

Analýza typů kryptoměnových burz a jejich různých funkcí a využití

Marek Lehar

Bakalářská práce
2024



Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav podnikové ekonomiky

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Marek Lehar**
Osobní číslo: **M21241**
Studijní program: **B0413A050024 Ekonomika a management**
Specializace: **Ekonomika a management podniku**
Forma studia: **Prezenční**
Téma práce: **Analýza typů kryptoměnových burz a jejich různých funkcí a využití**

Zásady pro vypracování

Úvod

Definujte cíle práce a použité metody zpracování práce.

I. Teoretická část

- Proveďte literární rešerši zdrojů k dané problematice kryptoměnových burz.

II. Praktická část

- Proveďte analýzu typů burz CEX a DEX a jejich fungování.
- Proveďte rozdílovou analýzu obchodování přes CEX a DEX.
- Proveďte zhodnocení analýzy a porovnání obou typů burz.

Závěr

Rozsah bakalářské práce: **cca 40 stran**
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

DRESCHER, Daniel. *Blockchain basics: a non-technical introduction in 25 steps*. Berkeley, California: Apress, 2017. ISBN 1484226038.
FANG, Lucius; HOR, Benjamin; AZMI, Erina a WIN WIN, Khor. *How to DeFi (Advanced)*. Independently published, 2021. ISBN 979-8530318443.
LAU, Darren et al. *How to DeFi (Beginner)*. 2nd ed. Independently published, 2021. ISBN 979-8530408434.
NARAYANAN, Arvind; BONNEAU, Joseph; EDWARD, Felten; MILLER, Andrew a GOLDFEDER, Steven. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, 2016. ISBN 978-0-691-17169-2.
TAPSCOTT, Don a TAPSCOTT, Alex. *Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world*. London: Portfolio/Penguin, 2018. ISBN 978-0-241-23786-1.

Vedoucí bakalářské práce: **Ing. Martin Jančík**

Datum zadání bakalářské práce: **5. února 2024**
Termín odevzdání bakalářské práce: **17. května 2024**

L.S.

prof. Ing. David Tuček, Ph.D.
děkan

doc. Ing. Petr Novák, Ph.D.
garant studijního programu

Ve Zlíně dne 5. února 2024

**PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ/DIPLOMOVÉ PRÁCE**

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně

Jméno a příjmení:

.....
podpis diplomanta

ABSTRAKT

Cílem této bakalářské práce je provedení analýzy a následného porovnání typů kryptoměnových burz z hlediska jejich funkčnosti a využití. Práce je rozčleněna do dvou částí, a to do části teoretické a části praktické. Teoretická část se věnuje literární rešerši a uvedením čtenáře do problematiky kryptoaktiv, tradičního modelu burz a přiblížení do oblasti kryptoměnových burz. Praktická část bakalářské práce se zabývá analýzou typů kryptoměnových burz včetně principů fungování a možnostmi obchodování s následnou komparací typů kryptoměnových burz.

Klíčová slova: Kryptoaktiva, burza, digitální aktivum, kryptoměnová burza, CEX, DEX, porovnání

ABSTRACT

The aim of this bachelor thesis is to analyse and then compare the types of cryptocurrency exchanges in terms of their functionality and use. The thesis is divided into two parts, namely a theoretical part and a practical part. The theoretical part is devoted to a literature research and introducing the reader to cryptoassets, the traditional model of exchanges and an introduction to the field of cryptocurrency exchanges. The practical part of the bachelor's thesis deals with the analysis of types of cryptocurrency exchanges, including the principles of functioning and trading possibilities, followed by a comparison of types of cryptocurrency exchanges.

Keywords: Cryptoasset, exchange, digital asset, cryptocurrency exchange, CEX, DEX, comparison

Tímto bych chtěl poděkovat mému vedoucímu Ing. Martinovi Jančíkovi za odborné vedení mé bakalářské práce. Jeho poznatky a rady v průběhu psaní práce byly velmi užitečné a nápomocné.

Dále bych chtěl poděkovat své rodině, která při mne vždy stojí a za každé situace mne vždy podporuje.

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

OBSAH

ÚVOD	9
CÍLE A METODY ZPRACOVÁNÍ PRÁCE	10
I TEORETICKÁ ČÁST	11
1 KRYPTOAKTIVA	12
1.1 DEFINICE KRYPTOAKTIV.....	12
1.1.1 Typy kryptoaktiv.....	12
1.1.2 Výhody a nevýhody kryptoaktiv.....	13
1.2 BLOCKCHAIN.....	13
1.2.1 Fork.....	13
1.2.2 Hash.....	14
1.2.3 Transakce.....	14
1.2.4 Kryptoměnové peněženky.....	14
1.3 BITCOIN.....	16
1.3.1 Těžba bitcoinů.....	16
1.4 ALTCOINY.....	17
1.4.1 Digital assets.....	17
2 BURZA	19
2.1 HISTORIE BURZY.....	19
2.2 FUNGOVÁNÍ BURZY.....	19
2.3 FUNKCE BURZY.....	19
2.3.1 Obchodní funkce.....	19
2.3.2 Cenotvorná funkce.....	20
2.3.3 Alokační funkce.....	20
2.3.4 Funkce spekulace.....	20
3 KRYPTOMĚNOVÉ BURZY	21
3.2 TYPY KRYPTOMĚNOVÝCH BURZ.....	21
3.2.1 Centralizovaná kryptoměnová burza (CEX).....	21
3.2.2 Decentralizovaná kryptoměnová burza (DEX).....	22
3.3 FUNKCE KRYPTOMĚNOVÝCH BURZ.....	24
3.3.1 Funkce centralizované kryptoměnové burzy.....	24
3.3.2 Funkce decentralizované kryptoměnové burzy.....	25
3.4 TYPY PŘÍKAZŮ.....	25
3.4.1 Market order.....	25
3.4.2 Limit order.....	26
3.4.3 Buy stop a Sell stop.....	26
3.4.4 SWAP.....	27
3.4.5 Take profit.....	27
3.4.6 Modifikované objednávky.....	28

II PRAKTICKÁ ČÁST.....	29
4 PRŮBĚH FUNGOVÁNÍ A OBCHODOVÁNÍ NA CEX	30
4.1 PRŮBĚH FUNGOVÁNÍ NA CEX	30
4.1.1 Registrace na CEX	30
4.2 BEZPEČNOST CEX	32
4.3 FUNGOVÁNÍ ORDER BOOKU NA CEX.....	33
4.3.1 Výhody order booku	33
4.3.2 Nevýhody order booku.....	33
4.4 PRŮBĚH OBCHODOVÁNÍ NA CEX	35
4.5 TRANSAKČNÍ POPLATKY CEX.....	38
5 PRŮBĚH FUNGOVÁNÍ A OBCHODOVÁNÍ NA DEX	40
5.1 PRŮBĚH FUNGOVÁNÍ NA DEX.....	40
5.2 BEZPEČNOST DEX	41
5.3 FUNGOVÁNÍ AMM NA DEX	42
5.3.1 Výhody AMM.....	42
5.3.2 Nevýhody AMM	42
5.4 PRŮBĚH OBCHODOVÁNÍ NA DEX	43
5.5 POSKYTOVÁNÍ LIKVIDITY	46
6 ZHODNOCENÍ ANALÝZY	48
6.1 POROVNÁNÍ FUNGOVÁNÍ CEX A DEX	48
6.2 POROVNÁNÍ BEZPEČNOSTI CEX A DEX	48
6.3 POROVNÁNÍ ORDER BOOKU A PROTOKOLU AMM	49
6.4 POROVNÁNÍ OBCHODOVÁNÍ CEX A DEX.....	49
6.5 POROVNÁNÍ TRANSAKČNÍCH POPLATKŮ CEX A DEX.....	50
ZÁVĚR	52
SEZNAM POUŽITÉ LITERATURY.....	53
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	59
SEZNAM OBRÁZKŮ	60
SEZNAM TABULEK.....	61
SEZNAM PŘÍLOH.....	62

ÚVOD

Kryptoaktiva jsou v posledním desetiletí v hledáčku nadšenců nových technologií a příznivců, kteří s nimi operují. Zásadní roli zde hrají kryptoměnové burzy, které umožňují uživatelům nakupovat, prodávat a obchodovat s těmito digitálními aktivy po celém světě. Postupný vývoj krypto ekosystému vedl k výraznému rozšíření kryptoaktivního trhu, který přinesl do světa financí nové obchodní příležitosti.

Tato bakalářská práce se zabývá tematikou různých typů kryptoměnových burz, a to v části teoretické a části praktické. Cílem této bakalářské práce je analyzovat způsoby, jakými tyto typy kryptoměnových burz fungují, jaké služby nabízejí a v neposlední řadě, jak se mezi sebou odlišují.

V teoretické části se tato bakalářská práce z počátku zaměřuje uvedením čtenáře do světa kryptoaktiv, kde jsou rozebrány klíčové aspekty od samotné definice, principu fungování až po finální členění. Další oblastí, kterou se tato bakalářská práce zabývá je tematika tradičních burz jako takových, která má za úkol čtenáři nastínit problematiku burz z hlediska historie, fungování a funkcí, kterými disponují. Klíčovou částí obsaženou v teoretické části této práce, je nastínění problematiky kryptoměnových burz, která zahrnuje jejich stručné rozdělení, funkce, které nabízejí a možnosti typů obchodních příkazů, které lze aplikovat právě na těchto typech kryptoměnových burz.

Praktická část zahrnuje komplexní pohled na centralizované a decentralizované kryptoměnové burzy, která analyzuje jejich principy fungování a obchodování na nich. První část praktické části se věnuje centralizovaným kryptoměnovým burzám, kde je vysvětleno, co je třeba učinit pro participaci obchodování na tomto typu kryptoměnové burzy a také jakými způsoby a dle jakých mechanismů uživatelé na centralizované kryptoměnové burze fungují a obchodují. Dále se praktická část zabývá analýzou fungování a obchodování na decentralizovaných kryptoměnových burzách, kde je taktéž podrobně vysvětleno, jak se uživatelé mohou podílet na fungování a obchodování na tomto typu kryptoměnové burzy.

V neposlední řadě se praktická část věnuje zhodnocením analýzy, ve které je podáno ucelené porovnání jednotlivých aspektů fungování a obchodování na centralizovaných a decentralizovaných kryptoměnových burzách.

CÍLE A METODY ZPRACOVÁNÍ PRÁCE

Cílem této bakalářské práce je analýza a následné porovnání typů kryptoměnových burz v kontextu jejich fungování a možností obchodování.

Teoretická část bakalářské práce je zpracována dle literární rešerše, která přibližuje a popisuje problematiku, která je stěžejním prvkem pro část praktickou.

Praktická část je rozdělena do dvou částí, a to do části analyzování a části zhodnocení, která se věnuje porovnání analyzované problematiky. Práce si klade za cíl zjistit princip fungování na typech kryptoměnových burz společně s jejich možnostmi využití a obchodování, které se na nich uskutečňuje.

Analýza zahrnuje prvky literární rešerše spojené s praktickým vyzkoušením.

I. TEORETICKÁ ČÁST

1 KRYPTOAKTIVA

První kapitola se zabývá definicí základních pojmů kryptoaktiv, blockchainu, Bitcoinu a altcoinů.

1.1 Definice kryptoaktiv

Kryptoaktiva představují digitální či virtuální platidlo postavené na kryptografických systémech, umožňující bezpečné online transakce bez nutnosti participace třetích stran. Termín kryptoměna zahrnuje různé šifrovací algoritmy a kryptografické postupy, jako je například šifrování eliptickou křivkou, používání veřejných a soukromých klíčů a aplikace hashovacích funkcí, které slouží k zabezpečení těchto digitálních záznamů (Frankenfield, 2023).

Kryptoaktiva potřebují kryptografické zabezpečení, které brání manipulaci s jejich systémem a vzniku nekonzistentních prohlášení pro různé uživatele. Oproti běžným fiat měnám (měny s nuceným oběhem) jsou bezpečnostní pravidla kryptoměn uplatňována čistě technologicky, nezávisle na centrální autoritě (Narayanan et al. 2016).

Kryptoaktiva přináší zásadní inovace převážně v technologickém průmyslu, zejména v oblasti platebních metod a kybernetické bezpečnosti, která zajišťuje bezpečné a efektivní transakce (Sehgal, ©2024).

1.1.1 Typy kryptoaktiv

Kryptoaktiva lze rozdělit do 3 základních typů, kterými jsou asset-referenced token (token vázaný na aktiva), electronic money token (elektronický peněžení token) a utility token (užitný token). Asset-referenced token lze chápat jako typ kryptoaktiva, který ve skutečnosti není tokenem elektronických peněz, ale jeho hodnota je udržována pomocí odkazu na jinou hodnotu, právo nebo jejich kombinaci zahrnující jednu nebo více národních měn daných zemí. Dalším typem kryptoaktiva je electronic money token, který představuje typ platebního elektronického prostředku, jehož cíl je udržovat stabilní hodnotu vůči hodnotě fiat měny dané země. Třetím typem kryptoaktiv je utility token, který již z jeho názvu není užíván jako platidlo či udržitel hodnoty, ale jako prostředek digitálního přístupu ke zboží nebo službám (Tomczak, 2022).

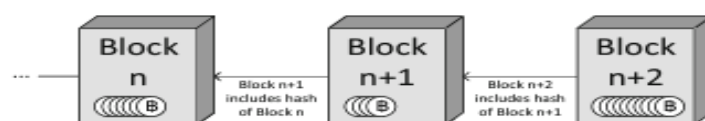
1.1.2 Výhody a nevýhody kryptoaktiv

Klíčová výhoda kryptoaktiv spočívá v jejich decentralizaci, kde kryptoaktiva nejsou řízeny žádnou centrální autoritou či jinou vyšší mocí. Další výhodou kryptoaktiv je jejich dostupnost, která spočívá v tom, že investorům či obchodníkům kryptoaktiv stačí pouze počítač nebo mobilní telefon s připojením na internet, aby mohli manipulovat se svými kryptoaktivy. Na druhou stranu za nevýhodu kryptoaktiv lze označit nezvratitelnost transakce kryptoaktiv, kdy při provádění transakce dojde k zadání špatné či neúplné adresy příjemce kryptoaktiv. Jako nevýhodu kryptoaktiv lze také označit jejich vysoká volatilita, kdy se ceny mění z minuty na minutu (Investopedia, 2023).

1.2 Blockchain

Blockchain reprezentuje řetězec bloků, který funguje jako veřejná účetní kniha obsahující úplné záznamy o transakcích. Tento systém zachycuje pořadí, v němž transakce proběhly. Každý blok v tomto řetězci potvrzuje integritu předchozího bloku až k počátečnímu bloku, označovanému jako blok geneze (genesis block). Rozvětvením řetězce není možné jakékoliv straně nahradit nebo upravit předchozí záznamy (Bhaskar, Chuen, 2015).

V blockchainu může být účastníkům nabídnut určitý stupeň osobní anonymity, což znamená, že není vyžadováno připojení dalších osobních údajů k jejich identitě ani jejich ukládání do centrální databáze (Tapscott a Tapscott, 2018).



Obrázek 1. Příklad Blockchainu (Xu et al., ©2019).

1.2.1 Fork

Fork nastává v situaci, kdy je za stejný předchozí blok napojeno několik různých bloků. K této události dochází, když mezi dobou, kdy je blok vytěžen a jeho šířením do sítě dojde k vytěžení jiného bloku. Fork může také vzniknout v důsledku změny bitcoinového nebo též altcoinového protokolu. Pojem fork se též používá k označení odvětvení softwaru za účelem jeho nezávislého vývoje (Stroukal, 2021).

