Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra obchodu a financí

Diplomová práce

Decentralizované finance

Bc. Marek Navrátil

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Marek Navrátil

Podnikání a administrativa

Název práce

Decentralizované finance

Název anglicky

Decentralized finance

Cíle práce

Diplomová práce je zaměřena na decentralizované finance (zkráceně DeFi), které poskytují finanční služby na základě technologie blockchain. Hlavním cílem této práce je analýza reálné využitelnosti DeFi, predikce vývoje, posouzení potenciálu a porovnání se současnou centralizovanou formou poskytování finančních služeb. Dílčím cílem práce je analýza a komparace zvolených DeFi a CeFi kryptoměnových platforem. Práce se také bude zabývat problematikou DeFi z pohledu legislativy a regulace.

Metodika

Hlavním zdrojem informací pro diplomovou práci je studium odborné literatury a internetových zdrojů zaměřených na kryptoměny a decentralizované finance. V teoretické části se diplomová práce nejprve zabývá vznikem, historií a technologií, na které DeFi stojí. Dále jsou charakterizovány jednotlivé DeFi platformy a možnosti, které nabízejí. Na základě získaných informací, vlastních poznatků a prostudovaných informačních zdrojů je vypracována praktická část práce. V praktické části práce je předvedeno na příkladu reálné využití kryptoměn a DeFi v praxi, ve kterém budou uvedeny klady i zápory současné podoby a navrženy možná opatření. Dále je uveden modelový příklad zdanění zisků z DeFi platforem. Tyto platformy budou komparovány vzájemně mezi sebou a také s jejich centralizovanou formou. Na základě syntézy teoretických a praktických poznatků budou zpracovány závěry a naplněny stanovené cíle diplomové práce.

Doporučený rozsah práce

60-80 stran

Klíčová slova

Kryptoměny, DeFi (decentralizované finance), Blockchain, Banky, Burzy,

---

Doporučené zdroje informací

CAMPBELL, R. H. – RAMACHANDRAN A. – SANTORO J. Defi and the Future of Finance. New Jersey: Wiley, 2021, 208 s. ISBN 1119836018.

LEWIS, Antony. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them. London: Penguin Books, 2018, 432 s. ISBN 0241237866.

STROUKAL, D. – SKALICKÝ J. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada, 2018, 195 s. ISBN 978-80-271-0742-1.

TAPSCOTT, D. – TAPSCOTT, A. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World. London: Penguin Books, 2018, 432 s. ISBN 1101980141.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. Zdeněk Toušek, Ph.D.

Garantující pracoviště

Katedra obchodu a financí

Elektronicky schváleno dne 12. 10. 2022

prof. Ing. Luboš Smutka, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 12. 03. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Decentralizované finance" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____

Poděkování

Velice rád bych touto cestou poděkoval Ing. Zdeňkovi Touškovi, Ph.D. za jeho vstřícný přístup, ochotu a pomoc při vedení diplomové práce.

Decentralizované finance

Abstrakt

Tato diplomová práce se zaměřuje na oblast decentralizovaných financí, která poskytuje finanční služby na technologii blockchain. Práce se zabývá analýzou reálné využitelnosti DeFi v praxi, komparací platforem i jejich nástrojů, riziky tohoto prostředí a dalšími. Teoretická část je nejprve věnována historii, pozadí vzniku a technologii kryptoměn, což je pro práci s decentralizovanými financemi zásadní. Dále jsou charakterizovány a do detailu rozebrány vybrané decentralizované platformy, které nejlépe vystihují škálu využitelnosti DeFi. Práce se také věnuje legislativě a chystané regulaci kryptoměn spolu s jejich zabezpečením. Praktická část nejprve navrhuje ideální cestu pro vstup do DeFi a představuje jednotlivé decentralizované nástroje, které jsou analyzovány, komparovány a názorně předvedeny. Komparace probíhá i mezi jednotlivými platformami dle různých parametrů. V další části se autor zabývá daňovou problematikou kryptoměn společně s názorným příkladem zdanění kryptoměn. Poté probíhá komparace centralizované a decentralizované formy platforem, na což navazuje porovnání současného finančního systému s decentralizovaným systémem. Závěrem autor predikuje události na kryptoměnovém trhu a konkretizuje svůj pohled na zvolenou problematiku.

Klíčová slova: Kryptoměny, DeFi (decentralizované finance), Blockchain, Banky, Burzy

Decentralized finance

Abstract

This thesis focuses on the field of decentralized finance, which provides financial services using blockchain technology. It deals with the analysis of the practical applications of DeFi, including a comparison of platforms and their tools, as well as the risks associated with this environment. The theoretical part begins by examining the history and emergence of cryptocurrencies, their underlying technology, which is essential for working with decentralized finance. Next, selected decentralized platforms that best illustrate the range of applicability of DeFi are characterized and discussed in detail. The paper also explores legislation and upcoming regulation of cryptocurrencies, along with their security implications. The practical part of the thesis proposes an ideal path for entering DeFi and introduces different types of decentralized tools, which are analysed, compared, and illustrated. The comparisons are also made between platforms based on various parameters. The author also discusses cryptocurrency tax issues, along with an illustrative example of how cryptocurrency is taxed. Then, a comparison is made between centralized and decentralized forms of platforms, followed by a comparison of the current financial system with the decentralized system. Finally, the author predicts future events in the cryptocurrency market and concretizes their view on the chosen aspect of DeFi.

Keywords: Cryptocurrency, DeFi (decentralized finance), Blockchain, Banks, Exchanges

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam použitých zkratek

1. Úvod

Decentralizované finance (dále jen „DeFi“) jsou pojem, který je stále relativně nový a mezi širokou veřejností poměrně neznámý. Jedná se o kryptoměnové odvětví, které nabízí inovativní přístup k finančním službám na základě technologie blockchain a chytrých kontraktů. Zatímco kryptoměny, ze kterých DeFi vychází, si své „místo“ ve světě financí již před nějakou dobou našly a jedná se o poměrně zavedenou formu investice, DeFi na větší rozšíření mezi veřejností stále čeká.

Bitcoin jako první kryptoměna přinesl před více než 13 lety decentralizaci platebního sytému. DeFi však tuto myšlenku rozvíjí dále a nabízí decentralizované nástroje v různých formách spoření, půjček, obchodování a jiných, bez nutnosti existence třetí strany. Protože toto odvětví není ovládáno žádnou centralizovanou formou, dává svým uživatelům svobodu a skutečnou kontrolu nad jejich financemi. S tím se však také pojí řada úskalí a bezpečnostních rizik, která budou v diplomové práci názorně předvedeny.

V diplomové práci budou představeny nejvýznamnější a nejvyužívanější decentralizované platformy, jejich možnosti, nabízené služby a vše, co jsou schopné svým uživatelům nabídnout. Bude ukázáno, že kryptoměnový svět neslouží pouze ke spekulaci, ale že v sobě skrývá v sobě mnohem větší potenciál. V práci bude také předvedeno, jak nabízených decentralizovaných nástrojů využít a na co si dát při práci s nimi pozor. Kromě samotného DeFi budou zastoupeny i centralizované formy kryptoměnového financování (zkráceně „CeFi) a také stále významnější problematika regulace a legislativy. Opomenout nelze ani daňové hledisko, které je mnohými opomíjeno.

Kryptoměny jsou společností včetně investorů již poměrně akceptované, přestože se názory na tuto problematiku stále velmi různí. Za dobu své existence však dokázaly, že se nejedná pouze o přechodnou módu. Decentralizované finance potenciál kryptoměn dále rozvíjejí a je možné, že se s nimi bude v dohledné budoucnosti široká veřejnost setkávat stále častěji.

Tato diplomová práce nabídne čtenáři celkový ucelený pohled na svět decentralizovaných financí a poskytne cenné informace i závěry pro všechny, kteří se zajímají o kryptoměny a budoucnost finančního sektoru.

2. Cíl práce a metodika

2.1 Cíl práce

Tato diplomová práce je zaměřena na decentralizované finance (zkráceně DeFi), které poskytují finanční služby na základě technologie blockchain a chytrých kontraktů. Hlavním cílem této práce je vyhodnocení reálné využitelnosti DeFi, predikce vývoje, posouzení potenciálu a porovnání se současnou centralizovanou formou poskytování finančních služeb na základě technického a ekonomického rozboru. Dílčím cílem práce je porovnání a rozbor zvolených DeFi a CeFi kryptoměnových platforem, které poskytují finanční služby. Práce se také bude zabývat problematikou DeFi z pohledu legislativy i regulace. Dále se práce bude také věnovat daňové problematice, která je často opomíjena, stejně jako zabezpečení držených kryptoměn.

2.2 Metodika

Hlavním zdrojem informací pro diplomovou práci je studium odborné literatury a internetových zdrojů zaměřených na kryptoměny i decentralizované finance. Použity jsou převážně relevantní internetové zdroje z důvodu neustálých změn v tomto odvětví, které dovolují použití literatury pouze v omezené míře. V teoretické části se diplomová práce nejprve zabývá vznikem, historií a technologií, na které DeFi stojí. Dále jsou charakterizovány a analyzovány jednotlivé DeFi platformy a možnosti, které nabízejí. Uvedené platformy jsou vybrány na základě dlouholetých osobních zkušeností autora v kryptoměnové oblasti. Na základě získaných informací, vlastních poznatků a prostudovaných informačních zdrojů je dále vypracována praktická část diplomové práce. V praktické části práce je předvedeno na příkladech reálné využití kryptoměn a DeFi v praxi, ve kterém budou uvedeny klady i zápory současné podoby a navržena možná opatření. Dále je uveden modelový příklad zdanění zisků z DeFi platforem. Tyto platformy budou komparovány vzájemně mezi sebou a také s jejich centralizovanou formou. Na základě syntézy teoretických a praktických poznatků budou zpracovány závěry a naplněny stanovené cíle diplomové práce.

3. Teoretická východiska

3.1 Počátek DeFi

Když vypukla ekonomická krize v roce 2008, přišel Bitcoin s myšlenkou decentralizovaného platebního systému, který nebude ovládaný žádnou centrální autoritou. Tuto ideu následující rok Satoshi Nakamoto zrealizoval a dal tak základ celému odvětví. Bitcoin byl jakousi první „vlaštovkou" decentralizovaných financí, přesto se mezi DeFi neřadí. První skutečné projekty decentralizovaných financí přišly až o mnoho let později.

Po mnoha pokusech dalších kryptoměn, tzv. „altcoinů", založených na technologii Bitcoinu, které se chtěli svézt na jeho úspěchu, vznikla kryptoměna Ethereum. Bitcoin přinesl decentralizovaný platební systém, Ethereum však chtělo jít dále a vytvořit platformu, na jejímž základu budou moci vývojáři vytvářet decentralizované aplikace. Vitalik Buterin tak vytvořil platformu, která je dodnes výchozí a nejrozšířenější pro většinu decentralizovaných aplikací a projektů.

Díky tzv. „smart contracts" mohly vznikat nové decentralizované aplikace (zkráceně „dApps"). Smart kontrakty jsou programy vytvořené v blockchainu, které tvoří základní stavební kámen DeFi.[1] Prvním z těchto „dApps" byl protokol Maker DAO, který také přinesl první „stablecoin". Tento protokol umožnil svým uživatelům půjčovat si finanční prostředky pomocí stablecoinu Dai. Maker tak poprvé přinesl alternativu při získávání cizích finančních prostředků a odpadla nutnost splňovat podmínky nastavené tradiční bankou. Jediné, co musí uživatel splňovat, je výše kolaterálu ve formě Etherea. Maker je dodnes jedním z nejdůležitějších a nejpoužívanějších DeFi projektů.[2]

V průběhu dalších let takto vznikly další decentralizované aplikace, které rozvíjely potenciál této kategorie. Mnoho z nich vzniklo v „nechvalně" proslulém období „ICO" v roce 2017. ICO znamená zkráceně Initial Coin Offering a je založené na podobném principu jako IPO u akcií. V tomto období sháněly nové projekty peníze pomocí decentralizovaného „fundraisingu". Tehdejší investoři investovali velké sumy v očekávání

[1] HARVEY, Campbell R., Ashwin RAMACHANDRAN a Joey SANTORO. *DeFi and the Future of Finance*. New Jersey: Wiley, 2021, s. 12. ISBN 9781119836018.

[2] *What Is MakerDAO And How It Works* [online]. New York: 101 Blockchains, 2022 [cit. 2022-12-27]. Dostupné z: https://101blockchains.com/makerdao/

vysokého zhodnocení. Některé projekty tak vybraly i částky v řádech miliard korun. Mnoho z těchto projektů však neuspělo a mnoho bylo vytvořeno pouze za účelem zisku. Byly vybrány vysoké částky na vytvořený „whitepaper“, tedy dokument, kde je popsán princip, smysl a fungování projektu, a poté již nedodaly výsledný produkt.[3] Přesto v tomto období vznikly mnohé projekty, které úspěšně fungují dodnes a řadí se mezi nejlepší DeFi protokoly.

Největší vzestup DeFi přišel v létě roku 2020, toto období se nazývá „DeFi Summer“. Jedním z katalyzátorů byla platforma Compound, která dovolila kromě půjčování stablecoinů za kolaterál také půjčovat své kryptoměny ostatním uživatelům a získávat tak úroky z půjčky. Další novou funkcí bylo poskytování likvidity, tzv. „liquidity providing“. Uživatelé začali být odměňováni úroky ve formě COMP tokenů za poskytnutí likvidity uživatele do protokolu. To následně vyústilo v rapidní nárůst počtu uživatelů této služby a zvýšení povědomí o DeFi mezi ostatní uživatele kryptoměn. Na tento úspěch kromě jiných navázal automatizovaný protokol Yearn Finance, který umožnil svým uživatelům maximalizovat svůj zisk pomocí automatického prohledávání DeFi trhu a vkládáním poskytnuté likvidity do různých protokolů. Díky tomu uživatel již nemusel vybírat mezi mnoha decentralizovanými aplikacemi, platforma mu automaticky vybrala z trhu možnost s největším „yieldem“ (úrokem). Tato funkce přilákala mnoho nových uživatelů díky své uživatelské přístupnosti.[4]

Po vydání a úspěchu těchto DeFi vznikly i ostatní protokoly na podobné bázi, které původní myšlenku buď vylepšovaly, nebo pouze kopírovaly. Na základě těchto událostí si DeFi upevnilo svojí pozici mezi kryptoměnami a její komunitou. Onen název „Defi Summer“ si toto období vysloužilo díky rapidnímu nárůstu v aktivitě, popularitě a množství finančních prostředků v decentralizovaných protokolech.

Decentralizované finance v této podobě by nikdy nemohly vzniknout bez původních kryptoměn, které jim dodnes poskytují technický základ. Nejdříve je tak nutné porozumět

---

[3] STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky / Dominik Stroukal, Jan Skalický*. Praha: Grada, 2018, s. 165-166. ISBN 9788027107421.

[4] *History Of DeFi – From Inception To 2021 And Beyond* [online]. Finematics, c2022 [cit. 2022-12-27]. Dostupné z: https://finematics.com/history-of-defi-explained/

základům fungování a technologiím, na nichž DeFi staví, a rozvíjí tak dále potenciál kryptoměn.

3.2 Bitcoin

Obrázek 1: Bitcoin logo

Zdroj: (Wikimedia, 2014)

První pokusy o digitální měny vznikly již v 80. a 90. letech minulého století. Byly to pokusy funkční, avšak nebyly úspěšné. Nedočkaly se širšího využití, protože příliš předběhly svou dobu a tehdejší technologie ještě nebyly na takové úrovni. První skutečnou kryptoměnou se stal až Bitcoin, který převzal některé principy od svých předchůdců, jako například známý „Proof of Work" systém, na kterém dodnes funguje většina kryptoměn.[5]

3.2.1 Historie

Příchod nové moderní kryptoměny již byl dobře načasovaný. V roce 2008, kdy probíhala tehdejší ekonomická krize, zaregistroval Satoshi Nakamoto doménu bitcoin.org a vydal dokument „Bitcoin: A Peer-to-Peer Electronic Cash System".[6] V tomto „white paperu" jsou popsány principy a fungování decentralizovaného platebního sytému s názvem Bitcoin. Dnes je tento whitepaper považován za definující moment počátku krytoměn. Oficiálně byla síť Bitcoinu spuštěna následující rok vytěžením prvního bloku v blockchainu.

[5] REIFF, Nathan. Dere There Cryptocurrencies Before Bitcoin?. Investopedia [online]. New York: Dotdash, 2019 [cit. 2022-11-07]. Dostupné z: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/

[6] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. 2008 [cit. 2021-01-13]. Dostupné z: https://bitcoin.org/bitcoin.pdf

Tento první blok se nazývá „Genesis“ a je v něm ukryta informace, která naráží na fakt, že je zde nová alternativa a lidé již nejsou odkázáni pouze na klasický bankovní systém.[7]

Dodnes není známo, kdo se pod pseudonymem Satoshi Nakamoto skrýval. Jelikož práce na kryptoměně byly dokončeny za pouhé 2 roky, je velmi pravděpodobné, že se za tímto jménem skrýval tým lidí vystupující pod jedním jménem.[8]

Bitcoin za svou historii zažil několik velkých býčích trhů, kdy jeho cena pokaždé raketově vzrostla, čímž se pokaždé dostal více do povědomí veřejnosti. Děje se tomu tak každé 4 roky, vždy po půlení bitcoinu. Tento proces zvaný „halving“ je jedním ze zásadních faktorů, které ovlivňují cenu jednotky BTC. Snižuje se při něm odměna těžařů a rychlost těžby, poptávka při tom roste. Výsledkem tohoto procesu je rostoucí cena. V tomto období se Bitcoin běžně dostává do titulků médií, načež po určité době, která je vždy obtížně určitelná, tato „investiční bublina“ splaskne, a na několik let začne medvědí trh. Takto při posledním býčím trhu v roce 2021 překročila cena 1 BTC psychologickou hranici 1 milionu korun. Investiční bublina následně opět splaskla, jak tomu vždy bývá, a cena se v době psaní této práce pohybuje na třetinové hodnotě oproti loňskému maximu.[9]

3.2.2 Charakteristika

Bitcoin je open source decentralizovaná peer-to-peer platební síť, která funguje na základě své komunity. Bitcoinová komunita se rozděluje na těžaře a koncové uživatele. Uživatelé platí při používání Bitcoinu transakční poplatky, které následně jdou těžařům, kteří schvalují a ověřují transakce od uživatelů. Těžaři také dostávají odměnu za svůj poskytnutý výpočetní výkon při samotné těžbě bloků.

---

[7] LEWIS, Antony. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them. Miami: Mango, 2018, s. 200. ISBN 978-1633538009.

[8] STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky / Dominik Stroukal, Jan Skalický*. Praha: Grada, 2018, s. 165-166. ISBN 9788027107421.

[9] *Bitcoin* [online]. CoinMarketCap, c2022 [cit. 2022-11-13]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/

Bitcoin je založen na asymetrické kryptografii, kde figurují dva typy klíčů. Soukromý klíč, který slouží k dešifrování dat, a klíč veřejný, který data šifruje a je přístupný všem uživatelům. Veřejný klíč představuje bitcoinovou adresu, pomocí které může kdokoliv nahlédnou do historie transakcí oné adresy a jejího zůstatku. Je tak zajištěna transparentnost a používá se pro přijímání Bitcoinu. K pohybům na adrese je však nutné mít soukromý klíč, který slouží jako přístup k adrese, a ten by měl znát pouze její vlastník. Bezpečnost zajišťuje hashovací funkce SHA-256, která šifruje hodnoty tak, že nelze rekonstruovat původní data, a dodnes nebyla prolomena.[10]

3.2.3 Blockchain

Blockchain je decentralizovaná distribuovaná databáze, kterou si lze představit jako řetězec po sobě jdoucích bloků. Tyto bloky jsou v síti těženy těžaři, které pro tuto těžbu poskytují svůj výpočetní výkon. Blockchain slouží jako účetní kniha, ve které jsou všechny záznamy transparentní a zpětně dohledatelné.

Uživateli je nejdříve vytvořena transakce, kterou těžař ověřuje, a následně vytvoří blok, který tuto transakci potvrdí a zařadí do blockchainu. Nový blok v blockchainu se tvoří přibližně každých 10 minut. Těžaři jsou ke své činnosti motivování odměnou za vytěžený blok. Tato odměna se snižuje s každým půlením Bitcoinu. Půlení nastává pokaždé, když se vytěží 210 000 bloků, což vychází přibližně na 4 roky. Nyní tato odměna činí 6,25 BTC.[11] Těžba je však dnes již natolik náročná, že jsou těžaři seskupeni v tzv. „poolech“, kde využívají svůj společný výpočetní výkon a odměnu si poměrově mezi sebou rozdělí.

Tento systém založený na těžbě je již zmíněný „Proof of Work“. Vyžaduje velmi vysoký výpočetní výkon a velké množství spotřebované elektrické energie. Dnes již existují efektivnější a více šetrné metody, které nejsou tak energeticky náročné.

---

[10] DOLEŽAL, Martin a Matouš VONDRÁK. *K čemu u kryptoměn slouží privátní a veřejný klíč?* [online]. Praha: FINEX MEDIA, 2022 [cit. 2022-11-13]. Dostupné z: https://finex.cz/kryptomeny-privatni-verejne-klice/

[11] CONWAY, Luke. What Is Bitcoin Halving? Definition, How It Works, Why It Matters [online]. New York: DotDash, 2022 [cit. 2022-11-13]. Dostupné z: https://www.investopedia.com/bitcoin-halving-4843769

Blockchain také řeší problém tzv. „dvojité platby“, kdy by se někdo pokusil tu samou částku „utratit“ ve více transakcích. Je tomu dosaženo díky ověřování transakcí těžaři, kdy je do bloku zařazena pouze transakce s vyšším počtem ověření. Aby někdo převzal kontrolu nad blockchainem a mohl tak provést dvojitou útratu, musel by disponovat více jak 51 % výpočetní síly celého blockchainu.[12] To je však v dnešní době vzhledem k náročnosti celého procesu těžby již nemožné.

3.3 Ethereum

Obrázek 2: Logo Ethereum

Zdroj: (Wikimedia, 2020)

Ethereum je dlouhodobě po Bitcoinu druhá největší kryptoměna z pohledu tržní kapitalizace i rozšířenosti. Na jeho platformě dnes stojí většina ostatních kryptoměn díky jeho revoluční technologii chytrých kontraktů. Ethereum je oproti Bitcoinu kryptoměna s mnohem větší využitelností než jako pouhé platidlo. Je proto označována jako kryptoměna druhé generace. Její technologie poskytuje základ tisícům ostatních kryptoměn a také decentralizovaných projektů, které fungují díky jeho síti a využívají ether při používání chytrých kontraktů.

[12] STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky / Dominik Stroukal, Jan Skalický. 2018, s. 172. ISBN 9788027107421.

3.3.1 Historie

Počátky Etherea se datují již k roku 2014, kdy byl zveřejněn whitepaper, ve kterém byly popsány základní principy a fungování této kryptoměny. Autorem tohoto dokumentu je původem kanadsko-ruský programátor Vitalik Buterin, který v dokumentu popisuje blockchain, umožňující nejen decentralizovaný platební systém, ale i decentralizované aplikace s různými způsoby využití.[13] K projektu se postupem času přidali další lidé, kteří pomohli myšlenku projektu více formalizovat. Jedním z nich byl i Gavin Wood, který vydal tzv. „yellowpaper". Jde o dokument, kde je popsán technický základ Etherea s názvem „Ethereum Virtual Machine".

Po vybrání finančních prostředků potřebných k vývoji bylo Ethereum spuštěno v červenci roku 2015 vytěžením svého prvního bloku.[14] Rychle se stalo populární mezi kryptoměnovou komunitou. Rok po spuštění však Ethereum postihl hackerský útok, po kterém bylo nutné udělat určité změny v protokolu, což zapříčinilo rozdělení jeho blockchainu do dvou. Vzniklo Ethereum a Ethereum Classic, přičemž Ethereum s novými změnami a početnější komunitou bylo výrazně úspěšnější a již od roku 2018 se drží jako druhá kryptoměna z pohledu tržní kapitalizace.[15] Ethereum se tak stalo lídrem „altcoinů" neboli alternativních kryptoměn, což je kategorie, do které se řadí všechny kryptoměny kromě Bitcoinu.

V roce 2020 začal očekávaný přechod z PoW schvalovacího mechanismu známého již od Bitcoinu na moderní „Proof of Stake" (dále PoS) mechanismus. Ethereum tak začalo fungovat paralelně na dvou blockchainech s cílem postupně přejít na „Proof of Stake" mechanismus. Důvodem k přechodu bylo mimo zvýšení rychlosti a efektivity platformy také řešení problému s inflační mírou Etherea tak, aby dosáhlo správné míry mezi inflací a deflací

---

[13] BUTERIN, Vitalik. *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.* [online]. 2014 [cit. 2022-11-18]. Dostupné z: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

[14] ANTONOPOULOS, Andreas M. a Gavin WOOD. Mastering Ethereum: Building Smart Contracts and DApps. Sebastopol: O'Reilly Media, 2018, s. 46-47. ISBN 978-1491971949.

