní podvod. Ponziho schéma má svůj původ v Bostonu roku 1920, kdy ho pro své podvody využil Ital Charles Ponzi, který nebyl první, kdo schéma použil, nicméně právě jeho zločiny toto téma proslavily. Průkopníkem toho podvodu byl Bernard Madoff, který obalamutil i ekonomiky a vysoce postavené úředníky a ze svého podvodu vydělal 40-60 bilionů amerických dolarů, než byl dopaden. (Frankel, 2012).

Ponziho schéma, jak uvádí Lewis (2016), spočívá v tom, že podvodník zaujme investory velkou návratností investic a prohlašuje je za bezpečné a výdělečné, zatímco samotné investice ve skutečnosti nikdy neproběhnou. Investoři jsou povzbuzováni, aby do systému dále investovali. Peníze vložené v prvotní fázi investování se použijí jako výplata prvních dividend, což investory uspokojí a přesvědčí je o výnosnosti investic, a díky tomu mají motivaci investovat více. Zároveň tento koncept posiluje, když investoři povzbuzují svou rodinu a známé, aby investovali také, čímž se zvětší množství peněz, které připadnou podvodnému schéma a tím se zvýší i velikost vyplacených dividend, což opět uspokojuje investory a posiluje na důvěryhodnosti celého podvodu. Celý systém je závislý na neustálém nárůstu počtu nových investorů, kteří vyplatí investory staré, a tím se podvod udržuje nad vodou (Burniske, a další, 2017).

Ponziho schéma není v oblasti kryptoměn žádnou novinkou, jak uvádí Burniske & Tatar ve své knize (2017), jeden z případů využití Ponziho schéma byla kryptoměna *OneCoin*, která lákala své investory na „garantovanou návratnost“. Burniske a Tatar dále uvádějí, že už při přečtení takového sloganu je potřeba být na pozoru a dále uvádějí, že garantovaná návratnost existuje pouze u některých výjimečných finančních produktů, často krytých pojištěním a podobně. Díky tomu, že OneCoin nebyl open-source, nemohla veřejnost nahlédnout do vývojového kódu a odhalit tak tento podvod předčasně. Zároveň *ledger*, tedy účetní kniha transakcí nebyla veřejně přístupná, jak tomu u kryptoměn bývá. Už těchto pár věcí by měli být pro investora upozorněním, že může jít o podvodnou investici.

Naštěstí, jak dále uvádí Burniske & Tatar (2017), komunita tento podvod odhalila a rychle se objevily webové příspěvky, které OneCoin označili jako podvod, potencionální pyramidové schéma a scam, načež později reagovala SEC (U.S. Security and Exchange

Commision), když vydala upozornění na OneCoin a podobné kryptoměny, a ještě více tak rozšířila povědomí o potencionálních podvodech v oblasti digitálních měn.

Burniske & Tatar (2017) ve své knize předávají základní čtyři informace, na co si dát pozor, abychom se vyvarovali Ponziho schéma:

1 Dlouhodobě konzistentní návratnost zisků
2 Tajné nebo komplexní investiční strategie, které vám odmítnou vysvětlit
3 Problémy s výplatou dividend
4 Investici vám nabízí někdo, kdo je investice součástí, tedy ve stejné lodi

Při pátrání po Ponziho schéma je doporučené navštívit web *pyramidschemealert.org*, který se soustřeďuje na poučení o Ponziho schéma a podvodech s tímto podvodem spojeným. Další doporučení, které uvádí Burniske & Tatar (2017) je vyhledat si danou investici na internetu a prověřit si minimálně její historii a jak se chová k jiným investorům, kteří do ní už investovali.

3.9.2 Pump and Dump podvod

Pump and dump podvod, jak popisují Burniske & Tatar (2017), spočívá v rychlém nárůstu a poklesu ceny kryptoměn na spotovém trhu. Tento podvod nejčastěji provádějí neorganizované malé skupiny, které, nejčastěji na sociálních sítích, systematicky nabudí investory na velký budoucí nárůst ceny kryptoměny, tak jak je uvedeno na obrázku č. 1 níže, často s konkrétními časovými milníky, na což nezkušení investoři reagují rychlým nákupem. Jakmile v danou dobu cena kryptoměny vzroste, podvodníci na předpokládaném vrcholu svojí vlastněnou kryptoměnu prodají a vysoce jí zhodnotí. Tento podvod je závislý na psychologii davu, kdy investoři věří v nárůst ceny a propagují proto kryptoměnu dál, čímž nalákají další investory, a cyklus se opakuje, dokud cena nenaroste a podvodníci nezhodnotí své peníze.

Pump and dump podvody se objevují nejčastěji u kryptoměn s malou celkovou tržní hodnotou, kdy podvodníkům stačí koupit polovinu veškeré dostupné měny za malou částku a pump-and-dump podvodem na takové kryptoměně několikanásobně vydělat.

Obrázek č. 1 Příklad pump-and-dump podvodu ve veřejné skupinové konverzaci

Zdroj: (Kamps, 2018), [online], [obrázek], [citováno 05.03.2023]

4 Vlastní práce

Cílem analytické části této odborné práce je vytvoření jednoduchého a efektivního kryptoměnového portfolia pro začínajícího investora, a to za pomoci informací získaných z teoretické části této odborné práce. Zároveň se bude tato část práce věnovat preventivním metodám, jak zabránit výběru podvodné nebo jinak potencionálně nebezpečné kryptoměny.

4.1 Vytváření kryptoměnového portfolia pro začínajícího investora

Tato kapitola se zabývá tvorbou kryptoměnového investičního portfolia, které je vhodné pro začínajícího investora, reaguje na současný vývoj kryptoměnového trhu, bere v potaz charakter investora, základy investování kryptoměn a využívá statistická data kryptoměnových směnáren a obdobných zdrojů pro sběr aktuálních, využitelných informací.

4.1.1 Charakter modelového začínajícího investora

Modelový začínající investor je mladý člověk, dvacet tři let starý, student vysoké školy s ekonomickým zaměřením. Má vědomosti z oblasti ekonomiky a matematiky a je racionálně smýšlející jedinec. Zajímá se o investování v obecném měřítku a zároveň soustřeďuje své síly ke studiu investování do kryptoměn. Modelový investor nemá téměř žádné předešlé zkušenosti s investováním, nemá přesně stanovené investiční cíle a nemá vědomosti na to, aby si vybudoval investiční portfolia, zvolil investiční strategii a správně zvolil kryptoměny, do kterých bude investovat.

4.1.2 Identifikace charakteru investora

Pro vytvoření kryptoměnového portfolia je potřeba si předem stanovit základní cíle a ambice našeho investičního chování. Vyšší potencionální zisk s sebou nese větší riziko ztráty. Zkoumání svého investičního charakteru je nezbytné pro budování racionálního investičního chování. Pro účely identifikace charakteru investora budou využity investiční trojúhelník a profil rizika investora.

Investiční trojúhelník

Investiční trojúhelník (Obrázek č. 2) je základním grafickým vyobrazením vztahu likvidity, rizikovosti a ziskovosti finančních produktů.

Rentabilita na vrcholu trojúhelníku představuje úroveň výdělečnosti finančního produktu. V případě kryptoměn má rentabilita vysoký investiční potenciál. Historicky vydělali kryptoměny investorům astronomické sumy díky rychlému růstu popularity kryptoměn. V současném, válkou a nemocemi komplikovaném ekonomickém klima však nelze jednoznačně určit, zdali bude cena kryptoměn růst na extrémně vysoké hodnoty, jako tomu bylo v listopadu 2021, vyobrazeno jako nejvyšší bod grafu č. 1. Zároveň je třeba zdůraznit, že největší podíl na celkové výnosnosti kryptoměn za celou dobu jejich existence má jednoznačně Bitcoin a hned na druhém místě Ether, a právě proto by aspoň jedna z těchto kryptoměn měla být součástí balancovaného kryptoměnového portfolia.