1.2.1.1 Soft a hard fork

V důsledku decentralizované povahy peer-to-peer sítě kryptoměn musí být veškeré aktualizace nebo změny schváleny všemi zapojenými uzly. K takovým změnám v kódu blockchainu dochází prostřednictvím chain forků, což v praxi znamená rozdělení sítě na dvě části, z nichž každá se řídí odlišnými sadami pravidel. Situaci, kdy došlo k takovému rozvětvení, označujeme jako událost soft fork, přičemž staré uzly si stále udržují možnost účastnit se sítě. Hard fork lze charakterizovat jako rozdvojení blockchainu, které se obvykle objevuje v důsledku nucené implementace podstatné změny v softwarovém kódu sítě. V důsledku této změny dochází k trvalému odlišení blockchainu na dva samostatné řetězce, kdy původní blockchain novou verzi neuznává (Lau et al., 2021).

1.2.2 Hash

K odhadu výstupu používají počítače kryptografický hash, dokud není dosaženo cílové hodnoty (specifikované v poli "bits" v záhlaví). Jediným způsobem, jak předpovědět výstup, je prostřednictvím náhodného odhadu. Blok, který je první vyřešen uzlem, je odeslán do sítě a přijímán jako další blok v řetězci (Bhaskar a Chuen 2015).

1.2.3 Transakce

Transakce jsou datovými jednotkami, které obsahují informace o transakci a časové razítko. Oba tyto prvky mohou být vyjádřeny jako počítačová čísla nebo řetězce. Řetězec bloků lze představit jako tabulku s třemi sloupci, kde každý řádek reprezentuje samostatnou transakci. V prvním sloupci je uloženo časové razítko transakce, ve druhém sloupci jsou obsaženy informace o transakci a ve třetím sloupci je uložen hash aktuální transakce spolu s jejími podrobnostmi a hash předchozí transakce (Di Pierro, 2017).

1.2.4 Kryptoměnové peněženky

Kryptoměnové peněženky bývají obvykle označovány jako softwarové nebo hardwarové. Softwarové peněženky představují softwarové programy, které lze stáhnout na počítač nebo mobilní telefon. Naopak hardwarové peněženky jsou fyzické trezory, které ukládají data kryptoaktiv na speciálně navržený pevný disk obsažený v zařízení (Suratkar et al., 2020).

1.2.4.1 Softwarové peněženky

Digitální kryptoměnové peněženky představují digitální softwarové aplikace, které jsou instalovány na pevný disk a mohou být využívány na stolním počítači, notebooku, chytrém telefonu nebo na jakémkoli jiném digitálním zařízení. Digitální peněženky bývají obvykle vystaveny riziku hackerských útoků, což vede většinu jednotlivců k používání více než jedné digitální peněženky pro přístup k jejich kryptoměnám a provádění transakcí (Barakat, 2022).

1.2.4.2 Hardwarové peněženky

Hardwarové kryptoměnové peněženky majitelům těchto peněženek zajišťují vyšší zabezpečení kryptoaktiv proti krádeži a neoprávněné manipulaci s nimi. Jsou to hardwarová zařízení, jako jsou USB nebo rukou držitelná zařízení. Tato zařízení disponují vlastním softwarem, který umožňuje jejich propojení s počítačem. Na hardwarových kryptoměnových peněženkách, nejsou kryptoaktiva fyzicky uložena, ale hardwarová peněženka slouží pouze jako uchovatel privátních klíčů nutných k provedení krypto transakce na blockchainu. Peněženku by uživatel měl uchovávat na bezpečném místě mimo jeho osobní počítač (Samer Barakat, 2022).



Obrázek 2. Hardwarová peněženka Ledger Nano X (Zdroj: Ledger.com, ©2024).

1.3 Bitcoin

Bitcoin představuje decentralizovanou elektronickou měnu a inovativní variantu elektronických peněz, kterou jednotlivci nebo počítače mohou vzájemně přenášet bez potřeby prostředníka, jako je například banka, na kterou by bylo nutné spoléhat. Tato měna není vydávána pod kontrolou jediné instituce či skupiny (Pritzker, 2020).

Bitcoin dominuje mezi kryptoaktivy v celosvětovém měřítku díky své tržní kapitalizaci. Byl uveden na trh v roce 2009 a jeho autorem je anonymní vývojář nebo skupina vývojářů známý pod jménem Satoshi Nakamoto, jehož nebo jejichž skutečná identita zůstává neznámá (Kokate, 2023).

1.3.1 Těžba bitcoinů

Během procesu těžby je hash bloku transakcí a souhrnných informací o předchozím bloku vypočítáván těžářem. Hodnota nonce (náhodné číslo, které se těžaři bitcoinů snaží najít, aby mohli vytěžit nový blok v blockchainu) je přiřazena bloku, a těžař náhodně volí hodnotu nonce tak, aby byl hash bloku menší než cílová hodnota, kterou je síť pravidelně přepočítávána. Náhodné pokusy o nalezení platného hashe, jsou nazývány proof-of-work (důkaz o vykonané práci). Tento proces vyžaduje výpočetní úsilí, které se měří v gigabajtech za sekundu (Gb/s). Čím většího výpočetního výkonu je těžářem dosaženo, tím většího podílu ze všech distribuovaných odměn je přiděleno tomuto těžaři (Küfeoğlu a Özkuran 2019).

1.3.1.1 Proof-of-work

Proof-of-work je matematický ekvivalent věrohodného házení kostkou. Je založen na asymetrických matematických problémech s řešením, které je obtížné vymyslet, ale snadné ověřit. Tento proces je realizován pomocí hashování. Funkce hashování přijímá náhodný textový vstup, ze kterého se generuje výstupní hash podle stanovených pravidel. Hashovací funkce, používána v protokolu Bitcoin, je známa jako SHA256. SHA256 splňuje takovou vlastnost, že z konkrétního výstupního hashe nelze odvodit vstup (Auer, 2019).

1.4 Altcoiny

Altcoiny (alternativní kryptoaktiva) se mohou odlišovat v různých aspektech, nicméně v základu všechny vycházejí z klíčové inovace, kterou představuje decentralizovaná veřejná účetní kniha Bitcoinu. V oblasti vytváření altcoinů dochází k inovacím v oblasti programovacích konceptů. Nové myšlenky, jako je implementace Turingova úplného programování na úrovni protokolu a chytrých smluv, představují změnu modelu ve způsobu uvažování o decentralizaci a digitálních penězích. Přestože implementace těchto funkcí do Bitcoinu může být obtížná, protože tato kryptoměna nebyla původně navržena pro tuto funkcionalitu, nová kategorie označovaná jako „Bitcoin 2.0“ byla vytvořena pro mince, jako je Ethereum, které se snaží těmto inovacím poskytnout prostor (Ong et al. 2015).

1.4.1 Digital assets

Digital assets (digitální aktiva) lze považovat aktiva, které splňují podmínku generující hodnoty pro svého vlastníka. Digitálním aktivem se rozumí vše, co je v digitální podobě a co generuje reálnou hodnotu. Za digitální aktiva lze označit již výše zmíněné kryptoaktiva, stablecoiny (kryptoaktivum, které bylo vytvořeno jako držitel cenové stability, které jsou spjaty s hodnotou fiat měny), NFT (token, který představuje digitální záznam o vlastnictví a pravosti), CBDC (digitální aktiva, které ztělesňují konkrétní měnu státu a jsou kryta centrální bankou daného státu) a security tokens (digitální aktiva, která představují digitální formu investic jako jsou cenné papíry či dluhopisy) (PRICEWATERHOUSECOOPERS, © 2024).

1.4.1.1 Ethereum

Ethereum představuje celosvětovou open-source platformu pro decentralizované aplikace. Ethereum lze chápat jako světový počítač, který nemá žádná omezení v jeho provozu. Vývojáři softwaru mají možnost vytvářet na této platformě smart contracty (chytré smlouvy), které řídí digitální hodnoty na základě předem stanovených podmínek a jsou dostupné kdekoli na světě (Lau et al., 2021).

1.4.1.2 ETH

ETH (Ether) v Ethereum ekosystému představuje vlastní kryptoměnu tohoto ekosystému, která funguje na ethereovém blockchainu. ETH není pouze jen prostředek směny nebo uchovatel hodnoty, ale funguje také i jako opatrovatel provádění smart contractů

a decentralizovaných aplikací, za které uživatelé těchto procesů musí platit poplatek v etherech nazývaný jako gas. Gas funguje jako mechanismus pro výpočet nákladů spojenými s těmito procesy (Bhatia a Tyagi 2021).

1.4.1.3 Smart contract

Smart contract (chytrá smlouva) může být definována jako programovatelná smlouva, jež umožňuje nastavit podmínky transakce mezi dvěma stranami bez potřeby důvěřovat další třetí straně při jejím provádění. Kdykoliv je splněna určitá podmínka, provádí chytrá smlouva operaci podle předem definovaného programování (Lau et al., 2021). Fungování smart contractu je založeno na blockchainu spojeném s automatizací (která eliminuje potřebu zásahu zprostředkovatelů při realizaci smluvních doložek), neměnnosti (po nasazení chytré smlouvy do blockchainu již chytrá smlouva nelze změnit, pouze ji lze smazat), autonomie (kde smart contract dokáže fungovat jako samo spustitelný program) a v neposlední řadě transparentnosti (kde smart contract je založen na veřejném blockchainu, a tak je viditelný všemi uživateli sítě) (Binance Academy, 2023).

1.4.1.4 Dapps

V rámci Etherea jsou Dapps definována jako rozhraní, které komunikují s blockchainem prostřednictvím chytrých smluv. Dapp je vizuálně a chováním podobný běžným webovým a mobilním aplikacím, s výjimkou toho, že interaguje s blockchainem a dalšími metodami. Některé z těchto postupů zahrnují vyžadování ETH pro používání Dapp, stejně jako ukládání uživatelských dat do blockchainu s cílem dosáhnout jejich neměnnosti (Lau et al., 2021).

Decentralizované aplikace jsou často charakterizovány jako aplikace bez nutnosti důvěřovat nebo jako peer-to-peer, přičemž vyznačujícím se prvkem je, že nejsou řízeny jediným serverem nebo subjektem, jak tomu bývá v modelu klient-server (Yano et al. 2020).

1.4.1.4.1.1 Peer-to-peer

Systémy peer-to-peer se skládají z jednotlivých počítačů uživatelů, kteří spolu komunikují přes síť. Všechny součásti hardwaru a softwaru počítačového systému, stejně jako všechny prvky počítačové sítě, mají nedomyslitelné riziko selhání nebo vzniku chyb (Drescher, 2017).

2 BURZA

Burzy cenných papírů a organizované mimoburzovní trhy mohou být popsány jako relativně autonomní ekonomické, organizační a technické systémy. Tyto systémy se skládají z různých dílčích subsystémů, které zajišťují širokou škálu činností, vzájemně však souvisejících (Rejnuš, 2014).

2.1 Historie burzy

Původ pojmu burza lze vysvětlit několika způsoby. Nejčastěji se odvozuje od jména patricijské rodiny Van der Boerse, která měla sídlo v Bruggách. Tato rodina hostila schůzky burzovních obchodníků ve svém domě. Termín burza, začal být používán v tomto smyslu v Bruggách kolem 15. století a odtud se rozšířil do Antverp a následně do celé Evropy (Veselá, 2019).

2.2 Fungování burzy

Obchodování na burze je striktně regulováno z časového hlediska. Burzovní dny jsou přesně stanoveny, tedy dny, kdy je povoleno obchodování, a to i v přesně daných hodinách, kdy lze uzavírat obchody nebo zadávat příkazy. Každá burza publikuje svůj kalendář nebo přehled burzovních dní, který poskytuje detailní informace o rozvržení burzovních dní v daném roce. Taktéž sděluje svůj harmonogram burzovního dne, obsahující přesný časový plán burzovního dne vzhledem k různým druhům prováděných obchodů a činností, které mohou účastníci v určité obchodní funkci vykonávat (Veselá, 2019).

2.3 Funkce burzy

2.3.1 Obchodní funkce

Obchodní funkce burzovního trhu zajišťuje, že určité instrumenty lze kdykoliv prodat za cenu, která vychází ze střetu nabídky a poptávky. Počet možných změn vlastnictví těchto instrumentů je neomezený. Likvidita investičních instrumentů je pro investory důležitá, protože snižuje náklady pro výstavce. Kdyby obchodovatelnost instrumentů nebyla zajištěna na burze, investoři by požadovali vyšší výnosy z jejich investic. Úroveň likvidity trhu lze posoudit na základě jeho vlastností, jako je šířka, pružnost, hloubka, důvěryhodnost a fair play (Veselá, 2019).

2.3.2 Cenotvorná funkce

Burza propojuje nabídku a poptávku po různých investičních nástrojích, což stanovuje aktuální ceny. Tyto ceny jsou důležité nejen pro investory, kteří hledají informace o výnosech, ale i pro ty, kteří zvažují nové investice. Cena je klíčovým ukazatelem atraktivity investice, zahrnující potenciální výnosy i náklady. Analytici a poradci sledují ceny, aby odhalili přeceněné či podhodnocené tituly nebo vhodné okamžiky, pro nákupy a prodeje. Emitenti také získávají důležité informace o cenách svých cenných papírů. Kromě toho makroekonomické subjekty a instituce, jako jsou centrální banky a vlády, využívají informace o cenách při formulaci politiky a shromažďování ekonomických dat pro různé účely (Veselá, 2019).

2.3.3 Alokační funkce

Alokační funkci plní burza v situaci, kdy organizuje primární i sekundární trh s investičními instrumenty. Nové cenné papíry jsou emitovány přes burzu, která přesouvá finanční prostředky od investorů k emitentům s ohledem na výnos, riziko a likviditu. Pro emitenty je důležitá cena a doba získání kapitálu (Veselá, 2019).

2.3.4 Funkce spekulace

Spekulace je činnost, která se zaměřuje na analýzu a odhad budoucích okolností ovlivňujících ceny investičních instrumentů. Je to náročná činnost z hlediska odbornosti, financí i psychiky. Spekulanti se dělí do dvou skupin, a to spekulanti „na býka“, kteří jsou optimističtí, nakupují a očekávají budoucí růst cen a spekulanti „na medvěda“, kteří prodávají a očekávají budoucí pokles cen (Veselá, 2019).

3 KRYPTOMĚNOVÉ BURZY

Tato část bakalářské práce se zaměřuje na definování kryptoměnové burzy, funkce kryptoměnových burz, typy kryptoměnových burz, rozdělení centralizovaných a decentralizovaných kryptoměnových burz.

3.1 Definice kryptoměnové burzy

Kryptoměnová burza představuje tržiště, kde jsou uživatelům dostupné možnosti nákupu a prodeje kryptoměn. Většina z těchto burz se specializuje pouze na služby obchodování mezi kryptoměnami, zatímco několik jich umožňuje obchodování mezi fiat měnami (například americkým dolarem nebo eurem) a kryptoaktivy. Podobně jako na tradičních burzách cenných papírů, i na kryptoměnových burzách se lidé obrací s cílem investovat a využít tak výhod z výkyvů cen kryptoměn. Existují tři hlavní typy kryptoměnových burz: centralizované burzy (CEX), které jsou provozovány společnostmi nebo organizacemi, decentralizované burzy (DEX), které nabízejí automatizovaný proces pro peer-to-peer obchody, a hybridní burzy, které kombinují obě uvedené formy (Xia et al., 2020).