[15] *Ethereum* [online]. CoinMarketCap, c2022 [cit. 2022-11-18]. Dostupné z: https://coinmarketcap.com/currencies/ethereum/

tokenu například pomocí snižování počtu „coinů“ v oběhu pomocí tzv. „burningu“ neboli pálení mincí.

3.3.2 Charakteristika

Ethereum dříve fungovalo podobně jako Bitcoin na mechanismu „Proof of Work“, kdy byly těžaři těženy jednotlivé bloky a ty se následně řadily do blockchainu. To se změnilo v září roku 2022, kdy Ethereum po dlouhém přechodu přešlo na nový mechanismus konsenzu PoS, který již nefunguje na bázi „neekologické“ těžby, ale je založen na systému „validátorů“. Ti ověřují jednotlivé transakce a bloky, k čemuž již není nutné vlastnit nákladné „těžební“ vybavení. Ověřování probíhá tak, že se validátoři shodují na validitě transakce ve třech po sobě jdoucích fázích. Platí, že čím více validátorů v systému je, tím je celý blockchain bezpečnější, respektive decentralizovanější.

Tento systém je bezpečnější a o více jak 99 % méně energeticky náročný než předchozí PoW.[16] Validátoři jsou odměňováni z transakčních poplatků v podobě ETH za svůj „staking“, čili uzamknutí určitého počtu tokenů do protokolu za účelem jejich úročení. Do sítě musí uzamknout minimálně 32 kusů ETH, aby se mohli stát validátory. Podobně jako u těžby se však validátoři mohou „sloučit“ do poolů, kde se jejich odměna poměrově rozdělí na základě jejich vložených prostředků.

„Ethereum 2.0“, jak se mezi komunitou „upgradu“ na PoS mechanismus říká, přineslo také tříštění blockchainu, díky čemuž daný validátor nemusí stahovat celý blockchain, ale stará se pouze o „svůj střípek“, což ve výsledků znamená větší propustnost transakcí a rychlost celé sítě.[17]

Ethereum dále nabízí možnost tokenizace, na platformě lze tokenizovat téměř cokoliv. V současnosti je již běžné, že lidé tokenizují umění, hudbu, různé komodity, ale i jiné kryptoměny. Vytvořit vlastní token na platformě Etherea je jednoduché a slouží k tomu

---

[16] DUGGAN, Wayne a Michael ADAMS. *What Is Ethereum 2.0? Understanding The Ethereum Merge* [online]. New Jersey: Forbes Media, c2022 [cit. 2022-11-18]. Dostupné z: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-ethereum-2-merge/

[17] *THE ETHEREUM VISION: A digital future on a global scale* [online]. Ethereum Foundation, 2022 [cit. 2022-12-27]. Dostupné z: https://ethereum.org/en/upgrades/vision/

ERC-20 tokenový standard. Populární jsou také tzv. nezaměnitelné tokeny neboli NFT, které zaručují vlastnictví daného majetku, kdy token nelze zaměnit s jiným díky jeho jedinečnosti.

3.3.3 Smart contracts

Základem Etherea jsou chytré kontrakty. Ty fungují spolu s decentralizovanými aplikacemi díky „Ethereum Virtual Machine“ (zkráceně EVM). Jde o virtuální a decentralizovaný stroj, díky kterému na platformě fungují nejen chytré kontrakty, ale i jakýkoliv jiný kód. Kdokoli může na platformě programovat v kompatibilním programovacím jazyce a vytvářet vlastní chytré kontrakty nebo cokoliv jiného. Toho bylo dosaženo díky tzv. „Turingovské úplnosti“, která zaručuje univerzálnost platformy.[18]

Chytré kontrakty fungují jako software, který zajistí a vynutí provedení daného kontraktu díky kryptografickému kódu při splnění nastavených podmínek. Lze si je představit jako digitální smlouvy. Díky nim je možné transparentně vykonávat rozličné úkony bez nutnosti zásahu třetích stran. Platformou je přitom garantováno jejich provedení při splnění podmínek. Celý smluvní proces je jednodušší, efektivnější, bezpečnější a odpadají při něm náklady na případné zprostředkovatele. Přináší tak mnoho výhod oproti smlouvám v klasické podobě. To, že chytré kontrakty fungují na blockchainu také znamená, že jsou transparentní, zpětně dohledatelné a nezaměnitelné.

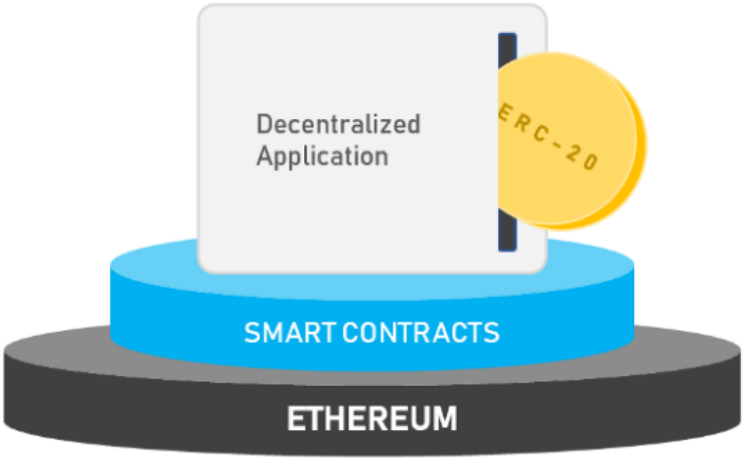
Nacházejí se však v právní šedé zóně, jelikož jejich právní vymahatelnost je obtížná a současné právo s chytrými kontrakty zatím nepočítá.[19] Jejich hlavní využití proto nyní najdeme převážně v decentralizovaných financích.

Na chytrých kontraktech také stojí decentralizované aplikace, důležitá součást DeFi. V EVM jsou tyto chytré kontrakty vykonány při splnění daných podmínek, přičemž každý může díky transparentnosti blockchainu nahlédnout do zdrojového kódu. Největší využití

[18] *Ethereum Virtual Machine (EVM)* [online]. CoinMarketCap, c2022 [cit. 2022-11-18]. Dostupné z: https://coinmarketcap.com/alexandria/glossary/ethereum-virtual-machine-evm

[19] KUDLÁČEK, Patrik. *Smart contracts. Co jsou to smart contracts neboli chytré kontrakty? K čemu jsou a jak fungují?* [online]. Praha: FINEX MEDIA, 2019 [cit. 2022-11-18]. Dostupné z: https://finex.cz/chytre-kontrakty-smart-contracts-co-jsou-a-jak-funguji/

dApps našlo v decentralizovaných burzách (zkráceně DEX), platformách určených k poskytování likvidity a půjčovacích „lending“ platformách.



Obrázek 3: Vizualizace platformy Ethereum

Zdroj: (Towards Data Science, 2018)

3.3.4 Stablecoin

Ethereum přineslo také další, dnes již běžnou a hojně používanou součást kryptoměn, tzv. stablecoiny. To jsou kryptoměny, které na rozdíl od ostatních vysoce volatilních kryptoměn mají stabilní kurz, což kombinují s výhodami klasických kryptoměn. Díky tomu fungují mnohem lépe jako prostředník směny. Stablecoin většinou kopíruje kurz „fiat“ měny, nejčastěji to bývá americký dolar, ale používá se i vazba na jiné měny, jako je například euro, libra, yen atd. Stablecoin dnes představuje určitého prostředníka jak mezi kryptoměnami samotnými, tak mezi kryptoměnami a fiat měnou.

Nejširší využití mají stablecoiny při obchodování na burzách, kde fungují jako určité „bezpečné“ místo pro investory, kteří si do stablecoinů ukládají zisky, nebo je dále využívají k obchodování díky nízkým poplatkům a snadné převoditelnosti mezi jednotlivými burzami. Při obchodování na kryptoměnové burze se dnes využívají nejčastěji stablecoinové páry s ostatními kryptoměnami, protože se jedná o nejrychlejší a nejlevnější řešení. Při využití stablecoinu jako prostředníka mezi jinými kryptoměnami, a tedy i jinými blockchainy lze často významně ušetřit na transakčních poplatcích.

Velmi často se stablecoiny využívají i v DeFi, kde se používají pro různé účely. Jedním z nich jsou půjčky, kde uživatel dostane po vložení zálohy (kolaterálu) půjčku v podobě stablecoinu. Dalším velmi oblíbeným využitím je poskytování likvidity, kdy uživatel za svou „službu“ dostává úrok. Díky své stabilní hodnotě je tento způsob využití mnohem bezpečnější než u klasických kryptoměn.[20] V některých zemích, kde krachuje místní ekonomika, je stablecoin dokonce využíván některými obyvateli jako uchovatel hodnoty.

Rozlišuje se několik druhů stablecoinů. Největší podíl na trhu mají centralizované stablecoiny, za kterými stojí firmy, držící na svých účtech peněžní prostředky ve fiat měně poměrem 1:1 k emitovaným stablecoinům. Právě centralizace je však největším bezpečnostním rizikem u tohoto typu, uživatel musí důvěřovat firmě, která za stablecoinem stojí. Mezi tento druh se řadí nejpoužívanější stablecoiny USDT, USDC a BUSD. Dalším typem jsou kontroverzní algoritmické stablecoiny. Ty fungují tím způsobem, že algoritmus udržuje stálou cenu na základě aktuální nabídky a poptávky. Tyto stablecoiny byly do letošního roku velice oblíbené díky svým vysokým úrokům, které poskytovaly při tzv. „yield farmingu“. Bohužel mnoho z nich zaniklo kvůli nestabilnímu systému algoritmu a mnoho investorů tak kompletně přišlo o své vložené finanční prostředky. Stablecoiny dále rozlišujeme na kolateralizované, kdy jsou kryté kolaterálem z kryptoměn. Typickým příkladem je historicky první stablecoin Dai vyvinutý na decentralizované platformě Maker DAO. Kryptoměny jsou vysoce volatilní, proto se do kolaterálu uzamyká větší množství kryptoměny, aby se udržela stabilita, a tento systém je tak relativně bezpečný. Posledním druhem jsou centralizované stablecoiny kryté komoditami, například zlatem a drahými kovy. Typický zástupce je například PAX Gold, tento druh však není příliš využíván.[21]

[20] HAYES, Adam. *Stablecoins: Definition, How They Work, and Types* [online]. New York: Dotdash Meredith, 2022 [cit. 2022-11-18]. Dostupné z: https://www.investopedia.com/terms/s/stablecoin.asp

[21] MIKULÁŠEK, Filip a Matouš VONDRÁK. *Co jsou to stablecoiny? Můžeme se spolehnout, že stabilně udrží svoji cenu?* [online]. Praha: FINEX MEDIA, c2022 [cit. 2022-11-19]. Dostupné z: https://finex.cz/co-jsou-stablecoiny-kryptomeny/

3.4 DeFi

V současné době existuje již více jak 200 DeFi projektů, přičemž naprostá většina z nich funguje na platformě Etherea.[22] Tyto blockchainové decentralizované aplikace si v průběhu posledních let mezi uživateli kryptoměn získaly vysokou popularitu. Je to především díky tomu, že pro získáni půjčky nebo využití jiné finanční služby není třeba žádných osobních dokladů a transakce se uskutečňují téměř okamžitě. Vše probíhá decentralizovaně mimo státní systémy. Toho mohou například využít i obyvatelé rozvojových zemí, kteří nemají přístup k bankovním službám.

Mezi hlavní devizy DeFi náleží kontrola uživatele nad svými finančními prostředky. Kromě obchodování s kryptoměnami je DeFi hojně používáno k získání úroků při poskytování likvidity do platformy. Jedná se o určitý druh „spořících účtů“ s vysokým úrokem. Zároveň je však nutné počítat s určitým rizikem, protože čím vyšší úrokové sazby platforma nabízí, tím více je uživatel vystaven riziku. Při případné chybě v chytrém kontraktu nebo zneužití této chyby hackery nemají uživatelé žádnou právní ochranu v podobě třetí strany. Je tak nutné při výběru DeFi platformy postupovat velmi obezřetně.

V době psaní této práce se pohybovala celková hodnota uzamčených finančních prostředků (označováno jako TVL neboli „Total Value Locked“) v DeFi protokolech kolem 70 miliard dolarů. To je pokles o více jak 75 % oproti vrcholu, kterého tento sektor dosáhl ke konci roku 2021. Jedná se o důsledek medvědího trhu, který postihl celý kryptoměnový sektor.[23]

Decentralizované finanční aplikace mají ze všech možných dosavadních využití blockchainové technologie zatím největší úspěch. Jedná se o další evoluci kryptoměn, která přináší alternativu a větší svobodu v rozhodování nad svými financemi. Je tak možné, že právě DeFi se v budoucnu stane lídrem v širším využití kryptoměn veřejností.

---

[22] *Ethereum DeFi Ecosystem* [online]. Los Angeles [cit. 2022-11-19]. Dostupné z: https://defiprime.com/ethereum

[23] *Total Value Locked* [online]. DefiLlama, 2022 [cit. 2022-12-27]. Dostupné z: https://defillama.com/

3.4.1 Compound

Obrázek 4: Compound logo

Zdroj: (PNG All, 2021)

Compound byla historicky jednou z prvních DeFi platforem a dodnes se řadí mezi nejvyužívanější na trhu. Patří mezi přední „lending" platformy, kde si uživatelé půjčují, nebo sami vypůjčují kryptoměny. Jak její název napovídá, umožňuje svým uživatelům vydělávat složenými úroky na svých kryptoměnách. Compound také jako první DeFi nabídlo svým uživatelům možnost kryptoměny půjčovat ostatním uživatelům pomocí chytrých kontraktů a zpopularizovalo tak toto odvětví mezi širší veřejností.

3.4.1.1 Historie

Počátky této platformy byly centralizované. Compound byl spuštěn v roce 2018 kalifornskou společností Compound Labs. Zpočátku neměla platforma žádný „governance" token, pomocí kterého by komunita tuto platformu řídila a vše tak bylo prováděno ze strany vývojářů Compound Labs. Aby se platforma mohla stát decentralizovanou, jak bylo původně zamýšleno, byl vydán v roce 2020 governance token COMP, který předal kontrolu nad platformou mezi její uživatele.[24] Compound je od té doby zcela decentralizovaný, firma Compound Labs již nemá žádné pravomoci a platforma je tak ovládána držiteli tokenu COMP, kteří o návrzích o změnách mezi sebou hlasují. Compound se tedy stal „DAO" neboli decentralizovanou autonomní organizací.

[24] *Compound: Overview & History* [online]. New York: Messari, 2020 [cit. 2022-12-19]. Dostupné z: https://messari.io/asset/compound/profile

Do začátku získala společnost finanční prostředky ve výši 33,2 milionu dolarů od několika významných „venture capital“ firem, z nichž jedna byla napojena na největší kryptoměnovou směnárnu Coinbase.[25] Firma tak pro tento projekt sehnala do začátku dostatečný obnos, který byl ještě podpořen „crowdfundingem“.

Compound v té době přišel s novým a v tehdy začínajícím DeFi odvětví revolučním modelem půjček, který dovolil svým uživatelům dosahovat příjmu z poskytování likvidity stejně tak snadno, jako si z protokolu půjčit. V současné době je Compound platforma již ve svojí třetí verzi, jež se více zaměřila na uživatelskou přívětivost, která v této oblasti tak často chybí.

3.4.1.2 Charakteristika

Platforma umožňuje uživatelům vkládat prostředky do poolu, ze kterého si půjčující mohou půjčit za předpokladu, že složí dostatečnou zálohu (kolaterál). Tím, že uživatel vloží své kryptoměny do tohoto poolu, dostává do své „peněženky“ úroky, které jsou získány od dlužníků platformy. Půjčky zde nemají žádnou dobu splatnosti, jelikož uživatelé interagují s celým poolem, tedy s celou platformou a půjčující tedy nenese žádné riziko nesplacení.

Uživatelé, kteří si z platformy půjčují kryptoměny, musí svou půjčku „přeplatit“ tím, že vloží do poolu kolaterál ve vyšší hodnotě, než je jejich půjčka. Pokud dlužník do platformy nevrátí požadované množství kryptoměn, jeho kolaterál mu chytrý kontrakt vezme. Stejně tak, pokud hodnota vypůjčeného aktiva stoupne nad hodnotu dlužníkova kolaterálu, může být jeho pozice zlikvidována. Vše funguje pomocí chytrých kontraktů, které určují úroky a podmínky těchto DeFi půjček, stejně tak, jako plynulý chod tohoto „lendingu“, který díky tomu může fungovat bez nutnosti třetí strany nebo jiné centrální autority.

Při vložení kryptoměn do platformy se jejich podoba převede na tzv. cTokeny, nativní tokeny, ve kterých jsou zabudované chytré kontrakty, díky nimž fungují procesy na Compound platformě. Pokaždé, když uživatel vloží kryptoměny na svůj účet v Compound,

[25] *What is cryptocurrency Compound (COMP) and how does it work?* [online]. Tallinn: Kriptomat, c2022 [cit. 2022-12-19]. Dostupné z: https://kriptomat.io/cryptocurrencies/compound/what-is-compound/

jsou tyto prostředky převedeny na cTokeny, se kterými následně provádí příslušné operace. Následné odměny se odvíjí dle množství držených cTokenů v peněžence a také dle proměnlivé úrokové míry. Ta se odvíjí podle dostupného množství daného aktiva. Čím větší likviditou dané aktivum disponuje, tím menší úrokovou míru bude generovat a naopak. Odměny jsou následně vypláceny v COMP tokenech.[26]

Pro správu celé platformy slouží governance token COMP, který lze získat využíváním platformy nebo přímo koupí na některé z burz, kde je token zalistován. Čím více těchto tokenů uživatelé drží, tím větší hlasovací právo mají, a mohou tak hlasovat o rozhodnutích ohledně budoucího směřování platformy. K předložení návrhu musí mít na svojí adrese uživatel delegováno minimálně jedno procento z celkového počtu COMP tokenů, tzn. minimálně 100 000 COMP tokenů. Jeden COMP token je přitom roven hodnotě jednoho hlasu. Uživatelé mohou své hlasy delegovat jiným uživatelům a podpořit je tak v jejich návrhu. Na schválení či zamítnutí návrhu na změnu v protokolu jsou vždy tři dny. Pokud je návrh schválen, následují další dva dny, kdy může kdokoliv vyjádřit nesouhlas předtím, než návrh vejde v platnost.[27] Těchto COMP tokenů bude celkem 10 milionů. Distribuce tokenu probíhá každých 15 vteřin, tedy pokaždé, když je vytvořen nový blok Etherea: 4,2 milionů bude celkově distribuováno mezi uživatele protokolu, dalších 2,4 milionu je vyhrazeno pro akcionáře zakládající firmy Compound Labs, Inc. a 2,2 milionu pro zakládající a stávající vývojářský tým Compound. Zbytek tokenů bude rozdělen mezi budoucí členy týmu Compound a komunitu platformy.[28]

---

[26] *Compound* [online]. New York: Gemini Trust Company, c2022 [cit. 2022-12-19]. Dostupné z: https://www.gemini.com/cryptopedia/what-is-compound-and-how-does-it-work#section-how-compound-crypto-liquidity-pools-work

[27] LESHNER, Robert. *Compound Governance: Steps towards complete decentralization* [online]. San Francisco: Medium, 2020 [cit. 2022-12-19]. Dostupné z: https://medium.com/compound-finance/compound-governance-5531f524cf68

[28] LESHNER, Robert. *Compound Governance is Live* [online]. San Francisco: Medium, 2020 [cit. 2022-12-19]. Dostupné z: https://medium.com/compound-finance/compound-governance-decentralized-b18659f811e0

3.4.1.3 Využití

Hlavním důvodem k využití této DeFi platformy je možnost okamžitého alternativního příjmu pomocí DeFi půjček u půjčujících a možnosti rychlé a snadné půjčky na straně potencionálních dlužníků platformy. Uživatelé mohou v současné době poskytovat likviditu celkem až u 5 různých kryptoměn, po jejichž vložení získají jejich alternativní podobu ve formě cTokenů. U každé kryptoměny je přitom nastavena jiná úroková míra a poměr kolaterálu. Uživatel může kdykoliv vyměnit své cTokeny za kryptoměny v „klasické" formě a k tomu úroky, které získal jejich poskytnutím do protokolu. Vlastností těchto cTokenů je také to, že se jedná o ERC-20 tokeny, a jako takové tedy mohou být obchodovány a využívány i v jiných decentralizovaných aplikacích využívající Ethereum jako svoji platformu. Je tak možné s nimi získávat úroky i na jiných DeFi platformách, než pouze na Compound.[29]

Poskytování likvidity je obdobné jako vkládání peněz do banky na spořící účet. V tomto případě poskytovatel dostává úroky za vložené kryptoměny v té kryptoměně, kterou vložil. Pokud si uživatel zvolí vklad ve stablecoinu USDC, bude mu vyplácen úrok v USDC.

Kromě poskytování likvidity se Compound také hojně používá k půjčování kryptoměn. Při tomto procesu je nutné si hlídat hodnotu dané kryptoměny, aby nepřesáhla jeho vložený kolaterál. Pokud se hodnota kolaterálu výrazněji propadne, je pozice zlikvidována, tedy automaticky prodána, aby splatila půjčku. Dlužníkovi zůstane půjčená částka, ovšem o kolaterál, který přesahuje hodnotu půjčky, dlužník přijde. Na platformě je možné zároveň poskytovat likviditu, ale také si půjčit. V tom případě slouží vklad jako kolaterál, který je nutno hlídat a na kterém se tvoří úrok.

[29] *What is Compound?* [online]. New York: Decrypt Media, 2020 [cit. 2022-12-19]. Dostupné z: https://decrypt.co/resources/compound-defi-ethereum-explained-guide-how-to

3.4.2 Uniswap

Obrázek 5: Uniswap logo

Zdroj: (Wikimedia, 2020)

Uniswap již od svého vzniku až do dnešních dnů platí za lídra v oblasti decentralizovaných burz. Byla to jedna z prvních burz tohoto druhu a jedna z prvních využívající ke svému chodu tzv. Automated Market Maker neboli „AMM“ na blockchainu. Dodnes je také nejvyužívanější a jde o lídra v oblasti DeFi. Své popularity tato burza dosáhla především díky velice obsáhlé nabídce tokenů, z nichž mnoho nelze obchodovat na jiném místě. Jde o průkopníka ve své kategorii a díky jejímu úspěchu vzniklo mnoho dalších decentralizovaných burz na podobné bázi.

3.4.2.1 Historie

Uniswap vznikl v roce 2018, kdy byla tato DEX (decentralizovaná burza) založena Adamem Hayesem. Ten se inspiroval u zakladatele Etherea, Vitalika Buterina, který rok po spuštění sítě Etherea zveřejnil příspěvek o AMM na sociální síti Reddit.[30] To následně autora této burzy inspirovalo ke stvoření Uniswapu.

[30] *Let's run on-chain decentralized exchanges the way we run prediction markets* [online]. Reddit, 2016 [cit. 2022-11-27]. Dostupné z: https://www.reddit.com/r/ethereum/comments/55m04x/lets_run_onchain_decentralized_exchanges_the_way/

V té době byla drtivá většina kryptoměnových burz centralizovaná, což byl opak původní myšlenky kryptoměn. Adam Hayes proto využil příležitosti a po získání potřebných financí k dokončení projektu byl Uniswap spuštěn v listopadu roku 2018. Velmi rychle získal potřebnou likviditu a začal vykazovat vysoký objem transakcí. Již v roce 2020 se Uniswap stal čtvrtou největší kryptoměnovou burzou na světě.[31]

Po spuštění platformy se začaly objevovat další podobné burzy založené na stejném principu, což spolu s dalšími DeFi produkty vyústilo ve velký „boom" DeFi v létě roku 2020, nazvaném jako „DeFi Summer". Uniswap v té době již byla největší decentralizovanou burzou a stála v čele vzestupu DeFi.

Uniswap prošel celkem třemi hlavními fázemi vývoje. V září roku 2020 byla spuštěna nová verze Uniswap V2, která přinesla vlastní governance token UNI. Díky němu mohou uživatelé rozhodovat o vývoji a budoucnosti této platformy. Každý uživatel burzy, který s ní interagoval před tímto termínem, byl odměněn formou tzv. „airdropu", kdy každý obdržel do své peněženky na burze 400 tokenů UNI. V době airdropu se pohybovala hodnota těchto 400 tokenů zhruba kolem 1 400 $. Na svém vrcholu v květnu roku 2021 to však již bylo více jak 17 000 $.[32]

V únoru 2021 objem této decentralizované burzy poprvé přesáhl hodnotu 100 miliard dolarů, a nedlouho poté vyšla aktuální verze Uniswap V3, která přinesla další vylepšení, z čehož hlavní je podpora NFT a efektivnější AMM.

Po každé velké aktualizaci se změnilo označení platformy, naposled z Uniswap V2 na Uniswap V3.