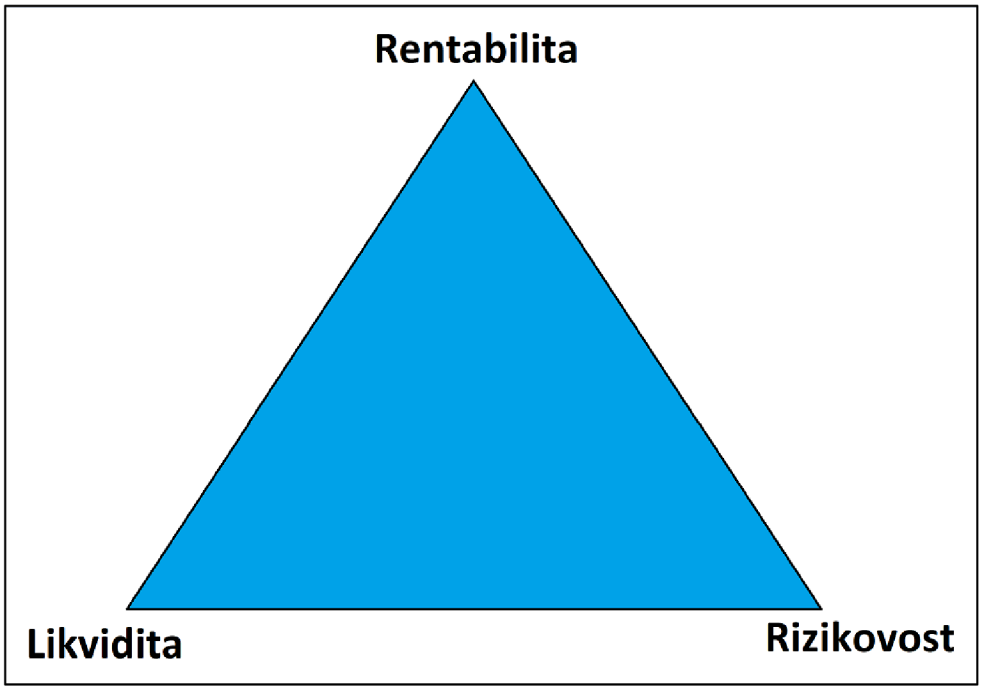
Likvidita, typicky vyobrazená v levém spodním rohu investičního trojúhelníku představuje schopnost přeměnit investované peníze zpět na použitelný disponibilní zisk, a to s co nejmenší ztrátou, nejčastěji způsobenou náhlou změnou ceny finanční komodity na trhu. Likvidita je v případě kryptoměn relativně vysoká. Investované peníze lze v případě CEX v rámci minut přeměnit zpět na disponibilní zisk, a to s relativně malým poplatkem.

Rizikovost neboli investiční risk je diskutabilně nejzásadnější vlastností veškerých finančních produktů a začínající investor musí tuto vlastnost dobře vyhodnotit, nejlépe třeba vypracováním svého profilu rizika.

Rizikovost jakožto vlastnost finančního produktu určuje výši potencionální ztráty vzniklé při obchodování a držbě. Ztráta vzniklá při investování může být téměř zanedbatelná, například běžnými tržními výkyvy, ovšem v některých případech může znamenat i kompletní bankrot investora, nebo i v nejhorších případech krach celého trhu.

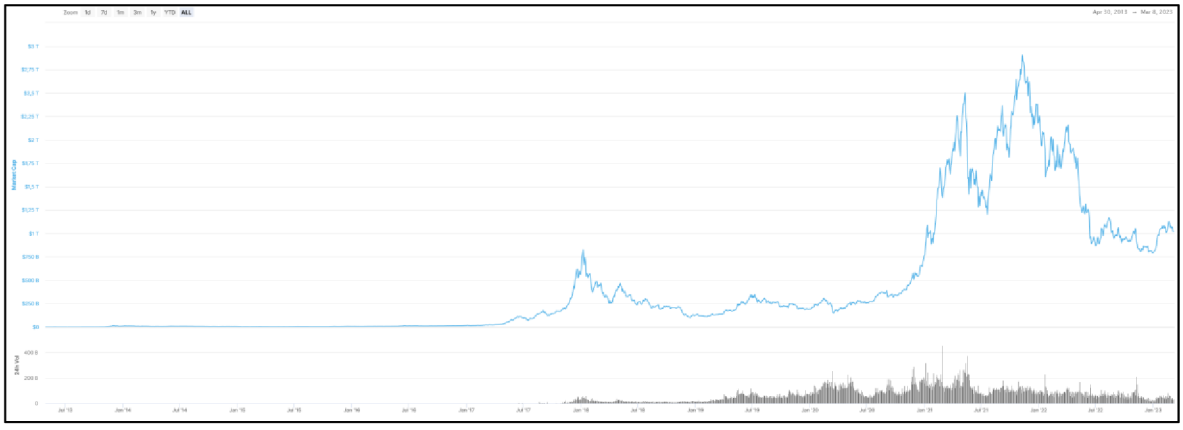
Rizikovost je klíčová vlastnost pro vybudování investičního portfolia, jelikož zásadně ovlivňuje, jaké finanční produkty do našeho portfolia zvolíme.

Obrázek č. 2 Základní model investičního trojúhelníku



Zdroj: Vlastní zpracování, [obrázek]

Graf č. 1 Agresivní vývoj kryptoměnového trhu v čase (v USD)



Zdroj: (Coinmarketcap.com, 2023), [online], [graf], [citováno 08.03.2023]

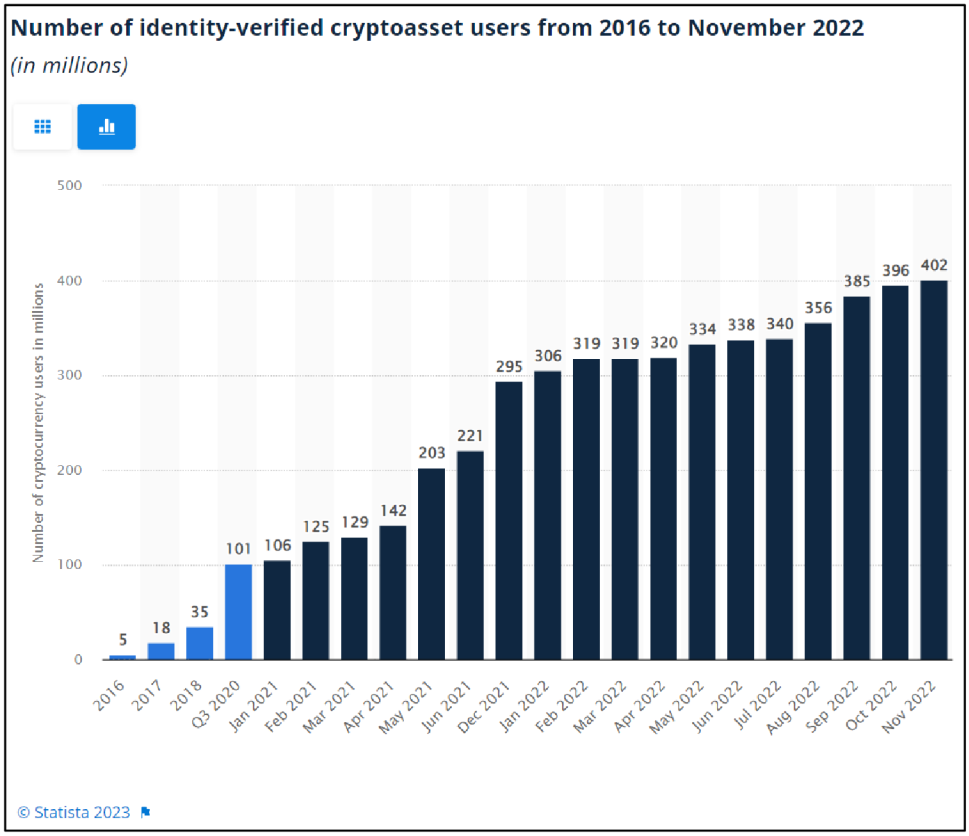
Přidáme-li váhy jednotlivým kategoriím investičního trojúhelníku, vidíme lépe charakter kryptoměn jakožto investičního produktu, viz. obrázek č. 3.

Rizikovosti byla přidělena váha 10, protože stejně jako akcie jsou kryptoměny vysoce náchylné k náhlým změnám v ceně, což nám vyjadřují například graf č. 1 a graf č. 3.

Likviditě byla dána váha 6, jelikož lze relativně snadně přeměnit kryptoměnu zpět na disponibilní peníze, a to minimálně v rámci centralizovaných směnáren, které mají největší podíl na objemu obchodování s kryptoměnami.

Výnosnost obdržela váhu 8. Kryptoměny mají vysoký rentabilní potenciál a mohou tak přinést vysoké zisky. Je možné, že bude jejich rentabilita postupem času růst, vzhledem k růstu popularity kryptoměn a dlouhodobě stoupajícímu trendu počtu jejich uživatelů, viz graf č. 2.