3.2 Typy kryptoměnových burz

3.2.1 Centralizovaná kryptoměnová burza (CEX)

Pod pojmem centralizovaná kryptoměnová burza se rozumí využití zprostředkovatele nebo třetí strany, která pomáhá s prováděním transakcí. Tento model je podobný bankovnímu uspořádání, kdy zákazník důvěřuje bance, že bude spravovat jeho peníze. Důvodem tohoto uspořádání je, že banky nabízejí bezpečnost a dohled, který jednotlivec sám nemůže zajistit. Stejný princip platí i pro centralizované kryptoměnové burzy. Uživatelé důvěřují, že burza bezpečně exekuuje jejich transakce a využívá síť uživatelů k nalezení obchodních partnerů (Reiff, 2023).

Centralizované kryptoměnové burzy vyžadují předložení úředních dokladů k ověření totožnosti. Důvodem je skutečnost, že centralizované kryptoměnové burzy jsou obchodními subjekty, a proto podléhají místním zákonům. To znamená, že při používání těchto burz není zachováno vaše soukromí, neboť jste nuceni sdílet své citlivé informace s centralizovanými subjekty (Roy, 2023).

Konkrétní typy centralizovaných kryptoměnových burz:

- **Coinbase** je významnou centralizovanou kryptoměnovou burzou a platformou, která umožňuje uživatelům nakupovat, prodávat a obchodovat s různými druhy kryptoměn. Slouží jako spojovací článek mezi tradičními finančními systémy a digitálním světem aktiv a nabízí jednoduché uživatelské rozhraní pro přístup, správu a provádění transakcí s kryptoměnami (Legge, 2023).
- **Kraken** je centralizovaná kryptoměnová burza se sídlem v San Franciscu, kde mají účastníci trhu možnost obchodovat s různými kryptoměnami. Účastníci mohou nakupovat nebo prodávat kryptoaktiva za různé fiat měny, včetně amerických dolarů, kanadských dolarů, eur a japonských jenů. Burza usnadňuje převod peněz mezi bankovními účty účastníků a digitálními peněženkami, stejně jako přesun kryptoměn mezi digitálními peněženkami a obchodními účty propojenými s kryptoměnovou burzou Kraken (Seth, 2023).
- **Binance** je centralizovaná kryptoměnová burza, na níž mají uživatelé možnost nakupovat, prodávat a obchodovat s rozmanitými kryptoaktivy, jako je bitcoin, ether a mnoho dalších altcoinů. Binance nabízí snadno použitelnou obchodní platformu, nízké poplatky a širokou škálu funkcí, včetně obchodování s marží a sázek. Binance Coin (BNB), vlastní kryptoměna burzy Binance, je možné použít k placení obchodních poplatků a jiných služeb na platformě (Khan, 2023).

3.2.2 Decentralizovaná kryptoměnová burza (DEX)

Decentralizovaná burza se obvykle používá pro označení směnných protokolů založených na blockchainu a aplikací, které tyto protokoly využívají. Koncept decentralizovaného směnného protokolu zahrnuje software umístěný na jednom či více distribuovaných účetních knihách, jako je například Ethereum, nebo do něj integrované. Tento software umožňuje peer-to-peer transakce, které jsou automaticky zaznamenávány v distribuované účetní knize. Uživatelé si zachovávají plnou kontrolu nad svými soukromými klíči po celou dobu transakčního procesu (Lin a Foundation, 2019).

3.2.2.1 *Order book*

Order book představuje seznam příkazů k nákupu a prodeji specifického aktiva na různých cenových úrovních. Decentralizované burzy založené na knize objednávek, jako jsou dYdX,

DeversiFi a Loopring, pracují podobně jako centralizované burzy, kde uživatelé mohou zadávat nákupní a prodejní příkazy za zvolené limitní ceny nebo za tržní ceny. Decentralizované burzy, které jsou založené na knize objednávek on-chain, mají všechny příkazy zaznamenané v blockchainu. Decentralizované burzy, které využívají off-chain order book, mají obchodní příkazy zaznamenané mimo blockchain (Fang et al., 2021).

3.2.2.2 Automated market makers (AMMs)

Automated market makers (automatizovaní tvůrci trhu) umožňují obchodování s kryptoaktivy bez nutnosti povolení a automaticky prostřednictvím skupin likvidity místo tradičního modelu trhu mezi kupujícími a prodávajícími. Na konvenční burzovní platformě kupující a prodávající stanovují různé ceny pro dané aktivum. Jakmile ostatní obchodníci najdou uvedenou cenu jako akceptovatelnou, obchod proběhne a tato cena se stane tržní cenou aktiv. AMM představují finanční nástroj jedinečný pro Ethereum a decentralizované finance (DeFi). Tato inovativní technologie je decentralizovaná, neustále dostupná pro obchodování a nezávislá na tradiční interakci mezi kupujícími a prodávajícími. Tento nový způsob výměny aktiv reflektuje ideály Etherea, kryptoaktiv a technologie blockchain obecně tak, že žádný jednotlivý subjekt neovládá systém, a kdokoli může přispívat k vytváření nových řešení a podílet se na nich (Cryptopedia Staff, 2023).

3.2.2.3 Liquidity pool

Liquidity pool (pool likvidity) představuje rezervy tokenů, které jsou umístěny ve smart kontraktech decentralizovaných kryptoměnových burz a jsou uživatelům k dispozici pro výměnu tokenů. Většina decentralizovaných kryptoměnových burz, které umožňují možnost poskytovat likviditu do poolů likvidity, využívají automatizované tvůrce trhu (AMM), což je matematická funkce, jež algoritmicky předdefinovává ceny kryptoaktiv. AMM je považována za jedno z nejnovějších vylepšení v oblasti DeFi. Toto řešení umožňuje nepřetržitý provoz trhu, vyšší dostupnost kapitálu a efektivitu (Fang et al., 2021).

Konkrétní typy decentralizovaných kryptoměnových burz:

- **Uniswap** je považován za nejoblíbenější decentralizovanou burzu (DEX). Příkladem jsou obchody mezi BTC a ETH jako ilustrativní příklad. Uniswap poskytuje smart contract (chytrou smlouvu) s uzamčenými prostředky pro obě tyto kryptoaktiva. Když obchodník plánuje směnit ETH za BTC, postačí, když své ETH odešle do chytré smlouvy. Následně chytrou smlouvou okamžitě posílá obchodníkovi odpovídající množství BTC, zatímco odeslané ETH jsou uzamčeny v rámci této chytré smlouvy. Směnný kurz je v podstatě stanoven poměrem BTC a ETH uložených v chytré smlouvě. BTC a ETH v chytré smlouvě zajišťují likviditu pro obchody mezi BTC a ETH na Uniswapu (Heimbach et al. 2021).
- **Pancakeswap** je decentralizovaná burza, která je postavena na Binance Smart Chain (BSC). Pancakeswap rovněž poskytuje služby automatického obchodování a podporuje limitní pokyny pro obchodování. Umožňuje ukládání tokenů, které jsou následně zpracovávány pomocí automatických obchodních robotů (MCOINS, 2023).
- **QuickSwap** je odnoží Uniswapu, neboť využívá stejný model fondu likvidity. Vznikl jako rychlá, cenově dostupná a kompatibilní alternativa k Uniswapu pro Ethereum. Hlavním rozdílem je, že QuickSwap je založen na Polygonu, zatímco Uniswap na Ethereum. Tím pádem uživatelé QuickSwapu mohou využívat bezpečnostních výhod auditovaného kódu Uniswapu a zároveň profitovat z vysokorychlostních transakcí a téměř nulových poplatků, které síť Polygon nabízí (Singh, 2023).

3.3 Funkce kryptoměnových burz

3.3.1 Funkce centralizované kryptoměnové burzy

Na centralizovaných burzách je možné nakupovat a prodávat kryptoaktiva několika způsoby. Může být využit tržní příkaz, který umožňuje okamžitý nákup nebo prodej kryptoaktiv za tržní cenu. Alternativně je možné zadat limitní příkaz, který umožňuje stanovit konkrétní cenovou hladinu, za kterou je kryptoaktivum kupováno nebo prodáváno. Jakmile cena aktiva dosáhne požadované úrovně, provede se příkaz. Některé burzy poskytují speciální obchodní platformy pro profesionální obchodníky s rozšířenými funkcemi, jako je obchodování s marží. Kromě toho nabízejí burzy digitální peněženky pro ukládání kryptoaktiv.

Uložením kryptoaktiv na burze však svěřujete burze své soukromé klíče a spoléháte na ni v oblasti zabezpečení svých prostředků. Některé burzy poskytují také služby úschovy pro finanční instituce a investiční společnosti, které investují do kryptoaktiv, ale nechtějí spravovat vlastní soukromé klíče (Cryptopedia Staff, 2021).

3.3.2 Funkce decentralizované kryptoměnové burzy

Uživatelé decentralizovaných kryptoměnových burz mohou přímo obchodovat ze svých peněženek, komunikovat s chytrými smlouvami obchodní platformy a udržovat plnou kontrolu nad svými prostředky. Dalším klíčovým prvkem decentralizovaných burz (DEXů) je využití poolů likvidity, což jsou předem financované fondy aktiv, které usnadňují obchodování. Tato financování, která poskytují uživatelé známí jako poskytovatelé likvidity, řeší problémy spojené s nedostatkem likvidity a umožňují uživatelům provádět obchody bez nutnosti povolení či důvěry. Poskytovatelé likvidity získávají transakční poplatky za obchody provedené s použitím jejich financovaných párů, což je motivuje k tomu, aby přispívali k likviditě platformy (Crooks, 2023).

3.4 Typy příkazů

Tato část bakalářské práce se zabývá vysvětlením tržních (market order) a limitních (limit order) objednávek, přes které se na (nejen) kryptoměnových burzách zadávají příkazy pro obchodování. Pro každou market objednávku musí existovat limitní objednávka, nelze tedy spárovat dvě limitní objednávky nebo dvě market objednávky. Například pro nákupní (buy market) objednávku musí existovat protistrana v podobě prodejní (sell limit) objednávky. Tímto způsobem dochází k párování burzovních objednávek a všechny ostatní tržní příkazy jsou pouze jiným pojmenováním nebo modifikací market a limit objednávek.

3.4.1 Market order

Princip příkazu market order je nákup či prodej kryptoaktiv za nejlepší dostupnou aktuální tržní cenu na zvoleném trhu. Market objednávka je obchodníkem zadána a broker garantuje její exekuci (plnění), avšak negarantuje vyplnění za aktuální tržní cenu. Tržní příkazy bývají vykonávány (téměř) okamžitě a obchodníky jsou využívány tehdy, když potřebují kryptoměnu rychle nakoupit či rychle prodat. U tržních příkazů se obchod provádí za nejlepší dostupnou cenu v knihách objednávek (order book), které představují limitní objednávky (Pyromallis a Szabo, 2019).

3.4.2 Limit order

Princip příkazu limit order je umístění nákupní objednávky (buy limit) pod aktuální tržní cenu nebo prodejní objednávky (sell limit) nad aktuální tržní cenu. Pokud je limitní objednávka obchodníkem umístěna do trhu, je tato objednávka viditelná v knize objednávek, čímž se zvyšuje likvidita obchodovaného instrumentu na zvolené tržní ceně. Limitní objednávka je obchodníkem do trhu zadána a broker garantuje její případné vyplnění za obchodníkem stanovenou nebo lepší cenu, avšak negarantuje, že objednávka bude skutečně vyplněna (Santosa, 2022). Limitní nákupní příkaz může být uskutečněn pouze v případě dosažení nebo překročení limitní hodnoty, zatímco limitní prodejní příkaz může být realizován pouze při dosažení limitní ceny nebo vyšší (Li et al., 2022).

3.4.3 Buy stop a Sell stop

3.4.3.1 Buy stop

Buy stop je typem tržního příkazu, který je umístěn obchodníkem do trhu nad aktuální tržní cenu obchodovaného instrumentu. Pokud tržní cena dosáhne tržní ceny stanovené obchodníkem, je buy stop objednávka exekuvována jako buy market objednávka a obchodník po její exekuci vstupuje do nákupní pozice (long). Buy market objednávka je pouze simulovaná objednávka v obchodníkově platformě, to znamená, že není viditelná ostatními účastníky trhu, jelikož není zobrazena v knize objednávek (nejedná se tedy o limitní objednávku) (Ushman, 2023).

3.4.3.2 Sell stop

Sell stop je typem tržního příkazu, který je umístěn obchodníkem do trhu pod aktuální tržní cenu obchodovaného instrumentu. Pokud tržní cena dosáhne tržní ceny stanovené obchodníkem, sell stop objednávka je exekuvována jako sell market objednávka a obchodník po její exekuci vstupuje do prodejní pozice (short). Sell market objednávka je pouze simulovaná objednávka v obchodníkově platformě, to znamená, že není viditelná ostatními účastníky trhu, jelikož není zobrazena v knize objednávek (nejedná se tedy o limitní objednávku) (Maverick, 2022).

3.4.4 SWAP

Krypto swap je proces, při kterém se kryptoaktivum pohodlně vyměňuje za stejnou hodnotu v jiném tokenu nebo minci. Nižší transakční náklady a rychlejší transakce jsou dva hlavní důvody, proč se uživatelé kryptoměnových burz rozhodují pro tento postup. Obvykle se swapy vztahují k okamžitým transakcím, což znamená, že uživatelé kryptoaktiv obvykle provádějí swapy okamžitě. Výhodou krypto swapu je uživatelům kryptoaktiv rozšířit jejich portfolio tím, že jednoduše vyměňují jeden krypto token za druhý. Tímto způsobem mají uživatelé kontrolu nad rizikem, kterému jsou vystaveni, a mohou co nejlépe využít investiční příležitosti na trhu. Na druhou stranu nevýhodou krypto swapu je obava ohledně ochrany soukromí, protože výměny jsou veřejné. Jednotlivci by mohli být postiženi ztrátou svých kryptoaktiv v případě jakéhokoli problému s protokolem, který zprostředkovává výměnu (Ahmed, 2023).

3.4.5 Take profit

Základní nastavení příkazu take profit (výběr zisku) pro ukončení pozice v zisku je umístění limitní objednávky na obchodníkem stanovenou tržní cenu obchodovaného instrumentu. Pod pojmem take profit se myslí vyplnění limitní objednávky sell limit v případě nákupní pozice (long) a buy limit v případě prodejní pozice (short). Take profit je pouze jiné pojmenování pro limitní objednávku využívanou k ukončení pozice v případě zisku na předem stanovené cenové hladině, jelikož burzovní prostředí pojem take profit nezná. Dalším způsobem, jak může obchodník ukončit pozici v zisku je použití objednávky MIT (market if touched), což je předem stanovená cenová hladina, kterou když daný trh dosáhne, je tato objednávka exekuvována jako market objednávka. V případě long pozice je pro take profit v případě použití MIT použita objednávka sell market a v případě short pozice je pro take profit v případě použití MIT použita objednávka buy market. Narozdíl od limitních objednávek není objednávka MIT viditelná v knize objednávek (order book) a je pouze simulována v obchodníkově platformě. Posledním způsobem jak pozici v zisku ukončit je její okamžitá likvidace pomocí market order a to okamžitě za nejlepší dostupnou tržní cenu (Chen, 2021).