---

[31] KHARIF, Olga. *DeFi Boom Makes Uniswap Most Sought-After Crypto Exchange* [online]. London: Bloomberg, 2020 [cit. 2022-11-27]. Dostupné z: https://www.bloomberg.com/news/articles/2020-10-16/defi-boom-makes-uniswap-most-sought-after-crypto-exchange

[32] *Uniswap* [online]. CoinMarketCap, c2022 [cit. 2022-11-27]. Dostupné z: https://coinmarketcap.com/currencies/uniswap/

3.4.2.2 Charakteristika

Všechny transakce jsou zde řízeny pomocí AMM. Ten funguje na bázi tzv. „liquidity poolů“ a algoritmů, které nastavují cenu tokenu. Burza využívající tento mechanismus ke svému chodu musí disponovat dostatečnou likviditou tokenů. Tento systém fungující pomocí chytrých kontraktů je odlišný od klasických centralizovaných kryptoměnových burz, které využívají knihu příkazů, a burza zde funguje jako prostředník, který si bere za směnu poplatky. Hypoteticky si lze AMM systém představit jako všechny příkazy z knihy příkazů smíchané v jednom velkém poolu, kde deterministický algoritmus určuje cenu dle stanovených pravidel. Typicky dle „střední“ ceny kryptoměny na trhu. Uniswap využívá svojí vlastní verzi AMM, tato varianta se nazývá „Constant Product Market Maker Model“ a její hlavní vlastnost je, že si vždy najde likviditu. Díky tomuto systému se nemůže stát, že by v některém poolu nebyla likvidita a transakci nešlo provést, bez ohledu na to, o jak velkou transakci se jedná. Dosáhne toho tak, že při nedostatečné likviditě navýší cenu tokenu, někdy až k nereálným částkám. Tento systém je proto vhodný spíše pro menší obchodní transakce, protože velké transakce, které berou likviditu z poolů, se zde nevyplatí.[33]

Burza je založena na poskytování likvidity ERC-20 tokenům, což jsou tokeny na platformě Etherea. Díky tomu je možné vytvořit jakýkoliv obchodní pár ERC-20 tokenů. Při obchodní transakci uživatel vloží stablecoin (typicky USDT) do liquidity poolu, a z něj si vezme odpovídající množství tokenů, které chtěl nakoupit. V liquidity poolu tak musí být vždy dostatek tokenů, aby se obchod uskutečnil. Burza je tedy závislá na poskytovatelích likvidity, kteří dostávají za uskutečněné transakce poplatky. Poplatek při transakci jde také do sítě Etherea, jelikož se vše odehrává na jeho platformě.

Uniswap také představil nový přístup k distribuci governance tokenu. Při aktualizaci platformy na Uniswap V2 bylo rozděleno mezi komunitu 15 % z celkového počtu tokenů, zbytek je distribuován postupně, celkově 4 roky. Až skončí distribuce tokenů v roce 2024 a všechny budou v oběhu, na platformě bude zavedena konstantní 2 % roční inflace tokenu.[34]

---

[33] YOUNESSI, Cyrus. *Uniswap — A Unique Exchange* [online]. San Francisco: Medium, 2018 [cit. 2022-11-27]. Dostupné z: https://medium.com/scalar-capital/uniswap-a-unique-exchange-f4ef44f807bf

[34] *Introducing UNI* [online]. Uniswap Labs, 2020 [cit. 2022-11-27]. Dostupné z: https://uniswap.org/blog/uni

Tím se zajistí motivace investorů, aby dále poskytovali likviditu na platformě a jejich token tak neztrácel na hodnotě. Zajistí se tak i budoucí fungování burzy, protože poskytování likvidity od uživatelů je pro její fungování nezbytné.

3.4.2.3 Využití

Uniswap nabízí svým uživatelům vícero funkcí. Tou základní, běžnou funkcí, je klasická směna kryptoměn neboli tzv. swap. Při něm lze na Uniswapu vyměnit jakýkoliv ERC-20 token, pokud jeho liquidity pool disponuje dostatečnou likviditou. Uživatel si přitom může nastavit maximální možnou míru akceptace změny ceny při transakci, tzv. „slippage".

Další funkcí je „liquidity farming" v liquidity poolech. Tato funkce již vyžaduje od uživatelů větší technickou znalost. Běžně na decentralizovaných burzách funguje poskytování likvidity tím způsobem, že investoři vloží kryptoměny do těchto poolů v poměru 50 ku 50, aby byly kryptoměny rozloženy rovnoměrně po celém intervalu své cenové hladiny. Uniswap ve verzi V3 však přišel s tzv. koncentrovanou likviditou, díky které již kryptoměnami není nutné pokrývat celý interval, ale vybrat si jen jeden specifický, který je reálný. V praxi to znamená, že nastavíme určitý interval, mimo který se likvidita poskytovat nebude. Pokud se cena zvýší nad tento interval, uživatel nedostane žádný příjem. Naopak, pokud se cena bude pohybovat ve zvoleném intervalu, uživatel dostane mnohem větší odměnu a zvýší tak efektivitu svých vložených kryptoměn. Poměr zvoleného páru kryptoměn je určen podle toho, jak si uživatel interval nastaví.[35]

Uživatelé platformy mohou dále vytvářet nové páry tokenů a vytvořit tak na platformě nový trh s vybranými tokeny, pokud jim poskytnou likviditu.

[35] *DeFi Insight: Concentrated liquidity on Uniswap V3* [online]. San Francisco: Medium, 2021 [cit. 2022-11-27]. Dostupné z: https://itsa-global.medium.com/defi-insight-concentrated-liquidity-on-uniswap-v3-9dce4e67c3e9

3.4.3 Nexus Mutual

Obrázek 6: Logo Nexus Mutual

Zdroj: (CoinMarketCap, 2022)

Nexus Mutual je DeFi platforma postavená na Ethereu, zaměřená na decentralizované pojištění chytrých kontraktů. S touto myšlenkou přišla jako první a vyplnila tak velice důležitou díru na trhu. Prostředí decentralizovaných financí v současné podobě není příliš bezpečné, zejména pro méně zkušené uživatele. Pojištění jejich vkladů může zvýšit důvěru v DeFi a přiblížit tím tento sektor více veřejnosti. Mimo ochrany proti chybám v chytrých kontraktech Nexus Mutual také nabízí možnost příjmu z vyplacených pojistných událostí ze společného poolu.

3.4.3.1 Historie

Společnost Nexus Mutual byla založena v roce 2017 Australanem Hugh Karpem na popud stále více se množících případů zneužití chytrých kontraktů a využívání chyb hackery v těchto kontraktech. Cílem je zamezit škodám, jako například při známém DAO útoku na Ethereum, kdy bylo zcizeno více jak 3,5 milionu ETH.[36] Samotný projekt byl spuštěn v květnu roku 2019.

Hugh Karp využil své dlouholeté zkušenosti z pojišťovacího prostředí k tomu, aby pojištění bylo zaměřeno více na subjekty využívající produkt, a ne na maximalizaci zisku, jak je normou u současných pojišťovacích firem. To je možné díky technologii blockchainu a chytrých kontraktů. Kromě svého zakladatele má společnost Nexus Mutual dalších 14

[36] *Nexus Mutual* [online]. Claymont: Golden, c2022 [cit. 2022-12-25]. Dostupné z: https://golden.com/wiki/Nexus_Mutual-GZ5KXPP

zaměstnanců včetně dozorčí rady. Dozorčí rada je kontroverzním prvkem v této oblasti, jelikož se jedná o centralizovaný prvek, má však velmi omezené pravomoci. Dle vyjádření týmu projektu se jedná o nutný prvek v tomto sektoru, který v případě potřeby pomůže například odhalit podvodné pojistné nároky, nebo zasáhnout v nouzovém případě. Mohou také vyloučit členy (uživatele) z platformy a „pálit“ tokeny. Pokud s členy dozorčí rady nebudou uživatelé platformy spokojeni, mohou je kdykoli pomocí hlasování odvolat. Jedná se o experty v oboru pojišťovnictví, práva, regulace a bezpečnosti chytrých kontraktů.

Společnost zpočátku nabízela jediný produkt, a to pojistku proti zemětřesení. Záhy se však přeorientovala na pojištění rizik plynoucí z kryptoměn. Do budoucna má platforma v plánu přidat i další produkty, které se již nebudou týkat pouze kryptoměnového sektoru, ale chtějí nabízet i produkty, jako například pojištění proti přírodním katastrofám a další. V kryptoměnovém sektoru chce Nexus Mutual rozšířit pojistné krytí i na kryptoměnové peněženky.[37]

3.4.3.2 Charakteristika

Hlavní myšlenka tohoto projektu spočívá v kolektivním diverzifikování rizika. V dřívějších dobách lidé sdružovali v komunitách své zásoby, aby byli připraveni na nenadálé události. Nexus Mutual staví na podobném principu, kdy jeho uživatelé sdružují svá aktiva do poolu, ze kterého jsou vypláceny případné škodné události. Nejedná se tedy o klasickou formu pojištění, uživatelé této platformy mezi sebou „sdílejí“ riziko s využitím blockchainu a chytrých kontraktů. Tento model by však na rozdíl od klasických pojišťoven měl být více zaměřen na „spravedlnost“ vůči jeho uživatelům, protože platforma není zaměřená na zisk, ale na společnou ochranu proti útokům v DeFi.[38]

---

[37] SAWINYH, Nick. *Nexus Mutual - Smart Contract Insurance. Interview with founder.* [online]. Los Angeles: DeFi Prime, 2019 [cit. 2022-12-25]. Dostupné z: https://defiprime.com/nexus-mutual

[38] KELLY, Liam. *DeFi Review: What Is Nexus Mutual? Introduction to NXM* [online]. New York: Crypto Briefing, 2020 [cit. 2022-12-27]. Dostupné z: https://cryptobriefing.com/defi-review-what-is-nexus-mutual-introduction-nxm/

Nativní token platformy se nazývá NXM. Vlastníci těchto tokenů vlastní všechen přebytek vygenerovaný z nákupů pojištění. Pojistný produkt je naceněn s přebytečnou marží, tento přebytek je vlastněn všemi členy poolu a zůstává vně poolu. Když má daný pool přebytečné prostředky, cena NXM se zvýší a jeho členové mohou vyměnit své NXM za ETH. V případě, že fond potřebuje více finančních prostředků, cena NXM se sníží, aby podpořila poskytnutí finančních prostředků do daného poolu. Tuto hladina sleduje tzv. „MCR level" (Minimal Capital Requirement), který udává, zda mohou být všechny pojistné nároky vyplaceny či nikoliv. Sleduje tak i finanční „zdraví" celého projektu. Cena je tedy závislá na množství kapitálu ve fondu v porovnání s potřebou krytí všech pojistných událostí. Samotný token lze získat pouze na platformě Nexus Mutual a nelze ho zakoupit na jiné burze. Nelze ho také zaslat nikomu jinému než členovi Nexus Mutual. Je tomu tak z důvodu, že token a jeho cena je přímo závislá na celkovém „zdraví" této platformy.[39]

K tomu, aby se uživatelé mohli připojit do poolu, musí zaplatit poplatek ve výši 0,002 ETH a vyplnit KYC dotazník, podobně jako na centralizovaných burzách, aby bylo možné ověřit jejich totožnost. Přestože se jedná o DeFi projekt, stále se jedná o legálně registrovanou společnost ve Velké Británii.

Členové platformy, jak se nazývají její uživatelé, jsou vyzváni při každé pojistné události, aby hlasovali, zda je nárok na pojistné krytí legitimní a zda má být pojistka vyplacena. Jsou tak zodpovědní za posouzení rizika u těchto událostí. Pokud se v hlasování shodnou s většinou, platforma je odmění NXM tokeny. Když hlasují proti většině, jejich tokeny budou na určitou dobu v poolu uzamknuty. Pokud se někteří pokusí plnit pojistné nároky, které jasně nesplňují pravidla pro pojistný nárok, mohou jim být jejich NXM tokeny odejmuty a „spáleny". Díky tomu, že je Nexus Mutual legálně registrovanou společností, mají všichni členové této platformy svá práva podložená právními dohodami.

Token NXM zajišťuje členství, odměňuje uživatele za jeho držení a jeho vlastníci mají hlasovací práva k řízení platformy Nexus Mutual. Kromě hlasování o vyplácení pojistek může také každý člen předložit návrh o změnách v protokolu. Po předložení daný návrh schvaluje dozorčí rada, která i určuje výši odměny v NXM tokenech, která bude následně

[39] KARP, Hugh a Reinis MELBARDIS. *NEXUS MUTUAL: A peer-to-peer discretionary mutual on the Ethereum blockchain.* [online]. London: Nexus Mutual, 2019 [cit. 2022-12-25]. Dostupné z: https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf

rozdělena mezi hlasující členy. Váha daného hlasu přitom závisí na množství NXM tokenů, které člen vloží při hlasování.[40]

3.4.3.3 Využití

Nexus Mutual nabízí v současné době produkt „Smart Contract Cover“, který chrání proti případným chybám v chytrých kontraktech a proti útokům na DeFi platformy. Prostřednictvím chytrých kontraktů se často realizují transakce v hodnotách milionů, někdy i miliard dolarů, a vzhledem k jejich komplexnosti je pojištění proti rizikům s nimi spojených důležité. V prostředí chytrých kontraktů nejsou neobvyklé hackerské útoky, chybné kódy v peněženkách nebo jiných decentralizovaných aplikacích, a spolu s rostoucí popularitou DeFi tato rizika úměrně rostou.

Cena pojistného krytí je závislá na členech nazvaných „Risk Assessors“ neboli hodnotitelé rizik, kterými se může stát jakýkoliv člen platformy. Tito členové nejdříve zhodnotí DeFi platformu a její chytré kontrakty, zda je bezpečná. Pokud ano, tak následně vloží své NXM tokeny do poolu pojistného krytí pro danou DeFi platformu. Tyto vklady jsou využívány pro pojistné krytí v případě nutnosti, členové tak jsou nuceni pečlivě vybírat a zvažovat chytré kontrakty, kterým své tokeny poskytnou. Výsledná cena pojistného krytí je vypočtena dle poptávky, časového úseku a množství vložených NXM tokenů. Hodnotitelé jsou vypláceni podílem na poplatku zaplaceným uživatelem služby. Výplata pojistky není úměrná případné ztrátě, ale množství pojistného krytí, které je uvedeno při koupi a založeno na velikosti vložených NXM tokenů v daném poolu.

Pro pojistné krytí může být vybrána jakákoliv DeFi platforma fungující na bázi Etherea za předpokladu, že je poskytnuto do poolu dostatek NXM tokenů pro krytí pojistky.

[40] WALTERS, Steve. *Nexus Mutual Review (NXM): Defi Smart Contract Insurance* [online]. Coin Bureau, 2020 [cit. 2022-12-25]. Dostupné z: https://www.coinbureau.com/review/nexus-mutual-nxm/

Pojistné krytí může být sjednáno na dny, ale i na roky. Nejčastěji je využíváno pojištění na známé DeFi platformy, jako jsou například Compound, Uniswap, Aave, Maker a další.[41]

3.4.4 PancakeSwap

Obrázek 7: PancakeSwap logo

Zdroj: (Crypto Logos, 2020)

PancakeSwap je decentralizovaná burza založená na blockchainu BNB Chain. Tento blockchain byl založen nejpoužívanější a největší centralizovanou burzou Binance a díky této odlišnosti, která přináší určité výhody, se stala velmi rychle populární. Burza nabízí široké spektrum funkcí, které jiné DEX nenabízí. V kombinaci s nízkými poplatky na platformě se jedná o jednu z nejvyužívanějších decentralizovaných burz. PancakeSwap funguje podobně jako jeho konkurenti na Ethereum blockchainu díky liquidity poolům na principu AMM, oproti nim však přinesla nové funkce, které se v DeFi dříve neobjevily.

3.4.4.1 Historie

PancakeSwap byl založen anonymními vývojáři v září roku 2020. V té době začalo být DeFi mezi kryptoměnovou komunitou velmi oblíbené, jelikož probíhalo období známé jako „DeFi Summer“. To se zásadním způsobem projevilo na přetížení sítě Etherea, která kvůli nadměrnému zájmu v té době měla vysoké poplatky a pomalé transakce. PancakeSwap

[41] *Nexus Mutual (NXM): A Decentralized Alternative to Insurance* [online]. New York: Gemini, 2021 [cit. 2022-12-25]. Dostupné z: https://www.gemini.com/cryptopedia/nexus-mutual-blockchain-insurance-nxm-crypto

toho využil a přinesl alternativu v podobě DeFi na jiném blockchainu s modelem nízkých poplatků, díky čemuž se stal rychle populárním. Již na začátku roku 2021 byl jednou z největších decentralizovaných burz z hlediska obchodovaného objemu a celkové hodnoty uzamknutých aktiv po boku největší DEX Uniswap.[42] Burze pomohla její uživatelská přívětivost a design, který dělá její používání snazší pro nové uživatele.

V dubnu roku 2021 byla platforma aktualizována na verzi PancakeSwap V2, která přinesla nové funkce.[43] Jednou z hlavních novinek byl predikční trh, který umožnil DeFi uživatelům nově obchodovat na vzestup či pokles ceny tokenu. Dalšími funkcemi bylo například automatické reinvestování zisků ze stakingu, nový systém „pálení" tokenů pro lepší inflační politiku tokenu CAKE a možnost uživatelů rozhodovat o množství nově vydaných tokenů. Tato verze je dodnes aktuální.

3.4.4.2 Charakteristika

PancakeSwap původně vznikl oddělením od jiné DEX, a to Uniswapu, která funguje stejně jako většina ostatních DeFi služeb na Ethereum blockchainu. Přesunutím projektu na tehdy nový BSC blockchain od centralizované burzy Binance umožnilo rapidně snížit výši poplatků a zrychlit služby.

Podobně jako ostatní DEX, i PancakeSwap využívá ke svému chodu liquidity pooly na principu AMM. Uživatelé poskytují platformě likviditu odměnou za poplatky z transakcí. Vše je přitom řízeno pomocí automatického počítačového algoritmu.

Protože se platforma nachází na BSC blockchainu, tak se zde obchoduje s BEP-20 tokeny, obdobně jako na platformě Etherea s ERC-20 tokeny. Neznamená to však, že by se zde nemohly obchodovat i tokeny jiné. Jsou pouze převedeny na svojí „wrapped" podobu, díky níž lze i například ERC-20 tokeny obchodovat na BNB blockchainu. Je to možné díky

---

[42] *PancakeSwap* [online]. New York: Messari, 2021 [cit. 2022-12-12]. Dostupné z: https://messari.io/asset/PancakeSwap/profile

[43] *PancakeSwap V2 and Current Roadmap Update* [online]. BSC News, 2021 [cit. 2022-12-12]. Dostupné z: https://www.bsc.news/post/PancakeSwap-v2-and-current-roadmap-update

tzv. „cross chain“ mostu mezi blockchainy.[44] Toto řešení využívají i jiné platformy, aby se mohly na jejich blockchainu obchodovat kryptoměny založené na jiných blockchainech.

Platforma byla jako jedna z mála DeFi projektů auditována a ověřena auditorskými společnostmi.[45] Platformy se také dodnes nedotkl žádný hackerský útok, a je tak považována za poměrně bezpečnou.

3.4.4.3 Využití

Kromě klasické směny tokenů má tato decentralizovaná burza mnoho funkcí, které jiné burzy nenabízejí. Jednou z výhod směňování tokenů na této burze je, že zde lze obchodovat s tokeny, které zatím nejsou obchodovatelné na jiných centralizovaných burzách. Lze se tak poměrně výhodně dostat k zajímavým investičním příležitostem.

Jednou z nejvyužívanějších funkcí PancakeSwapu je staking kryptoměn v poolech. Tyto „Syrup Pools“, jak jsou nazvány, jsou chytré kontrakty, do kterých uživatelé vloží své tokeny. Za to pak dostávají odměnu v podobě CAKE tokenu nebo jiné kryptoměny. Typicky se vkládají tokeny CAKE, dnes však již lze uzamykat do těchto poolů více kryptoměn. Tato funkce je často využívaná novými tokeny, které se chtějí dostat do oběhu a obecného povědomí investorů. Staking se zde provádí buď automaticky (od verze V2), nebo manuálně. Liší se mezi sebou výší poplatků a také je zde možnost své tokeny do protokolu „uzamknout“ na určitou dobu odměnou za vyšší APY neboli „Annual Percentage Yield“.

Dále se zde vyskytují také klasické liquidity pooly, ve kterých může být poskytovatel likvidity odměňován částí utržených poplatků, které jiní uživatelé zaplatili. Poskytovatel likvidity dostane odměnu ve formě tokenu, který následně vloží do vybrané „farmy“. V této farmě pak typicky dostává odměnu ve formě CAKE tokenu, ale při zvolení jiné farmy může dostávat i jiné tokeny, přičemž každá farma se liší svým APY. To je v případě nových farem většinou vysoké, dosahuje až řádu stovek procent, avšak s vyšší poptávkou toto číslo

[44] DOLEŽAL, Martin. *Recenze decentralizované burzy PancakeSwap* [online]. Praha: FINEX MEDIA, c2014-2022 [cit. 2022-12-12]. Dostupné z: https://finex.cz/recenze/PancakeSwap/

[45] *Is PancakeSwap safe?* [online]. PancakeSwap, 2022 [cit. 2022-12-12]. Dostupné z: https://docs.PancakeSwap.finance/#is-PancakeSwap-safe

postupně klesá. Na platformě lze také provozovat vlastní farmy, pořádají se zde aukce farem, kde se účastníci uchází o privilegium provozování vlastní farmy likvidity.[46]

Na platformě také nalezneme trh s NFT, kde s nimi lze obchodovat. Lze zde najít oficiální kolekce vytvořené přímo vývojáři, nebo zde mohou uživatelé vytvářet své vlastní NFT kolekce, které lze dále obchodovat. Výhodou obchodování NFT na této platformě je opět BNB blockchain, díky kterému se uživatelé vyhnou vysokým poplatkům. Všechny poplatky zaplacené na platformě na NFT trhu jsou využity k „pálení" CAKE tokenů, což redukuje jeho inflační míru a posunuje více směrem k deflačnímu tokenu.[47]

Další nabízenou funkcí je loterie. Uživatelé si zakupují digitální „ticket", který obsahuje nahodilou čtyř číselnou kombinaci. K výhře stačí mít stejné dvě a více čísel, přičemž s každou další shodou se výhra zvyšuje. Do této „Win" sekce burza zahrnuje i decentralizovaný predikční trh, kde lze spekulovat na růst či pokles ceny nativního tokenu blockchainu BNB nebo tokenu CAKE.

PancakeSwap také zavedl nový termín „IFO" neboli „Initial Farm Offering". Jedná se o obdobu známého „ICO" (Initial Coin Offering), pouze s tím rozdílem, že pomáhá sehnat kapitál do nově vzniklých DeFi projektů. Platforma těmto projektům poskytne potřebnou likviditu a uživatelé jsou odměňováni v podobě CAKE tokenů za svojí poskytnutou likviditu.[48] Jedná se tak o decentralizovanou podobu fundraisingu.

---

[46] WALTERS, Steve. *PancakeSwap Review: BNB Chain's One Stop Defi Solution* [online]. Coin Bureau, 2022 [cit. 2022-12-12]. Dostupné z: https://www.coinbureau.com/review/PancakeSwap-cake/

[47] *PancakeSwap NFT Marketplace: A New Era Of NFT Trading On BSC* [online]. Chain Debrief, 2021 [cit. 2022-12-12]. Dostupné z: https://chaindebrief.com/PancakeSwap-nft-marketplace-bsc/

[48] *PancakeSwap* [online]. DayTrading, c2022 [cit. 2022-12-12]. Dostupné z: https://www.daytrading.com/PancakeSwap

3.5 Hrozby a rizika spojené s DeFi

Podstatou DeFi projektů je jejich decentralizace, a přesto, že přináší mnoho výhod, přináší také spoustu rizik a hrozeb, především pro nezkušené a začínající uživatele. Tím, že zde není prakticky žádný vládní dohled či ochrana investorů, činí z nezkušených uživatelů snadný cíl pro podvodníky. V centralizovaném systému mohou pomoci řešit problém banky, policie, soudy a jiné orgány. V decentralizovaném systému je v případě již vyskytnutého problému většinou uživatel odkázán sám na sebe, případně na ochotu dané platformy.

DeFi protokoly ve většině případů nevyžadují žádnou formu ověření uživatele, jako je například u centralizovaných burz často používané KYC, a přestože je většina kryptoměnových transakcí transparentní a adresy všech zúčastněných známé, podvodníkům se většinou daří s ukradenými prostředky uniknout. Pro DeFi také existuje velice málo legislativních požadavků. Do dnešní doby je odhadováno množství zcizených kryptoměn na přibližně 20 miliard dolarů.[49] Stejně jako u kryptoměn samotných jde stále o relativně nové začínající odvětví, které v sobě skrývá mnoho nástrah a rizik. V roce 2021 se DeFi podílelo 76 % na celkovém celosvětovém počtu hackerských útoků, které se zaměřují převážně na chyby v nových projektech a nezkušené uživatele.[50] Například u DeFi lending protokolu Alchemix umožnila chyba v kódu vybrat kolaterál ve výši 6 milionu dolarů bez splacení půjčky.[51] Stejně tak postihly tyto útoky i jiné známé platformy, některé se rozhodli své uživatele vyplatit, přestože nemuseli, a jiné zase ne.