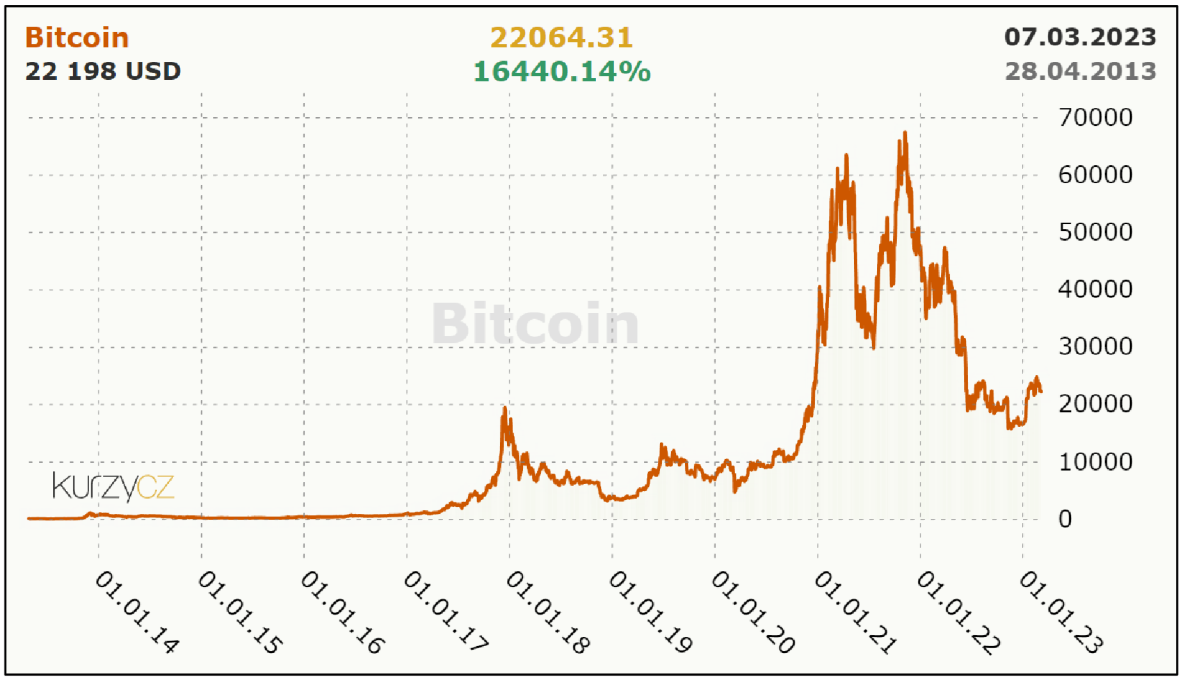
Graf č. 2 Množství verifikovaných uživatelů kryptoměn mezi lety 2016–2022



Zdroj: (Best, 2023), [online], [graf], [citováno 13.03.2023]

Zároveň lze výnosnost kryptoměn odvodit z historického vývoje ceny BTC, jakožto stěžejní měny kryptoměnového trhu, kterou lze vidět v grafu č. 3. Hned na první pohled je evidentní, že jsou cena BTC a celková zásoba trhu kryptoměn (graf č. 1) téměř identické a obě vysoce volatilní.

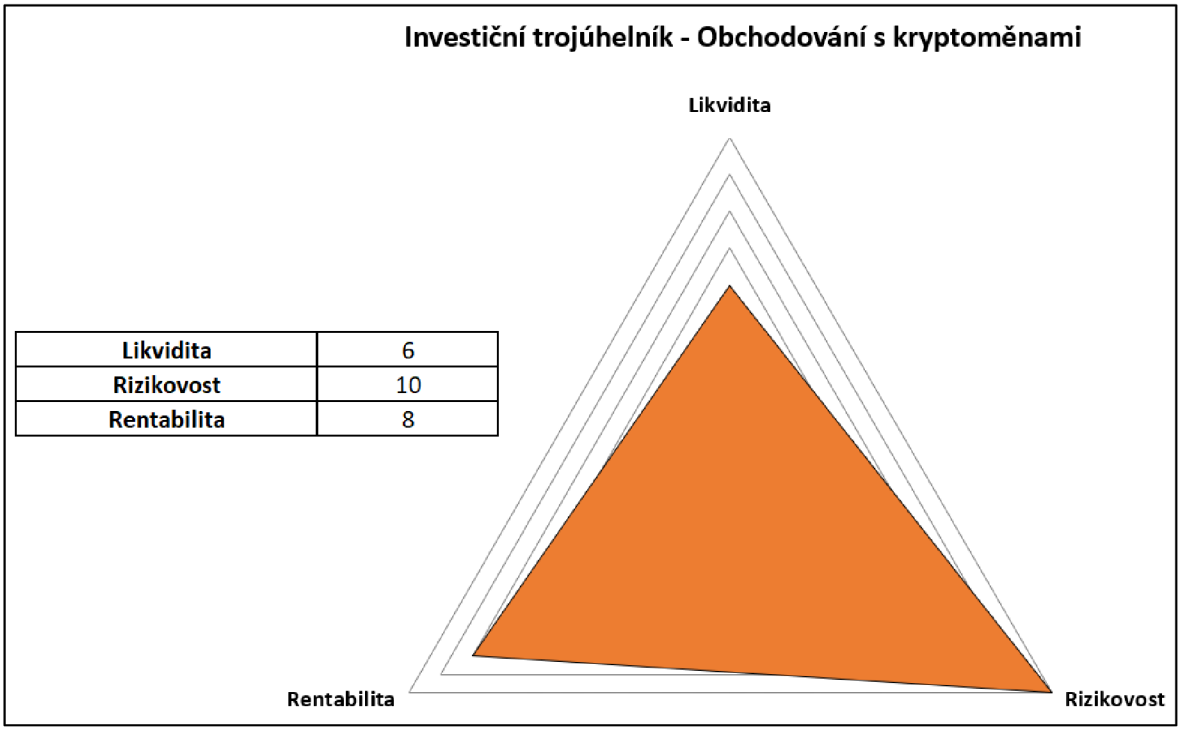
Graf č. 3 Agresivní vývoj ceny kryptoměny BTC v čase (v USD)



Zdroj: (Kurzy.cz, 2023), [online], [graf], [citováno 08.03.2023]

Určení vah jednotlivým prvkům modelového investičního trojúhelníku umožnilo lépe zařadit kryptoměny mezi ostatní investiční produkty. Jak lze vypozorovat z obrázku č. 3, modelového investičního trojúhelníku s dosazenými váhami jednotlivým prvkům, kryptoměny jsou velice podobné akciím a jiným agresivním finančním produktům svým chováním na trhu – jsou vysoce rizikové, ale zároveň mají vysoký výnosový potenciál. Stanovené váhy jsou pouze modelové a mohou se změnit v rámci chování trhu, národní a nadnárodní ekonomiky, nebo jiných socio-ekonomických vlivů.

Obrázek č. 3 Investiční trojúhelník v rámci obchodování s kryptoměnami



Zdroj: Vlastní zpracování, [obrázek]

Rizikový profil investora

Rizikový profil investora umožňuje lépe se rozhodnout, jaké kryptoměny zařadit do investičního portfolia a proč. Bere v potaz, jaké jsou cíle a ambice investora, kolik by si investor představoval vydělat peněz a za jakého rizika je ochoten tyto peníze vydělat. Rizikový profil má typicky podobu tří typů investičního charakteru, a to:

1) Konzervativní (Pesimistický)
2) Mírný
3) Agresivní (Optimistický)

Konzervativní investor je typicky více pasivní, nemá zájem o vysoce rizikové finanční produkty a volí spíše klidnější investiční metody pro vydělání zisku. Jeho cílem je dosažení zisku s ohledem na rostoucí inflaci, kterou svým ziskem kompenzuje a chrání tak svůj kapitál před zbytečnou ztrátou (Fxstreet.cz, 2022). V běžném životě jsou tito investoři klidní a předem kalkulují své výnosy a ztráty, na což potřebují velké množství času a energie.

Mírný investor je více připravený na přijímání rizik a je připraven na svých penězích vydělat. Vyjadřuje zlatý střed v investičním charakteru – přijímá rozumné riziko při rozumných očekáváních na výdělek a své rozhodování optimalizuje tak, aby své peníze aspoň minimálně zhodnotil, nebo aspoň zachránil před inflací.

Agresivní investor je připraven podstoupit velká rizika, aby své investice zhodnotil. Je připravený utrpět větší kontrolované ztráty a znásobit tak své zisky. Agresivní investoři jsou v běžném životě typicky více impulzivní a činí rychlejší rozhodování.

Charakter investora je ovlivněn několika podstatnými faktory, které je potřeba zhodnotit při zkoumání svého rizikového profilu investora. Jak uvádí web fxstreet.cz (2022), jde například o psychologii investora (jeho chování, temperament, vlastnosti apod.), jeho věk, množství zkušeností, nejvyšší dosažené vzdělání, délka investičního horizontu a očekávaná velikost investičního portfolia. Lze stanovit i další faktory, které umožní dosáhnout vyšší přesnosti výsledků. Pro vytvoření svého profilu rizika lze využít veřejně dostupných testů, typicky online, které mají podobu několika otázek a výsledkem je odhad vašeho charakteru investora. Tyto testy sestávají typicky z deseti otázek formou tří odpovědí (A, B, C) které úzce korelují s charakterem investora (A – konzervativní, B – mírný, C – agresivní).