3.4.6 Modifikované objednávky

Krom výše zmíněných základních typů burzovních příkazů, se lze setkat i s takzvanými modifikovanými objednávkami. Tyto objednávky jsou často kombinací výše zmíněných objednávek, případně se jedná o jejich časovou duraci nebo speciální typy příkazů hojně využívanými obchodníky s velmi vysokým kapitálem, kteří z nějakého důvodu nechtějí být ostatními účastníky trhu detekováni. Mezi tyto objednávky patří například objednávka stop limit, kdy obchodník určí stop cenu (cena, při které se obchodníkovi exekuuje market objednávka) a limitní cena (určena vzdáleností v pipech nebo dolarech od stop ceny). Limitní cena představuje cenové rozpětí, ve kterém tato market objednávka může být vyplněna. Výhodou této modifikované objednávky je, že obchodníkovi garantuje vstup nebo výstup z pozice v předem stanoveném cenovém rozpětí a omezuje negativní dopad případného skluzu v plnění (slippage). Nevýhodou této modifikované objednávky je, že pakliže v případě náhlého a prudkého poklesu likvidity nemusí být obchodník schopen vstoupit do pozice nebo ukončit pozici v předem stanoveném cenovém rozpětí a do pozice nevstoupí vůbec nebo jen částečně, a to samé platí pro výstup z pozice (Eurex, ©2024).

Dalším příkladem modifikované objednávky je časové ohraničení platnosti limitních objednávek – objednávka typu good till cancelled je platná, dokud obchodník tuto objednávku nezruší nebo dokud není trhem vyplněna, objednávka typu good till day je platná do konce obchodní seance stanovené burzou nebo dokud není objednávka trhem vyplněna v rámci aktuální obchodní seance (Eurex, ©2024).

Existují i další modifikace objednávek nebo speciální objednávky jako hidden orders a iceberg orders, ale jejich využití a definice je nad rámec této kapitoly.

II. PRAKTICKÁ ČÁST

4 PRŮBĚH FUNGOVÁNÍ A OBCHODOVÁNÍ NA CEX

Tato část bakalářské práce se zaměřuje na postupové kroky registrace, fungování a obchodování na centralizované kryptoměnové burze. Konkrétní centralizovanou kryptoměnovou burzou pro ukázkou, bude použita centralizovaná kryptoměnová burza Coinbase.

4.1 Průběh fungování na CEX

4.1.1 Registrace na CEX

Pro fungování na centralizované kryptoměnové burze Coinbase, je nutné dovršit věku 18 let a podstoupit kroky registrace zahrnující i KYC (know your customer), díky kterému si centralizovaná kryptoměnová burza ověřuje totožnost uživatele centralizované kryptoměnové burzy. Samotný proces KYC bude popsán v kapitole níže.

Prvním krokem registrace na centralizovanou kryptoměnovou burzu je zadání svého jména, příjmení společně se svou soukromou emailovou adresou a vytvořením svého privátního hesla, přes které se uživatel přihlašuje na platformu.

Druhým krokem je ověření své emailové adresy, kdy Coinbase zašle ověřovací email, na který uživatel klikne, a tím může pokračovat dále v registraci na centralizovanou kryptoměnovou burzu. Jakmile je emailová adresa uživatelem ověřena, Coinbase nabídne 2 možnosti kryptoměnového burzovního účtu, a to osobní nebo podnikatelský.

Třetím krokem registrace na centralizovanou kryptoměnovou burzu Coinbase, je vybrání státu, ve kterém má uživatel svou státní příslušnost a zadání telefonního čísla, přes které Coinbase zasílá ověřovací kódy jak při přihlašování do platformy, které je nutno ověřit i při samotné registraci, kdy centralizovaná kryptoměnová burza Coinbase zašle na telefonní číslo ověřovací kód, aby byla zjištěna skutečnost vlastnictví telefonního čísla. Coinbase vyžaduje po uživateli kryptoměnové burzy telefonní číslo i z důvodu ověřování transakcí s velkým objemem obchodovaného aktiva.

Čtvrtým krokem registrace na centralizovanou kryptoměnovou burzu je přidání platební metody, přes kterou uživatel operuje se svými prostředky právě na této burze. Zadání platební metody slouží pro zasílání a taktéž pro přijímání peněz. Coinbase nabízí 2 možnosti platebních metod a těmi jsou bankovní účet, který nabízí možnost přijímání SEPA (bezhotovostní převod prováděný v eurech) plateb nebo platební karty jako je Visa nebo Mastercard.

Při zvolení platební metody bankovní účet, je nutno podstoupit následující kroky. Prvním krokem je zadání názvu banky, u které má uživatel svůj osobní nebo podnikatelský účet. Druhým krokem je vypsání čísla účtu IBAN (mezinárodní číslo bankovního účtu) nebo BIC (podnikatelské identifikační číslo). Po zadání těchto kroků, Coinbase vyžaduje ověření bankovního účtu posláním symbolické platby 1-2 eur, která obvykle trvá 1-2 pracovní dny. Po uplynutí této lhůty ověření bankovního účtu, uživatel obdrží prostřednictvím emailu, že uživatelův účet byl úspěšně ověřen. Je důležité, aby uživatel při odesílání ověřovací platby si ověřil, že se jedná skutečně o účet, na který byl vyzván, aby poslal tuto symbolickou platbu.

Výhodou platební metody přes bankovní účet je možnost obchodování s větším obnosem peněz. Na druhou stranu nevýhoda spočívá v tom, že platby trvají obvykle 4-5 dnů. Výhodou platební metody přes platební kartu spočívá v okamžitých platbách, ovšem nevýhodou je možnost obchodování s menším obnosem peněz.

Pátým krokem a posledním krokem registrace na centralizovanou kryptoměnovou burzu Coinbase, je ověření identity a totožnosti uživatele. Tento proces nazývaný zkratkou KYC (poznaj svého zákazníka), je důležitým krokem, bez kterého není možné operovat na centralizované kryptoměnové burze. Na výběr jsou 3 typy možností ověření totožnosti uživatele a těmi jsou cestovní pas, řidičský průkaz nebo občanský průkaz. Tyto dokumenty lze naskenovat nebo vyfotit přes svůj mobilní telefon, kdy je zapotřebí naskenovat nebo vyfotit všechny strany zvoleného dokumentu, které centralizované kryptoměnové burzy vyžadují. Příkladem může být přední a zadní strana občanského průkazu.

4.1.1.1 *Proces KYC*

Proces KYC (poznání svého zákazníka) chrání poskytovatele centralizovaných kryptoměnových burz před podvody a jinými nezákonnými činnostmi jako je praní špinavých peněz. Proces KYC se skládá z několika kroků zahrnující sběr nezbytných informací o uživateli centralizované kryptoměnové burzy a těmi jsou již výše zmíněné naskenované nebo vyfocené dokumenty (občanský průkaz, cestovní pas, řidičský průkaz). Obvykle se do tohoto procesu zahrnují nejen tyto dokumenty, ale i pořízení fotografie či krátké video s obličejem uživatele, aby autority centralizovaných kryptoměnových burz, které operují s těmito doklady při ověřování totožnosti uživatele, mohli posoudit, jestli se skutečně jedná o pravou identitu uživatele. Cílem procesu KYC je zajistit, aby finanční instituce měla dostatečné a potřebné informace o uživateli, dle kterých lze posoudit veškerá rizika spojená s obchodním vztahem mezi uživatelem a finanční institucí.

4.2 **Bezpečnost CEX**

Centralizované kryptoměnové burzy disponují mnoha bezpečnostními opatřeními pro své uživatele, ale také i pro ně samotné. Klíčovým bezpečnostním prvkem centralizovaných burz je zabezpečení vlastnictví kryptoaktiv obchodníků, kdy centralizované kryptoměnové burzy zajišťují bezpečnou úschovu pomocí kombinace softwarových a hardwarových peněženek. Hardwarové peněženky, kterým se jinak také nazývá studené peněženky jsou zpravidla méně náchylné k hackerským útokům, protože jsou takzvaně offline. Pro ochranu účtů svých klientů centralizované kryptoměnové burzy vyžadují, aby uživatelé využívali 2FA (dvoufaktorové ověření), které zvyšuje zabezpečení burzovního účtu ověřením přihlášení do účtu. Ověření přihlášení může být provedeno několika způsoby jako zasláním sms zprávy na telefonní číslo, které uživatel má propojené s burzovním s ověřovacím kódem, emailové zprávy s ověřovacím kódem nebo například již výše zmíněná centralizovaná kryptoměnová burza Coinbase nabízí dvoufaktorové ověření pomocí potvrzení přihlášení v mobilní aplikaci, na které je uživatel přihlášen stejnými přihlašovacími údaji jako na počítači. Centralizované kryptoměnové burzy používají složité šifrovací techniky k zabezpečení uživatelských dat a transakcí, přes které zabraňují neoprávněnému přístupu k uživatelským údajům (například dokumenty zaslané platformě pro ověření identity), a tím zachovávají uživatelům soukromí. Bezpečnostní opatření,

keré je již zmíněno v kapitole KYC (poznej svého zákazníka), slouží ke zmírnění rizik vedoucí k nekalým praktikám, jako je praní špinavých peněz, financování terorismu nebo krádež identity uživatele.

4.3 Fungování order booku na CEX

Order book funguje na bázi zadávání tržních příkazů k nákupu či prodeji kryptoaktiva v reálném čase, kde dochází k párování právě těchto příkazů a odráží tak množství měnících se nabídek a poptávek. Každý příkaz, který je zapsán do order booku reflektuje cenu nabídky, která představuje nejvyšší částku, kterou je kupující daného kryptoaktiva ochoten zaplatit a cenu poptávky, která představuje nejnižší cenu, kterou je prodávající daného aktiva ochoten přijmout. V order booku se příkazy exekuuji podle dle časové priority ceny, což znamená, že právě tyto příkazy jsou exekuoávány na základě nejvyšší nabídky a nejnižší poptávky. V případě, že se nejvyšší nabídka a nejnižší poptávka po kryptoaktivu překrývají, přednost má právě ten příkaz, který byl zadán do order booku jako první (McGleenon, 2023).

4.3.1 Výhody order booku

Klíčovou výhodou order booku je možnost sledování všech zadaných objednávek pro širokou veřejnost, a tím je umožněno obchodníkům sledovat změny nabídek a poptávek v reálném čase, které napomáhá k určení přesné ceny, za kterou obchodníci chtějí kryptoaktiva nakupovat nebo prodávat, což jim dává větší kontrolu nad svými obchody. Tyto ceny jsou určovány na základě síly nabídky a síly poptávky, což zajišťuje spravedlivou cenu pro všechny obchodníky (Onomy Protocol, 2021).

Další výhodou order booku je možnost tvorby složitějších obchodních strategií a nástrojů, kde obchodníci mohou operovat s různými typy příkazů, které jsou zadávány na burzu k obchodování jako jsou tržní objednávka (market), limitní objednávka (limit) a další typy objednávek, které jsou již výše zmíněné v teoretické části.

4.3.2 Nevýhody order booku

Klíčovou nevýhodou order booku je složitost pro začínající obchodníky, pro které order book se může zdát složitý vzhledem k rychlým změnám cen, která se mění v reálném čase. Další nevýhodou order booku je vysoká volatilita trhu, která může vést k neprovedení či náročnému provedení příkazů s velkým objemem obchodovaných aktiv, aniž by tento příkaz negativně neovlivnil cenu obchodovaného aktiva. Nevýhoda z hlediska možnosti manipulace obchodovaných aktiv a jejich cen

jsou obchodníci, kteří v úmyslu vyděláním co nejvíce peněz, cenu obchodovaného aktiva manipulují pomocí obchodních robotů a to tím, že vyvolávají vysoký nákupní či prodejní tlak obchodovaného aktiva zadáním obrovského množství burzovních příkazů, a tak dochází k manipulaci ceny (Unchainedcrypto, 2023).



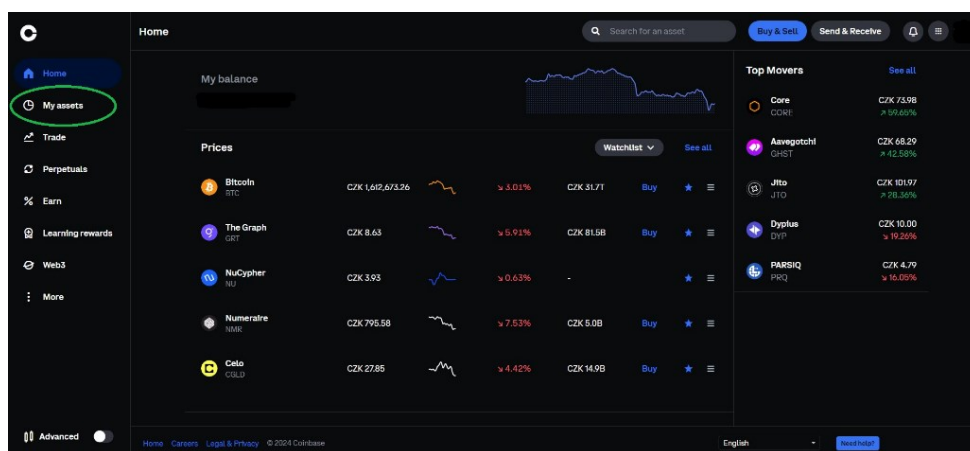
AMOUNT (BTC)	PRICE (USD)
0.00002088	66144.10
0.31609974	66144.00
0.00598642	66143.00
0.15750000	66142.50
0.62431738	66142.00
0.00112766	66141.50
0.00009122	66140.70
0.06705897	66140.30
0.10700000	66140.00
0.48383166	66138.80
0.09000000	66138.00
0.04983552	66137.40
0.21924692	66135.90
0.15517408	66135.80
0.16670105	66132.00
0.07560689	66131.60
0.01500000	66130.50
USD SPREAD 5.76	
0.07600000	66124.70
0.00100000	66124.40
0.66177768	66123.90
0.09305000	66123.10
0.06931901	66121.90
0.07061424	66121.50
0.10586572	66118.90
0.15750000	66118.10
0.02000000	66117.00
0.48534210	66116.00
0.66913828	66112.00
0.30251981	66111.30
0.45396600	66110.70
0.00000151	66109.10
0.00002275	66108.40
0.39567872	66108.00

Obrázek 3. Příklad order booku (Zdroj: Vlastní zpracování).

4.4 Průběh obchodování na CEX

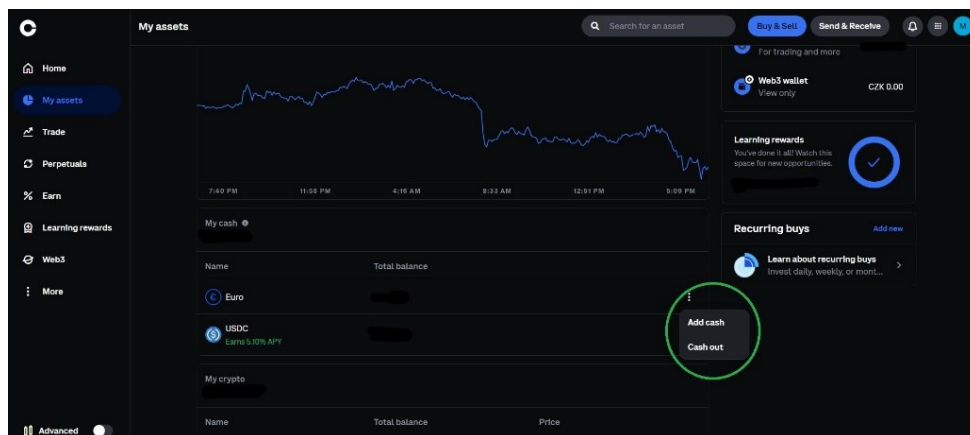
Aby uživatel centralizované kryptoměnové burzy mohl provádět obchody s kryptoaktivy je zapotřebí, aby podstoupil depozitní proces. Depozitním procesem je myšleno vklad svých finančních prostředků nebo převod svých kryptoměn ze své soukromé softwarové či hardwarové peněženky na platformu.