V DeFi vzniká každým dnem více a více projektů, z čehož u naprosté většiny jde o kopie již zavedených projektů, nebo jde o zcela podvodné projekty. Rozeznat takové projekty bývá občas těžké i pro zkušené uživatele, protože některé z těchto podvodů vypadají naprosto legitimně a jejich autoři do marketingu investují vysoké částky. Před

---

[49] *Kryptoměny a DeFi: Co jsou to decentralizované finance? Jedná se o ekosystém budoucnosti?: Rizika a nevýhody DeFi – Na co si dát pozor?* [online]. Praha: FINEX MEDIA, c2014-2022 [cit. 2022-12-26]. Dostupné z: https://finex.cz/rubrika/kryptomeny/defi/

[50] *Understanding the Risks of DeFi* [online]. San Francisco: Medium, 2022 [cit. 2022-12-26]. Dostupné z: https://medium.com/akropolis/understanding-the-risks-of-defi-5e3547433135

[51] *DeFi Investment Risks* [online]. San Francisco: Coinbase, c2022 [cit. 2022-12-26]. Dostupné z: https://help.coinbase.com/en/coinbase/trading-and-funding/advanced-trade/defi-investment-risks

investicí do nového projektu je tak nutná důkladná analýza jeho whitepaperu, jeho vývojového týmu, tokenomiky (ekonomiky nativního tokenu) a celého projektu. A to jak na webových stránkách projektu, tak na online fórech, zda ostatní neevidují bezpečnostní rizika spojené s daným projektem. Kromě vlastní analýzy mohou projektu dodat důvěryhodnost různé firmy zaměřující se na audit chytrých kontraktů, jako jsou například Hacken, CertiK nebo Consensys.

Podstatou DeFi a chytrých kontraktů je open source kód, do kterého může každý nahlédnout. Tento kód bývá velice komplexní, lze s ním interagovat v mnoha směrech a může obsahovat chyby, kterých pak mohou díky otevřenosti kódu zneužít hackeři, kteří tyto chyby specificky vyhledávají. Vývojáři decentralizovaných projektů neustále posouvají hranice možného, a s tím se nevyhnutelně pojí výskyt různých chyb. Ochranou může být audit chytrých kontraktů, vypsané odměny na nalezení chyby, časté testování a pravidelná údržba decentralizovaných aplikací.

Nejenom s decentralizovanými aplikacemi, ale i s kryptoměnami obecně se pojí riziko spojené s privátními klíči, které je nutné zabezpečit. V dnešní době existuje již mnoho způsobů, jak tyto klíče bezpečně uchovat, přičemž dodnes je nejbezpečnější ukládat své kryptoměny do hardwarových offline „cold“ peněženek, jako je například francouzský Ledger nebo český Trezor. Jakmile jsou privátní klíče uchovávány v „hot“ peněženkách, tedy softwarových peněženkách připojených k internetu, je riziko mnohem větší kvůli neustálému online připojení. Tyto peněženky se používají většinou z důvodu větší uživatelské přívětivosti a také bývají většinou zdarma, na rozdíl od hardwarových peněženek.

Typickými příklady softwarových peněženek jsou desktopové aplikace, mobilní peněženky a automaticky vytvořené peněženky na burzách, kde je vysoce nedoporučené skladovat větší množství kryptoměn z důvodu vysoké náchylnosti ať už na hackerský útok nebo na stabilitu dané platformy. Z poslední doby je známý příklad burzy FTX, která zkrachovala a její uživatelé tak přišli o své finanční prostředky uložené na jejich

peněženkách, nebo platformy jako BlockFi, Celsius a další.[52] Člověk zakoupené kryptoměny nikdy nevlastní, dokud je nemá uložené mimo burzu ve své peněžence.

Pro bezpečné uložení privátních klíčů je nejlepší vlastnit hardwarová zařízení. Tato zařízení generují privátní klíče a skladují je bez připojení k internetu. Neskladují tak přímo kryptoměny, ale jejich adresy neboli klíče, které uvádějí jejich místo v blockchainu. To je ideální řešení pro uložení většího množství kryptoměn a jejich dlouhodobější držení. Pokud dojde k jejich ztrátě, tak je lze nahradit jinou hardwarovou peněženkou a pomocí tzv. „recovery seedu", který se vždy vytváří, lze klíče obnovit.

Kromě bezpečnostních rizik je také třeba počítat v tomto odvětví s ještě vyšší volatilitou tokenů, než je tomu u klasických kryptoměn. Je tomu tak především u nově vzniklých projektů a obecně projektů s nízkou tržní kapitalizací. U DeFi z toho plyne riziko především u půjček, jelikož vysoká fluktuace ceny kolaterálu může mít za následek likvidaci dané půjčky. Dále je také potřeba hlídat vytíženost platforem, v dobách nejvyššího vytížení sítě Etherea dosahovaly poplatky v rámci sítě i řádů stovek dolarů, což činilo menší transakce neproveditelnými. To by se již nemělo stát s Ethereum 2.0, které přešlo na nový PoS systém, přesto se jedná o něco, co se může stát i jiným platformám při jejich vysokém zatížení, pokud na to nebudou připraveny.

3.5.1 Impermanent loss

„Impermanent loss" neboli dočasná ztráta je riziko, které se pojí s poskytováním likvidity. Toto riziko se objevuje u decentralizovaných burz, kde je využíván model AMM. Uživatelé zde neobchodují proti druhé straně jako u centralizované burzy, ale s liquidity poolem, kde je cena kryptoměn ovlivňována právě pomocí AMM. Impermanent loss se vyskytne pokaždé, když je poskytována likvidita v liquidity poolech s výjimkou stablecoinů, které svoji hodnotu nemění, a dalších alternativ.

[52] OLINGA, Luc. *FTX, BlockFi, Voyager, Celsius: Awful Year For Crypto Investors* [online]. New York: TheStreet, 2022 [cit. 2022-12-26]. Dostupné z: https://www.thestreet.com/investing/cryptocurrency/ftx-blockfi-voyager-celsius-awful-year-for-crypto-investors

Ve většině decentralizovaných burz je poměr dvou kryptoměn v liquidity poolech 50 ku 50. S tím, jak se následně mění ceny daných kryptoměn, tak se v poolu mění i jejich množství na každé straně tak, aby byl poměr zachován. AMM tak kalibruje hodnotu tokenů a může se stát, že tokeny z „poolu" budou mít následně menší hodnotu, než by měly na volném trhu. Impermanent loss se vypočítává jako rozdíl hodnoty při pouhém držení kryptoměn a při držení v liquidity poolu. Je tak důležité pečlivě vybírat, jakému páru kryptoměn likviditu poskytovat, zkoumat jejich historické ceny a korelaci jejich cenové křivky.

Příčinou je vysoká volatilita kryptoměn a ztráta se více zvyšuje společně s rozdílem cen kryptoměn. Ztráta se dá zmírnit výběrem méně volatilních kryptoměn, jako je například Bitcoin nebo Ethereum, které jsou oproti kryptoměnám s menší tržní kapitalizací méně volatilní. Další možnost jsou stablecoiny, které by neměly ze své podstaty být volatilní vůbec. Ty však nenabízejí takový zisk a jedná se spíše o konzervativní variantu investice. Existují také liquidity pooly s wrapped tokeny, kde se vyskytuje daná kryptoměna a její wrapped verze ve stejné hodnotě. Ztráta tedy nemůže v takových případech nastat. Existují i platformy, kde poměr není striktně nastaven na 50/50 a lze do poolu vložit i více kryptoměn než dvě.[53]

Poskytovatelé likvidity jsou ke své činnosti motivování kromě „yieldu" také podílem na transakčních poplatcích. Tyto poplatky jsou přerozděleny mezi poskytovatele dle výše jejich vkladů. To je i smyslem poskytování likvidity, zisk na transakčních poplatcích by měl být vždy vyšší než impermanent loss, jinak tato činnost nemá pro investora význam. Dočasná ztráta může být dočasná, ale také permanentní. Permanentní je v případě, že poskytnuté kryptoměny budou vyjmuty z liquidity poolu dříve, než se vrátí na své původní ceny.

3.6 Legislativa v ČR, regulace a její vztah ke kryptoměnám

Znalost legislativy a pohledu českých státních orgánů na tuto problematiku je důležité pro všechny zúčastněné, tzn. pro investory, těžaře, obchodníky a uživatele

[53] VONDRÁK, Matouš. *Impermanent loss: Zásadní problém při poskytování likvidity. Co to je a jak se tomu bránit?* [online]. Praha: FINEX MEDIA, 2021 [cit. 2022-12-26]. Dostupné z: https://finex.cz/co-to-je-impermanent-loss-jak-se-branit/

kryptoměn obecně. První zmínka o kryptoměnách českými státními orgány proběhla až 5 let po uvedení kryptoměn. V průběhu let se přidávala další stanoviska společně s větším rozšířením kryptoměn a tím, jak se stále více dostávaly do obecného povědomí.

Onou první zmínkou bylo stanovisko České národní banky (dále ČNB), ve kterém bylo řečeno, že Bitcoin nepovažuje za platební službu, bezhotovostní platební prostředek nebo investiční nástroj podle zákona č. 284/2009 Sb., o platebním styku.[54] Česká národní banka bere kryptoměny jako nehmotný movitý majetek, a ne jako virtuální peníze nebo obdobu cenných papírů. V návaznosti na toto stanovisko vydalo své sdělení i Ministerstvo financí, které uvedlo, že z hlediska účetního bere kryptoměny jako zásoby „svého druhu" dle vyhlášky č. 500/2002 Sb.[55] Finanční správa uvádí, že jde o zboží, a ne o investiční produkt.

V roce 2017 vyšel Daňový balíček novely zákona o DPH, který se o kryptoměnách zmiňuje, a kde je uvedeno, že příjemce plnění je ručitelem za neodvedenou daň z tohoto plnění v případě, že úplata byla poskytnuta v kryptoměnách zcela nebo alespoň částečně. Od DPH jsou však kryptoměny při jejich obchodování osvobozeny. Evropský soudní dvůr v roce 2015 na základě soudního sporu ve Švédsku uvedl, že kryptoměny jsou oběživo a kryptoměnové transakce jsou tak osvobozeny od DPH.[56] Úpravy se kryptoměny také

[54] HAMPL, Mojmír. *Náš postoj ke kryptoměnám? Nepomáhat, nechránit, neškodit, nevodit za ruku* [online]. Praha: ČNB, 2017 [cit. 2022-12-26]. Dostupné z: https://www.cnb.cz/cs/verejnost/servis-pro-media/autorske-clanky-rozhovory-s-predstaviteli-cnb/Nas-postoj-ke-kryptomenam-Nepomahat-nechranit-neskodit-nevodit-za-ruku/

[55] *Sdělení Ministerstva financí k účtování a vykazování digitálních měn* [online]. Praha: Ministerstvo financí ČR, 2018 [cit. 2022-12-26]. Dostupné z: https://www.mfcr.cz/assets/cs/media/Ucetnictvi_2018_Sdeleni-MF-k-uctovani-a-vykazovani-digitalnich-men.pdf

[56] *ROZSUDEK SOUDNÍHO DVORA* [online]. Lucemburk: Soudní dvůr Evropské unie, 2015 [cit. 2022-12-26]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=CS

dočkaly v Zákonu o EET, kde je napsáno, že virtuální měny mají povinnost podléhat EET. To již však s koncem EET není aktuální.[57]

Ministerstvo financí ČR hledalo v minulosti způsob, jak se k této problematice stavět, proběhla tedy veřejná konzultace, po které ministerstvo vydalo dokument, ve kterém se zabývalo stávající právní úpravou a riziky spojenými s kryptoměnami. Byl také podán návrh na změnu AML (Anti-Money Laundering) zákona, který ukládá určité povinnosti všem, kteří poskytují služby spojené s virtuální měnou. Tyto povinnosti se týkají ověřování identity zákazníka, dokumentování postupů proti praní špinavých peněz a registrační povinnost do registru poskytovatelů služeb spojených s virtuálními měnami.[58]

Přestože se v současné době již jedná o více zavedenou formu investice, Česká republika dodnes nemá pro kryptoměny v zákonu o dani z příjmu žádnou úpravu, a to ani formou výjimky na rozdíl od „běžných" investic, jako jsou cenné papíry, investice do nemovitostí, do zlata a jiné. Je tak nutné vycházet z obecných právních předpisů.

V roce 2021 se člen bankovní rady ČNB Ondřej Dědek vyjádřil, že centrální banka nemá žádný důvod kryptoměny omezovat, dle jeho názoru je Bitcoin aktivum a ne měna.[59] Stanovisko ČNB se tedy v zásadě nemění a pravděpodobně ani v dohledné době měnit nebude. Regulace tak nebude přicházet ze strany ČNB, ale ze strany Evropské unie, která je v tomto ohledu již aktivní.

---

[57] *Evidence tržeb - Metodický pokyn k aplikaci zákona o evidenci tržeb* [online]. Praha: Finanční správa, 2016 [cit. 2022-12-26]. Dostupné z: https://www.etrzby.cz/assets/cs/prilohy/Metodika-k-evidenci-trzeb_v1.0.pdf

[58] WOLF, Karel. *České „kladivo na kryptoměny"? Co má změnit chystaný zákon* [online]. Praha: Internet Info, 2019 [cit. 2022-12-26]. Dostupné z: https://www.lupa.cz/clanky/ceske-kladivo-na-kryptomeny-co-ma-zmenit-chystany-zakon/

[59] KREJČÍ, Jaroslav. *Kryptoaktiva nebudeme omezovat, řekl Dědek z ČNB. O měnách ale podle banky nemůže být řeč* [online]. Praha: CZECH NEWS CENTER, 2021 [cit. 2023-03-13]. Dostupné z: https://www.e15.cz/kryptomeny/kryptoaktiva-nebudeme-omezovat-rekl-dedek-z-cnb-o-menach-ale-podle-banky-nemuze-byt-rec-1384390

3.6.1 Regulace v rámci EU

OECD neboli Organizace pro hospodářskou spolupráci a rozvoj ve své studii „Why Decentralised Finance Matters and the Policy Implications“ uvádí, že vzhledem k decentralizované povaze je velmi těžké určit odpovědnou osobu, a tak by mohly být určité odpovědnosti přeneseny na vývojáře daného projektu, nebo jeho DAO. Dále studie silně doporučuje rozvoj mezinárodní spolupráce ohledně této problematiky, jelikož z důvodu decentralizace nelze u projektů určit lokaci jejich působení a v důsledku toho ani jurisdikci.[60]

V rámci EU byla dokončena nová evropská legislativa MiCA („Markets in Crypto-Assets“), která bude regulovat celé odvětví kryptoměn. Návrh této regulace byl poprvé představen v září roku 2020 v rámci tzv. digitálního finančního balíčku. Regulace se zaměří především na poskytovatele kryptoměnových služeb (dále CASP neboli „crypto-assets service provider), kteří budou muset disponovat licencí pro poskytování těchto služeb. Whitepaper bude nově povinný pro nově vznikající tokeny a vydavatelé tokenů se budou řídit danými podmínkami k přípravě whitepaperů. Regulace se mimo jiné také dotkne stablecoinů, které budou procházet schvalovacím procesem a budou omezeni v množství emitovaných tokenů. MiCA bude také vyžadovat po velkých CASP údaje o jejich environmentální a klimatické stopě, protože těžba kryptoměn je velice energeticky náročná a například těžba Bitcoinu zanechává větší uhlíkovou stopu než celé státy.

Celé kryptoměnové odvětví bude muset plnit nové požadavky na kybernetickou bezpečnost a řídit se pravidly proti manipulaci s trhy a zneužití informací. Všech se také dotkne omezení anonymity a soukromí v důsledku nových přísnějších AML pravidel.[61] Nová regulace se ale nedotkne platforem, které jsou skutečně decentralizované a nikdo je nekontroluje. Regulace se tak bude týkat v DeFi odvětví z části centralizovaných platforem, kde lze spojit poskytování kryptoměnových služeb s konkrétní osobou, která má z dané platformy příjmy nebo ji kontroluje. Tyto osoby budou považovány za CASP. Uživatelé

[60] *Studie OECD k decentralizovaným financím (DeFi)* [online]. Praha: Ministerstvo financí ČR, 2022 [cit. 2022-12-26]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/inovace-na-financnim-trhu/aktuality/2022/studie-oecd-k-decentralizovanym-financim-46368/

[61] *Pre-recorded address by Commissioner McGuinness for event at EU Delegation in London on the EU Crypto-Asset Strategy* [online]. Brusel: European Commission, 2022 [cit. 2022-12-26]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_7529

těchto platforem, typicky poskytovatelé likvidity, tímto dotčeni nebudou za předpokladu, že nebudou záměrně shromažďovat prostředky od jiných uživatelů a následně poskytovat likviditu.[62]

Cílem této regulace je ochrana spotřebitele, zajištění finanční stability a větší bezpečnosti kryptoměnového odvětví. Samotná myšlenka regulace jde však proti základním principům kryptoměn. Kryptoměny a poskytovatelé kryptoměnových služeb budou objektem regulace a neustálé supervize. Očekává se, že regulace vejde v platnost v roce 2024.[63]

Evropská komisařka pro finance Mairead McGuinness na konferenci v Londýně ohledně chystané regulace mimo jiné uvedla, že Evropská unie momentálně pracuje na digitálním euru. Digitální euro by nemělo nahradit hotovost, ale mělo by ho pouze doplňovat. Jednalo by se o jistou obdobu stablecoinu se silně centralizovanou povahou. Jeho forma zatím není jistá, ale pravděpodobně by využívalo technologie blockchainu stejně jako stablecoiny. Jeho využití by bylo především jako platební prostředek, a ne jako investiční nástroj, na rozdíl od stablecoinů. Emitováno a kryto by přitom bylo Evropskou centrální bankou, která by této měně zajišťovala důvěryhodnost. Digitální euro je momentálně ve fázi zkoumání, tato fáze by měla být dokončena do října 2023, další etapa testování a experimentování bude probíhat přibližně tři roky.[64] Digitálního eura se tedy hned tak brzy nedočkáme.

---

[62] *Decentralized Finance a jiné peer-to-peer služby* [online]. Praha: Blockchain Legal, 2022 [cit. 2022-12-26]. Dostupné z: https://www.kryptoregulace.cz/defi/

[63] *European Council Approves Crypto Regulation Bill* [online]. New York: Dotdash Meredith, 2022 [cit. 2022-12-26]. Dostupné z: https://www.investopedia.com/eu-on-crypto-regulations-6747785

[64] *Digitální euro* [online]. Frankfurt nad Mohanem: Evropská centrální banka, c2022 [cit. 2022-12-26]. Dostupné z: https://www.ecb.europa.eu/paym/digital_euro/html/index.cs.html

4. Vlastní práce

4.1 Decentralizované platformy a jejich nástroje

4.1.1 Jak začít s DeFi?

V současné době není vstup do světa decentralizovaných financí a interakce s jejími nástroji příliš jednoduchý. Avšak u kryptoměn samotných lze již v tomto ohledu pozorovat značný posun, a to zejména v uživatelské přívětivosti, která od minulých let výrazně pokročila. Také nákup a manipulace s nimi je „začátečníkům“ mnohem přístupnější, než bývá zvykem u většiny DeFi platforem. Decentralizované finance v současné době vyžadují mnohem větší technickou znalost, a proto se stále příliš nehodí pro technicky méně zdatné uživatele, což prozatím brání většímu rozšíření tohoto odvětví. Rizika spojená s tímto odvětvím jsou veliká, a proto je také nutná dávka obezřetnosti při používání těchto nástrojů, obzvláště pokud s nimi uživatel nemá předchozí zkušenosti.

Postupem času se objevily některé nástroje a funkce decentralizovaných platforem i na centralizovaných burzách (dále CEX). Jejich jednoznačnou výhodou je snadné používání a intuitivní design. Uživatel zvyklý na klasické kryptoměnové burzy tak může tyto možnosti využívat ve svůj prospěch a se značně menším rizikem. Nevýhodou tohoto řešení jsou však typicky menší výdělky na nástrojích jako je staking kryptoměn a liquidity farming. Další výhody i nevýhody těchto přístupů budou v práci dále rozvedeny.

Při vstupu do decentralizovaných aplikací je vhodné si nejprve určit preferovanou platformu, kterou chce uživatel používat. Nejčastěji používané jsou decentralizované aplikace na bázi sítí Etherea a BNB. Pro názorný příklad bude zvolena platforma BNB kvůli větší uživatelské přívětivosti u některých decentralizovaných aplikací a nižším poplatkům. BNB je také vhodné pro menší transakce, jelikož transakční poplatky v síti Etherea neboli „gas fees“ mohou dosahovat v závislosti na vytížení sítě vysokých hodnot.

V této kapitole bude názorně uveden jeden ze způsobů, jak může nezkušený uživatel začít používat decentralizované finance, přičemž v následující kapitole budou uvedeny jednotlivé nástroje a možnosti, jak s vynaloženými prostředky v DeFi naložit. Optimálně by měl začínající uživatel začít s auditovanou DeFi platformou, která je uživatelsky přívětivá a nabízí široký sortiment služeb, které může využít a otestovat si tak možnosti

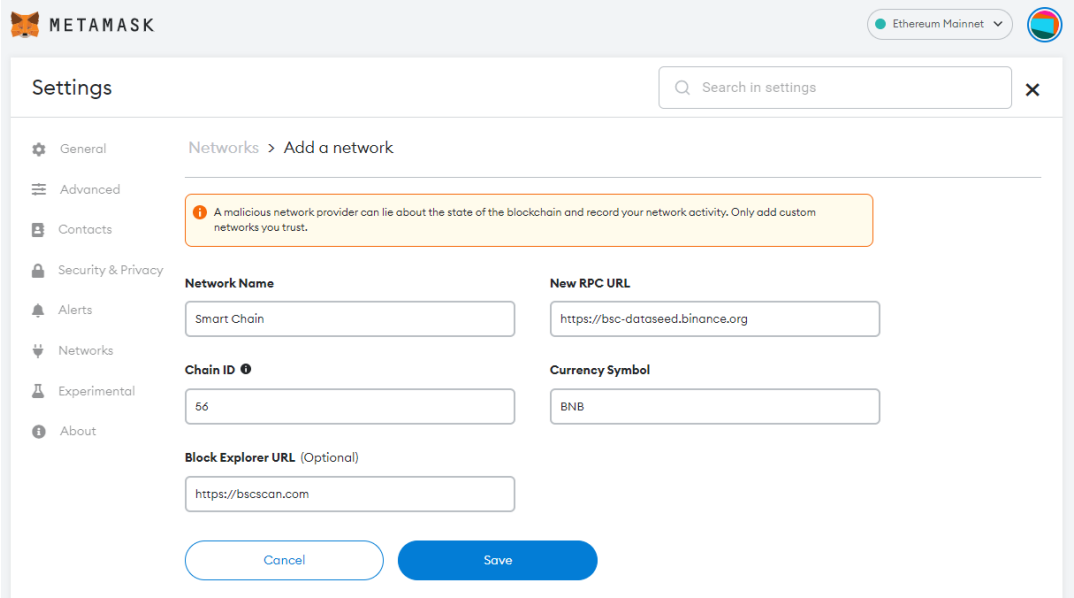
decentralizovaných financí. Takovou platformou je například již uvedený PancakeSwap, na kterém bude ukázán následující příklad.

Před vstupem do světa decentralizovaných financí je však nutné využít služeb centralizovaných kryptoměnových burz pro nákup a převod fiat měny na kryptoměnu. V CeFi, které je obecně méně rizikové a více přístupné, lze zůstat a získávat úroky na již držených kryptoměnách. Pro účely této práce však jdeme za hranici centralizovaných burz. Nejprve je nutné zvolit, jakou kryptoměnovou peněženku budeme používat. Všeobecně nejpoužívanější desktopovou peněženkou je MetaMask. Pokud bychom chtěli využívat mobilní zařízení, pak nejvhodnější volbou nejen z hlediska jednoduchosti používání by mohl být Trust Wallet.

MetaMask peněženka funguje jako bezplatné rozšíření prohlížeče. Po jejím stažení je nutné peněženku nejprve nastavit. MetaMask, stejně jako ostatní kryptoměnové peněženky, vygeneruje „seed“, který funguje jako přístupový klíč k peněžence. Tento seed lze využít k obnově peněženky v případech, jako je ztráta zařízení, krádež, či jiné. Je tedy velice důležité si seed poznamenat a uložit na bezpečné místo. Bez něj se v případě ztráty nelze k drženým kryptoměnám dostat.

Po prvotním nastavení peněženky je dále nutné nastavit MetaMask na BNB blockchain, jelikož ve výchozím nastavení je nastaven pro Ethereum platformu. K připojení na jiný než Ethereum blockchain, je nutné zadat ručně údaje daného blockchainu, které lze najít na oficiálních stránkách platformy PancakeSwap.[65] Po připojení je peněženka připravena k držení kryptoměn na bázi BNB platformy.