Příklad otázek takového testu lze najít na webu idnes.cz (2015), který vznikl ve spolupráci s UniCredit Bank.

Výsledek testu je zjištěn sečtením počtu zodpovězených odpovědí typu A, typu B a typu C a typ odpovědí, který má největší počet vybraných odpovědí nejlépe vystihuje investiční charakter testovaného investora, a tedy i profil rizika.

Začínající investor by měl být schopen na základě výsledku svého rizikového profilu lépe určit, do jakých investičních produktů, v tomto případě kryptoměn, investovat. Rizikový profil umožňuje lépe si utřídit myšlenky o investování a zároveň racionálním způsobem určit, jakého je investor investičního charakteru a jak velká je připraven podstoupit rizika. Tyto schopnosti začínajícímu investorovi typicky schází.

4.1.3 Výběr vhodné investiční strategie

Teď když je nám znám charakter investora a víme, kolik peněz by si investor přál vydělat, jaké je ochoten přijmout riziko, a jaký je jeho investiční horizont. Dále je žádoucí zvolit vhodnou investiční strategii, podle které se bude dále odvíjet investorovo investiční chování. Začínající investor, který nemá zkušenosti s kryptoměnami by se měl řídit jednou z následujících strategií, které nejsou složité a vyžadují minimum zkušeností s investováním. Zároveň je potřeba dodat, že šikovný investor bude investiční strategie kombinovat v závislosti na svých cílech.

HODLování

Základní investiční strategií při investování do kryptoměn je HODLování. Jak už bylo zmíněno v teoretické části, HODLování spočívá v dlouhodobé držbě kryptoměn s cílem počkat, až bude mít investovaná částka několikanásobně vyšší hodnotu než v době nákupu.

Investiční horizont této investiční strategie může činit jeden rok až desítky let. Výhoda této strategie spočívá v její jednoduchosti. Investor si nakoupí vybrané kryptoměny, nejčastěji přes CEX, a pouze průběžně sleduje cenovou křivku. Není potřeba často obchodovat, stačí měnu hlídat a dlouhodobě držet (HODLovat).

Tato strategie je vhodná pro všechny typy začínajících investorů, jelikož není potřeba znát velké množství informací ohledně obchodování, a není tak složité své peníze znásobit. Tato strategie je obzvlášť zajímavá pro konzervativní investory, jelikož je zde dlouhý investiční horizont, a díky tomu dostatek času na rozhodování.

Dollar-cost averaging (DCA)

Tato strategie je vhodná pro všechny typy investorů do kryptoměn. DCA spočívá v malých pravidelných investicích. Výhodou této metody je pravidelné navyšování celkové investované částky, což může znamenat větší potencionální zisky. Velkou nevýhodou této strategie mohou být vysoké náklady za poplatky spojené s pravidelným nakupováním kryptoměn.

Podkategorií této metody je *micro-investing*, které stejně jako DCA spočívá v pravidelných investicích, ale jde o mnohem menší pravidelné nákupy. Může jít třeba o nákup 0,003 BTC (přibližně 145 Kč) každý měsíc.

Value investing

Value investing spočívá ve včasné identifikaci investičních příležitostí, které se jeví jako nezajímavé teď, ale mohou být vysoce výnosné později, nebo jsou jednoduše málo populární, ale i přesto potencionálně rentabilní. *Value* investoři investují do podceněných komodit, společností, finančních produktů a dalších a to s cílem své investice dlouhodobě zhodnotit. Investiční horizont této strategie může být i několik desítek let, kdy investor například čeká až hodnota firmy, do které investor investoval své peníze, vzroste na hodnotě. Příkladem mohou být první Bitcoin investoři, kteří viděli v BTC potenciál, který se v dnešní době jednoznačně projevil.

Growth investing

Obdobou *value investing* je *growth investing*, kdy se investoři snaží předpovědět budoucí hodnotu investic a zainvestovat do nich v době, kdy jsou cenově dostupnější. Zatímco *value* investor hledá podceňované investice s velkým potencionálem, *growth* investor investuje například do projektů nebo kryptoměn, které jsou teprve v procesu růstu a investováním do nich zvyšuje jejich kapitál a očekává výplatu v budoucnu. Tato strategie je svým charakterem dlouhodobá.

Momentum investing

Momentum investing je charakteristické aktivním přístupem na trhu. Investoři na základě dat technických analýz investičních produktů zvažují prodej a koupi, a to v relativně

krátkém čase. *Momentum investing* má krátké časové rozpětí mezi investicemi, jelikož investoři musí rychle reagovat na změny cen na trhu. Tento přístup k investování přináší výnosy typicky v malých průběžných částkách a je hodně závislý na historickém vývoji investice a popularitě mezi lidmi.

4.1.4 Výběr kryptoměn & diverzifikace portfolia

Kryptoměny, které lze zařadit do investičního portfolia lze vybrat na základě investičního charakteru investora, jeho profilu rizika, zvolené investiční strategie, očekávaného zisku a dostupného disponibilního kapitálu. V této podkapitole jsou nastíněné některé druhy kryptoměnových coinů a tokenů, které jsou z pohledu investování potencionálně výdělečné a dostupné začínajícím investorům. Jak uvádí Buchko (2018), jakékoliv investiční portfolio je nezbytné diverzifikovat, aby se předešlo potencionální ztrátě. Investor, který nemá diverzifikované portfolio a sází tak na jednoho koně riskuje, že v případě velkého poklesu hodnoty na trhu může přijít o vše co doposud investoval. Buchko dále říká, že je vhodné mít aspoň jednu velkou investici (>5 miliard USD) dle celkové tržní kapitalizace kryptoměny, jednu střední investici (250 milionů – 5 miliard USD) dle celkové tržní kapitalizace kryptoměny, a jednu menší (<250 milionů USD) investici dle celkové tržní kapitalizace kryptoměny. To znamená minimálně tři kryptoměny v investičním portfoliu, každá s velmi rozdílným podílem na trhu. Nicméně například pro konzervativního investora není vhodné volit kryptoměny s tržní kapitalizací pod 250 milionů USD, jelikož ho vystavují zbytečně vysokému riziku ztráty.

4.1.5 Kryptoměny vhodné do kryptoměnového investičního portfolia

V této podkapitole shrnu některé zajímavé kryptoměny, které podle jejich charakteru a způsobu fungování přiřadím modelovému začínajícímu investorovi do jeho kryptoměnového investičního portfolia.

Vybrané měny s tržní kapitalizací větší jak 5 miliard USD (Velké investice)

Kryptoměny s tržní kapitalizací větší jak 5 miliard USD se dají kategorizovat jako nejbezpečnější z kryptoměn. Jejich cena je, relativně, nejstabilnější. Všechny tyto měny jsou vhodné pro začínající investory.

Některé vybrané kryptoměny s kapitalizací nad 5 mld USD, které lze zařadit do investičního portfolia:

1) Bitcoin (BTC), tržní kapitalizace činí 466 miliard USD, charakterem měna
2) Ethereum (Ether – ETH), tržní kapitalizace činí 204,6 miliard USD, charakterem Dapp platforma
3) Tether (USDT), tržní kapitalizace činí 72,8 miliard USD, charakterem *stablecoin* (kryptoměna, která má poměr 1:1 s FIAT měnou, 1 USDT =~ 1,01 USD)
4) Binance coin (BNB), tržní kapitalizace činí 48,7 miliard USD, charakterem měna CEX
5) Dogecoin (DOGE), tržní kapitalizace činí 9,6 miliard USD, charakterem měna
6) Binance USD (BUSD), tržní kapitalizace činí 8,3 miliard USD, charakterem stablecoin
7) Avalanche (AVAX), tržní kapitalizace činí 5,38 miliard USD, charakterem Dapp platforma, přímý rival Ethereu a zároveň poslední kryptoměna s tržní kapitalizací nad 5 mld USD

Vybrané měny s tržní kapitalizací od 250 milionů do 5 miliard USD (Střední investice)

Tyto kryptoměny jsou považovány za investici středního rozsahu. Často jde o méně populární, nebo velice specializované kryptoměny, které nejsou podporované velkým kapitálem. Často tyto kryptoměny selhávají získat dostatečnou popularitu a vracejí se zpět do kategorie investic nižšího rozsahu.