Příkladem pro obchodování je použita již zmíněná centralizovaná kryptoměnová burza Coinbase. Vložení finančních prostředků na platformu Coinbase se provádí v uživatelském rozhraní přes kolonku my assets (moje prostředky).



Obrázek 4. Postup přidání prostředků (Zdroj: Vlastní zpracování)

Druhým krokem tohoto procesu po kliknutí na kolonku my assets je kliknutí na 3 níže zvýrazněné rozhraní, které se dělí na add cash (přidat prostředky) a cash out (vybrat prostředky).



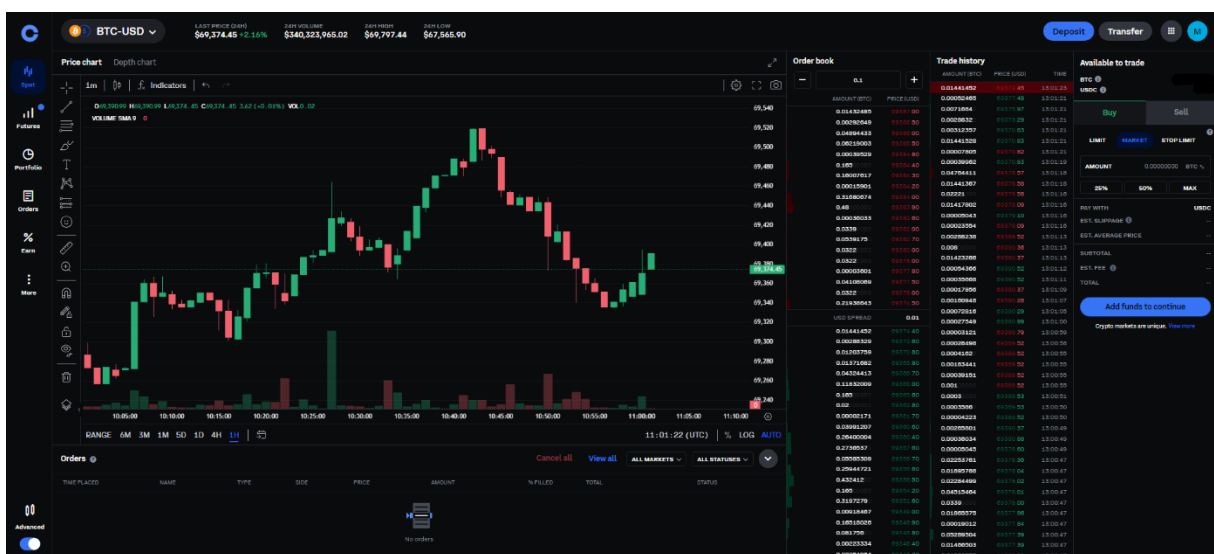
Obrázek 5. Postup přidání a výběru prostředků (Zdroj: Vlastní zpracování).

Uživatel musí zvolit možnost add cash, díky kterému se uživateli zobrazí veškeré podrobné informace pro přidání prostředků (referenční číslo, IBAN, název organizace, bankovní sídlo, jméno banky, národnost banky, bankovní adresa), které musí uživatel vyplnit při zaslání finančních prostředků na platformu. Je důležité, aby uživatel tyto údaje vyplnil přesně tak, jak to platforma vyžaduje, protože v případě, že uživatel tyto údaje vyplní nesprávně, nedojde k připsání finančních prostředků.

Vzhledem k tomu, že platforma nedisponuje možností obchodování pomocí české koruny, tak uživatel musí mít na paměti, že finanční prostředky, které se objeví v uživatelském rozhraní, nemusí být přesně v takové výši, kterou zaslal, protože při převodu české koruny na cizí měnu dochází ke kurzovým rozdílům.

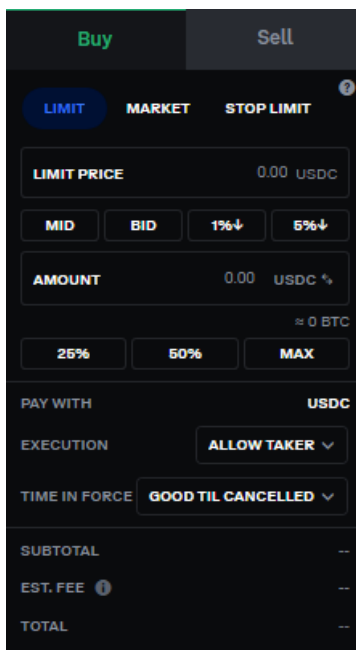
Po úspěšném přidání finančních prostředků na platformu má uživatel na výběr dvě možnosti manipulace s nimi. První možností je nákup, prodej, výměna kryptoaktiv přímo v uživatelském rozhraní v kolonce Buy and Sell (nakoupit nebo prodat). Tato možnost uživateli umožňuje okamžitě nakoupit či prodat svá kryptoaktiva, přičemž při zvolení této možnosti dochází k vyšším transakčním poplatkům než u druhé možnosti nákupu či prodeje kryptoměn, která bude zmíněna níže.

Druhou možností obchodování na centralizované kryptoměnové burze Coinbase, je přepnutí na pokročilou možnost obchodování tlačítkem advanced v uživatelském rozhraní v levém dolním rohu, které umožňuje uživateli sledovat grafy zvoleného páru kryptoaktiv, order book, obchodní historii a také zadávat složitější obchodní příkazy jako jsou market objednávky, limitní objednávky a stop limit objednávky.

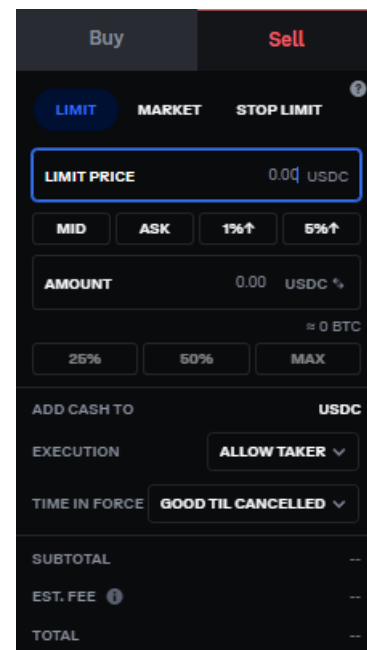


Obrázek 6. Coinbase advanced (Zdroj: Vlastní zpracování).

Coinbase advanced je pokročilá platforma pro obchodování kryptoaktiv, která nabízí širší možnosti zadávání obchodních příkazů. Těmito příkazy se rozumí market objednávky, limitní objednávky a stop limit objednávky. Market objednávky jsou prováděny okamžitě za aktuální tržní cenu bez nutnosti zadávání limitu, jak je tomu u limitních objednávek. Limitní objednávky jsou typem objednávky, které umožňují obchodníkům si určit, v jaké cenové hladině se zadaný příkaz má vykonat. V případě, že obchodník zadává limitní příkaz k nákupu kryptoaktiva, tak limitní objednávka bude provedena za stanovenou cenu obchodníkem nebo lepší (pod aktuální tržní cenu). V případě, že obchodník zadává limitní příkaz k prodeji kryptoaktiva, tak limitní objednávka bude provedena za stanovenou cenu obchodníkem nebo lepší (nad aktuální tržní cenu). Dalším typem obchodního příkazu jsou stop-limit objednávky, které kombinují typy příkazů stop a limitní objednávky. Fungování toho typu příkazu je založeno na zadání dvou cen, a to ceny stop a ceny limitní. Když tržní cena dosáhne obchodníkem zadané stop ceny, automaticky se tento příkaz přemění na limitní objednávku, která bude exekurována za obchodníkem zadanou nebo lepší cenu.



Obrázek 7. Ukázka nákupu kryptoaktiva (Zdroj: Vlastní zpracování).



Obrázek 8. Ukázka prodeje kryptoaktiva (Zdroj: Vlastní zpracování).

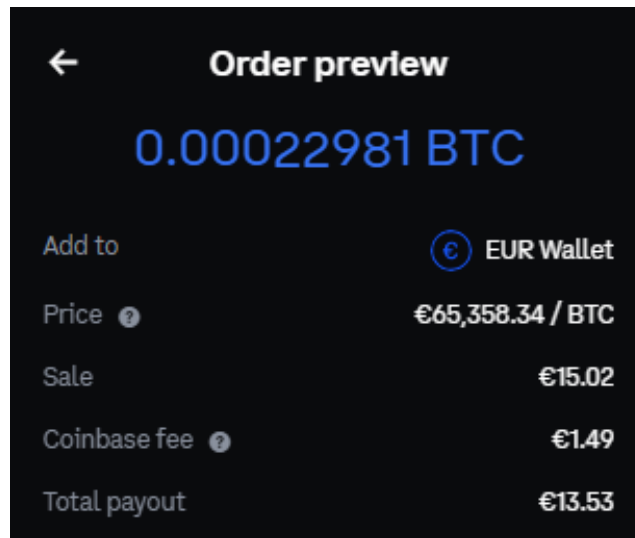
4.5 Transakční poplatky CEX

Poplatky, které se uplatňují na centralizovaných kryptoměnových burzách využívají schéma taker (strana, která z trhu odebírá likviditu prostřednictvím market objednávek, které se exeukují okamžitě) a maker (strana, která tvoří likviditu trhu prostřednictvím zadávání limitních objednávek), přičemž každá strana za provedenou transakci platí poplatky, ale obvykle strana taker, zaplatí na prováděné transakci vyšší poplatek než strana maker. Důvodem nižšího poplatku strany makera je ten, že zpravidla strana maker zvyšuje centralizovaným kryptoměnovým burzám likviditu. Výše poplatků na centralizovaných kryptoměnových burzách je nastavena tak, aby podpořila obchodování s velkými objemy kryptoaktiv u prováděných obchodů. Výše poplatků je ovlivňována a postupně snižována množstvím provedených obchodů, které obchodník uskuteční za uplynulých 30 dnů. Z hlediska běžného uživatele centralizované kryptoměnové burzy je zpravidla nevýhodné provádět malé a méně časté obchody z důvodu nákladové efektivnosti, ale to ovšem neplatí pro ty uživatele, kteří na centralizované kryptoměnové burze operují pouze za účelem nákupu kryptoaktiv a jejich následného uchování. Již výše zmíněná centralizovaná kryptoměnová burza Coinbase má poplatky nastavené ve schématu taker a maker strany v procentuálním vyjádření, kde při realizování obchodů s hodnotou nižší než 10000 amerických dolarů si strana taker účtuje poplatek ve výši 0,6 % z provedené transakce, zatímco strana maker 0,4 % z provedené transakce. Při obchodování s větším objemem obchodovaných kryptoaktiv než zmíněných 10000 amerických dolarů, se poplatky snižují dle množství provedených obchodů uživatele (Sharma, 2024).

Pricing Tier	Taker Fee	Maker Fee
\$0 - \$10K	0.60%	0.40%
\$10K - \$50K	0.40%	0.25%
\$50K - \$100K	0.25%	0.15%
\$100K - \$1M	0.20%	0.10%

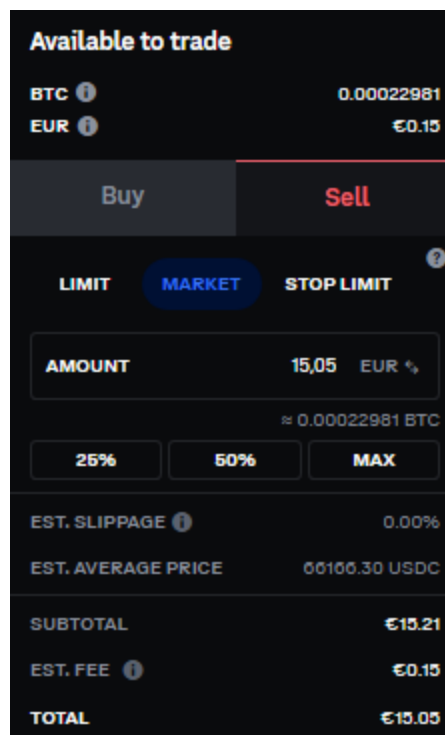
Obrázek 9. Ukázka transakčních poplatků stran Taker a Maker (Zdroj: Reiff, 2023).

Pro ukázkou srovnání poplatků v uživatelském rozhraní je použito již zmíněné kryptoaktivum Bitcoin.



Obrázek 10. Ukázka poplatku v uživatelském rozhraní Coinbase (Zdroj: Vlastní zpracování).

Pro ukázkou srovnání poplatků v uživatelském rozhraní a možností přepnutí do složitějšího rozhraní advanced je použito již zmíněné kryptoaktivum Bitcoin.



Obrázek 11. Ukázka poplatku v Coinbase advanced (Zdroj: Vlastní zpracování).

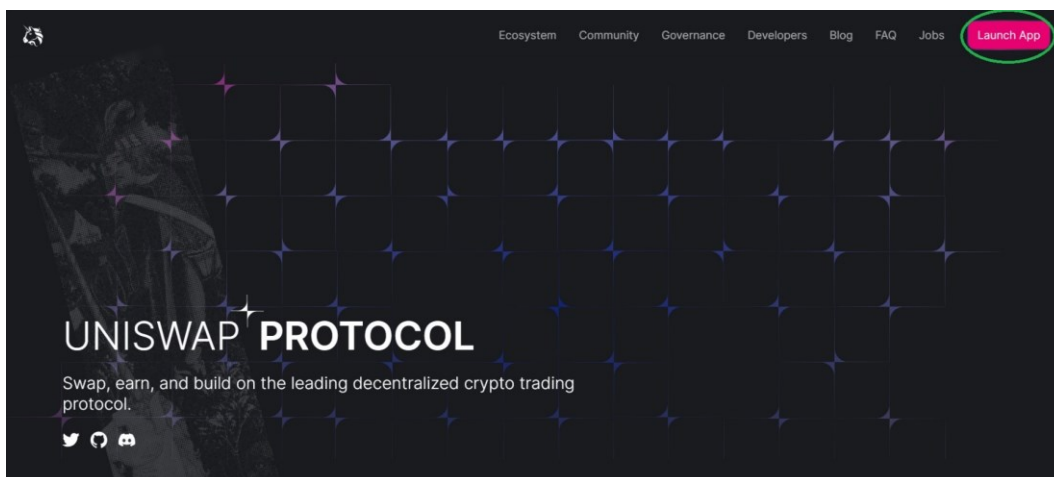
5 PRŮBĚH FUNGOVÁNÍ A OBCHODOVÁNÍ NA DEX

Tato část bakalářské práce se zaměřuje na postupové kroky fungování a obchodování na decentralizované kryptoměnové burze. Konkrétní decentralizovanou kryptoměnovou burzou pro ukázkou, bude použita decentralizovaná kryptoměnová burza UniSwap.