[65] *Connect Your Wallet to PancakeSwap* [online]. PancakeSwap, c2023 [cit. 2023-03-11]. Dostupné z: https://docs.pancakeswap.finance/get-started/connection-guide

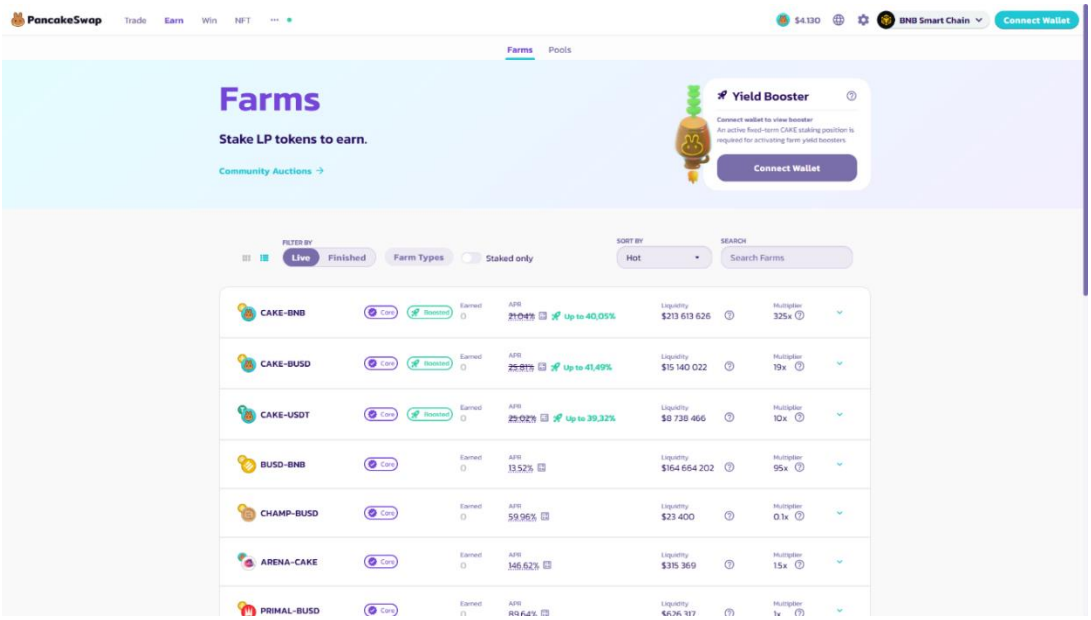


Obrázek 8: Připojení MetaMask peněženky na BNB blockchain

Zdroj: (MetaMask, 2023)

Jakmile má uživatel ve své kryptoměnové peněžence dostupné kryptoměny, musí zvolenou peněženku připojit k vybrané DeFi platformě. Propojení peněženky s platformou lze přirovnat k přihlašování se do centralizovaných služeb. Rozdílem je, že v tomto případě dotyčný nevyplňuje své osobní údaje, a jediným identifikátorem je tak jeho kryptoměnová adresa peněženky. Propojení platformy s peněženkou vyžaduje menší poplatek, stejně jako každá akce, kterou uživatel v jakékoliv kryptoměnové síti pokaždé provede. Pro pohyb tokenů v síti je nutné daný úkon „zaplatit“ menším poplatkem, aby mohla být transakce uskutečněná. Zvolená BNB platforma však vyžaduje poplatky minimální.

Následné propojení s DeFi platformou je jednoduché. Stačí kliknout na „Connect“ tlačítko a zvolit MetaMask peněženku, či jinou v případě alternativy. Peněženka se následně propojí s decentralizovanou platformou a uživatel daného DeFi může začít využívat decentralizovaných služeb pomocí kryptoměn, které má uložené na své propojené peněžence.



Obrázek 9: Prostředí DeFi platformy PancakeSwap

Zdroj: (PancakeSwap, 2023)

4.1.2 Nástroje DeFi platforem

4.1.2.1 Staking

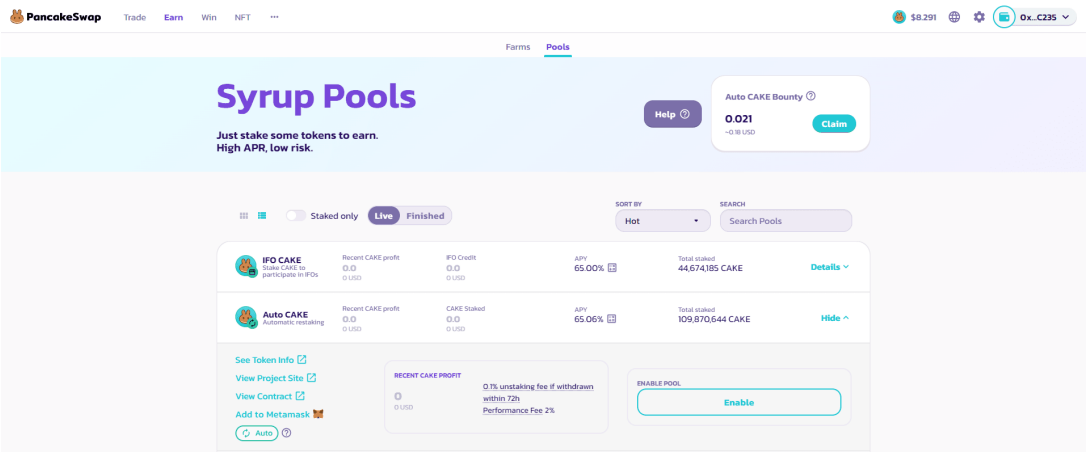
Po prvotním nastavení a propojení všeho nutného k přístupu do platformy PancakeSwap má uživatel vícero možností, jak své prostředky zhodnotit. Je nutné však upozornit, že každá akce, respektive spuštění chytrých kontraktů, má v prostředí decentralizovaných financí svou cenu. V případě PancakeSwap činí spuštění chytrých kontraktů 0,25 % z celkové hodnoty transakce. Z toho 0,17 % jde do liquidity poolů jako odměna za poskytování likvidity, 0,0225 % jde do rezervního fondu PancakeSwap, a 0,0575 % je určeno pro tzv. protiinflační „burning“ CAKE tokenu.[66] U dalších akcí na platformě je poplatek také velmi nízký, lišit se může dle typu interakce.

Při prvním kontaktu s investicemi tohoto druhu je vhodné pro seznámení se s tímto specifickým prostředím začít od „snazší“ varianty. Onou snazší variantou je staking v rozličných poolech. Tyto pooly jsou ve své podstatě chytré kontrakty, do kterých jsou

[66] *Token Swaps* [online]. PancakeSwap, c2023 [cit. 2023-03-11]. Dostupné z: https://docs.pancakeswap.finance/products/pancakeswap-exchange/trade

kolektivně vkládány kryptoměny. Při založení nových poolů bývá jejich APY neboli zisk včetně složeného úročení, velmi vysoké, až v řádu stovek procent. S přibývajícím počtem uživatelů v poolu však tato výnosnost časem klesá a většinou se ustálí v nižších desítkách procent. Například APY u největšího poolu s nativním tokenem platformy CAKE se v jeho začátcích v roce 2020 běžně pohyboval kolem 140 %. Postupem času však tato hodnota klesala, a v době psaní této práce APY CAKE poolu činí až 48,9 % v případě uzamknutí tokenů do poolu na jeden rok. Pokud uživatel zvolí flexibilní staking, pak tato výnosnost činí pouhých 2,28 %.[67] Rozdělení na flexibilní a uzamknutý staking přinesla až aktualizace na novou verzi PancakeSwap V2, do té doby byl staking pouze flexibilní s vysokým APY.

Princip stakingu je zde jednoduchý. Uživatel své kryptoměny vloží do vybraného poolu, ve kterém se úročí a jeho následná míra interakce závisí pouze na tom, jestli zvolí manuální či automatický staking. Automatický staking nebude vyžadovat jinou akci než aktivaci poolu a následné vyjmutí kryptoměn z poolu, tokeny se zde reinvestují automaticky. V případě manuálního stakingu lze zisky reinvestovat manuálně a nalézt tak vhodnější strategii. Při automatickém je také strháván výkonnostní poplatek, který výnosnost lehce snižuje.

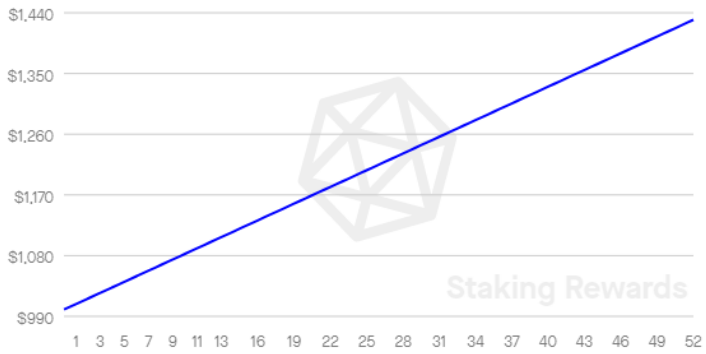


Obrázek 10: Staking na platformě PancakeSwap

Zdroj: (PancakeSwap, 2023)

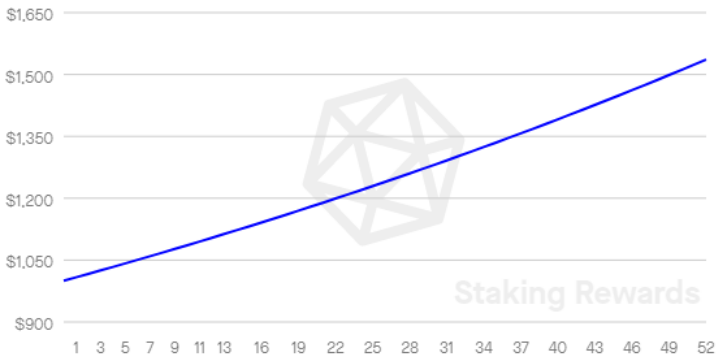
[67] *Syrup Pools* [online]. PancakeSwap, c2023 [cit. 2023-03-11]. Dostupné z: https://pancakeswap.finance/pools

Staking lze provádět i na jiných DeFi platformách. Ve většině případů se jedná o staking nativního tokenu platformy, kde se APY pohybuje v řádech desítek procent, podobně jako u CAKE tokenu. Tuto výnosnost lze vždy zvýšit správnou „compound“ strategií neboli složeným úročením. U některých platforem, jako je například PancakeSwap, lze nastavit automatický compound, který za mírný poplatek provádí neustále složené úročení místo samotného uživatele. V níže uvedených grafech lze pozorovat staking nativního tokenu platformy PancakeSwap po dobu jednoho roku ve výši 1 000 $ a vliv reinvestování zisků na výsledné APY. Na prvním grafu je vidět zhodnocení bez složeného úročení, které dosáhlo za 52 týdnů 43,07 %, respektive 430,74 $. Po využití složeného úročení však tato výnosnost stoupne na 53,8 %, tedy roční zhodnocení ve výši 538,01 $.



Graf 1: Roční staking tokenu CAKE bez reinvestování

Zdroj: (Staking Rewards, 2023)



Graf 2: Roční staking tokenu CAKE s reinvestováním

Zdroj: (Staking Rewards, 2023)

Další možností je staking stablecoinů, který má výhodu, že zde není riziko poklesu původní hodnoty investice, respektive uživatel na něm nemůže prodělat vlivem tržní volatility. Stablecoin má konstantní hodnotu a díky stakingu se tak token neustále zhodnocuje. APY u stablecoinů v DeFi stakingu se pohybuje kolem 4 % v závislosti na typu stablecoinu a použité platformě.[68]

4.1.2.2 Liquidity providing

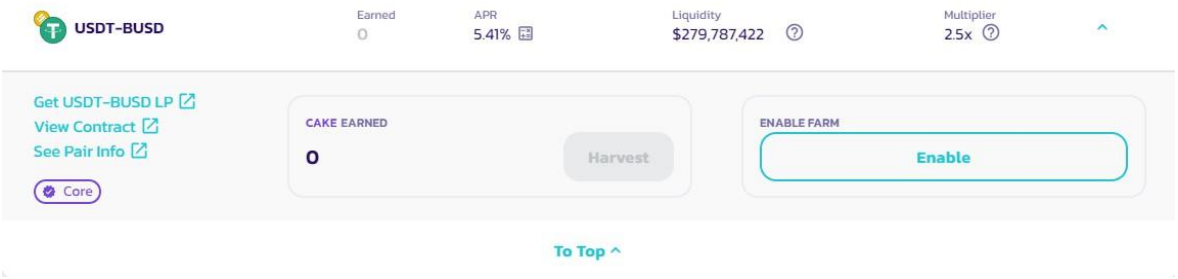
Dalším hojně využívaným DeFi nástrojem je zhodnocení držených kryptoměn pomocí liquidity poolů, respektive poskytováním likvidity. Jde o komplexnější nástroj, převážně kvůli již uvedené impermanent loss. I přes to je však poskytování likvidity jednou z nejvyužívanějších nástrojů decentralizovaných financí a lze říci, že se jedná o jednu ze základních funkcí tohoto odvětví kryptoměn. V případě PancakeSwap uživatel získává za poskytování likvidity odměnu ve formě tzv. LP tokenů, které jsou složeny z vybraného páru a které může vložit následně do poolu, kde staking probíhá. Získané LP tokeny mohou být ve formě CAKE tokenu nebo jiného, které uživatel vloží a získává více tokenů CAKE nebo jiné v závislosti na typu farmy. Uživatelé se přitom nemusí omezovat pouze na jednu farmu, ale vygenerované LP tokeny mohou použít na vícero různých farem a pomocí různých strategií se snažit získat co nejvyšší úrokovou míru.

Jak již bylo uvedeno výše, tak z transakčních poplatků jde 0,17 % poskytovatelům likvidity do liquidity poolu, přičemž následně se tento poplatek rozděluje dle míry zainteresovanosti uživatele v daném poolu. Velikost zisku je přitom také ovlivněna likviditou a objemem celkových obchodů ve vybraném poolu. Pokud bychom vzali například data u páru USDT/WBNB[69], tak zjistíme, že při denním objemu 24,3 milionu $ budou celkové transakční poplatky za daný den z tohoto poolu činit 41,4 tisíc $. Tyto poplatky jsou následně rozděleny mezi uživatele. Kromě samotného poskytování likvidity

[68] *Stablecoins* [online]. Berlin: Staking Rewards, c2023 [cit. 2023-03-11]. Dostupné z: https://www.stakingrewards.com/stablecoins/

[69] *USDT / WBNB* [online]. PancakeSwap, c2023 [cit. 2023-03-11]. Dostupné z: https://pancakeswap.finance/info/pairs/0x16b9a82891338f9bA80E2D6970FddA79D1eb0daE?chain=bsc

lze následně uzamykat získané LP tokeny do farem, ve kterých je uživatel odměněn úrokem většinou ve formě nativního tokenu dané decentralizované platformy. V tomto případě se jedná o 6 % úrok ve formě CAKE tokenu, který uživatel dostane navíc s podílem z transakčních poplatků, a navýší tak výnosnost svého poskytování likvidity.



Obrázek 11: Uzamykání LP tokenů do farmy

Zdroj: (PancakeSwap, 2023)

Podobně jako staking pooly, tak i liquidity pooly ztrácejí na výnosnosti v přímé závislosti na rostoucím počtu připojených účastníků. Pooly, které dříve dosahovaly zhodnocení až 150 %, jako například nejvyužívanější pár CAKE – BNB, se dnes pohybují pod hranicí 40 %. Do toho je nutné započítat riziko impermanent loss, které mohou, ale také nemusí vyvážit příjmy z vybraných poplatků a farem, respektive odměn pro poskytovatele likvidity. Kdo se chce vyhnout impermanent loss, může zvolit konzervativní cestu stablecoinového páru, které dříve dosahovaly APY v rozmezí 10–20 %. Dnes se však tato úroková míra v prostředí medvědího trhu pohybuje kolem 3 %.

Princip a důležitost impermanent loss vysvětlí následující příklad. Bude uvažována investice do liquidity poolu USDT/BNB ve výši 1 000 $. Aby bylo splněno pravidlo 50 ku 50, vložíme 1 BNB a 500 USDT. Ve zvoleném liquidity poolu se celkově nachází 100 BNB a 50 000 USDT. K výpočtu celkové likvidity slouží rovnice konstantního produktu, kterou využívají i AMM většiny DEX.

$$\mathbf{y * x = k} \qquad (1)$$

kde

y je množství první kryptoměny;

x je množství druhé kryptoměny;

k je konstanta.

Dle rovnice (1) tedy celková likvidita poolu činí 5 000 000 (100 * 50 000 = 5 000 000), a náš podíl v liquidity poolu je 1 %. Ceny se následně začnou hýbat a cena BNB se změní z 500 $ na 600 $. To následně vytvoří příležitost pro arbitráž, jelikož se v daném poolu dá nyní koupit BNB levněji než jinde. Využití této arbitráže zapříčiní následné odebírání BNB a přidávání USDT. Tím se cena BNB v poolu také dostane na 600 $, což změní hodnoty našeho podílu v poolu. Nový poměr je 600 (p), protože nyní za 600 USDT pořídíme 1 BNB a konstanta (k) je stále stejná celková likvidita poolu.

x (BNB) = √ (k / p) = √ (5 000 000 / 600) = 91,29 BNB
y (USDT) = √ (k * p) = √ (5 000 000 * 600) = 54 772,26 USDT
91,29 * 54 772,26 ≈ 5 000 000

Podíly v poolu se tedy změnily na hodnoty 91,29 BNB a 54 772,26 USDT z důvodu, že BNB zvýšilo svoji cenu na 600 $. Náš podíl na celkovém liquidity poolu je stále 1 %. V případě, že by uživatel chtěl z poolu vystoupit a likviditu vybrat, získal by 0,91 BNB a 547,72 USDT.

0,91 * 600 + 547,72 = 1095,46 $

Tím je dosáhnuto zisku 95,46 $ oproti naší původní investici. Pokud by však kryptoměny byly pouze drženy v peněžence a neposkytovala se s nimi likvidita v liquidity poolu, zisk by činil 100 $

1 * 600 + 500 = 1 100 $

Impermanent loss neboli dočasná ztráta by tedy byla 4,54 $, ke kterým je dále nutné připočítat transakční poplatky v síti za přidávání a odebírání likvidity z platformy. Dočasná ztráta se poté stává stálou v momentu výběru z poolu.

Jak již bylo uvedeno výše, tak se lze dočasné ztrátě vyvarovat vybráním správného liquidity poolu na platformě, který své uživatele dostatečně odměňuje za vkládání likvidity formou podílu na transakčních poplatcích a různých formách yield farmingu.

4.1.2.3 Lending

Další oblíbený nástroj a možnost, jak zhodnotit své prostředky ve světě DeFi, je lending na platformě Compound, což je především „půjčovací“ protokol. Při využití tohoto nástroje uživatel dostává pravidelné úroky za své poskytnuté vklady, které může následně reinvestovat a zvýšit tak své APY. Pro přesun kryptoměn mezi platformami lze využít například stablecoinů, nebo jiných tokenů. Jejich přesun je snadný a postupovat lze stejně, jako u již zmíněného postupu výše. Po zvolení preferované platformy se propojí peněženka s platformou. U některých lending platforem si lze vybrat, na jakém blockchainu chce uživatel operovat a snížit tak své transakční poplatky. K tomu je vhodná již výše uvedená peněženka MetaMask, která podporuje vícero blockchainů a lze mezi nimi pohodlně přepínat. Jakmile si uživatel vybere kryptoměnu, které chce dodávat likviditu, a dané platformě ji poskytne, začíná do MetaMask peněženky konstantně přijímat úroky přibližně každých 12 vteřin, respektive pokaždé, kdy je vytvořen nový blok.

Úroková míra u lendingu se liší dle poskytnuté kryptoměny, respektive podle vybraného poolu, a samozřejmě také závisí na aktuálních podmínkách trhu. Tento druh investice býval dříve výnosnější, avšak s příchodem medvědího trhu a následnému klesajícímu zájmu o DeFi začaly úrokové míry klesat. V současné době se tak APY u lendingu typicky pohybuje v rozmezí 2–6 % v závislosti na použité platformě. APY se zde přitom dříve pohybovalo mnohem výše. Je proto zřejmé, že v současné ekonomické situaci a tržních podmínkách není tento nástroj využíván v takové míře, jak tomu bývalo v předchozích letech. Pro retailové investory není tento úrok ve srovnání s jinými alternativami příliš atraktivní. Není zde však takové riziko jako při aktivním obchodování a uživatelé neboli „lenders“ získávají pasivně nový kapitál. Lending může být také užitečný například pro situace, kdy subjekt drží kryptoměny ve svém portfoliu, může si proti těmto krypto aktivům půjčit a přesunout tuto půjčku následně do klasických finančních instrumentů.

Lending se dá také využít s pákou, díky čemuž lze zvýšit jeho výnosnost. Řekněme, že uživatel vloží 1 000 $ do poolu X a proti tomu si půjčí maximum, které mu dovoluje LTV neboli „loan to value“. Pokud bude LTV 80 %, pak si může proti 1 000 $ půjčit maximálně 800 $. Tuto částku následně opět vloží do poolu X a tím získá 1,8x páku, protože nyní disponuje 1 800 $ oproti původním 1 000 $. Za předpokladu, že by „Supply APY“ u poskytování byly 3 % a „Borrow APY“ 1,5 % u půjčení, tak díky 1,8násobné páce vyjde, že

tzv. Loop APY neboli lending s pákou bude činit 6,7 %. V případě použití momentálních dat na platformě Compound[70] lze díky páce zvýšit APY například z původních 2,37 % u stablecoinu USDC na platformě Compound na výsledných 5,01 % za předpokladu využití maximálního LTV.

APY se v případě lendingu odvíjí mimo poptávky a nabídky také od tzv. „utilization rate“. Tento ukazatel představuje v procentuálním vyjádření množství kolaterálu, který je v daný moment půjčován, respektive jak velká část poolu je půjčována. Z této metriky lze odvodit zájem o DeFi lending u dané kryptoměny. Pokud by se tento ukazatel pohyboval v ideálním rozmezí 80-90 % (záleží na zvolené kryptoměně), pak by se zvedl i ukazatel APY, který by následně přilákal více likvidity, což následně vyústí v ponížení APY a větší balanc mezi nabídkou a poptávkou.

Obrázek 12: Vliv "utilization rate" na APY

Zdroj: (Compound, 2023)

4.1.2.4 Yield farming

Yield farming je strategie uživatelů DeFi, která kombinuje předchozí uvedené nástroje ve snaze maximalizovat profit. Uživatelé mohou přesouvat držené kryptoměny mezi

[70] *Markets* [online]. Compound Labs, c2023 [cit. 2023-03-13]. Dostupné z: https://app.compound.finance/markets?market=137_USDC_0xF25212E676D1F7F89Cd72fFEe66158f541246445

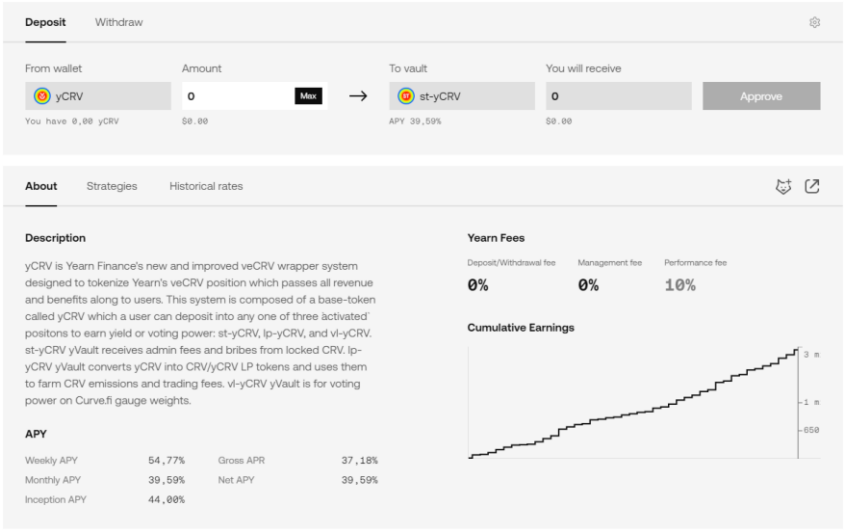
jednotlivými platformami a hledat co nejvýnosnější strategii nebo zůstat u jedné platformy, kde mezi sebou kombinují například poskytování likvidity, „farming“ LP tokenů a staking.

Přestože může být yield farming méně rizikový než samotné obchodování s kryptoměnami, tak mnohdy může nést i větší riziko. Zatímco některé pooly vykazují zhodnocení v řádu jednotek až desítek procent, jiné dosahují stovek až tisíců procent. Takové pooly jsou ovšem velice rizikové, většinou se jedná o nové a neznámé platformy, které mohou selhat, mít špatně napsaný chytrý kontrakt, nebo se může jednat o tzv. „rug pull“, tedy podvod, při kterém tvůrce platformy či kryptoměny vybere veškerou likviditu. Pooly s takovým APY lze doporučit jen velmi zkušeným uživatelům decentralizovaných financí, kteří tyto rizika dokážou identifikovat, zhodnotit důvěryhodnost projektu a vyhnout se tak případným ztrátám.

Jedním z nejznámějších nástrojů pro efektivní yield farming je platforma Yearn.finance, která funguje jako agregátor aktuálních příležitostí yield farmingu pro decentralizované aplikace postavené na bázi Etherea. Platforma funguje na principu, že uživatel vloží své kryptoměny do chytrého kontraktu, který pomocí jeho algoritmu alokuje tyto prostředky do ostatních chytrých kontraktů, respektive do dalších platforem tak, aby zajistil co největší yield neboli APY.