Vybrané kryptoměny s kapitalizací od 250 milionů USD do 5 miliard USD:

1) Uniswap (UNI), tržní kapitalizace 4,7 miliard USD, charakterem Dapp platforma
2) Chainlink (LINK), tržní kapitalizace 3,5 miliard USD, charakterem Dapp platforma zaměřená na smart contracts
3) Cosmos (ATOM), tržní kapitalizace 3,4 miliard USD, charakterem Dapp platforma, méně populární přímý rival Ethereu
4) Monero (XMR), tržní kapitalizace 2,7 miliard USD, charakterem speciální měna se zaměřením na anonymní transakce, díky tomu často spojovaná s kriminalitou
5) Decentraland (MANA), tržní kapitalizace 1,1 miliard USD, charakterem měna virtuálního světa (ve své podstatě herní měna)

6) Aave (AAVE), tržní kapitalizace 1,07 miliard USD, charakterem protokol pro půjčování kryptoměn jak ze strany věřitele, tak ze strany dlužníka
7) The Sandbox (SAND), tržní kapitalizace 921 milionů USD, charakterem měna virtuálního světa (herní měna) založená na decentralizovaných autonomních organizacích (*DAOs*) a *NFTs* (zaměnitelné tokeny)
8) DAO Maker (DAO), tržní kapitalizace 252 milionů USD, charakterem platforma pro vytváření decentralizovaných autonomních organizací (*DAOs*)

Vybrané měny s tržní kapitalizací do 250 milionů USD (Malé investice)

Kryptoměny s kapitalizací do 250 milionů USD jsou často začínající kryptoměny, kterým se povedlo dostat se na vlnu popularity, nebo může jít o zajímavé *growth / value* investice, které se zhodnotí postupem času. Každopádně jsou tyto kryptoměny relativně cenově dostupné, ale je zde větší pravděpodobnost, že jde o podvodnou kryptoměnu, která má za úkol pouze získat na popularitě, následně obohatit své tvůrce a pak navždy zaniknout a zároveň jsou tyto kryptoměny poměrně rizikové.

1) Hive (HIVE), tržní kapitalizace 190 milionů USD, charakterem platforma pro Dapps, služby a sociální sítě
2) Solar (SXP), tržní kapitalizace 150 milionů USD, charakterem měna
3) Ronin (RON), tržní kapitalizace 129 milionů USD, charakterem nativní měna blockchainu pro provoz online her (Axie Infinity)
4) PlayDapp (PLA), tržní kapitalizace 115 milionů USD, charakterem nativní měna blochchainu pro provoz online her (Along with the Gods – MMORPG pro chytré telefony)
5) Braintrust (BTRST), tržní kapitalizace 116 milionů USD, charakterem měna speciální sítě pro vyhledávání talentovaných lidí, kterým poskytne pracovní možnosti, s Braintrust spolupracují například Nestle, Nike, nebo Porsche

4.1.6 Jak odhalit podvodné kryptoměny

Před zvolením kryptoměn do investičního portfolia je třeba segregovat kryptoměny podle jejich důvěryhodnosti. Kryptoměny mají dlouhou historii podvodů, které jejich uživatelům prodělali miliardy amerických dolarů. Pravděpodobně nejznámější podvod

spojený s kryptoměnami je kryptoměna OneCoin, která byla zmíněna v teoretické části této odborné práce.

Burniske & Tatar (2017) shrnují čtyři základní kroky, jak se vyhnout Ponziho schéma, pravděpodobně nejčastějšího podvodu spojeného s kryptoměnami. První radou je dávat pozor na sliby dlouhodobě konzistentní návratnosti zisků z investice, druhý krok, jak uvádí autoři, říká, že je třeba dbát na to, jak se kryptoměna prezentuje a zdali nezadržuje, nebo cíleně nekomplikuje informace o jejich investiční strategii a podnikovým cílům. Třetím krokem, kteří autoři zmiňují je vyhnout se kryptoměnám, které mají problémy s výplatou dividend. Ve své podstatě jde o zdržování ze strany podvodníků – technické chyby, nefunkční weby, odložené a neuskutečněné transakce a podobně. Poslední čtvrtá rada spočívá v tom, že je třeba dát si pozor na ukvapené nadšení z kryptoměn o kterých vám řekl známý. Jenom proto, že váš kolega, kamarád, milenec apod. investuje do nějaké kryptoměny a je to skvělá kryptoměna ještě neznamená, že je to pravda. Jednoduchým řešením je selský rozum a vyhledávání na internetu. Lež má krátké nohy, ale utíká těm, kteří za ní neběží.

Další způsoby, jak odhalit podvodné kryptoměny, uvádí americká federální obchodní komise pro ochranu spotřebitele (2022):

a) Pouze podvodníci vyžadují platby v kryptoměnách, ať už online nebo osobně.
b) Pouze podvodníci garantují výnosy nebo velké zisky.
c) Nikdy nekombinujte online randění s investováním, pokud se s vámi někdo spojí a chce vám vysvětlit, jak investovat do kryptoměn, jde pravděpodobně o podvod.
d) Náhodný investiční manažer vás kontaktuje relativně bez důvodu.
e) Podvodník předstírá, že je celebrita, nebo jiná veřejná známá osoba nebo entita, která vám údajně znásobí kryptoměny, které jim odešlete.
f) Podvodník předstírá, že je součást úřadů, policejních ochranných složek apod.

V obecné rovině lze říci že je nezbytné být neustále na pozoru a vždy věnovat patřičné množství času a energie studiu každé kryptoměny, do které chceme investovat, vyhýbat se příliš jednoduchým ziskům a složitým investičním strategiím a nenechat si o investování jen

tak něco namluvit od lidí, které dobře neznáme. Podvodných kryptoměn už bylo spousta a dnešní podvodníci jsou šikovnější než kdy předtím.

4.1.7 Modelové investiční portfolio začínajícího investora

Teď když jsme obeznámeni s investičním charakterem investora, profilem rizika, byla zvolena investiční strategie, vybrány kryptoměny, do kterých lze investovat a byli jsme poučeni o způsobech, jak předcházet podvodům s kryptoměnami, jsme připraveni vytvořit modelové investiční portfolio.

Konzervativní modelové investiční portfolio

V případě konzervativního investora je vhodné vytvořit investiční portfolio, které využívá dlouhodobé investiční strategie a investuje do kryptoměn, které jsou považované za stabilní.

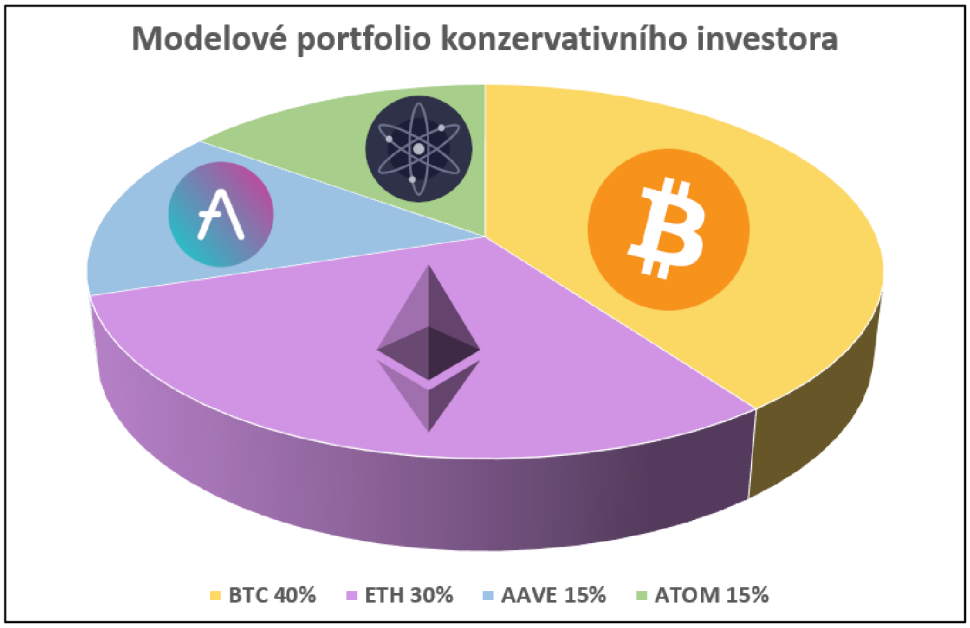
Nejvhodnější investiční strategií pro konzervativního investora je HODLování, která má dlouhý investiční horizont a představuje relativně malé riziko, minimálně oproti jiným investičním strategiím. Tuto investiční strategii lze kombinovat se strategií DCA, respektive její podkategorií *micro-investing*, která umožní konzervativnímu investorovi vložený kapitál dlouhodobě a v malých částkách zvětšovat.