5.1 Průběh fungování na DEX

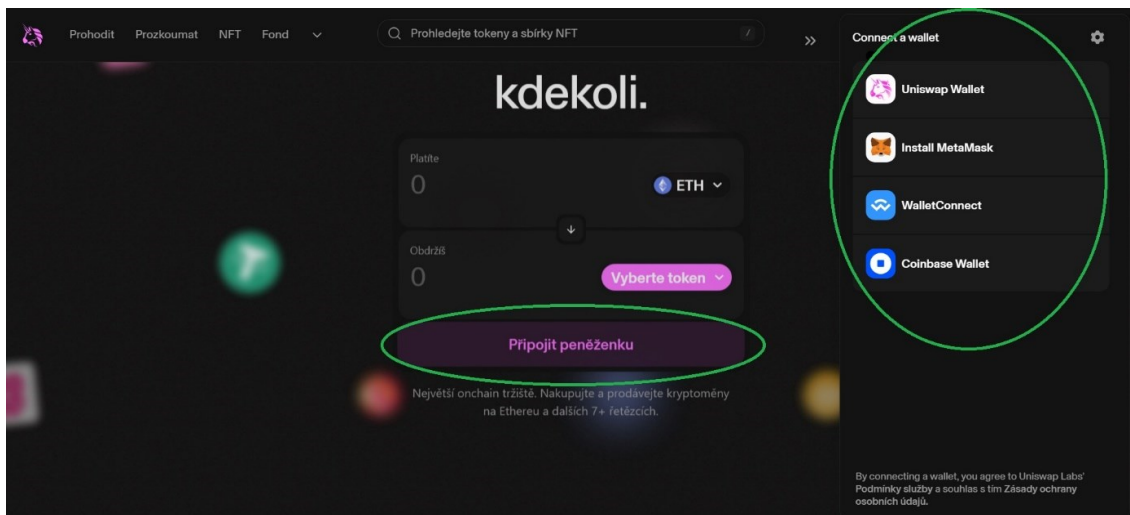
Pro fungování na decentralizovaných burzách uživatelé nejsou povinni podstoupit proces registrace s ověřením totožnosti procesem KYC. Uživatelům decentralizovaných kryptoměnových burz, stačí pouze připojení své vlastní soukromé kryptoměnové peněženky, která musí být podporována z hlediska fungování samotnou decentralizovanou kryptoměnovou burzou. Pro proces vysvětlení fungování je použita decentralizovaná kryptoměnová burza UniSwap.

Prvním krokem, který uživatel musí učinit, je zadání webové adresy do vyhledávače v daném prohlížeči. Jakmile se uživatel ocitne na webové stránce UniSwap, musí učinit krok přesměrování tlačítkem launch app v pravém horním rohu, přes které se otevře UniSwap aplikace.



Obrázek 12. Ukázka přepnutí do aplikace UniSwap (Zdroj: Vlastní zpracování).

Druhým krokem po učinění prvního kroku je připojení své soukromé kryptoměnové peněženky. Decentralizovaná kryptoměnová burza UniSwap nabízí 4 možnosti kompatibility kryptoměnových peněženek, přes které se uživatel může připojit. Typy kryptoměnových peněženek jsou zmíněné v obrázku níže.



Obrázek 13. Ukázka kompatibility kryptoměnových peněženek s platformou (Zdroj: Vlastní zpracování).

5.2 Bezpečnost DEX

Bezpečnost na decentralizovaných kryptoměnových burzách zajišťuje blockchain a smart kontrakty zakotvené právě v tomto blockchainu. Tyto smart kontrakty jsou klíčovým prvkem, které zajišťují bezpečnost na decentralizovaných kryptoměnových burzách. Zranitelnost decentralizovaných kryptoměnových burz závisí na kvalitě a zpracování kódu smart kontraktu. Vzhledem k tomu, že kód smart kontraktu je dostupný pro všechny, mohla by zde naskytnout situace, kdy by zkušení hackeri mohli tuto chybu v kódu identifikovat a následně zneužít. Vývojáři kódů smart kontraktů mohou riziko chyby v kódu eliminovat pomocí bezpečnostních auditů, testování kódu pomocí vzájemného hodnocení a důkladných testovacích postupů s velkým důrazem na pečlivost. Některé decentralizované kryptoměnové burzy umožňují možnost nastavení více podpisových transakcí, což v praxi znamená, že každá prováděná transakce vyžaduje souhlas více účastníků prováděné transakce, což zvyšuje bezpečnost v oblasti ztráty finančních prostředků (Tagade,2023).

5.3 Fungování AMM na DEX

Fungování protokolu AMM je založeno na bázi využití poolu likvidity, kdy uživatelé právě do těchto poolu ukládají svá kryptoaktiva, a tím zajišťují likviditu. Tyto pooly likvidity následně pomocí algoritmů stanovují ceny kryptoaktiv dle poměru právě těchto aktiv v poolu. Tento mechanismus v rámci kryptoměnového ekosystému AMM odstraňuje potřebu tradičního order booku, a tím usnadňuje a zrychluje provádění výměny kryptoaktiv. AMM pobízí uživatele k poskytování likvidity tím, že nabízí odměny ve formě podílů na transakčních poplatcích nebo jiné odměny (Sergeenkov, 2023).

5.3.1 Výhody AMM

Klíčovou výhodou AMM je plné vlastnictví kryptoaktiv, které pomocí smart contractu poskytují možnost obchodování bez prostřednictví třetí strany. Obchodování probíhá pouze ze soukromé kryptoměnové peněženky uživatele, a tak zde je menší riziko ztráty právě těchto kryptoaktiv vůči protistraně. Výhoda, která je spjata s obchodováním bez prostřednictví třetí strany spočívá v nižších transakčních poplatcích právě v důsledku absence třetí strany, kdy uživatelé obchodují přímo s primárním zdrojem a nemusí zde účinkovat protistrana. Protokol AMM zkrátil dobu provedení transakcí, díky které se snížil prudký rozdíl v ceně mezi okamžikem nákupu a prodeje (slippage). Výhoda pro uživatele decentralizovaných kryptoměnových burz, které fungují na protokolu AMM je možnost získání pasivního příjmu ze svých kryptoaktiv, který plyne z poplatků na decentralizovaných kryptoměnových burzách (Dolapo, 2024). Princip získávání pasivního příjmu z poskytování likvidity do poolů likvidity je popsán v kapitole 5.6.

5.3.2 Nevýhody AMM

Klíčovou nevýhodou protokolu AMM pro uživatele decentralizované kryptoměnové burzy je impermanent loss. Impermanent loss (pomíjivá ztráta) vzniká, když uživatel poskytuje likviditu do fondu likvidity a cena uživatelem vložených kryptoaktiv se změní s dobou, kdy kryptoaktiva do fondu likvidity byly vloženy. Impermanent loss je vratná v momentě, kdy kryptoaktiva dosáhnou původní cenové hladiny v době poskytnutí likvidity, avšak pokud jsou kryptoaktiva z poolu likvidity vyjmuta dříve, než by došlo k vrácení se na původní cenovou hladinu, tak impermanent loss se stává ztrátou trvalou (Rouse, 2023.) Další nevýhodou AMM je, že pro uživatele představují vzdání se kontroly nad vykonávaným obchodním procesem, protože AMM fungují na předem stanovených matematických

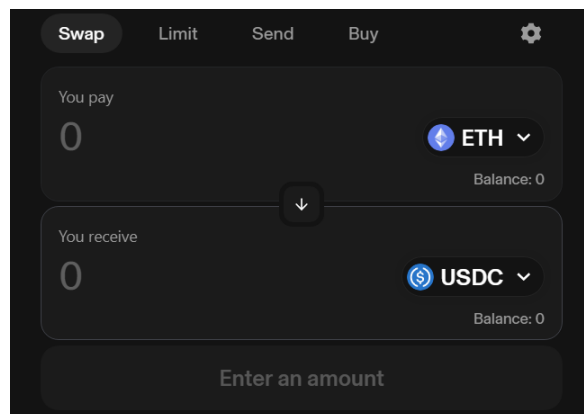
algoritmech, a tak uživatelé mají velmi omezený vliv na určování hodnoty kryptoaktiv. Za nevýhodu lze také považovat omezení možností typů objednávek, kde protokol AMM nabízí pouze základní typy objednávkových příkazů jako market a limit, které pro zkušené obchodníky nemusí být dostačující vzhledem k jejich obchodní strategii (Semin, 2023).

5.4 Průběh obchodování na DEX

Aby uživatel decentralizované kryptoměnové burzy mohl provádět obchody, musí vlastnit kryptoměnovou peněženku, kterou uživatel připojí na platformu. Obchodování na decentralizovaných kryptoměnových burzách probíhá právě pomocí těchto soukromých kryptoměnových peněženek, což umožňuje uživatelům nepřetržitou kontrolu na svými kryptoaktivy společně s jejich kompletní správou. Obchody na decentralizovaných kryptoměnových burzách probíhají přímo na blockchainu mnoha druhů kryptoaktiv, a to prostřednictvím smart kontraktů. Na decentralizovaných kryptoměnových burzách jsou objednávky exekuvány pomocí algoritmů, přičemž párování právě těchto objednávek se uskutečňuje přímo mezi obchodníky, a to pomocí již zmíněných smart kontraktů. Tyto smart kontrakty obsahují určitá pravidla pro exekuci objednávek zadanými obchodníky a určitá pravidla pro manipulaci s kryptoaktivy. Pro ukázkou obchodování na decentralizované kryptoměnové burze je použita decentralizovaná kryptoměnová burza UniSwap.

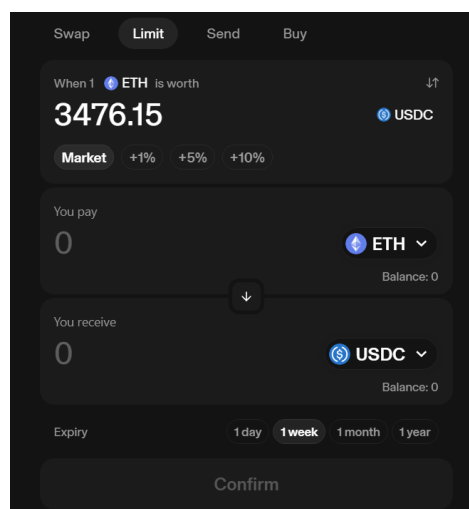
Uživatel decentralizované burzy UniSwap, po úspěšném připojení pomocí své privátní kryptoměnové peněženky, má možnost se účastnit obchodování na Uniswapu. Decentralizovaná kryptoměnová burza UniSwap disponuje možnostmi typů objednávek a také možností poskytování likvidity do poolů likvidity a nákup non-fungible tokenů (NFT).

První možností obchodování na decentralizované kryptoměnové burze UniSwap je typ objednávky zvaný swap. Swapem se rozumí proces, u kterého dochází k přímé výměně kryptoaktiva za jiné kryptoaktivum, bez nutnosti participace fiat měny. U swapu dochází k exekuci objednávky okamžitě s nižšími transakčními poplatky, než je tomu u jiných typů objednávek. Decentralizovaná kryptoměnová burza UniSwap nabízí možnost swapu až 100 různých kryptoaktiv.



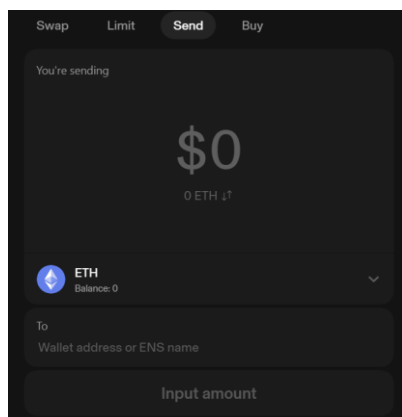
Obrázek 14. Ukázka SWAPU na platformě UniSwap (Zdroj: Vlastní zpracování).

Druhou možností obchodování na UniSwapu je možnost zadání swap limitní objednávky, kde si uživatel musí zvolit požadovanou hranici ceny kryptoaktiva, při které se uskuteční výměna uživatelem vybraných kryptoaktiv. Samotná burza UniSwap upozorňuje na to, že u objednávky nemusí dojít k její exekuci, když cena kryptoaktiva nedosáhne požadované hranice ceny.



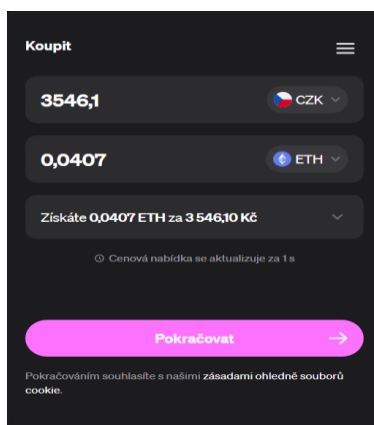
Obrázek 15. Ukázka zadání limitní objednávky na platformě UniSwap (Zdroj: Vlastní zpracování).

Třetí možností obchodování je posílání zvolených kryptoaktiv v uživatelem zvolené výši, které vlastní, na adresy jiné než vlastní kryptoměnové peněženky nebo ENS (Ethereum Name Service) jméno jiným uživatelům.



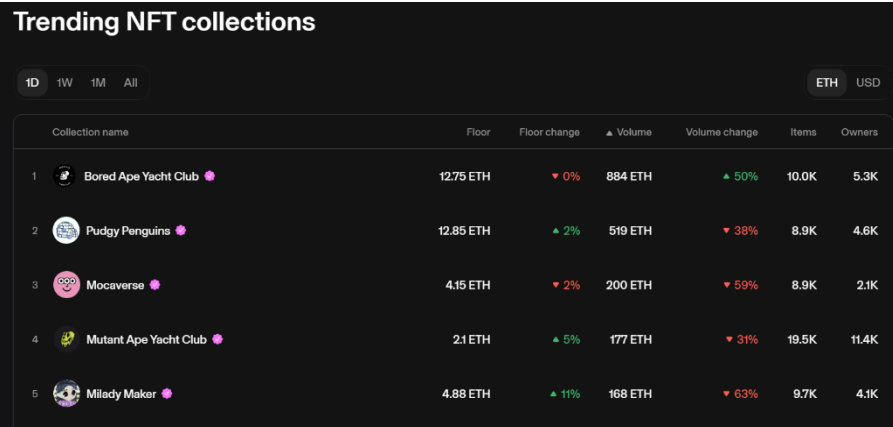
Obrázek 16. Ukázka posílání kryptoaktiv (Zdroj: Vlastní zpracování).

Čtvrtou možností obchodování na decentralizované kryptoměnové burze UniSwap je nákup kryptoaktiva. Nákup kryptoaktiv na decentralizované kryptoměnové burze UniSwap nevyžaduje deponitní proces, jako je tomu u centralizované kryptoměnové burzy Coinbase, ale i tak zde figuruje proces směny fiat měny. Proces nákupu kryptoaktiva spočívá ve zvolení fiat měny a kryptoaktiva, které uživatel hodlá zakoupit. Nákup probíhá přes službu MoonPay, která zprostředkovává převod fiat měny za kryptoaktiva. Je nutné, aby uživatel poskytl svou emailovou adresu a fakturační údaje předtím, než bude vyzván k vyplnění čísla kreditní či debetní karty. Zakoupené kryptoaktiva uživatel inkasuje do své s platformou kompatibilní a spojené kryptoměnové peněženky.



Obrázek 17. Ukázka zakoupení kryptoaktiv na platformě UniSwap (Zdroj: Vlastní zpracování).

Decentralizovaná kryptoměnová burza UniSwap nabízí možnost nákupu non-fungible token (NFT), které lze nakupovat pomocí ETH nebo fiat měny. Non-fungible token představuje digitální záznam o vlastnictví a pravosti založený na blockchainu, který je neduplikovatelný. UniSwap nabízí 100 kolekcí těchto NFT, ve kterých lze nalézt různé typy těchto NFT.