Za tuto službu si platforma účtuje 10 % jako tzv „performance fee“ přičemž výnosy se různí dle zvoleného „vaultu“, který lze chápat jako pool. APY se zde pohybuje od 3 % u stablecoinů až po 45 % u rozličných vaults, které kombinují staking či liquidity pooly. Zajímavou možností je například využití vaultu, který v sobě kombinuje stablecoin USDT, BTC a ETH, čímž je zmírněno riziko při relativně vysokém APY.[71]

[71] *Vaults* [online]. Yearn.finance, c2023 [cit. 2023-03-11]. Dostupné z: https://yearn.finance/vaults



Obrázek 13: Prostředí Yearn.finance

Zdroj: (Yearn.finance, 2023)

Každý z výše uvedených DeFi nástrojů je vhodný pro jiný druh investování v závislosti na jeho náročnosti a komplexity používání. Nejdůležitějším faktorem v rozhodování je tak samotný uživatel těchto nástrojů, jeho zkušenosti a jeho vztah k riziku. V tabulce níže je znázorněna komparace v této kapitole již uvedených DeFi nástrojů na různých platformách z pohledu výnosnosti, rizika, náročnosti používání, likvidity a možnosti hlasovacího práva.

DeFi nástroj	Staking	Lending	LP
APY[72]	≈ 20–45 %	≈ 2–10 %	≈ 20–40 %
Riziko	Střední	Nízké	Vysoké
Náročnost	Nízká	Střední	Vysoká
Likvidita	Střední	Vysoká	Střední
Governance	Ano	Ne	Ano

Tabulka 1: Komparace DeFi nástrojů

Zdroj: vlastní zpracování

Z výše uvedené tabulky se jeví jako nejvhodnější decentralizovaný nástroj staking, který se vyznačuje vysokým zhodnocením v poměru s nízkou náročností a nepříliš vysokým rizikem, jež závisí především na vybrané platformě a její bezpečnosti. Jeho likvidita závisí na tom, zda uživatel dané tokeny do platformy uzamkne či nikoliv, a pokud ano, tak na jakou dobu. Výnosnost se přitom úměrně zvyšuje s dobou uzamknutí tokenů. Staking má spolu s poskytováním likvidity oproti půjčování tokenů výhodu v hlasovacích právech, kdy uživatelé mohou přímo ovlivnit dění na platformě nebo se podílet na jejím vývoji. Naopak nevýhodou poskytování likvidity je její technická náročnost, která vyžaduje větší znalosti a předešlé zkušenosti uživatelů, především v oblasti impermanent loss. Lending je především v současné době nepříliš zajímavá alternativa z důvodu nízkého zhodnocení, kterého lze běžně dosáhnout i pomocí klasických bezrizikových finančních instrumentů. Celkově lze tedy i na základě výše provedeného rozboru doporučit staking, který je například na platformě PancakeSwap uživatelsky přívětivý a vykazuje dlouhodobě vysoké a udržitelné APY. Záleží však na osobních zkušenostech, cílech a preferencích uživatele.

Atributy riziko a náročnost používání byly ohodnoceny na základě dlouholetých zkušeností autora i ostatních uživatelských hodnocení. Data pro APY byly převzaty z DeFi agregátoru DeFiLlama, který shromažďuje data o decentralizovaných platformách. Jedná se o průměrné běžně dosahované APY na již uvedených platformách. V DeFi lze dosahovat

[72] *Yields* [online]. DeFiLlama, c2023 [cit. 2023-03-11]. Dostupné z: https://defillama.com/yields

vyšších hodnot zhodnocení na neauditovaných platformách, avšak s mnohem větším rizikem.

DeFi platforma	PancakeSwap	Uniswap	Compound	Yearn.finance
Blockchain	BNB Chain	Ethereum	Ethereum	Ethereum
Token	CAKE	UNI	COMP	YFI
Tržní kapitalizace[73]	813 252 266 $	5 589 552 697 $	431 063 481 $	273 301 027 $
Uzamčená hodnota[74] **(TVL)**	2 461 215 087 $	4 180 698 925 $	1 566 347 124 $	471 011 945 $
Poplatky	0,25 %	0,30 %	Ne	10 %
Podporovaná aktiva[75]	3259	941	20	49
Útoky	Ano	Ne	Ne	Ne
Audit	Ano	Ano	Ano	Ano
Anonymní vývojáři	Ano	Ne	Ne	Ne

Tabulka 2: Komparace DeFi platforem

Zdroj: vlastní zpracování

Dle tabulky číslo 2 a na základě provedeného rozboru v této práci vychází platforma PancakeSwap jako nejvhodnější DeFi platforma. Záleží však na osobních preferencích a investičních úmyslech. Pro začínající uživatele je platforma nejpřívětivější svým UI, pro zkušenější je lákavá počtem nabízených kryptoměn a obchodovatelných párů ve spojení s nízkými poplatky. Jako jedinou z uvedených ji však postihl hackerský útok a její vývojářský tým je anonymní, což obvykle není dobrá vlastnost. Lze ji však doporučit, neboť

[73] *Today's Cryptocurrency Prices by Market Cap* [online]. Dover: CoinMarketCap, c2023 [cit. 2023-03-11]. Dostupné z: https://coinmarketcap.com/tokens/

[74] *Decentralized Exchanges* [online]. Singapore: CoinGecko, c2023 [cit. 2023-03-11]. Dostupné z: https://www.coingecko.com/en/exchanges/decentralized

[75] Tamtéž

dlouhodobě spolehlivá, auditovaná a jedna z nejpoužívanějších. Její velkou výhodou jsou nízké poplatky na síti díky použité platformě BNB Chain.

Uniswap se svou tržní kapitalizací ovládá trh decentralizovaných platforem. Podobně jako PancakeSwap nabízí širokou škálu kryptoměn, přičemž mnoho z nich je nabízených právě jen na Uniswapu. Toho mohou využít například uživatelé, kteří se zaměřují na nové tokeny s potencionálním vysokým zhodnocením. Platforma není složitá na používání, přesto již vyžaduje předchozí zkušenost na rozdíl od platformy PancakeSwap. Její nevýhodou je blockchain Etherea, kvůli které byl Uniswap určitou dobu nepoužitelný pro malé transakce vzhledem k vysokým „gas" poplatkům. To by se však již mělo změnit s novou verzí Etherea.

Lending protokol Compound láká na to, že na platformě nejsou žádné transakční poplatky, uživatel zaplatí pouze poplatky v síti za provedené transakce. Jeho využitelnost spočívá především v půjčování si kryptoměn za kolaterál, jelikož lending samotný ve srovnání s ostatními alternativami příliš zajímavý není. Přesto je však platforma hojně využívána především díky své dlouholeté spolehlivosti a jménu. Z uživatelského hlediska je platforma složitější a podobně jako většina DeFi platforem vyžaduje určité předešlé zkušenosti.

Yearn.finance je agregátor, který nabízí velice zajímavé možnosti zhodnocení ve svých vaults, bere si však za tyto služby poměrně vysoký poplatek. Výhodou je minimalistické uživatelské prostředí, které je s určitými zkušenostmi snadno použitelné. Platforma je vhodná pro uživatele, kteří hledají vysoké zhodnocení a zároveň nechtějí sestavovat komplexní strategie pro yield farming.

Závěrem lze konstatovat, že primárně záleží na individuálních preferencích a potřebách uživatele, kterou platformu a jaký přístup zvolí.

4.2 Daňová problematika

Lidé investují do kryptoměn podobně jako u jiných typů investic s cílem zisku. Mnoho, ne-li většina však začíná s kryptoměnami bez toho, aniž by se nejdříve zajímali o jejich zdanění. Zdanění kryptoměn, podobně jako daně samotné, není jednoduchá problematika. Měl by ji však znát každý investor, aby se do budoucna mohl vyhnout případným problémům s finančním úřadem.

Jelikož se dle ČNB kryptoměny nepovažují za obdobu cenných papírů (viz kapitola „Legislativa v ČR, regulace a její vztah ke kryptoměnám“), daní se dle §10 Zákona o daních z příjmů – Ostatní příjmy. Daň je odlišná pro obě právní formy, tedy fyzické a právnické osoby. U fyzických osob činí 15 % a u právnických osob 19 %. Zdanit je třeba zisk z každé ziskové transakce u obou právních forem. To je častým omylem investorů, kteří stále často daní zisk z kryptoměn až v momentu, kdy zisk převedou na svůj bankovní účet.

Fyzická osoba nepodnikající si nemusí pro investování do kryptoměn zřizovat živnostenský list. Dle §10 Zákona o daních z příjmů se jako výdaj uplatňuje při zdanění pořizovací cena dané kryptoměny společně s poplatky zaplacenými při pořízení. Kryptoměny spadají pod § 10 odst. 1 písm. b) ZDP, na příjmy do 30 tisíc korun se nevztahuje osvobození příležitostných příjmů, jedná se o správu vlastního majetku, ne o činnost, a i tyto příjmy se musí zdanit. Naopak, pokud příjmy fyzické osoby převyšují 48násobek průměrné mzdy, zisky se daní 23 %, což je sazba, která nahrazuje dřívější solidární daň. V případě, že investor nedosáhne zisku, ale má pouze ztrátu, je základ daně nula. Pokud by byly kryptoměny například předmětem dědického řízení či byly darovány, tak se postupuje dle ZDP.[76]

Právnická osoba si může oproti fyzické osobě uplatnit vůči zisku aktuálního roku ztrátu z posledních 5 let. Tato ztráta přitom může pocházet z jiné činnosti, než jsou investice do kryptoměn. Daň si dále může ponížit o uplatněné náklady. Jak již bylo v této práci uvedeno, od DPH jsou kryptoměny osvobozeny a jsou brány jako oběživo. DPH se tedy neplatí podobně jako při převodu fiat měn.

Pokud fyzická osoba kryptoměny těží, musí si zřídit živnostenské oprávnění, konkrétně volnou živnost, obor činnosti „poskytování softwaru, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály“. Nutnost založení živnosti je zdůvodněna tím, že se jedná o poskytovanou službu a soustavnou činnost, při které „těžař“ nabývá majetek vlastní činností. Tím pádem jde o podnikání. Další povinností při těžbě kryptoměn je nutnost přihlášení k sociálnímu a zdravotnímu pojištění, což se pojí se založením živnosti obecně. Příjmy z těžby se daní

[76] SUCHAN, Stanislav. *Zdanění kryptoměn u fyzických osob* [online]. Brno: Seyfor, 2022 [cit. 2023-03-12]. Dostupné z: https://money.cz/novinky-a-tipy/dane/zdaneni-kryptomen-u-fyzickych-osob/

15% sazbou dle §7 Zákona o dani z příjmu.[77] Moment zdanění poté nastává při směně kryptoměny za fiat měnu, či jiné.

Při přímém nákupu zboží či určité služby za kryptoměny se daní hodnota pořizovaného majetku či služby. Zdaňuje se přitom dle původu nabytí kryptoměny, zda se jednalo o těžbu či o obchodování. Toto je oficiální stanovisko finanční správy, kterému ale kontradikuje rozsudek Krajského soudu v Brně, kde bylo v roce 2022 judikováno, že použití kryptoměn pro nákup zboží není zdanitelným příjmem.[78] Lze tak pozorovat určitý zmatek až disonanci mezi postojem státních orgánů ke kryptoměnám.

Pokud bychom naopak prodávali zboží či poskytovali služby výměnou za kryptoměny, tak se pro základ daně bere hodnota zboží či služby v daný moment směny a v českých korunách. Pokud jsou následně kryptoměny drženy a dojde k jejich zhodnocení, daní se opět dle §10 ZDP.[79]

V případě DeFi se příjmy daní stejně jako u ostatních kryptoměn dle §10 ZDP jako ostatní příjmy. Veškeré zisky z půjček a poskytování likvidity se daní až při směně těchto kryptoměn.

Pro výpočet základu daně lze využít známých účetních metod FIFO (First In, First Out), nebo vážený aritmetický průměr. Pokud by byl nákup kryptoměny jednorázový, investor by žádné další kryptoměny nedokupoval a následně by je prodal, tak jako základ daně poslouží pouze rozdíl mezi nákupní a prodejní cenou. V praxi se ale běžně kryptoměny dokupují, což dělá následný výpočet základu daně složitější. V případě vysokého objemu transakcí lze využít speciální aplikace, které tyto procesy automatizují a základ daně vypočítají.

V následujícím příkladu si uvedeme postup výpočtu základu daně. Nejdříve použijeme metodu FIFO, kdy do výpočtu zahrnujeme nejdéle drženou kryptoměnu.

---

[77] *Informace k daňovému posouzení transakcí s kryptoměnami* [online]. Praha: Generální finanční ředitelství, 2022 [cit. 2023-03-12]. Dostupné z: https://www.financnisprava.cz/assets/cs/prilohy/d-seznam-dani/Info_kryptomeny_GFR.pdf

[78] *Rozsudek KSBR ze dne 17.02.2022* [online]. Zlín: AION CS, 2022 [cit. 2023-03-12]. Dostupné z: https://www.zakonyprolidi.cz/judikat/ksbr/30-af-29-2020-48

[79] *Jak na zdanění kryptoměn* [online]. Brno: Banky.cz, 2022 [cit. 2023-03-12]. Dostupné z: https://www.banky.cz/clanky/jak-na-zdaneni-kryptomen-kompletni-navod/

Rozhodli jsme se tedy prodat své portfolio, které se skládá z několika různých kryptoměn. Nejdříve jsme nakoupili 10 ETH za 83 458 Kč, o něco později jsme nakoupili 1 BTC za 299 210 Kč, 1000 CAKE za 32 960 Kč, poté 100 UNI za 31 719 Kč, a nakonec jsme se rozhodli dokoupit 2 ETH za 46 799 Kč. Všechny tyto kryptoměny jsme přitom prodali ve stejný den za částku 810 282 Kč (přepočteno kurzem platného v den prodeje 22,54 Kč za 1 $). V případě kryptoměn se nezdaňují za jednotlivé kalendářní roky nerealizované zisky v případě, že byly pouze drženy, a ne aktivně obchodovány. Budeme tedy předpokládat pouhé držení kryptoměn v peněžence.

Pro samotný výpočet nejdříve vybereme nejdéle drženou kryptoměnu, tedy 10 ETH, a od její nákupní ceny odečteme cenu prodejní. Tento postup pak postupně aplikujeme na všechny dále nakoupené. Pro všechny přepočty přitom používáme kurz, který byl platný v den prodeje. V tabulce č. 1 lze přehledně pozorovat celý postup výpočtu základu daně. Výsledná daň z příjmu fyzických osob pak činí 47 420 Kč při zisku 316 136 Kč.

Datum nákupu	Kryptoměna	Nákupní cena	Prodejní cena	Zisk
10.10.2020	10 ETH	83 458 Kč	284 806 Kč	201 348 Kč
26.10.2020	1 BTC	299 210 Kč	381 967 Kč	82 757 Kč
31.01.2021	1000 CAKE	32 960 Kč	74 220 Kč	41 260 Kč
21.07.2021	100 UNI	31 719 Kč	12 331 Kč	- 19 388 Kč
19.06.2022	2 ETH	46 799 Kč	56 958 Kč	10 159 Kč
Celkem	-	**494 146 Kč**	**810 282 Kč**	**316 136 Kč**

Tabulka 3: Výpočet základu daně pomocí metody FIFO

Zdroj: vlastní zpracování

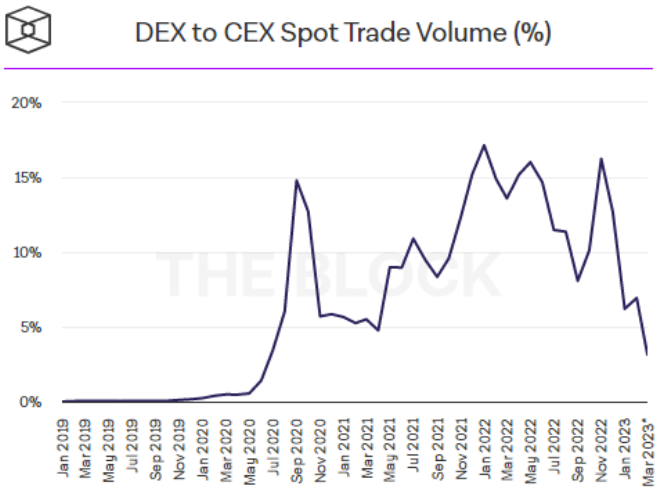
V případě využití metody váženého aritmetického průměru nám vyjde rozdílná výše daně z příjmu. Výpočet probíhá tak, že nejdříve zprůměrujeme nákupní cenu našeho prodávaného portfolia. Dále tento vypočtený průměr (98 829 Kč) odečteme od výsledné prodejní ceny. Základ daně je pak roven jejich rozdílu, v tomto případě 711 453 Kč. Po použití sazby pro daň z příjmu fyzických osob pak tato daň činí 106 718 Kč, tedy o 125 %

více než v případě použití metody FIFO. Je proto v zájmu investora zvolit správnou účetní metodu při určení základu daně.

4.3 Komparace DeFi a CeFi

Kromě decentralizovaných nástrojů lze vlastněné kryptoměny zhodnotit i s centralizovanými nástroji na centralizovaných platformách neboli CeFi. Mezi centralizované finance v kryptoměnovém světě řadíme klasické obchodní platformy, jako jsou burzy nebo směnárny. Nalezneme mezi nimi ale také platformy založené přímo na staking či lending kryptoměn.

Decentralizované projekty jsou stále relativně nové oproti známým centralizovaným burzám. Oba typy platforem mají svá pozitiva i negativa, některé se přitom snaží vzít si to „dobré“ z obou světů a tyto výhody kombinovat. V této kapitole budou oba přístupy komparovány. Na níže uvedeném grafu lze pozorovat, že decentralizované burzy mají obzvláště v této době mnohem menší podíl na spotovém trhu než burzy centralizované. Podobně jsou na tom i trhy s deriváty. To je samozřejmě ovlivněno uživatelsky přívětivějším prostředím centralizovaných burz, délkou působení na trhu, jejich marketingem a dalšími vlivy. Vrcholu popularity DEX dosáhly na přelomu let 2021 a 2022, v současnosti jsou na ústupu, což je zapříčiněno současnou situací na trhu.



Graf 3: Komparace obchodovaného objemu na DEX spotových trzích vůči CEX

Zdroj: (The Block, 2023)

Hlavním rozdílem mezi oběma druhy platforem je „Know your customer“ (dále KYC) ověřování uživatelů, které bylo zavedeno na centralizovaných burzách k ověření identity, aby se zabránilo praní špinavých peněz a finančním podvodům. Decentralizované platformy uživatele nijak neověřují a transakce jsou zcela anonymní, uživatelé tedy nemusí dokládat původ svých kryptoměn.

Obvykle mají také decentralizované projekty nižší poplatky díky absenci prostředníků, což bývá typicky vyváženo většími nároky na technickou zdatnost a zkušenosti uživatele. Například v roce 2021 provedla poradenská společnost KPMG test, ve kterém provedla obchod se 100 000 $. Decentralizovaná burza Uniswap za tuto transakci účtovala poplatek 0,05 %, a CEX Binance a Kraken požadovali 0,1 % a 0,2 %.[80] Není tomu tak však pokaždé. V případě vysokého vytížení sítě je možné zaplatit na poplatcích i stovky dolarů. Informace o výši tohoto poplatku je však pokaždé uvedena před potvrzením transakce a uživatel musí zvážit, zda se mu poplatek vyplatí.

Dalším z důležitých rozdílů je, že na centralizovaných burzách uživatel nakoupené kryptoměny nevlastní. Vlastní je daná burza a v případě krachu či jiného problému se k nim uživatel již nemusí dostat. Naopak u DEX je vlastníkem stále uživatel. Ten má kryptoměny uložené ve své peněžence, která je propojená s DeFi platformou. Spolu s tím se ovšem pojí větší zodpovědnost za vlastněné kryptoměny a větší nároky na technickou zdatnost.

Větší nároky na technickou zdatnost lze uplatnit na DeFi obecně. Je tomu tak většinou z důvodu méně dostupných finančních prostředků na vývoj než u centralizovaných platforem, urychleného vývoje, nebo i tím, že decentralizované projekty často přímo cílí na zkušenější uživatele. V DeFi ve většině případů ani není žádná uživatelská podpora, jak tomu bývá zvykem u centralizovaných platforem. S tím se pojí i mnohem větší již výše zmíněné riziko, jako jsou různé hackerské útoky, podvody a jiné, kterým se lépe vyhne zkušenější uživatel DeFi.

[80] *Crypto Insights #2. Decentralised Exchanges & Automated Market Makers – Innovations, Challenges & Prospects* [online]. Hong Kong: KPMG Huazhen, 2021 [cit. 2023-03-12]. Dostupné z: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2021/10/crypto-insights-part-2-decentralised-exchanges-and-automated-market-makers.pdf

Takoví uživatelé také spíše využijí možnosti governance tokenů na decentralizovaných platformách, které jim dovolují podílet se na řízení daného projektu. Prostřednictvím DAO neboli decentralizované autonomní organizace dané platformy hlasují držitelé governance tokenů o různých návrzích, které určují budoucí směřování platformy nebo mění její nastavení.

Mimo již uvedené decentralizované platformy existují také platformy centralizované s převzatými prvky decentralizace, jako je například nejpoužívanější a největší centralizovaná burza Binance.

4.3.1 Binance

Jak již bylo uvedeno, Binance je dlouhodobě nejvyužívanější a nejúspěšnější kryptoměnovou burzou. Nabízí nízké transakční poplatky a velmi široký výběr obchodovatelných kryptoměn. Její úspěch spočívá ve snadné uživatelské přístupnosti, intuitivnímu UI a rozsáhlému počtu funkcí, které nabízí a neustále je rozrůstá. Pro některé může být i výhodou podpora českého jazyka a české zastoupení burzy, které může být nápomocné v případě nenadálých problémů.

Binance vytvořil také spolu s vlastní kryptoměnou BNB i blockchain BNB Chain, který je základem například pro jednu z nejvyužívanějších DeFi platforem PancakeSwap. Tokeny BNB se pak využívají jako platební prostředek na BNB platformách, k úhradě poplatků nebo figuruje v rozličných poolech.

Poplatky má Binance historicky nízké, a i díky tomu je burza natolik oblíbená a využívaná. Transakční poplatek zde činí u běžného uživatele 0,1 % a dále se snižuje v závislosti na obchodovaném objemu. Tento poplatek může být dále snížen, pokud k jeho úhradě bude použito BNB, v takovém případě jde o 0,075 %. Poplatek je v základu stejný jak pro „makera“, tedy uživatele, který nabídku na trhu vytváří, tak i pro „takera“, který si z nabídek vybírá. Maker poplatek lze dále snížit na 0 %, pokud obchodník využije pár, který obsahuje nativní stablecoin platformy BUSD. Stejně tak lze odstranit transakční poplatek u některých BTC párů s fiat měnami.[81]

[81] *Poplatky za obchodování* [online]. Montrouge: Binance, c2023 [cit. 2023-03-12]. Dostupné z: https://www.binance.com/cs/fee/schedule

Binance nabízí mimo klasické obchodování kryptoměn jako mnoho jiných burz také maržové obchodování, obchodování s futures kontrakty, opčními kontrakty, ale také Binance Earn, kde uživatel nalezne možnosti ke zhodnocení držených kryptoměn. APY u stakingu zde dosahuje až 37 % pro kryptoměny a 3,5 % pro „stablecoiny.[82] Pokud by si chtěl na kryptoměny uživatel půjčit, Binance mu nabídne na stablecoin sazbu 5,54 %.[83] Dále lze na platformě nalézt i nástroje typické jen pro DeFi. Mimo staking platforma nabízí i poskytování likvidity na své zabudované decentralizované burze Binance DEX. Tyto nástroje jsou však postaveny na centralizované Binance infrastruktuře. Jedná se tak o zajímavý hybrid mezi centralizovanými a decentralizovanými financemi, tzv. Ce-DeFi. Jednoznačnou výhodou je větší jednoduchost používání, nízké poplatky a dobré jméno platformy, které zaručuje bezpečnost. Může se tak jednat o vhodný počáteční bod k seznámení se s DeFi a naučení s jeho nástroji. Nevýhodou tohoto hybridního systému je však nízké APY na nabízených nástrojích a rizika spojená s DeFi, jako je například impermanent loss, které se objevuje i zde. Přesto se může jednak o zajímavou alternativu. Pokud uživatel hodlá držet kryptoměny na burze delší dobu, může je tímto způsobem zároveň i zhodnotit. Držení kryptoměn na burzách se ovšem nedoporučuje, jelikož je zde větší riziko ztráty. K uchování kryptoměn slouží nejlépe kryptoměnové hardwarové peněženky v této práci již zmíněné.