Do investičního portfolia je vhodné zvolit minimálně dvě kryptoměny, které jsou bezpečné a mají tržní kapitalizaci vyšší než 5 miliard USD. Jako ideální kandidáti se jeví BTC a ETH, které jsou dominantou světa kryptoměn. Jejich potencionální výdělečnost je velice zajímavá a pro konzervativního investora, který je ochotný čekat roky na správnou situaci k prodeji nahromaděných kryptoměn, jsou tyto kryptoměny ideální. Jako další kryptoměny je vhodné zvolit minimálně dvě kryptoměny s tržní kapitalizací mezi 250 miliony USD a 5 miliardy USD. Zde lze zvolit z poměrně velkého množství kryptoměn, například XMR, ATOM, nebo AAVE, které v posledních letech zažívají růst popularity, ale stále jde o relativně stabilní měny, u kterých se nečeká náhlý krach. V případě konzervativního investora není vhodné volit žádné kryptoměny s tržní kapitalizací pod 250 milionů USD, jelikož tyto kryptoměny představují zbytečné investiční riziko a i vzhledem ke zvolené investiční strategii dlouhodobé držby a micro-investování jsou nevhodné.

Investiční portfolio konzervativního investora (Graf č. 4) je založeno na dlouhodobé investiční strategii s malými opakovanými investice. Dále obsahuje čtyři kryptoměny, z toho dvě kryptoměny s tržní kapitalizací nad 5 miliard USD a tři kryptoměny s tržní kapitalizací

mezi 250 miliony USD a 5 miliardami USD. Stabilnější kryptoměny mají větší podíl na portfoliu.

Graf č. 4 Modelové investiční portfolio konzervativního investora



Zdroj: Vlastní zpracování, [graf]

Investiční portfolio vyobrazené výše je z modelových portfolií to nejbezpečnější a nejvhodnější pro začínající investory. Představuje relativně nízké riziko ztráty, je jednoduché na pochopení a nenáročné na provoz.

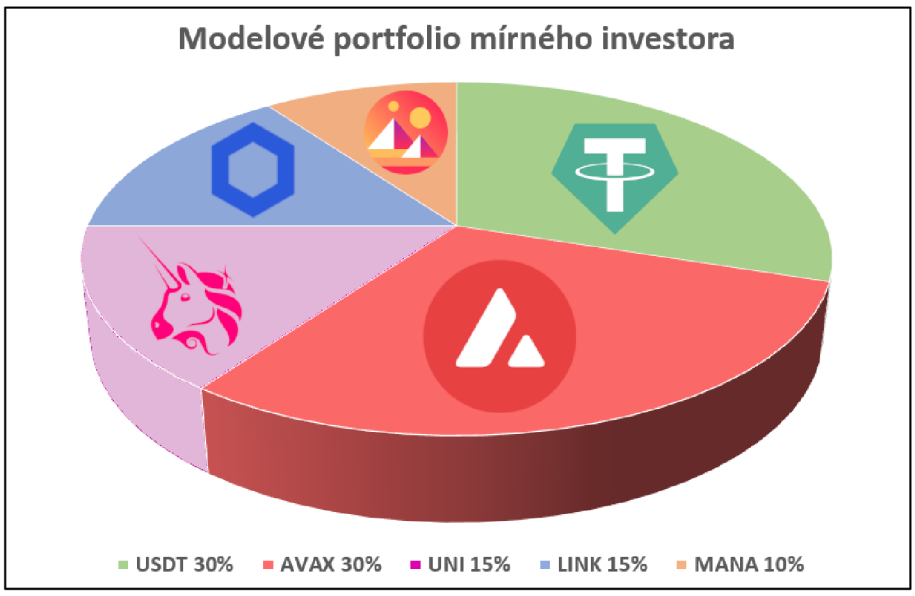
Mírné investiční portfolio

Investoři mírné povahy oproti konzervativním investorům uvítají lehce agresivnější přístup k investování. Mírné investiční portfolio je vhodné založit primárně na dlouhodobé investiční strategii. Vhodné dlouhodobé strategie pro mírného investora jsou HODLování, *value investing*, nebo *growth investing*. Krátkodobé investiční strategie u mírného investora postrádají smysl, jelikož vystavují investora zbytečně vysokému riziku.

Modelové investiční portfolio mírného investora obsahuje minimálně jednu, ale klidně dvě kryptoměny s tržní kapitalizací nad 5 miliard USD. Příkladem takových kryptoměn mohou být USDT, BUSD, nebo AVAX. Dále obsahuje jednu až tři kryptoměny s tržní kapitalizací mezi 250 miliony USD a 5 miliardy USD, kde lze zvolit například UNI, LINK nebo MANA.

Investiční portfolio mírného investora (Graf č. 5) je založeno na dlouhodobé investiční strategii, nebo jejich kombinaci. Dále obsahuje pět kryptoměn, z toho dvě kryptoměny s tržní kapitalizací nad 5 miliard USD a tři kryptoměny s tržní kapitalizací mezi 250 miliony USD a 5 miliardami USD. Stabilnější kryptoměny mají opět větší podíl na portfoliu.

Graf č. 5 Modelové investiční portfolio mírného investora



Zdroj: Vlastní zpracování, [graf]

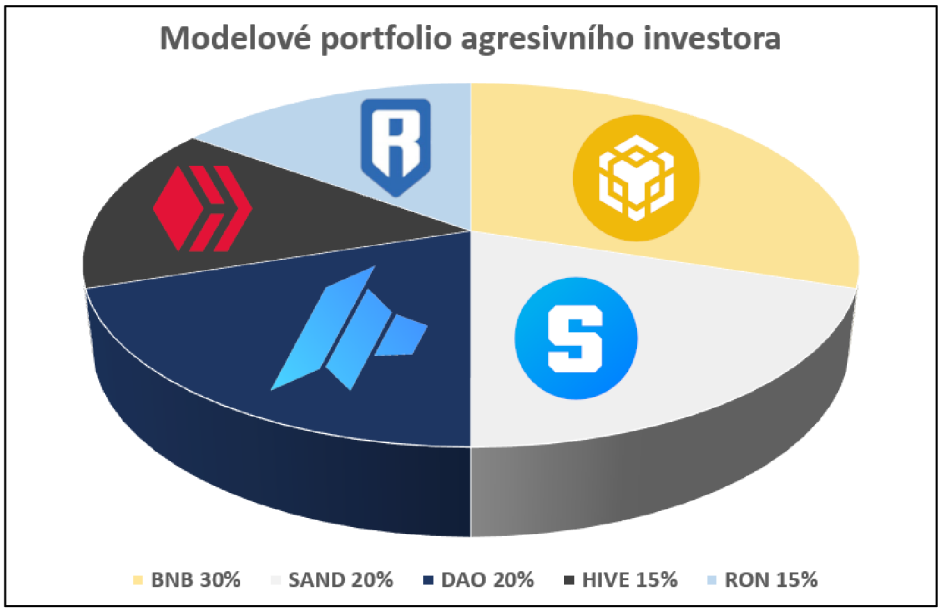
Agresivní investiční portfolio

Investoři agresivní povahy jsou připraveni podstoupit větší riziko pro získání výnosů, čímž se jim zpřístupňují možnosti pro investování v kratších investičních horizontech. Investiční portfolio agresivního investora lze zakládat například na strategii *momentum investing*, která je aktivnější oproti předešlým zmíněným investičním strategiím. *Momentum investing* umožní investorovi provádět transakce častěji, s větším rizikem a větším potencionálem rentability. Je možné kombinovat rychlejší *momentum investing* strategii pro kryptoměny s tržní kapitalizací do 250 milionů USD třeba s *HODLing* strategií pro kryptoměny s tržní kapitalizací nad 5 miliard USD, aby bylo dosaženo větší diverzity.

Modelové investiční portfolio mírného investora obsahuje minimálně jednu, ale klidně dvě kryptoměny s tržní kapitalizací nad 5 miliard USD. Příkladem takových kryptoměn mohou být BTC, nebo BNB. Dále obsahuje jednu až dvě kryptoměny s tržní kapitalizací mezi 250 miliony USD a 5 miliardy USD, kde lze zvolit například SAND, nebo DAO. Zároveň lze do portfolia přidat jednu až dvě kryptoměny s tržní kapitalizací menší než 250 milionů USD, tedy více rizikové kryptoměny jako například SXP, nebo RON. V případě těchto rizikovějších kryptoměn je potřeba dobře prozkoumat co tyto kryptoměny dělají, jací jsou jejich tvůrci a zdali projekt stále úspěšně pokračuje. Investoři, kteří uvidí větší potenciál v počítačových virtuálních realitách mohou volit kryptoměny jako právě RON, nebo PLA, zatímco investoři se zájmem o originální projekty mohou volit spíše BTRST, nebo HIVE.