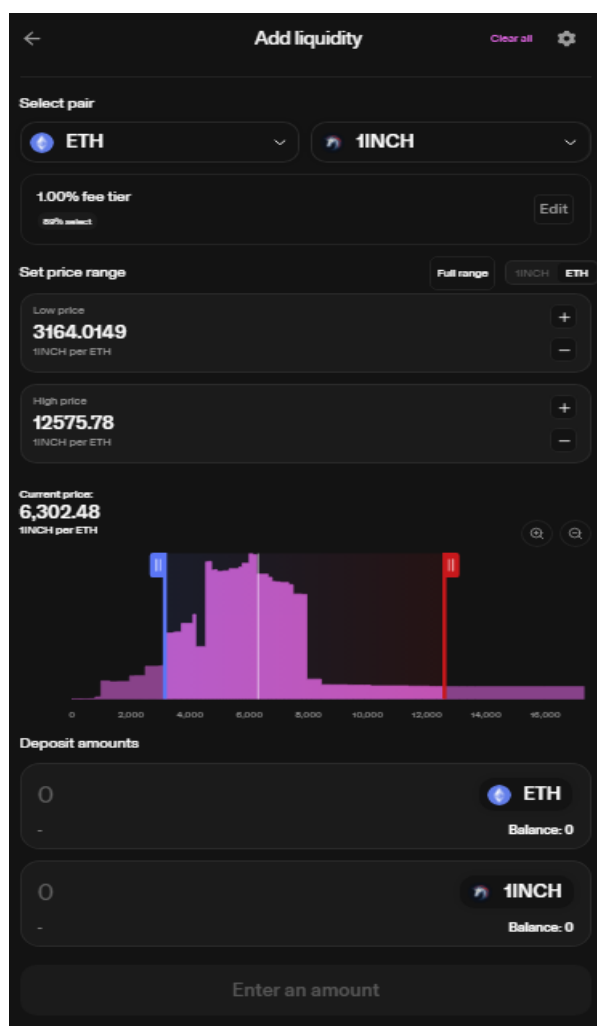


Collection name	Floor	Floor change	Volume	Volume change	Items	Owners
1 Bored Ape Yacht Club	12.75 ETH	▼ 0%	884 ETH	▲ 50%	10.0K	5.3K
2 Pudgy Penguins	12.85 ETH	▲ 2%	519 ETH	▼ 38%	8.9K	4.6K
3 Mocaverse	4.15 ETH	▼ 2%	200 ETH	▼ 59%	8.9K	2.1K
4 Mutant Ape Yacht Club	2.1 ETH	▲ 5%	177 ETH	▼ 31%	19.5K	11.4K
5 Mlady Maker	4.88 ETH	▲ 11%	168 ETH	▼ 63%	9.7K	4.1K

Obrázek 18. Ukázka typů NFT na platformě UniSwap (Zdroj: Vlastní zpracování).

5.5 Poskytování likvidity

Na decentralizovaných kryptoměnových burzách uživatelé těchto burz mají možnost získávat pasivní příjem z poolů likvidity poskytováním likvidity právě do těchto poolů. Tohoto pasivního příjmu uživatelé dosáhnou tak, že přispějí do poolu likvidity tím, že vloží uživatelem vybranou dvojici tokenů v daném poměru vybraných kryptoaktiv. Po přidání prostředků do poolu likvidity uživatelé získají liquidity provider tokeny (tokeny poskytovatele likvidity), které představují uživatelův podíl v poolu likvidity. Vklad prostředků, které uživatel do poolu likvidity vložil, slouží k provádění transakcí, přičemž výměnou za poskytnutý vklad poskytovatelů likvidity, je podíl na poplatcích generovaný právě z těchto transakcí. Podíl se kumuluje z provedených transakcí a je vybrán tak, že uživatel vrátí liquidity provider tokeny zpět do poolu likvidity výměnou za vložená původní kryptoaktiva společně s nakumulovanými poplatky. Ukázka přidání páru kryptoaktiv ETH a 1INCH na decentralizované kryptoměnové burze UniSwap, je vyobrazen v obrázku níže.



Obrázek 19. Ukázka přidání páru při poskytování likvidity
(Zdroj: Vlastní zpracování)

6 ZHODNOCENÍ ANALÝZY

6.1 Porovnání fungování CEX a DEX

Pro fungování na centralizované kryptoměnové burze je nutné dovršit věku 18 let a podstoupit proces registrace zahrnující i ověření totožnosti KYC. Díky procesu KYC má centralizovaná kryptoměnová burza přehled a jistotu o totožnosti svých uživatelů, aby nedocházelo k nekalým praktikám jako je například praní špinavých peněz. Naopak decentralizované kryptoměnové burzy nabízejí odlišný přístup, kde uživatelé nejsou povinni podstoupit proces registrace včetně procesu KYC, a k tomu, aby mohli na decentralizované burze fungovat a operovat, jim stačí pouze připojení své soukromé kryptoměnové peněženky na platformu, se kterou je vybraná decentralizovaná kryptoměnová burza kompatibilní. Tímto způsobem se fungování a obchodování na decentralizovaných a centralizovaných kryptoměnových burzách odlišuje, protože uživatelé decentralizované kryptoměnové burzy nejsou povinni poskytovat své osobní údaje včetně procesu ověření identity KYC.

6.2 Porovnání bezpečnosti CEX a DEX

V porovnání bezpečnosti centralizovaných a decentralizovaných kryptoměnových burz je zřejmé, že u obou typů kryptoměnových burz jsou užívány jiné postupy zabezpečování právě těchto burz. Centralizované kryptoměnové burzy fungují podobně jako tradiční finanční instituce, u kterých figuruje centralizovaný správce, který spravuje prostředky uživatelů centralizovaných kryptoměnových burz. U centralizovaných kryptoměnových burz je nutné projít procesem registrace s procesem ověření totožnosti KYC. Uživatelé burzovních účtů na centralizovaných kryptoměnových burzách, jsou povinni používat dvoufázové ověřování pro případ přihlášení do platformy či provádění obchodů na platformě. Oproti tomu, decentralizované kryptoměnové burzy nedisponují burzovními uživatelskými účty, a proto tato funkce dvoufázového ověření není možná, protože na decentralizovaných burzách uživatelé obchodují pouze pomocí svých soukromých kryptoměnových peněženek. Co se týče dvoufázového ověření realizovaných obchodů, tak zde figuruje výjimka, že některé decentralizované kryptoměnové burzy disponují možností nastavení vícepodpisových transakcí. Na decentralizovaných kryptoměnových burzách je bezpečnost zajišťována pomocí smart kontraktů vepsaných do blockchainu, které musí být důkladně prověřovány a auditovány. Kdyby nedocházelo k pravidelnému

testování a auditování právě těchto smart kontraktů, kde právě kód smart kontraktu je veřejný, tak by mohlo docházet k častým hackerským útokům, kteří by mohli jednoduše odhalit chybu v kódu smart kontraktu, a tak právě tuto chybu následně zneužít ve svůj prospěch. Obecně lze říct, že bezpečnost na decentralizovaných kryptoměnových burz závisí na kvalitě a zpracování kódu smart kontraktu. Výhodou veřejné dostupnosti kódu smart kontraktu je ta, že samotná komunita obchodníků na decentralizovaných kryptoměnových burzách může přispívat k identifikaci chyb samotného kódu a tím zvyšovat bezpečnost.

6.3 Porovnání order booku a protokolu AMM

Principy fungování order booku a AMM (automated market maker) jsou velmi odlišné. Order book pracuje na základě tržních burzovních příkazů (market order, limit order), které se realizují v reálném čase, zatímco fungování AMM je založeno na poolu likvidity, kam uživatelé ukládají svá kryptoaktiva, a tím poolu likvidity zajišťují likviditu. V order booku se objednávky v něm zapsané exekují dle časové priority ceny, což znamená, že jsou prováděny na základě nejvyšší nabídky a nejnižší poptávky, zatímco v protokolu AMM se transakce exekují okamžitě na základě stavu poolu likvidity a matematických algoritmů. Rizika, která se objevují u obou těchto mechanismů jsou následující. Riziko order booku je manipulace trhu umělým zvyšováním či snižováním hodnoty kryptoaktiv, zatímco mechanismus AMM může mít omezení v cenové efektivitě při provádění obchodů s velkým objemem obchodovaných aktiv a také riziko nedostatečné likvidity v poolu likvidity. Porovnání těchto dvou mechanismů ukazuje jejich rozdílné fungování, chování a obchodování společně s jejich výhodami, nevýhodami a omezeními pro každý tento mechanismus.

6.4 Porovnání obchodování CEX a DEX

Princip obchodování na centralizovaných kryptoměnových burzách se odlišuje od principu obchodování na decentralizovaných kryptoměnových burzách již od samotného začátku, a to tím, že na centralizovaných kryptoměnových burzách je nutné podstoupit depozitní proces, který představuje převod vlastních finančních prostředků na platformu či převod kryptoaktiv ze své soukromé kryptoměnové peněženky, zatímco na decentralizovaných burzách není povinné tento proces podstoupit. Největším rozdílem obchodování na typech centralizovaných a decentralizovaných kryptoměnových burz spočívá ve správě svého majetku. U centralizovaných kryptoměnových burz se finanční majetek spravuje pomocí

centralizovaného správce, což nese velké riziko neoprávněné manipulace s uživatelským finančním majetkem. Příkladem této neoprávněné a zároveň pro uživatele nevědomé manipulace s jejich prostředky, byl krach centralizované kryptoměnové burzy FTX. Centralizovaná kryptoměnová burza FTX neoprávněně užívala finančních prostředků všech svých uživatelů, a to vedlo k tomu, když uživatelé centralizované kryptoměnové burzy FTX své prostředky z této burzy chtěli vybrat, ale nebylo jim to umožněno, protože burza neměla tyto prostředky na vyplacení v důsledku zmíněné neoprávněné manipulace s finančními prostředky uživatelů. Oproti tomu na decentralizované kryptoměnové burze k tomuto dojit nemůže, protože uživatelé decentralizovaných kryptoměnových burz se svými prostředky nakládají samostatně pomocí svých soukromých kryptoměnových peněženek, díky čemuž přebírají veškerou kontrolu nad správou svého finančního majetku. Samostatnost ve správě kryptoaktiv obchodníkům dává větší svobodu a kontrolu nad svými prostředky, ale také i větší zodpovědnost a péči, které musí věnovat bezpečnosti svých privátních klíčů. Na centralizovaných kryptoměnových burzách se objednávky párují a exekuuji dle mechanismů centralizovaných kryptoměnových burz. Na druhou stranu se objednávky na decentralizovaných kryptoměnových burzách párují a exekuuji pomocí algoritmů a smart kontraktů vepsaných do blockchainu. Centralizované kryptoměnové burzy uživatelům nabízí určitou míru pohodlí a integrace s tradičními finančními systémy, zatímco decentralizované kryptoměnové burzy nabízejí vyšší úroveň transparentnosti a anonymity.

6.5 Porovnání transakčních poplatků CEX a DEX

Na centralizovaných kryptoměnových burzách jsou poplatky definovány dle schématu stran taker a maker, kde taker představuje stranu, která z trhu odebírá likviditu prostřednictvím market objednávek, u kterých dochází k okamžité exekuci a strana maker, která představuje stranu, která tvoří likviditu trhu prostřednictvím zadávání limitních objednávek. Zpravidla platí, že strana taker obvykle platí více na transakčních poplatcích než strana maker. Struktura schématu centralizovaných kryptoměnových burz taker a maker je navržena tak, aby podporovala obchodování s většími objemy kryptoaktiv. Na druhou stranu u decentralizovaných kryptoměnových je struktura výpočtu výše transakčních poplatků je velmi odlišná. Poplatky na decentralizovaných kryptoměnových burzách jsou definovány třemi složkami, a to rozdílem mezi nabídkou a poptávkou, burzovních poplatků a gas poplatků. Výše poplatků na decentralizovaných kryptoměnových burzách, je ovlivněna výpočtem výkonem spravované sítě a cenou poplatku gas

v momentě probíhajícího obchodu. Vzhledem k uživatelům kryptoměnových burz, kteří preferují obchodování spíše s většími objemy na úkor vyšších poplatků, tak těmto uživatelům by spíše měli vyhovovat burzy centralizované. Na druhou stranu, pokud obchodníci chtějí obchodovat s menšími objemy a jsou schopni přijmout riziko závislosti výpočetního výkonu, tak těmto uživatelům by spíše měli vyhovovat burzy decentralizované.

ZÁVĚR

Cílem této bakalářské práce bylo analyzovat a porovnat typy kryptoměnových burz z hlediska jejich funkčnosti a využití. V důsledku provedené analýzy a následného porovnání typů kryptoměnových burz bylo zjištěno, že centralizované a decentralizované kryptoměnové burzy přistupují k fungování a obchodování odlišným způsobem. Těmito odlišnými způsoby je myšleno fungování na jiných mechanismech, kde centralizované burzy vyžadují ověření totožnosti uživatele, zatímco decentralizované burzy nikoliv a obchodování skrze odlišné formy financování prováděných obchodů, kde na centralizované kryptoměnové burze uživatel obchoduje skrze předem vložených vlastních finančních prostředků, zatímco na decentralizované kryptoměnové burze uživatelé provádějí obchody přímo pomocí svých kryptoměnových peněženek.

Teoretická část se zabývala literární rešerší v oblasti definování kryptoaktiv, tradičního modelu burzy a taktéž problematikou typů kryptoměnových burz. První část teoretické části se věnovala oblasti kryptoaktiv, ve které byly rozebrány klíčové aspekty týkající se jejich definice, principů fungování a v neposlední řadě jejich pestré členění. Další oblastí nezbytnou k pochopení fungování kryptoměnových burz byla rozebrána problematika tradičních burz, která se zabývala historií, jakým způsobem fungují a taktéž jaké nabízejí funkce. Teoretickou část uzavírá tematika samotných kryptoměnových burz, která zahrnuje rozdělení typů kryptoměnových burz, jejich funkce a možnosti typů burzovních objednávkových příkazů, které se uplatňují právě na těchto typech kryptoměnových burz.

Praktická část věnovala pozornost analýze centralizovaných a decentralizovaných kryptoměnových burz, která vycházela z literární rešerše teoretické části. Analýza podává komplexní přehled o fungování a obchodování na obou typech kryptoměnových burz, která zahrnovala i aspekty bezpečnosti včetně možností typů obchodních burzovních příkazů uplatnitelných právě na těchto burzách s následným vyhodnocením, které se týkalo jednotlivého porovnání vycházející z provedené analýzy.

Závěrem lze říci, že praktická část naplnila stanovené cíle a doufám, že tato práce přispěla k lepšímu pochopení problematiky kryptoměnových burz a poskytla ucelený přehled o fungování a obchodování na kryptoměnových burzách.

SEZNAM POUŽITÉ LITERATURY

AHMED, Khalid, 2024. *Crypto Swap*. Online. WallStreetMojo. Dostupné z: <https://www.wallstreetmojo.com/crypto-swap/>. [cit. 2024-03-15].

AUER, Raphael, 2019. *Beyond the Doomsday Economics of „Proof-of-Work“ in Cryptocurrencies* [online]. SSRN Scholarly Paper. [vid. 2024-01-25]. Dostupné z: <https://papers.ssrn.com/abstract=3331413>

BARAKAT, Samer; HAMMOURI, Qais a YAGHI, Khalil, 2022. *COMPARISON OF HARDWARE AND DIGITAL CRYPTO WALLETS*. Online. Journal of Southwest Jiaotong University. roč. 57, č. 6, s. 380-386. ISSN 0258-2724. Dostupné z: <https://doi.org/10.35741/issn.0258-2724.57.6.36>. [cit. 2024-01-25].

BINANCE ACADEMY, 2019. *Co jsou chytré kontrakty?* Online. Binance Academy. Dostupné z: <https://academy.binance.com/cs/articles/what-are-smart-contracts>. [cit. 2024-03-21].