Burza Binance si za svých 6 let fungování vytvořila silnou reputaci bezpečné a důvěryhodné burzy, která často po směnárně Coinbase slouží jako vstupní bod do světa obchodování kryptoměn. Jediný incident se stal v roce 2019, kdy bylo hackerským útokem z burzy ukradeno 7 000 BTC za více jak 40 milionů dolarů. Uživatelů burzy se to ale nijak nedotklo, jelikož Binance všechny poškozené odškodnilo. Burza je přitom pojištěna proti

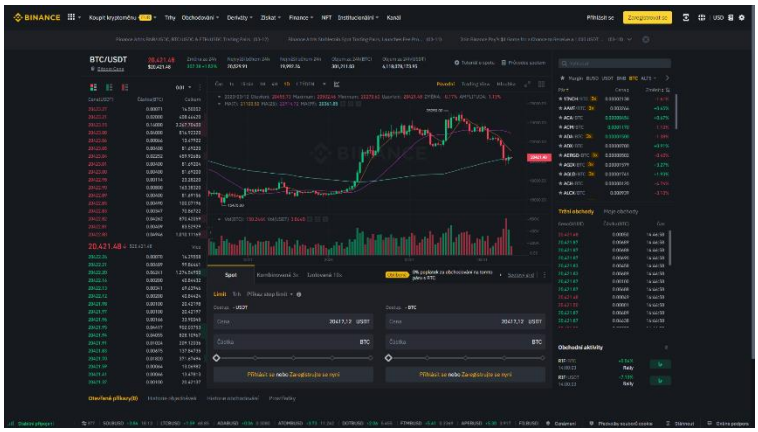
[82] *Binance Earn* [online]. Montrouge: Binance, c2023 [cit. 2023-03-12]. Dostupné z: https://www.binance.com/cs/earn

[83] *Kryptopůjčky* [online]. Montrouge: Binance, c2023 [cit. 2023-03-12]. Dostupné z: https://www.binance.com/cs/loan

podobným útokům do částky 1 miliardy dolarů.[84] Všechny vlastněné kryptoměny má uložené offline.

Binance je vysoce komplexní platforma, která nabízí mnohem více funkcí, než je pouhé obchodování kryptoměn. Její oblíbenost mezi kryptoměnovou komunitou spočívá ve velké nabídce obchodovatelných kryptoměn a nabízených funkcí. Platforma nabízí k obchodování 356 kryptoměn a podporu 72 fiat měn, což je v kontextu ostatních platforem velmi vysoký počet, a díky neustálým inovacím i propracovanému marketingu se stále drží na vrcholu tohoto odvětví i popularity.

Existují ale i jiné centralizované platformy, které nabízejí typicky decentralizované nástroje v centralizované formě s mnohem větší výnosností. Takovou platformou je například populární Nexo.



Obrázek 14: Prostředí obchodní platformy Binance

Zdroj: (Binance, 2023)

4.3.2 Nexo

Nexo je přední centralizovaná lending platforma, která je zaměřena na půjčování a úročení zakoupených kryptoměn. Založena byla již v roce 2018 a je jednou z prvních

[84] LAM, Eric. *Hackers Steal $40 Million Worth of Bitcoin From Binance Exchange* [online]. Londýn: Bloomberg, 2019 [cit. 2023-03-12]. Dostupné z: https://www.bloomberg.com/news/articles/2019-05-08/crypto-exchange-giant-binance-reports-a-hack-of-7-000-bitcoin#xj4y7vzkg

svého druhu. V průběhu let nasbírala více jak 200 licencí a registrací v jurisdikcích po celém světě a její nativní token schválila Komise pro kontrolu cenných papírů v USA, což platformě přidává na důvěryhodnosti.[85] Po krachu konkurentů Celsius a BlockFi má nyní Nexo monopol mezi centralizovanými lending platformami.

Uživatelé mohou Nexo využít na půjčení kryptoměn za fiat měnu či stablecoiny, nebo také na půjčování kryptoměn platformě. Za půjčení kryptoměn uživatel dostane úrok, který mu je vyplácen denně. V případě, že si uživatel chce z platformy kryptoměny půjčit, vypočte se výše jeho půjčky poměrem k jeho kolaterálu. Jedná se tedy o podobný princip jako v DeFi. Vše je ovšem centralizované, což má svá pozitiva, ale i negativa. Například LTV, tedy „Loan to Value", je zde mnohem nižší než u DeFi platforem a uživatel si tak může půjčit méně oproti svému kolaterálu.

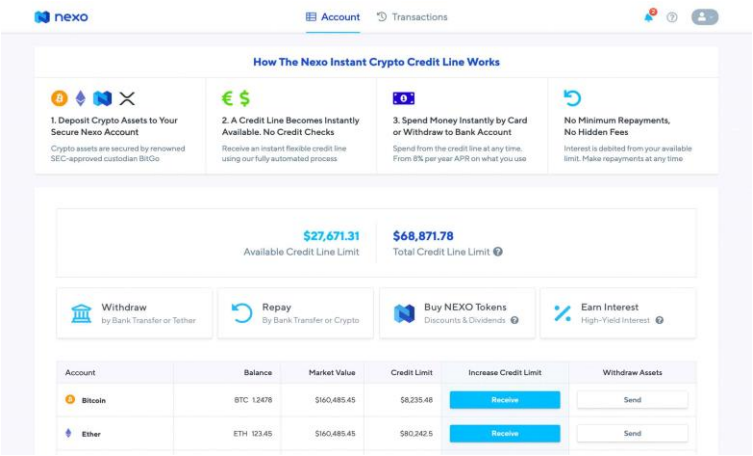
Odměny za lending v Nexo platformě jsou poměrně vysoké a APY u některých kryptoměn převyšuje výnosy v DeFi platformách. APY se zde přitom odvíjí od vybrané kryptoměny a také věrnostní úrovně uživatele. Úroveň se zde odvíjí dle výše podílu tokenu NEXO v portfoliu. To dále ovlivňuje nejen úrok z poskytnutých kryptoměn, ale také úroky pro půjčky. Při základní úrovni se jedná až o 12 % APY na kryptoměny a až 8 % na stablecoiny. Pokud uživatel bude držet více jak 10 % ze svého portfolia v NEXO tokenech, pak dosáhne až na 36 % úrok z kryptoměn a až 12 % ze stablecoinů. Úroky jsou přitom vypláceny denně.

Podobný princip funguje i u půjček. Pokud si chce uživatel kryptoměny půjčit, pak mu při základní úrovni Nexo nabídne úrok 13,9 % RPSN. Naopak, pokud je na nejvyšší úrovni, pak RPSN činí 6,9 %, a pokud je LTV uživatele méně jak 20 %, jeho úrok bude dokonce nulový. Při půjčování kryptoměn je využit interní systém Nexo Oracle, který analyzuje data, řídí distribuci půjček, spravuje splátkové kalendáře a schvaluje jednotlivé půjčky. K určení úvěruschopnosti uživatele není potřeba bankovních výpisů ani jiných údajů. Systém vypočte dobu splácení půjčky a výši kolaterálu pomocí LTV, který je zde určen pro každou kryptoměnu zvlášť. Pokud je například LTV 50 %, tak si uživatel může půjčit až do 50 % hodnoty dané kryptoměny.

[85] *Licenses & Registrations* [online]. Zug: Nexo, c2023 [cit. 2023-03-12]. Dostupné z: https://nexo.io/licenses-and-registrations

Mezi další funkce Nexo patří například také swapy kryptoměn, při jejichž využití uživatelé získají „cashback“ 0,5 %. Platforma dále nabízí zřízení kreditní karty, která vznikla ve spolupráci s MasterCard, na kterou se také vztahuje cashback ve výši až 2 %. Nexo nabízí i možnost páky, kdy si lze půjčit až 3x více kryptoměn a využít tak například pomocí tohoto nástroje momentální situace na trhu.[86]

Platforma je zcela centralizovaná, podléhá tak státním autoritám, což může být některými vnímáno jako nevýhoda. Oproti tomu, ale nabízí podporu pro 43 fiat měn a 62 kryptoměn. Díky obsáhlému počtu spoluprací s různými institucemi je platforma vnímána jako vysoce důvěryhodná. Nexo také nikdy nepodlehlo hackerskému útoku, což je v kryptoměnovém světě spíše výjimkou. Platforma je pojištěna na 375 milionů dolarů pro kryptoměny držené na platformě, které jsou dále uloženy v off-line hardwarových peněženkách a ty jsou uloženy v trezorech s vysokým zabezpečením.[87]



Obrázek 15: Prostředí platformy Nexo

Zdroj: (Nexo, 2023)

Decentralizované a centralizované kryptoměnové platformy mají své klady i zápory, které znemožňují jednoznačně určit, který druh platforem je lepší. Při výběru je nutné brát

[86] *Why choose Nexo?* [online]. Zug: Nexo, c2023 [cit. 2023-03-12]. Dostupné z: https://support.nexo.io/s/article/why-choose-nexo

[87] *Security and Insurance* [online]. Zug: Nexo, c2023 [cit. 2023-03-12]. Dostupné z: https://support.nexo.io/s/article/security-and-insurance

především v úvahu, pro koho je platforma určená. V tabulce číslo 4 jsou uvedené platformy komparovány z různých hledisek. Platforma PancakeSwap byla zvolena jako zástupce DeFi a Binance i Nexo jsou vybraní zástupci CeFi.

Platforma	PancakeSwap	Binance	Nexo
Aktiva	3259	356	62
Podpora FIAT	Ne	72	43
Transakční poplatky	0,25 %	až 0,1 %	Ne
Earn APY	≈ 45 %	≈ 37 %	≈ 36 %
Stablecoin APY	Ne	≈ 3,5 %	≈ 12 %
Borrow RPSN	Ne	≈ 5,4 %	≈ 6,9 %
Čeština	Ne	Ano	Ne
Maximální páka	100x	125x	3x
Uživatelská podpora	Ne	Ano	Ano
KYC	Ne	Ano	Ano
Governance	Ano	Ne	Ne

Tabulka 4: Komparace jednotlivých parametrů u zvolených platforem

Zdroj: vlastní zpracování

Platforma Binance je díky svým nízkým poplatkům a uživatelské přívětivosti ideální volbou pro začínající uživatele. Zaujme podporou českého jazyka, na poměry centralizovaných platforem širokou nabídkou altcoinů i různých nástrojů, pomocí kterých může uživatel zhodnotit držené kryptoměny. Mimo to nabízí i hybridní DeFi nástroje, na kterých si uživatelé mohou vyzkoušet výhody decentralizovaných nástrojů a umožňuje jim tak nahlédnout do této oblasti kryptoměnového světa. Nevýhodou pro některé může být absence anonymity z důvodu vyžadování KYC na všech centralizovaných platformách. Pro takové jsou ideální decentralizované platformy, kde je zajištěna plná anonymita. Naopak

výhodou centralizace je podpora fiat měn, tedy státních měn, pomocí kterých lze nakoupit kryptoměny například přes SEPA platby či debetní nebo kreditní karty.

Centralizované platformy mívají často výhodu ve větší uživatelské přívětivosti především díky rozsáhlejšímu financování jejich vývoje. Nexo je zajímavou alternativou k typickým centralizovaným burzám, především díky jeho relativně snadnému a výnosnému zhodnocení kryptoměn. Zhodnocení stablecoinů je na této platformě výnosnější než u decentralizovaných konkurentů, a jeho relativně snadné UI dovoluje i nezkušeným uživatelům využít takových nástrojů, jako je borrowing či lending. Při půjčení tokenů nabídne platforma kompetitivní RPSN, které může být i nulové při splnění již výše zmíněných podmínek. Silné zabezpečení a spolupráce se státními organizacemi po celém světě dělají z Nexo jednu z nejdůvěryhodnějších kryptoměnových platforem a zajímavou alternativu pro zkušené i nezkušené uživatele.

Plně decentralizovaná platforma PancakeSwap již vyžaduje určité zkušenosti v oblasti kryptoměn, jedná se však o nejsnazší vstupní bod do DeFi především díky uživatelsky přívětivému prostředí a jednoduchému designu. Nevýhodou platformy, ale i DeFi obecně je neexistující uživatelská podpora, která zde nemůže existovat již z podstaty decentralizace. Uživatelé jsou vlastníky svých kryptoměn v peněžence a sami si zodpovídají za všechny provedené akce. Jakmile je provedena interakce s chytrým kontraktem, nelze tuto akci již vrátit zpátky. To v kombinaci s celkově vyšším rizikem v DeFi indikuje, že pro tento typ platforem je vyžadována určitá technická zdatnost a znalost kryptoměnového prostředí obecně. Tyto nevýhody jsou však vyváženy možností většího zhodnocení držených kryptoměn. V případě PancakeSwap je to velmi vysoké APY u stakingu jejich nativního tokenu CAKE, pomocí kterého může uživatel dále ovlivnit budoucnost či směřování platformy, jelikož se jedná o governance token. PancakeSwap dále nabízí velice obsáhlou nabídku podporovaných kryptoměn. To je výhoda především pro investory, kteří mají strategii založenou na kryptoměnách s nízkou tržní kapitalizací.

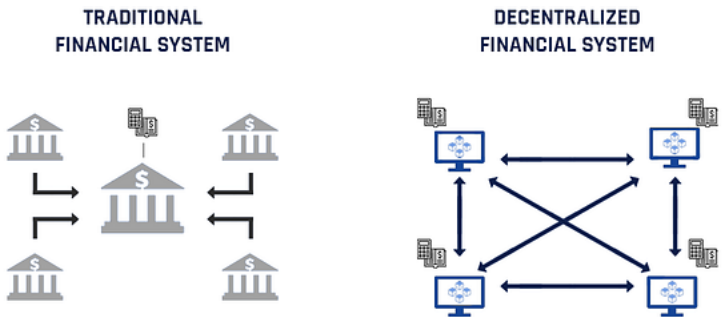
Pro začínající uživatele lze jednoznačně doporučit centralizované platformy, které poskytují nejmenší riziko, podporu fiat měn, přívětivé UI a uživatelskou podporu. Pokud má však uživatel zájem o vyšší zhodnocení svých držených kryptoměn, chce mít nad nimi plnou kontrolu a chce využít vícero nástrojů a možností, jak své kryptoměny zhodnotit, pak právě jemu jsou určeny platformy decentralizované.

4.3.3 DeFi a současný finanční systém

V souvislosti s decentralizovanými financemi se často mluví o kontrastu se současným finančním systémem. Oba systémy jsou však velice odlišné a jejich porovnání je tak náročné. Decentralizované finance jsou založeny na blockchainu a chytrých kontraktech, díky čemuž nepotřebují třetí stranu ani žádnou státní autoritu. Jejich uživatelé si za své finanční prostředky zodpovídají sami a jsou plně zodpovědní za své interakce v blockchainu.

Tradiční finanční systém je oproti tomu plně centralizovaný. Je založen na finančních institucích, například bankách, které zde fungují jako prostředník, a na centrální autoritě, která na vše dohlíží. Banka pak klientům spravuje svěřené finanční prostředky i aktiva a nabízí další služby, které mohou být řešeny prostřednictvím chytrých kontraktů.

Hlavní rozdíl tedy spočívá v tom, že DeFi systém není nijak regulován, není nikým ovládán, řízen je distribuovanou sítí uživatelů a k přesouvání financí není potřeba žádných prostředníků. Záznamy uložené na blockchainu jsou transparentní a všem dostupné v reálném čase, na rozdíl od centralizovaného systému, kde je často obtížné vystopovat peněžní toky.



Obrázek 16: Infografika DeFi a tradičního finančního systému

Zdroj: (Stably, 2019)

Pokud si chce například někdo vypůjčit finanční prostředky od banky, jeho osoba je důkladně prověřena včetně úvěruschopnosti. V DeFi jsou tyto procesy automatizovány chytrými kontrakty, a i vzhledem k chybějícímu KYC a anonymitě si může každý půjčit

libovolnou částku, dokud má dostupný kolaterál. V DeFi také může kdokoliv stát na straně věřitele nebo dlužníka, což vytváří více přístupný a flexibilní trh.

Dalším rozdílem je neexistence vstupní bariéry do ekosystému decentralizovaných financí. Kdokoli, kdo umí programovat, se může podílet na vyvíjení nebo přímo vyvíjet různé finanční nástroje založené na již vytvořených blockchainech. Využití open source kódu programátory a následné experimentování s volně přístupnými vývojářskými nástroji bez jakýchkoliv restrikcí či bariér může přinést benefity ve formě lepších finančních instrumentů. Centralizovaný systém je oproti tomu „zatížen“ mnohými regulacemi a nutnými licencemi. Vstup do tohoto prostředí je tak mnohem obtížnější, stejně jako provádění případných inovací.

Dalším důležitým hlediskem je vzhledem k decentralizované povaze DeFi odolnost vůči cenzuře. Žádný státní aparát nemůže zabránit decentralizovaným projektům a spojeným transakcím ve funkčnosti a provedení, což je velikou výhodou u opresivních státních režimů, které vysoce zasahují do soukromí svých občanů.

Naopak výhodou centralizace je dlouhodobě zavedená infrastruktura zahrnující banky, platební systémy a regulace, díky kterým je tento systém spolehlivý a vysoce stabilní. Stabilitu dále podporuje státní regulativní dohled a silný právní rámec. V případě selhání jsou navíc deposity v bankách pojištěny, a bankovní poradci mohou svým klientům v případě potřeby poskytnout profesionální finanční poradenství. DeFi je naopak v nynější podobě oproti centralizovanému systému velice rizikové a pro nezkušené uživatele skrývá mnoho bezpečnostních rizik a nástrah. Velkou výhodou centralizace je snadná dostupnost tradičních finančních služeb a jejich snadné používání, kterému se decentralizované projekty v současné době nemohou rovnat.

Funkce	Služba	DeFi	CeFi	Tradiční finanční systém
Obchodování	**Finanční převody**	DeFi stablecoiny	CeFi stablecoiny	Klasické peněžní systémy
	Obchodování aktiv	DEX (PancakeSwap)	CEX (Binance)	Burzy a OTC (over the counter)
	Obchodování derivátů			
Úvěry	**Zajištěné úvěry**	DeFi lending platformy (Compound)	CeFi lending platformy (Nexo)	Bankovní/nebankovní instituce
	Nezajištěné úvěry	Půjčky bez kolaterálu (Aave)	Kryptoměnové banky (Silvergate)	Bankovní/nebankovní instituce
Investování	**Investiční nástroje**	Kryptoměnové decentralizované fondy (Yearn.finance)	Kryptoměnové fondy (Grayscale)	Investiční fondy

Tabulka 5: Přehledová tabulka kryptoměnového a tradičního finančního systému

Zdroj: vlastní zpracování

Současný finanční systém je kontrolován velkými finančními institucemi, které mají kontrolu nad finančními trhy. Od roku 2008, kdy finanční krize odhalila slabiny tohoto systému, stoupá poptávka po více transparentním a decentralizovaném systému. Na to reagoval v roce 2009 Satoshi Nakamoto vytvořením decentralizované sítě Bitcoinu. Decentralizované finance, v podobě, v jaké je známe nyní, na původní myšlenku navázaly a dále ji rozvinuly. Byla tak vytvořena alternativa, která poskytuje svým uživatelům nástroje, díky kterým mohou získat plnou kontrolu nad svými financemi a osobními daty.

Centralizované i decentralizované finance mají své klady i zápory. DeFi je však stále relativně nové odvětví, a jako každá nová technologie sebou nese určitá rizika. Prozatím se jedná o zajímavou alternativu ke klasickému finančnímu systému, která stále zkoumá svůj potenciál. Při rozhodování potencionálních uživatelů budou hrát roli osobní preference, míra tolerance rizika, investiční strategie a místní regulace. Do budoucna bude důležité, jak se k tomuto odvětví postaví regulační orgány, a do jaké míry budou oba druhy finančních systémů spolupracovat.

4.4 Názor a predikce

Trh s decentralizovanými projekty, stejně jako celý trh s kryptoměnami momentálně prochází medvědím trhem. V případě kryptoměn je střídání býčího a medvědího trhu vcelku pravidelné a je závislé na půlení neboli tzv. halvingu Bitcoinu. Děje se tomu tak přibližně každé 4 roky a průběh každého cyklu bývá velice podobný. Při každém půlení se snižuje nabídka a tím se zvyšuje poptávka po Bitcoinu i jeho hodnota. To má za následek celkově větší poptávku po kryptoměnách společně s větším zájmem médií i veřejnosti.

Po dosažení vrcholu v každém cyklu přijde i pád, který je u kryptoměn vždy drastický. V celkové tržní kapitalizaci jde přibližně o 80-90 % korekci z předchozího dosaženého maxima. V takovém období o kryptoměnách není příliš slyšet v médiích, davová „psychóza" z býčího trhu opadá, a stejně tak opadá i investiční zájem veřejnosti. Médii pak kolují různé negativní články o Bitcoinu i jiných kryptoměnách, a často se spekuluje o zániku kryptoměn a je zmiňováno tzv. splasknutí bubliny. To se pokaždé změní s půlením Bitcoinu, kdy se po určité době, která je u každého cyklu odlišná, opět celý koloběh nastartuje a započne býčí trh. Veřejnost se poté začne o kryptoměny více zajímat, což má pozitivní vliv na jejich cenu.

V době psaní této práce prochází kryptoměnový trh svým třetím cyklem, kdy vrcholu již bylo dosaženo, avšak stále není známé dno tohoto cyklu. Je možné, že se tomu tak stalo 22. listopadu 2022, kdy tržní kapitalizace spadla pod úroveň 800 miliard dolarů[88], nelze to však prozatím s jistotou tvrdit. Určit přesně dno tohoto cyklu lze až v nastávající den půlení BTC, kdy započne čtvrtý cyklus, tento den připadá na 9. dubna 2024.[89]

V následující tabulce je přehledně znázorněn vliv půlení Bitcoinu na celý kryptoměnový trh z pohledu celkové tržní kapitalizace u každého dosud proběhlého cyklu.

[88] *Global Cryptocurrency Charts* [online]. Dover: CoinMarketCap, c2023 [cit. 2023-03-13]. Dostupné z: https://coinmarketcap.com/charts/

[89] *Bitcoin Halving Countdown* [online]. Montrouge: Binance Academy, c2023 [cit. 2023-03-13]. Dostupné z: https://academy.binance.com/en/halving

Cykly	Tržní kap. v den půlení BTC	Maximální tržní kap. cyklu	% nárůst	Dosažené dno	% pokles
1. cyklus	138 000 000 $ (28.11.2012)[90]	15 891 900 416 $ (05.12.2013)	11 416 %	3 233 929 984 $ (14.01.2015)	- 80 %
2. cyklus	10 235 998 868 $ (09.07.2016)	835 510 337 536 $ (07.01.2018)	8 062 %	100 715 455 995 $ (15.12.2018)	- 88 %
3. cyklus	163 885 241 188 $ (11.05.2020)	2 973 212 260 893 $ (10.11.2021)	1 714 %	?	?

Tabulka 6: Porovnání vlivu půlení BTC u jednotlivých cyklů na tržní kapitalizaci kryptoměnového trhu

Zdroj: vlastní zpracování

Na základě historických dat a dlouholetých autorových zkušeností lze konstatovat, že ideální čas k nákupu kryptoměn je v období medvědího trhu přibližně kolem jednoho roku po dosažení tzv. „peaku“, respektive maxima tržní kapitalizace v daném cyklu. V tomto období se zatím pokaždé kryptoměnový trh ocitl na svém cenovém dně. Je tak možné, že trh již svého cenového dna dosáhl v čtvrtém kvartálu roku 2022. To však zatím nelze s jistotou tvrdit. Dle autorových predikcí tomu tak s největší pravděpodobností již bylo, přičemž další začátek „bull runu“ neboli býčího trhu odhaduje na základě uvedených faktů a předchozích událostí zhruba v období kolem druhého a třetího kvartálu roku 2024. Je ovšem nutné zdůraznit, že přestože se historie často opakuje, nemusí to platit i pro další cykly. Kryptoměnový trh je velice volatilní a nelze tak s jistotou predikovat jeho budoucí vývoj. Důkazem toho jsou události třetího cyklu, kdy byl tento cyklus „napůlen“, a přestože svého maxima dosáhl dle původních předpokladů ve čtvrtém kvartálu roku 2021, nastal v letním období menší medvědí trh, se kterým nikdo nepočítal. Uvedená spekulace vychází ze zkušeností autora a historického sledu událostí. Nelze ji brát jako investiční radu, slouží pouze pro vzdělávací účely.

Decentralizované finance jsou odvětvím kryptoměn, a proto se jich bitcoinové cykly také týkají. Většina decentralizovaných platforem je založena na blockchainové síti Etherea, které je ovlivněno stejně jako ostatní altcoiny cenou Bitcoinu. Jakmile se trh ocitne v býku

[90] Tato hodnota byla získána odhadem, protože přesné tržní hodnoty před rokem 2013 nejsou dostupné. Ostatní data z: *Global Cryptocurrency Charts* [online]. Dover: CoinMarketCap, c2023 [cit. 2023-03-13]. Dostupné z: https://coinmarketcap.com/charts/

a zejména cena altcoinových tokenů začne opět rapidně stoupat, podpoří se vývoj nových projektů i množství inovací v tomto oboru. Spolu s tím se zvedne i zájem o decentralizované finance, což může přinést mnohem větší pozornost na tento sektor i větší využití těchto nástrojů veřejností, než tomu bylo doposud. Bude ovšem zapotřebí zapracovat na UI těchto platforem, aby se více přiblížily „běžné“ veřejnosti a jejich benefitů tak mohli využít i ti, kteří jsou méně technicky zdatní.