Investiční portfolio agresivního investora (Graf č. 6) je založeno na krátkodobé investiční strategii, nebo v kombinaci s dlouhodobou strategií. Dále obsahuje pět kryptoměn, z toho jednu kryptoměnu s tržní kapitalizací nad 5 miliard USD, dvě kryptoměny s tržní kapitalizací mezi 250 miliony USD a 5 miliardami USD a dvě kryptoměny s tržní kapitalizací menší než 250 milionů USD. Stabilnější kryptoměny mají jako v předešlých modelových portfoliích větší podíl na portfoliu.

Graf č. 6 Modelové investiční portfolio agresivního investora



Zdroj: Vlastní zpracování, [graf]

5 Výsledky a diskuse

Výsledkem této odborné práce jsou tři modelová investiční kryptoměnová portfolia pro začínající investory vytvořená na základě charakteru investora, profilu rizika, investičních strategií, diverzifikace portfolia, volby kryptoměn do portfolia a prevence proti podvodným kryptoměnám.

Definice modelového investora

Nejprve byla vytvořena charakteristika modelového začínajícího investora, ve které lze nalézt shrnutí investorova chování, zkušeností s investováním, vzdělání apod., které jsou klíčové pro vytvoření tří modelových portfolií dle investičního charakteru.

Charakter investora a profil rizika

Následně byl vypracován profil rizika a prozkoumán charakter investora, které dali vzniknout třem kategoriím investorů dle jejich investičního chování – konzervativní investor, mírný investor a agresivní investor.

Investiční strategie

V návaznosti byly navrhnuty v současnosti používané kryptoměnové investiční strategie, které umožnili začínající investory lépe segregovat do jejich skupin dle investičního chování. Mezi zmíněné investiční strategie patří HODLování, DCA, *Micro-investing, Growth investing*, *Value investing* a *momentum investing*, kde každá z nich nabídla odlišný pohled na možnost investování do kryptoměn.

Kryptoměny a diversifikace portfolia

V tomto kroku bylo vysvětleno, jakým způsobem je vhodné diversifikovat kryptoměnové investiční portfolio a jakým způsobem lze investice rozdělit dle tržní kapitalizace. Tržní kapitalizace (market cap) se rozdělili do tří kategorií – kryptoměny s tržní kapitalizací do 250 milionů USD, které jsou považovány za malé, riskantnější investice, dále kryptoměny s tržní kapitalizací od 250 milionů USD do 5 miliard USD, které jsou považovány za střední investice a nakonec kryptoměny s tržní kapitalizací nad 5 miliard USD, které jsou považovány za nejstabilnější a nejméně rizikové, velké investice.

Návrh vhodných kryptoměn dle jejich tržní kapitalizace

Následně byly na základě předchozí kapitoly navrženy kryptoměny do kryptoměnového portfolia dle jejich tržní kapitalizace. Pro velké investice byly navrhnuty kryptoměny BTC, ETH, USDT, BNB, DOGE, BUSD a AVAX, pro střední investice byly navrhnuty kryptoměny UNI, LINK, ATOM, XMR, MANA, AAVE, SAND a DAO, a pro malé, riskantnější investice byly navrhnuty kryptoměny HIVE, SXP, RON, PLA a BTRST.

Prevence před podvodnými kryptoměnami

V poslední přípravné kapitole byly shrnuty některé základní metody, jak předejít volbě podvodné kryptoměny (Burniske, a další, 2017) a byly představeny vybrané typické podvodné situace, na které upozornila americká federální obchodní komise pro ochranu spotřebitele (Federal Trade Commision, 2022).

Vytváření modelových investičních portfolií

Poslední část vlastní práce sloužila pro samotné vytváření modelových kryptoměnových investičních portfolií, na základě informací získaných z teoretické a vlastní práce. Výsledkem vlastní práce jsou tři modelová investiční kryptoměnová portfolia, vytvořena na základě tří kategorií investičního chování – jedno portfolio pro konzervativního investora, jedno pro mírného investora a jedno pro agresivního investora. Tato portfolia byla složena i na základě získaných informací o investičních strategiích, diverzifikaci portfolia, metod prevence podvodných kryptoměn a výběru samotných kryptoměn na základě jejich tržní kapitalizace.

Diskuse odborné práce

Jak je patrné z vytvořených grafů č. 4, 5 a 6, úspěšně se podařilo vytvořit balancované investiční portfolio pro každého ze tří modelových investorů. Každopádně tato portfolia jsou pouze modelová a neberou v potaz veškerá možná kritéria, která by mohla tvorbu portfolia dále ovlivnit, jelikož už by to bylo nad rámec této odborné práce. Nicméně by bylo možné zvážit faktory jako počáteční kapitál, cílový kapitál, zahrnout matematicko-statistické metody pro výpočet výnosnosti, nebo návratnosti, nebo pracovat s měsíčním příjmem jednotlivých investorů a na základě toho určit doporučenou měsíční investici, nebo rozšířit portfolio o další kryptoměny. Všechny tyto faktory by mohli pomoci k vytvoření přesnější a

lepšího investičního portfolia. Dále by bylo možné zkoumat investiční chování z pohledu pohlaví, náboženství, kultury, státní příslušnosti, socio-ekonomické vlivy na investování apod. Každopádně vytvořená modelová portfolia více než dostatečně poslouží pro začínající investory, avšak bylo by možné portfolia dále zkoumat, zahrnout více faktorů a kryptoměn a vytvořit tak portfolio přesnější, respektive více na míru.

5.1 Závěr

Hlavním cílem této odborné práce bylo vytvořit modelové kryptoměnové investiční portfolio pro začínajícího investora na základě několika faktorů. V souvislosti s tímto cílem byly prozkoumány investiční strategie, charakter investora, profil rizika, diverzifikace portfolia, kryptoměny a další. Výsledkem jsou tři modelová kryptoměnová investiční portfolia pro tři typy investorů – pro konzervativního investora, mírného investora a agresivního investora. Všechny tyto typy portfolií jsou vhodné pro cílového začínajícího investora.

Zároveň byly formou dílčího cíle vysvětleny metody prevence proti podvodným kryptoměnám a byly zmíněny konkrétní případy, ať už jde o Pump & Dump, Ponziho schéma, nebo třeba imitace celebrit, nebo státních příslušníků pro účely získání rychlého zisku od nepozorných investorů. Všechny informace v této odborné práci byly čerpány z odborné tištěné literatury, zahraničních webových článků a veřejně dostupných statistik.

Do budoucna by bylo vhodné více zkoumat chování investorů, způsoby, jakými investují, kolik mají typicky základní kapitál a podobně. Dále by se dalo detailněji rozpracovat každé kryptoměnové portfolio a bylo by zajímavé vytvářet kryptoměnová portfolia i pro zkušené investory, kteří hledí na investování úplně odlišným způsobem než investoři začátečníci.

6 Seznam použitých zdrojů

99bitcoins.com. Bitcoin All Time High (ATH). *99 Bitcoins - We Translate Bitcoin to Plain English.* [Online] [Citace: 17. Říjen 2022.] https://99bitcoins.com/bitcoin/historical-price/all-time-high/#charts.

Ammous, Saifedean. 2018. *The Bitcoin standard: the decentralized alternative to central banking.* Hoboken, New Jersey : John Wiley & Sons, 2018. ISBN 978-1-119-47386-2.

Beigel, Ofir. 2022. 7 Best Bitcoin Mining Pools. *99bitcoins.com.* [Online] 1. Březen 2022. [Citace: 29. Říjen 2022.] https://99bitcoins.com/bitcoin-mining/pools/.

Best, Raynoer de. 2023. statista.com. *statista.com - Global Cryptocurrency userbase.* [Online] 08. Březen 2023. https://www.statista.com/statistics/1202503/global-cryptocurrency-user-base/.

Bhalla, Anshika. 2021. A Detailed History Of Blockchain: From The Establishment To Broad Adoption. *Blockchain-council.org.* [Online] 3. Červen 2021. [Citace: 28. Říjen 2022.] https://www.blockchain-council.org/blockchain/a-detailed-history-of-blockchain-from-the-establishment-to-broad-adoption/.

Binance.com. Kryptoměnová burza | Binance. *Binance.com/cs.* [Online] [Citace: 16. Říjen 2022.] https://www.binance.com/cs.

Burniske, Chris a Tatar, Jack. 2017. *Cryptoassets: The Innovative Investors Guide to Bitcoin and Beyond.* 1. místo neznámé : McGraw Hill, 2017. str. 368. ISBN 1260026671.

Cambridge, University of. 2022. Cambridge Bitcoin Electricity Consumption Index. *University of Cambridge Judge Business School.* [Online] 15. Říjen 2022. [Citace: 15. Říjen 2022.] https://ccaf.io/cbeci/index.

Coinmarketcap.com. 2023. *coinmarketcap.com - Global cryptocurrency charts.* [Online] 08. Březen 2023. https://coinmarketcap.com/charts/.