CROOKS, Nathan, 2023. *What are decentralized exchanges?* Online. The Block. Dostupné z: <https://www.theblock.co/learn/245709/what-are-decentralized-exchanges>. [cit. 2024-01-31].

CRYPTOPEDIA, 2023. *What Are Automated Market Makers (AMM)?* Online. Gemini. Dostupné z: <https://www.gemini.com/cryptopedia/amm-what-are-automated-market-makers>. [cit. 2024-01-26].

DEVI BHASKAR, Nirupama a KUO CHUEN, David LEE, 2015. Bitcoin Mining Technology. In: *Handbook of Digital Currency*. Academic Press. s. 45-65. ISBN 978-0-12-802117-0.

DI PIERRO, Massimo, 2017. *What Is the Blockchain?* Online. *Computing in Science & Engineering*. roč. 19, č. 5, s. 92-95. ISSN 1521-9615. Dostupné z: <https://doi.org/10.1109/MCSE.2017.3421554>. [cit. 2024-01-24].

DOLAPO, Olayiwola, 2023. *What is an Automated Market Maker (AMM)? A Complete Guide*. Online. DoomDroom. Dostupné z: <https://droomdroom.com/guide-to-automated-market-maker/>. [cit. 2024-04-29].

DRESCHER, Daniel, 2017. *Blockchain basics: a non-technical introduction in 25 steps*. Berkeley, California: Apress, ISBN 1484226038.

EIMBACH, Lioba; Ye WANG a Roger WATTENHOFER, 2021. *Behavior of Liquidity Providers in Decentralized Exchanges* [online]. B.m.: arXiv. [vid. 2024-01-26]. Dostupné z: doi:10.48550/arXiv.2105.13822

EUREX, ©2024. *Order types*. Online. Dostupné z: <https://www.eurex.com/ex-en/trade/order-book-trading/order-types>. [cit. 2024-04-29].

FRANKENFIELD, Jake, 2023. *Cryptocurrency Explained With Pros and Cons for Investment*. Online. Investopedia. Dostupné z: <https://www.investopedia.com/terms/c/cryptocurrency.asp>. [cit. 2024-01-23].

CHEN, James, 2021. *Take-Profit Order (TP): Definition, Use in Trading, and Example*. Online. Investopedia. Dostupné z: <https://www.investopedia.com/terms/t/take-profitorder.asp>. [cit. 2024-03-22].

INVESTOPEDIA, 2024. *Cryptocurrency Explained With Pros and Cons for Investment*. Online. Investopedia. Dostupné z: <https://www.investopedia.com/terms/c/cryptocurrency.asp>. [cit. 2024-03-21].

KHAN, Atif, 2024. *What is Binance? A Complete Guide*. Intellipaat. [online] [vid. 2024-01-26]. Dostupné z: <https://intellipaat.com/blog/what-is-binance/>

KOKATE, Chandrakant, 2023. *(PDF) Cryptocurrency: Advantages and Disadvantages of the Creative Commons Attribution License (CC BY 4.0)*. Online. ResearchGate. Dostupné z: https://www.researchgate.net/publication/376892783_Cryptocurrency_Advantages_and_Disadvantages_of_the_Creative_Commons_Attribution_License_CC_BY_40. [cit. 2024-01-24].

KÜFEOĞLU, Sinan a ÖZKURAN, Mahmut, 2019. Bitcoin mining: A global review of energy and power demand. Online. *Energy Research & Social Science*. roč. 58. ISSN 22146296. Dostupné z: <https://doi.org/10.1016/j.erss.2019.101273>. [cit. 2024-01-25].

LAU, Darren et al., 2021. *How to DeFi (Beginner)*. 2nd ed. Independently published. ISBN 979-8530408434.

LEDGER, ©2024. *Ledger Nano X*. Online. Ledger. Dostupné z: <https://shop.ledger.com/products/ledger-nano-x>. [cit. 2024-03-15].

ROY, Gaurav, 2023. *What is a Centralized Cryptocurrency Exchange (CEX)?* Online. Ledger. Dostupné z: <https://www.ledger.com/academy/topics/crypto/what-is-a-centralized-cryptocurrency-exchange-cex>. [cit. 2024-05-07].

LEGGÉ, Michelle, 2023. *Coinbase*. Online. Koinly: Calculate Your Bitcoin and Crypto Taxes. Dostupné z: <https://koinly.io/crypto-glossary/coinbase/>. [cit. 2024-01-26].

LI, Ruoyue; XIE, Yankai; NING, Zhiqiang; ZHANG, Chi a WEI, Lingbo, 2022. *Privacy-Preserving Decentralized Cryptocurrency Exchange without Price Manipulation*. Online. In: 2022 IEEE/CIC International Conference on Communications in China (ICCC). IEEE, s. 274-279. ISBN 978-1-6654-8480-0. Dostupné z: <https://doi.org/10.1109/ICCC55456.2022.9880750>. [cit. 2024-03-10].

LIN, X. Lindsay, 2019. *Deconstructing Decentralized Exchanges*. Online. Stanford Journal of Blockchain Law. Dostupné z: <https://stanford-jblp.pubpub.org/pub/deconstructing-dex/release/1>. [cit. 2024-01-25].

MAVERICK, J.B, 2022. *Buy Limit vs. Sell Stop Order: What's the Difference?* Online. Investopedia. Dostupné z: <https://www.investopedia.com/ask/answers/050515/what-difference-between-buy-limit-and-sell-stop-order.asp>. [cit. 2024-03-22].

MCGLEENON, Brian, 2023. *What is an order book?* Online. The Block. Dostupné z: <https://www.theblock.co/learn/251469/what-is-an-order-book>. [cit. 2024-04-29].

MCOINS, 2023. *Decentralizované burzy (DEX) - Počátky a nebezpečí*. Online. MCoins. Dostupné z: <https://www.mcoins.cz/decentralizovane-burzy-dex-pocatky-nebezpeci>. [cit. 2024-05-07].

NARAYANAN, Arvind; BONNEAU, Joseph; EDWARD, Felten; MILLER, Andrew a GOLDFEDER, Steven, 2016. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

NORVILL, R.; VUJICIC, D.; BUNTINX, J.B.; WU, Y.; WOOD, G. et al., 2021. *Blockchain for Business: How It Works and Creates Value*. Online. Wiley Online Library. Dostupné z: <https://onlinelibrary.wiley.com/doi/10.1002/9781119711063.ch4>. [cit. 2024-03-24].

ONG, Bobby; LEE, Teik Ming; LI, Guo a CHUEN, David LEE Kuo, 2015. *Evaluating the Potential of Alternative Cryptocurrencies*. Online. In: Handbook of Digital Currency. Elsevier, s. 81-135. ISBN 9780128021170. Dostupné z: <https://doi.org/10.1016/B978-0-12-802117-0.00005-9>. [cit. 2024-01-24].

ONOMYPROTOCOL, 2021. *Order Book Trading — How It Works*. Online. Medium. Dostupné z: <https://medium.com/onomy-protocol/order-book-trading-how-it-works-806633ae92ba>. [cit. 2024-04-29].

PRICEWATERHOUSECOOPERS, ©2024. *Demystifying cryptocurrency and digital assets*. Online. PwC. Dostupné z: <https://www.pwc.com/us/en/tech-effect/emerging-tech/understanding-cryptocurrency-digital-assets.html>. [cit. 2024-03-24].

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

PYROMALLIS, Christo a SZABO, Claudia, 2019. *Modelling and Analysis of Adaptability and Emergent Behavior in a Cryptocurrency Market*. Online. IEEE Xplore. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/9002829>. [cit. 2024-03-01].

REIFF, Nathan, 2023. *What Are Centralized Cryptocurrency Exchanges?* Online. Investopedia. Dostupné z: <https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-exchanges/>. [cit. 2024-01-25].

REJNUŠ, Oldřich, 2014. *Finanční trhy*. 4., aktualiz. a rozš. vyd. Partners. Praha: Grada. ISBN 978-80-247-3671-6.

ROUSE, Margaret, 2023. *Impermanent Loss*. Online. Techopedia. Dostupné z: <https://www.techopedia.com/definition/impermanent-loss>. [cit. 2024-04-29].

SANTOSA, Ari Budi, 2022. *Understanding Different Types of Crypto Trading Order*. Online. Pintu Academy. Dostupné z: <https://pintu.co.id/en/academy/post/crypto-trading-order-type>. [cit. 2024-05-07].

SEHGAL, Hemal, ©2024. *The Impact of Cryptocurrency on the Tech Industry*. Online. Blockchain Technology, Mobility, AI and IoT Development Company USA, Canada. Dostupné z: <https://www.solulab.com/cryptocurrency-tech-industry-impact/>. [cit. 2024-03-27].

SEMIN, Michael, 2023. *What is AMM (Automated Market Maker) and what is the difference with CLMM (Concentrated Liquidity Market Makers)*. Online. ReHold. Dostupné z: <https://rehold.io/blog/what-is-amm-automated-market-maker-and-what-is-the-difference-with-clmm-concentrated-liquidity-market-makers>. [cit. 2024-04-29].

SERGEENKOV, Andrey, 2021. *What Is an Automated Market Maker?* Online. AMMs Explained. Dostupné z: <https://www.coindesk.com/learn/what-is-an-automated-market-maker/>. [cit. 2024-05-07].

SETH, Shobhit, 2024. *What Is Kraken? How It Works, How It Stands Out, and Issues*. Online. Investopedia. Dostupné z: <https://www.investopedia.com/tech/what-kraken/>. [cit. 2024-01-26].

SHARMA, Manoj, 2024. *Crypto.com vs. Coinbase*. Online. Investopedia. Dostupné z: <https://www.investopedia.com/crypto-com-vs-coinbase-5188428>. [cit. 2024-04-29].

SINGH, Shailey, 2023. *What is QuickSwap, and how does it work?* Online. Cointelegraph. Dostupné z: <https://cointelegraph.com/explained/what-is-quickswap-and-how-does-it-work>. [cit. 2024-01-26].

STROUKAL, Dominik a SKALICKÝ, Jan, 2021. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Třetí rozšířené vydání. Finance pro každého. Praha: Grada Publishing. ISBN 978-80-271-1043-8.

SURATKAR, Saurabh; SHIROLE, Mahesh a BHIRUD, Sunil, 2020. *Cryptocurrency Wallet: A Review*. Online. In: *4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*. IEEE, 2020, s. 1-7. ISBN 978-1-7281-6509-7. Dostupné z: <https://doi.org/10.1109/ICCCSP49186.2020.9315193>. [cit. 2024-01-25].

TAGADE, Kanishk, 2023. *Smart Contract Audit | Services*. Online. Astra Security Blog. Dostupné z: <https://www.getastra.com/blog/security-audit/smart-contract-security/>. [cit. 2024-04-29].

TAPSCOTT, Don a TAPSCOTT, Alex, 2018. *Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world*. London: Portfolio/Penguin. ISBN 978-0-241-23786-1.

TOMCZAK, Tomasz, 2022. *Crypto-assets and crypto-assets' subcategories under MiCA Regulation*. Online. Capital Markets Law Journal. roč. 17, č. 3, s. 365-382. ISSN 1750-7227. Dostupné z: <https://doi.org/10.1093/cmlj/kmac008>. [cit. 2024-04-11].

UNCHAINEDCRYPTO, 2023. *What Are Crypto Order Books And How they Work?* Online. Unchained. Dostupné z: <https://unchainedcrypto.com/crypto-order-books/>. [cit. 2024-04-29].

USHMAN, Dan, 2023. *What Is a Buy Stop Order?* Online. TrendSpider Learning Center. Dostupné z: <https://trendspider.com/learning-center/what-is-a-buy-stop-order/>. [cit. 2024-03-24].

VESELÁ, Jitka, 2019. *Investování na kapitálových trzích*. 3. vydání. Praha: Wolters Kluwer, ISBN 978-80-7598-212-4.

XIA, Pengcheng; WANG, Haoyu; ZHANG, Bowen; JI, Ru; GAO, Bingyu et al., 2020. *Characterizing cryptocurrency exchange scams*. Online. Computers & Security. roč. 98. ISSN 01674048. Dostupné z: <https://doi.org/10.1016/j.cose.2020.101993>. [cit. 2024-01-25].

XU, Xiwei; Ingo WEBER a Mark STAPLES, ©2019. *Architecture for Blockchain Applications* [online]. Cham: Springer International Publishing. [vid. 2024-01-24]. ISBN 978-3-030-03034-6. Dostupné z: doi:[10.1007/978-3-030-03035-3](https://doi.org/10.1007/978-3-030-03035-3)

YANO, Makoto; Chris DAI; Kenichi MASUDA a Yoshio KISHIMOTO, 2020. *Blockchain and Crypto Currency: Building a High Quality Marketplace for Crypto Data*. Singapore: Springer Singapore. Economics, Law, and Institutions in Asia Pacific. ISBN 9789811533754.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

FIAT Měna s nuceným oběhem

Dapps Decentralizované aplikace

ETH Nativní kryptoaktivum Ethera

BTC Bitcoin

CEX Centralizovaná kryptoměnová burza

DEX Decentralizovaná kryptoměnová burza

MIT Market-If-Touched

KYC Know-Your-Customer

BIC Podnikatelské identifikační číslo

SEZNAM OBRÁZKŮ

Obrázek 1. Příklad Blockchainu (Xu et al., ©2019).....	13
Obrázek 2. Hardwarová peněženka Ledger Nano X (Zdroj: Ledger.com, ©2024).	15
Obrázek 3. Příklad order booku (Zdroj: Vlastní zpracování).	34
Obrázek 4. Postup přidání prostředků (Zdroj: Vlastní zpracování).....	35
Obrázek 5. Postup přidání a výběru prostředků (Zdroj: Vlastní zpracování).	35
Obrázek 6. Coinbase advanced (Zdroj: Vlastní zpracování).	36
Obrázek 7. Ukázka nákupu kryptoaktiva (Zdroj: Vlastní zpracování).	37
Obrázek 8. Ukázka prodeje kryptoaktiva (Zdroj: Vlastní zpracování).	37
Obrázek 9. Ukázka transakčních poplatků stran Taker a Maker (Zdroj: Reiff, 2023).	38
Obrázek 10. Ukázka poplatku v uživatelském rozhraní Coinbase (Zdroj: Vlastní zpracování).....	39
Obrázek 11. Ukázka poplatku v Coinbase advanced (Zdroj: Vlastní zpracování).	39
Obrázek 12. Ukázka přepnutí do aplikace UniSwap (Zdroj: Vlastní zpracování).	40
Obrázek 13. Ukázka kompatibility kryptoměnových peněženek s platformou (Zdroj: Vlastní zpracování).....	41
Obrázek 14. Ukázka SWAPU na platformě UniSwap (Zdroj: Vlastní zpracování).....	44
Obrázek 15. Ukázka zadání limitní objednávky na platformě UniSwap (Zdroj: Vlastní zpracování).....	44
Obrázek 16. Ukázka posílání kryptoaktiv (Zdroj: Vlastní zpracování).	45
Obrázek 17. Ukázka zakoupení kryptoaktiv na platformě UniSwap (Zdroj: Vlastní zpracování).....	45
Obrázek 18. Ukázka typů NFT na platformě UniSwap (Zdroj: Vlastní zpracování).	46
Obrázek 19. Ukázka přidání páru při poskytování likvidity (Zdroj: Vlastní zpracování) ...	47

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha P I: Název přílohy

PŘÍLOHA P I: NÁZEV PŘÍLOHY