Názory na DeFi se mění, podobně jako na kryptoměny, společně s tím, v jaké fázi se aktuálně celý kryptoměnový trh nachází. Často zde funguje psychologie davu, a tak zatímco v býčím trhu panuje všeobecný pozitivní sentiment a většina odborníků se předbíhá s cenovými očekáváními, tak naopak v medvědím trhu, kdy přicházejí neustálé korekce trhu, se veřejnost od kryptoměn odklání a mnohdy je i zastáván názor, že se předchozí růst již nebude opakovat. Názory se tedy různí především s vývojovým stádiem kryptoměnového cyklu a při investičním rozhodování je třeba od tohoto faktoru odhlédnout a nepodléhat emocím.

S největší pravděpodobností DeFi nenahradí současný finanční systém, podobně jako kryptoměny nenahradí současný platební systém. Nynější podoba to ani neumožňuje, a nikdo neví, kam se bude budoucnost DeFi ubírat. Prozatím je současný stav celého sektoru přirovnáván ke stavu internetu v 90. letech, kdy také nikdo nevěděl, kam až se jeho vývoj a použitelnost může dostat. Do budoucna je však pravděpodobné, že decentralizované finance budou s tradičním systémem financí koexistovat a stále více spolupracovat. To by mohlo být přínosné pro obě strany a profitovat by z toho mohl následně i koncový uživatel.

5. Závěr

Tato práce se komplexně zabývá problematikou decentralizovaných financí v kryptoměnovém odvětví. Byla zkoumána jejich podstata, účel, potenciál a provedena analýza současného reálného využití finančních služeb a možností, které přináší.

V teoretické části se autor nejdříve věnoval historii a pozadí vzniku decentralizovaných financí. K porozumění tohoto kryptoměnového odvětví je nejdříve zapotřebí znalostí o kryptoměnách samotných. Proto se autor zpočátku věnuje původním kryptoměnám, tedy Bitcoinu a Ethereu, na kterých je vysvětlen princip fungování kryptoměn, jejich technologie, ale i vznik, historie a pozadí jejich vývoje. V této části je také detailně popsán princip blockchainu, stejně tak jako stěžejního prvku decentralizovaných financí, chytrých kontraktů.

V další části teoretické práce byly vybráni 4 zástupci decentralizovaných financí, které dle autora dobře vystihují diverzitu jednotlivých decentralizovaných platforem a možnosti, které toto odvětví kryptoměn v současné době nabízí. Tito zástupci jsou rozebráni z hlediska jejich historie, vzniku, použité technologie a principu fungování. Dále jsou charakterizovány a analyzovány z pohledu současného i budoucího využití.

Autor se poté zabýval hrozbami i riziky spojenými s decentralizovanými financemi, které jsou v tomto oboru poměrně časté, jelikož se stále jedná o relativně nové a rizikové odvětví. Jsou zde popsána a vysvětlena největší rizika, se kterými se může potencionální uživatel v případě interakce s DeFi setkat, a je vysvětleno, jak se jim vyhnout. Část je také věnována kritickému tématu zabezpečení kryptoměn a jejich bezpečnému uložení v hardwarových peněženkách, což je bohužel uživateli kryptoměn často podceňováno.

Další kapitola je věnována celkovému postoji legislativy České republiky ke kryptoměnám i decentralizovaným financím. Je zde uveden a popsán kompletní vztah českých státních orgánů k této problematice, který bohužel zatím není u všech orgánů koordinovaný. Dále je zde rozepsána současná problematika regulace a celkový vztah Evropské unie ke kryptoměnám i jejich chystané regulaci.

Praktická část diplomové práce se nejdříve zabývá DeFi z pohledu začínajícího uživatele a uvádí názorný postup, jak začít s decentralizovanými platformami interagovat a využívat jejich nástrojů. Tyto nástroje jsou posléze charakterizovány, analyzovány a mezi sebou vzájemně komparovány. Porovnány jsou zde z různých hledisek i platformy uvedené

v teoretické části práce, které tyto nástroje nabízí. V kapitole je také uveden modelový příklad dočasné ztráty, tedy jednoho z nejčastějších rizik při investování s decentralizovanými financemi.

S využíváním těchto nástrojů, ale i kryptoměn obecně, se pojí daňová problematika, kterou se zabývá další kapitola. Zdanění kryptoměn je často přehlížené téma a mnoho jejich uživatelů ani neví, vzhledem k nejednotnému a nerozhodnému postoji státních orgánů, jak tyto příjmy z kryptoměn správně danit. V této kapitole je proto tato problematika přehledně objasněna a zpracována včetně uvedení modelového příkladu zdanění kryptoměn z praxe pomocí používaných metod.

V další části práce jsou charakterizovány rozdíly mezi centralizovanými a decentralizovanými obchodními platformami, jejichž zástupci a funkce jsou analyzovány a následně komparovány z relevantních hledisek. Nelze přitom jednoznačně určit ideální obchodní platformu pro každého, protože každý typ platformy, ať už centralizované či decentralizované, slouží různým typům uživatelů s odlišnými preferenci. Na to následně navazuje kapitola, ve které se autor zabývá porovnáním současného stavu decentralizovaných financí s tradičním finančním systémem. Analyzuje zde rozdíly obou systémů, uvádí jejich klady i zápory a komparuje je z různých hledisek.

Na závěr této diplomové práce autor predikuje na základě svých dlouholetých zkušeností z tohoto oboru budoucí vývoj kryptoměn, odhaduje ideální dobu k jejich nákupu i následnému prodeji, a vysvětluje při tom fungování Bitcoinových cyklů a jejich vliv na celý kryptoměnový trh. Autor se dále zamýšlí nad budoucností decentralizovaných financí a psychologické stránce investování, kdy upozorňuje na rizika davové psychózy.

Dle autora se decentralizované finance v současné podobě nemohou dočkat masovějšího využití mezi širší veřejností. Vývoj v této oblasti je však velmi rychlý a současný stav lze přirovnat ke stavu internetu v 90. letech minulého století. Nelze předvídat, kam se jejich vývoj bude ubírat. Je však možné, že se do budoucna některé jejich prvky přenesou do tradičních financí, a že tyto dva velice odlišné světy budou vedle sebe koexistovat, možná i spolupracovat, aby nabídly svým uživatelům lepší produkty.

Tato diplomová práce je určena nejen pro zasvěcené uživatele kryptoměn, ale i pro všechny, kteří se zajímají o budoucnost finančního sektoru a o nové technologie, které mohou změnit způsob, jakým obchodujeme a investujeme.

6. Seznam použitých zdrojů

ANTONOPOULOS, Andreas M. a Gavin WOOD. Mastering Ethereum: Building Smart Contracts and DApps. Sebastopol: O'Reilly Media, 2018, s. 46-47. ISBN 978-1491971949.

Binance Earn [online]. Montrouge: Binance, c2023 [cit. 2023-03-12]. Dostupné z: https://www.binance.com/cs/earn

Bitcoin [online]. CoinMarketCap, c2022 [cit. 2022-11-13]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin/

Bitcoin Halving Countdown [online]. Montrouge: Binance Academy, c2023 [cit. 2023-03-13]. Dostupné z: https://academy.binance.com/en/halving

BUTERIN, Vitalik. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. [online]. 2014 [cit. 2022-11-18]. Dostupné z: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

Compound: Overview & History [online]. New York: Messari, 2020 [cit. 2022-12-19]. Dostupné z: https://messari.io/asset/compound/profile

Connect Your Wallet to PancakeSwap [online]. PancakeSwap, c2023 [cit. 2023-03-11]. Dostupné z: https://docs.pancakeswap.finance/get-started/connection-guide

CONWAY, Luke. What Is Bitcoin Halving? Definition, How It Works, Why It Matters [online]. New York: DotDash, 2022 [cit. 2022-11-13]. Dostupné z: https://www.investopedia.com/bitcoin-halving-4843769

Compound [online]. New York: Gemini Trust Company, c2022 [cit. 2022-12-19]. Dostupné z: https://www.gemini.com/cryptopedia/what-is-compound-and-how-does-it-work#section-how-compound-crypto-liquidity-pools-work

Crypto Insights #2. Decentralised Exchanges & Automated Market Makers – Innovations, Challenges & Prospects [online]. Hong Kong: KPMG Huazhen, 2021 [cit. 2023-03-12]. Dostupné z: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2021/10/crypto-insights-part-2-decentralised-exchanges-and-automated-market-makers.pdf

Decentralized Exchanges [online]. Singapore: CoinGecko, c2023 [cit. 2023-03-11]. Dostupné z: https://www.coingecko.com/en/exchanges/decentralized

Decentralized Finance a jiné peer-to-peer služby [online]. Praha: Blockchain Legal, 2022 [cit. 2022-12-26]. Dostupné z: https://www.kryptoregulace.cz/defi/

DeFi Insight: Concentrated liquidity on Uniswap V3 [online]. San Francisco: Medium, 2021 [cit. 2022-11-27]. Dostupné z: https://itsa-global.medium.com/defi-insight-concentrated-liquidity-on-uniswap-v3-9dce4e67c3e9

DeFi Investment Risks [online]. San Francisco: Coinbase, c2022 [cit. 2022-12-26]. Dostupné z: https://help.coinbase.com/en/coinbase/trading-and-funding/advanced-trade/defi-investment-risks

Digitální euro [online]. Frankfurt nad Mohanem: Evropská centrální banka, c2022 [cit. 2022-12-26]. Dostupné z: https://www.ecb.europa.eu/paym/digital_euro/html/index.cs.html

DOLEŽAL, Martin. Recenze decentralizované burzy PancakeSwap [online]. Praha: FINEX MEDIA, c2014-2022 [cit. 2022-12-12]. Dostupné z: https://finex.cz/recenze/PancakeSwap/

DOLEŽAL, Martin a Matouš VONDRÁK. K čemu u kryptoměn slouží privátní a veřejný klíč? [online]. Praha: FINEX MEDIA, 2022 [cit. 2022-11-13]. Dostupné z: https://finex.cz/kryptomeny-privatni-verejne-klice/

DUGGAN, Wayne a Michael ADAMS. What Is Ethereum 2.0? Understanding The Ethereum Merge [online]. New Jersey: Forbes Media, c2022 [cit. 2022-11-18]. Dostupné z: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-ethereum-2-merge/

Ethereum [online]. CoinMarketCap, c2022 [cit. 2022-11-18]. Dostupné z: https://coinmarketcap.com/currencies/ethereum/

Ethereum DeFi Ecosystem [online]. Los Angeles [cit. 2022-11-19]. Dostupné z: https://defiprime.com/ethereum

Ethereum Virtual Machine (EVM) [online]. CoinMarketCap, c2022 [cit. 2022-11-18]. Dostupné z: https://coinmarketcap.com/alexandria/glossary/ethereum-virtual-machine-evm

European Council Approves Crypto Regulation Bill [online]. New York: Dotdash Meredith, 2022 [cit. 2022-12-26]. Dostupné z: https://www.investopedia.com/eu-on-crypto-regulations-6747785

Evidence tržeb - Metodický pokyn k aplikaci zákona o evidenci tržeb [online]. Praha: Finanční správa, 2016 [cit. 2022-12-26]. Dostupné z: https://www.etrzby.cz/assets/cs/prilohy/Metodika-k-evidenci-trzeb_v1.0.pdf

Global Cryptocurrency Charts [online]. Dover: CoinMarketCap, c2023 [cit. 2023-03-13]. Dostupné z: https://coinmarketcap.com/charts/

HAMPL, Mojmír. Náš postoj ke kryptoměnám? Nepomáhat, nechránit, neškodit, nevodit za ruku [online]. Praha: ČNB, 2017 [cit. 2022-12-26]. Dostupné z: https://www.cnb.cz/cs/verejnost/servis-pro-media/autorske-clanky-rozhovory-s-predstaviteli-cnb/Nas-postoj-ke-kryptomenam-Nepomahat-nechranit-neskodit-nevodit-za-ruku/

HARVEY, Campbell R., Ashwin RAMACHANDRAN a Joey SANTORO. DeFi and the Future of Finance. New Jersey: Wiley, 2021, s. 12. ISBN 9781119836018.

HAYES, Adam. Stablecoins: Definition, How They Work, and Types [online]. New York: Dotdash Meredith, 2022 [cit. 2022-11-18]. Dostupné z: https://www.investopedia.com/terms/s/stablecoin.asp

History Of DeFi – From Inception To 2021 And Beyond [online]. Finematics, c2022 [cit. 2022-12-27]. Dostupné z: https://finematics.com/history-of-defi-explained/

Informace k daňovému posouzení transakcí s kryptoměnami [online]. Praha: Generální finanční ředitelství, 2022 [cit. 2023-03-12]. Dostupné z: https://www.financnisprava.cz/assets/cs/prilohy/d-seznam-dani/Info_kryptomeny_GFR.pdf

Introducing UNI [online]. Uniswap Labs, 2020 [cit. 2022-11-27]. Dostupné z: https://uniswap.org/blog/uni

Is PancakeSwap safe? [online]. PancakeSwap, 2022 [cit. 2022-12-12]. Dostupné z: https://docs.PancakeSwap.finance/#is-PancakeSwap-safe

Jak na zdanění kryptoměn [online]. Brno: Banky.cz, 2022 [cit. 2023-03-12]. Dostupné z: https://www.banky.cz/clanky/jak-na-zdaneni-kryptomen-kompletni-navod/

KARP, Hugh a Reinis MELBARDIS. NEXUS MUTUAL: A peer-to-peer discretionary mutual on the Ethereum blockchain. [online]. London: Nexus Mutual, 2019 [cit. 2022-12-25]. Dostupné z: https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf

KELLY, Liam. DeFi Review: What Is Nexus Mutual? Introduction to NXM [online]. New York: Crypto Briefing, 2020 [cit. 2022-12-27]. Dostupné z: https://cryptobriefing.com/defi-review-what-is-nexus-mutual-introduction-nxm/

KHARIF, Olga. DeFi Boom Makes Uniswap Most Sought-After Crypto Exchange [online]. London: Bloomberg, 2020 [cit. 2022-11-27]. Dostupné z: https://www.bloomberg.com/news/articles/2020-10-16/defi-boom-makes-uniswap-most-sought-after-crypto-exchange

KREJČÍ, Jaroslav. Kryptoaktiva nebudeme omezovat, řekl Dědek z ČNB. O měnách ale podle banky nemůže být řeč [online]. Praha: CZECH NEWS CENTER, 2021 [cit. 2023-03-13]. Dostupné z: https://www.e15.cz/kryptomeny/kryptoaktiva-nebudeme-omezovat-rekl-dedek-z-cnb-o-menach-ale-podle-banky-nemuze-byt-rec-1384390

Kryptoměny a DeFi: Co jsou to decentralizované finance? Jedná se o ekosystém budoucnosti?: Rizika a nevýhody DeFi – Na co si dát pozor? [online]. Praha: FINEX MEDIA, c2014-2022 [cit. 2022-12-26]. Dostupné z: https://finex.cz/rubrika/kryptomeny/defi/

Kryptopůjčky [online]. Montrouge: Binance, c2023 [cit. 2023-03-12]. Dostupné z: https://www.binance.com/cs/loan

KUDLÁČEK, Patrik. Smart contracts. Co jsou to smart contracts neboli chytré kontrakty? K čemu jsou a jak fungují? [online]. Praha: FINEX MEDIA, 2019 [cit. 2022-11-18]. Dostupné z: https://finex.cz/chytre-kontrakty-smart-contracts-co-jsou-a-jak-funguji/

LAM, Eric. Hackers Steal $40 Million Worth of Bitcoin From Binance Exchange [online]. Londýn: Bloomberg, 2019 [cit. 2023-03-12]. Dostupné z: https://www.bloomberg.com/news/articles/2019-05-08/crypto-exchange-giant-binance-reports-a-hack-of-7-000-bitcoin#xj4y7vzkg

LESHNER, Robert. Compound Governance is Live [online]. San Francisco: Medium, 2020 [cit. 2022-12-19]. Dostupné z: https://medium.com/compound-finance/compound-governance-decentralized-b18659f811e0

LESHNER, Robert. Compound Governance: Steps towards complete decentralization [online]. San Francisco: Medium, 2020 [cit. 2022-12-19]. Dostupné z: https://medium.com/compound-finance/compound-governance-5531f524cf68

Let's run on-chain decentralized exchanges the way we run prediction markets [online]. Reddit, 2016 [cit. 2022-11-27]. Dostupné z: https://www.reddit.com/r/ethereum/comments/55m04x/lets_run_onchain_decentralized_exchanges_the_way/

LEWIS, Antony. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them. Miami: Mango, 2018, s. 200. ISBN 978-1633538009.

Licenses & Registrations [online]. Zug: Nexo, c2023 [cit. 2023-03-12]. Dostupné z: https://nexo.io/licenses-and-registrations

Markets [online]. Compound Labs, c2023 [cit. 2023-03-13]. Dostupné z: https://app.compound.finance/markets?market=137_USDC_0xF25212E676D1F7F89Cd72fFEe66158f541246445

MIKULÁŠEK, Filip a Matouš VONDRÁK. Co jsou to stablecoiny? Můžeme se spolehnout, že stabilně udrží svoji cenu? [online]. Praha: FINEX MEDIA, c2022 [cit. 2022-11-19]. Dostupné z: https://finex.cz/co-jsou-stablecoiny-kryptomeny/

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. 2008 [cit. 2021-01-13]. Dostupné z: https://bitcoin.org/bitcoin.pdf

Nexus Mutual [online]. Claymont: Golden, c2022 [cit. 2022-12-25]. Dostupné z: https://golden.com/wiki/Nexus_Mutual-GZ5KXPP

Nexus Mutual (NXM): A Decentralized Alternative to Insurance [online]. New York: Gemini, 2021 [cit. 2022-12-25]. Dostupné z: https://www.gemini.com/cryptopedia/nexus-mutual-blockchain-insurance-nxm-crypto

OLINGA, Luc. FTX, BlockFi, Voyager, Celsius: Awful Year For Crypto Investors [online]. New York: TheStreet, 2022 [cit. 2022-12-26]. Dostupné z: https://www.thestreet.com/investing/cryptocurrency/ftx-blockfi-voyager-celsius-awful-year-

PancakeSwap [online]. DayTrading, c2022 [cit. 2022-12-12]. Dostupné z: https://www.daytrading.com/PancakeSwap

PancakeSwap [online]. New York: Messari, 2021 [cit. 2022-12-12]. Dostupné z: https://messari.io/asset/PancakeSwap/profile

PancakeSwap NFT Marketplace: A New Era Of NFT Trading On BSC [online]. Chain Debrief, 2021 [cit. 2022-12-12]. Dostupné z: https://chaindebrief.com/PancakeSwap-nft-marketplace-bsc/

PancakeSwap V2 and Current Roadmap Update [online]. BSC News, 2021 [cit. 2022-12-12]. Dostupné z: https://www.bsc.news/post/PancakeSwap-v2-and-current-roadmap-update

Poplatky za obchodování [online]. Montrouge: Binance, c2023 [cit. 2023-03-12]. Dostupné z: https://www.binance.com/cs/fee/schedule

Pre-recorded address by Commissioner McGuinness for event at EU Delegation in London on the EU Crypto-Asset Strategy [online]. Brusel: European Commission, 2022 [cit.

2022-12-26]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_7529

REIFF, Nathan. Dere There Cryptocurrencies Before Bitcoin?. Investopedia [online]. New York: Dotdash, 2019 [cit. 2022-11-07]. Dostupné z: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/

Rozsudek KSBR ze dne 17.02.2022 [online]. Zlín: AION CS, 2022 [cit. 2023-03-12]. Dostupné z: https://www.zakonyprolidi.cz/judikat/ksbr/30-af-29-2020-48

ROZSUDEK SOUDNÍHO DVORA [online]. Lucemburk: Soudní dvůr Evropské unie, 2015 [cit. 2022-12-26]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=CS

SAWINYH, Nick. Nexus Mutual - Smart Contract Insurance. Interview with founder. [online]. Los Angeles: DeFi Prime, 2019 [cit. 2022-12-25]. Dostupné z: https://defiprime.com/nexus-mutual

Security and Insurance [online]. Zug: Nexo, c2023 [cit. 2023-03-12]. Dostupné z: https://support.nexo.io/s/article/security-and-insurance

Sdělení Ministerstva financí k účtování a vykazování digitálních měn [online]. Praha: Ministerstvo financí ČR, 2018 [cit. 2022-12-26]. Dostupné z: https://www.mfcr.cz/assets/cs/media/Ucetnictvi_2018_Sdeleni-MF-k-uctovani-a-vykazovani-digitalnich-men.pdf

Stablecoins [online]. Berlin: Staking Rewards, c2023 [cit. 2023-03-11]. Dostupné z: https://www.stakingrewards.com/stablecoins/

STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky / Dominik Stroukal, Jan Skalický. Praha: Grada, 2018, s. 165-172. ISBN 9788027107421.

Studie OECD k decentralizovaným financím (DeFi) [online]. Praha: Ministerstvo financí ČR, 2022 [cit. 2022-12-26]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/inovace-na-financnim-trhu/aktuality/2022/studie-oecd-k-decentralizovanym-financim-46368/

SUCHAN, Stanislav. Zdanění kryptoměn u fyzických osob [online]. Brno: Seyfor, 2022 [cit. 2023-03-12]. Dostupné z: https://money.cz/novinky-a-tipy/dane/zdaneni-kryptomen-u-fyzickych-osob/

Syrup Pools [online]. PancakeSwap, c2023 [cit. 2023-03-11]. Dostupné z: https://pancakeswap.finance/pools

THE ETHEREUM VISION: A digital future on a global scale [online]. Ethereum Foundation, 2022 [cit. 2022-12-27]. Dostupné z: https://ethereum.org/en/upgrades/vision/

Today's Cryptocurrency Prices by Market Cap [online]. Dover: CoinMarketCap, c2023 [cit. 2023-03-11]. Dostupné z: https://coinmarketcap.com/tokens/

Token Swaps [online]. PancakeSwap, c2023 [cit. 2023-03-11]. Dostupné z: https://docs.pancakeswap.finance/products/pancakeswap-exchange/trade

Total Value Locked [online]. DefiLlama, 2022 [cit. 2022-12-27]. Dostupné z: https://defillama.com/

Understanding the Risks of DeFi [online]. San Francisco: Medium, 2022 [cit. 2022-12-26]. Dostupné z: https://medium.com/akropolis/understanding-the-risks-of-defi-5e3547433135

Uniswap [online]. CoinMarketCap, c2022 [cit. 2022-11-27]. Dostupné z: https://coinmarketcap.com/currencies/uniswap/

USDT / WBNB [online]. PancakeSwap, c2023 [cit. 2023-03-11]. Dostupné z: https://pancakeswap.finance/info/pairs/0x16b9a82891338f9bA80E2D6970FddA79D1eb0daE?chain=bsc

Vaults [online]. Yearn.finance, c2023 [cit. 2023-03-11]. Dostupné z: https://yearn.finance/vaults

VONDRÁK, Matouš. Impermanent loss: Zásadní problém při poskytování likvidity. Co to je a jak se tomu bránit? [online]. Praha: FINEX MEDIA, 2021 [cit. 2022-12-26]. Dostupné z: https://finex.cz/co-to-je-impermanent-loss-jak-se-branit/

WALTERS, Steve. Nexus Mutual Review (NXM): Defi Smart Contract Insurance [online]. Coin Bureau, 2020 [cit. 2022-12-25]. Dostupné z: https://www.coinbureau.com/review/nexus-mutual-nxm/

WALTERS, Steve. PancakeSwap Review: BNB Chain’s One Stop Defi Solution [online]. Coin Bureau, 2022 [cit. 2022-12-12]. Dostupné z: https://www.coinbureau.com/review/PancakeSwap-cake/

What is Compound? [online]. New York: Decrypt Media, 2020 [cit. 2022-12-19]. Dostupné z: https://decrypt.co/resources/compound-defi-ethereum-explained-guide-how-to

What is cryptocurrency Compound (COMP) and how does it work? [online]. Tallinn: Kriptomat, c2022 [cit. 2022-12-19]. Dostupné z: https://kriptomat.io/cryptocurrencies/compound/what-is-compound/

What Is MakerDAO And How It Works [online]. New York: 101 Blockchains, 2022 [cit. 2022-12-27]. Dostupné z: https://101blockchains.com/makerdao/

Why choose Nexo? [online]. Zug: Nexo, c2023 [cit. 2023-03-12]. Dostupné z: https://support.nexo.io/s/article/why-choose-nexo

WOLF, Karel. České „kladivo na kryptoměny“? Co má změnit chystaný zákon [online]. Praha: Internet Info, 2019 [cit. 2022-12-26]. Dostupné z: https://www.lupa.cz/clanky/ceske-kladivo-na-kryptomeny-co-ma-zmenit-chystany-zakon/

Yields [online]. DeFiLlama, c2023 [cit. 2023-03-11]. Dostupné z: https://defillama.com/yields

YOUNESSI, Cyrus. Uniswap — A Unique Exchange [online]. San Francisco: Medium, 2018 [cit. 2022-11-27]. Dostupné z: https://medium.com/scalar-capital/uniswap-a-unique-exchange-f4ef44f807bf