Crypto.com. 2022. Crypto Tokens vs Coins - What's the Difference? *crypto.com.* [Online] 20. Červen 2022. [Citace: 15. Říjen 2022.] https://crypto.com/university/crypto-tokens-vs-coins-difference.

Ethereum.org. 2022. Proof-of-Stake (PoS). *ethereum.org.* [Online] 10. Říjen 2022. [Citace: 16. Říjen 2022.] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

—. 2022. The Merge. *Ethereum.org.* [Online] 28. Říjen 2022. [Citace: 28. Říjen 2022.] https://ethereum.org/en/upgrades/merge/.

Ethereumprice.org. Ethereum Price History. *ethereumprice.* [Online] [Citace: 17. Říjen 2022.] https://ethereumprice.org/history/.

Federal Trade Commision, FTC. 2022. consumer.ftc.gov. *consufer.ftc.gov - What To Know About Cryptocurrency and Scams.* [Online] Duben 2022. https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams#scams.

Frankel, Tamar. 2012. *Th e Ponzi scheme puzzle: a history and analysis of con artists and.* 1. New York : Oxford University Press, 2012. str. 227. ISBN 978-0-19-992661-9.

Fxstreet.cz. 2022. *fxstreet.cz - Rizikový profil investora a jak jej určit.* [Online] 19. Prosinec 2022. https://www.fxstreet.cz/tym-robomarkets-rizikovy-profil-investora-co-to-je-a-jak-jej-urcit.html.

George, Benedict. 2022. Centralized Exchange (CES) vs. Decentralized Exchange (DEX): What's the Difference? *Coindesk.com.* [Online] 5. Srpen 2022. [Citace: 16. Říjen 2022.] DEXs, CEXs. https://www.coindesk.com/learn/centralized-exchange-cex-vs-decentralized-exchange-dex-whats-the-difference/.

idnes.cz. 2015. *idnes.cz - Jaký typ investora jste.* [Online] 16. Srpen 2015. https://www.idnes.cz/finance/investovani/kviz-jaky-jste-typ-investora.A150813_153901_inv_kho.

Jemison, Kyle. 2021. *Crypto Master 21: THE EXPLANATION OF BLOCKCHAIN TECHNOLOGY, AS WELL AS BITCOIN AND CRYPTOCURRENCY TRADING. A Beginner's Guide to Definitions, Cryptocurrency Exchanges, Indicators.* 2. Srpen 2021. ASIN: B09BRD3THK.

Kamps, Josh. 2018. ResearchGate.net. *ResearchGate.net.* [Online] 2018. [Citace: 5. Březen 2023.] https://www.researchgate.net/publication/329193706_To_the_moon_defining_and_detecting_cryptocurrency_pump-and-dumps.

Kurzy.cz. 2023. Kurzy.cz. *Kurzy.cz - Bitcoin, aktuální a historické ceny vývoje kryptoměny Bitcoin.* [Online] 08. Březen 2023. https://www.kurzy.cz/komodity/bitcoin-graf-vyvoje-ceny/usd-10-let.

Lau, Darren, a další. 2021. *How To Defi (Advanced).* 1. místo neznámé : Coin Gecko, 2021. str. 296. ISBN 979-8530318443.

—. 2020. *How To DeFi (Beginner).* 1. s.l. : Teaspoon publishing, 2020. p. 200. ISBN 979-8640579109.

Lewis, Mervyn K. 2016. *Understanding Ponzi Schemes: Can Better Financial Regulation Prevent Investors from Being Defrauded?* 1. místo neznámé : Edward Elgar Publishing, 2016. str. 200. ISBN 1786433400.

Quest, Martin. 2018. *Cryptocurrency Master Bundle: Everything You Need To Know About Cryptocurrency and Bitcoin Trading, Mining, Investing, Ethereum, ICOs, and the Blockchain.* 1. místo neznámé : CreateSpace Independent Publishing Platform, 2018. str. 261. ISBN 1721961631.

Satoshi, Nakamoto. 2007. *Bitcoin Paper.* 2007.

Smith, Tim. 2021. Spot Market: Definition, How They Work, and Example. *Investopedia.com.* [Online] 29. Září 2021. [Citace: 30. Říjen 2022.] https://www.investopedia.com/terms/s/spotmarket.asp.

Steven, Buchko. 2018. coincentral.com. *coincentral.com - How to build a proper cryptocurrency trading portfolio.* [Online] 27. Duben 2018. https://coincentral.com/how-to-build-a-proper-cryptocurrency-trading-portfolio/#heading-h2-1.

7 Seznam obrázků, tabulek, grafů a zkratek

7.1 Seznam obrázků

7.2 Seznam tabulek

7.3 Seznam grafů

7.4 Seznam použitých zkratek

1) *DeFi (Decentralized finance)* – Decentralizované finance
2) *Dapps (Decentralized applications)* – Decentralizované aplikace fungující na blockchainu
3) *USD (United States Dollar)* – Americký dolar, FIAT měna
4) *JPY (Japanese Yen)* – Japonský yen, FIAT měna
5) *ETH (Ether)* – Ether, digitální kryptografická měna
6) *PoS (Proof-of-Stake)* – Proof-of-Stake, protokol pro validaci kryptografických měn
7) *PoW (Proof-of-Work)* – Proof-of-Work, protokol pro těžbu kryptografických měn
8) *CEXs (Centralized Exchanges)* – Centralizované směnárny
9) *DEXs (Decentralized Exchanges)* – Decentralizované směnárny
10) *OLED (Organic light-emitting diode)* – Dioda, která využívá organický materiál jako svou elektroluminiscenční látku

11) *BTC (Bitcoin)* – Bitcoin, digitální kryptografická měna
12) *DAO (Decentralized Autonomous Organizations)* – Decentralizovaná autonomní organizace, vytvořená přes technologii blockchainu
13) *ERC-20 (Ethereum Request for Comments 20)* – Protokol pro vytváření zaměnitelných tokenů na síti Etherea
14) *ERC-721 (Ethereum Request for Comments 721)* – Protokol pro vytváření nezaměnitelných tokenů na síti Etherea
15) *P2P (Peer-2-Peer, nebo Peer-to-Peer)* – P2P, může znamenat směnku mezi dvěma osobami; populární síťový protokol pro přenos soubor na lokální síti
16) *NYSE (New York Stock Exchange)* – Nejznámější spotový trh světa v New Yorku, Spojených státech amerických
17) *HODLing (Buy-and-hold)* – Hodlování, dlouhodobá investiční strategie často používaná při investování do kryptoměn
18) *DCA (Dollar-cost averaging)* – DCA, dlouhodobá investiční strategie spočívající v pravidelných investicích
19) *USDT (United States Dollar Tether)* – USDT, digitální kryptografická měna, stablecoin
20) *FIAT (Fiduciary money)* – FIAT, sám o sobě bezcenný objekt, který slouží pouze směně, k obchodování (Kč, USD, YEN apod.)
21) *NFT (Non-fungible token)* – NFT, nezaměnitelné tokeny, nejčastěji spojované s autentickým digitálním uměním
22) *MMORPG (Massively multiplayer online role-playing game)* – MMORPG, masivně multiplayerová online role-playing hra; kategorie počítačových her
23) *BNB (Binance Coin)* – BNB, digitální kryptografická měna
24) *DOGE (Dogecoin)* – Dogecoin, digitální kryptografická měna
25) *BUSD (Binance United States Dollar)* – BUSD, digitální kryptografická měna
26) *AVAX (Abalanche)* – AVAX, digitální kryptografická měna
27) *UNI (Uniswap)* – UNI, digitální kryptografická měna
28) *LINK (Chainlink)* – LINK, digitální kryptografická měna
29) *ATOM (Cosmos)* – ATOM, digitální kryptografická měna
30) *XMR (Monero)* – XMR, digitální kryptografická měna
31) *MANA (Decentraland Mana)* – MANA, digitální kryptografická měna
32) *AAVE (Aave)* – AAVE, digitální kryptografická měna

33) *SAND (The Sandbox)* – SAND, digitální kryptografická měna
34) *DAO (DAO Maker)* – DAO, digitální kryptografická měna
35) *HIVE (Hive)* – HIVE, digitální kryptografická měna
36) *SXP (Solar)* – SXP, digitální kryptografická měna
37) *RON (Ronin)* – RON, digitální kryptografická měna
38) *PLA (PlayDapp)* – PLA, digitální kryptografická měna
39) *BTRST (Braintrust)* – BTRST, digitální kryptografická měna
40) *RON (Ronin)* – RON, digitální kryptografická měna
41) *RON (Ronin)* – RON, digitální kryptografická měna
42) *FTC (Federal Trade Commission)* – FTC, federální obchodní komise situovaná ve Spojených státech amerických