

VILNIAUS UNIVERSITETAS
EKONOMIKOS IR VERSLO ADMINISTRAVIMO FAKULTETAS

FINANSAI IR BANKININKYSTĖ

Magistranto Edo Karapetjano
MAGISTRO BAIGIAMASIS DARBAS

FINANSINIŲ NUSIKALTIMŲ ICO PROJEKTUOSE TYRIMAS	INVESTIGATION OF FINANCIAL CRIME IN ICO PROJECTS
---	---

Darbo vadovė: Prof. Dr. Alfreda Šapkauskienė

Vilnius, 2025

TURINYS

IVADAS	2
1. FINANSINIŲ NUSIKALTIMŲ ICO PROJEKTUOSE LITERATŪROS APŽVALGA	5
1.1 Decentralizuotų ekosistemų bei ICO projektų samprata	5
1.2 Decentralizuotų ekosistemų raida ir nusikaltimai ICO projektų kontekste	9
1.3 Pirminio viešo žetonų siūlymo nusikaltimo masto įtakos veiksnių nustatymo ir tyrimo teoriniai aspektai	13
1.3.1 Pagrindinės finansinių nusikaltimų sritys ICO projektuose	21
1.3.2 Decentralizuotų ir centralizuotų keityklų vaidmuo ICO projektuose bei finansinių nusikaltimų analizė.....	23
1.4 Finansinių nusikaltimų pirminiuose monetų siūlymuose tyrimų vertinimas ir pavyzdžiai. 26	
1.4.1 ICO rizikos balo kaip kintamojo naudojimas finansinių nusikaltimų ICO projektuose tyrimuose.....	29
1.4.2 Populiarumo kaip kintamojo naudojimas finansinių nusikaltimų ICO projektuose tyrimuose.....	30
1.4.3 Projekto surinktos sumos kaip priklausomojo kintamojo naudojimas finansinių nusikaltimų ICO projektuose tyrimuose	31
1.5 Finansinių nusikaltimų pirminiuose monetų siūlymuose tyrimo metodų identifikavimas 32	
2. FINANSINIŲ NUSIKALTIMŲ ICO PROJEKTUOSE EMPYRINIO TYRIMO METODOLOGIJA.....	36
2.1 Tyrimo tikslas, modelis ir hipotezės	36
2.2 Empyrinio tyrimo modelis	38
3. FINANSINIŲ NUSIKALTIMŲ ICO PROJEKTUOSE EMPYRINIS TYRIMAS.....	42
3.1 Finansinių nusikaltimų pirminiuose monetų siūlymuose empyrinis tyrimas	42
3.1.1 Keityklos tipo kaip kintamojo įtaka ICO projektų finansinio nusikaltimo mastui empyrinis tyrimas.....	45
3.1.2 Projekto populiarumo kaip kintamojo įtaka ICO projektų finansinio nusikaltimo mastui empyrinis tyrimas.....	48
3.1.3 Projekto rizikos balo kaip kintamojo įtaka ICO projektų finansinio nusikaltimo mastui empyrinis tyrimas.....	51
IŠVADOS IR PASIŪLYMAI.....	54
LITERATŪROS IR ŠALTINIŲ SĄRAŠAS	56
SANTRAUKA	62
SUMMARY	64
PRIEDAI.....	66

IVADAS

Darbo temos aktualumas. Kriptovaliutų skaičius pasaulyje sparčiai auga, o ši staigų didėjimą daugiausia lemia tai, kad privatūs ir juridiniai investuotojai palankiai vertina šią naują technologinę sritį. Kriptovaliutos tampa ne tik investiciniu turtu, bet ir atsiskaitymo priemone (Boyko, 2020). Pastebima, kad nuo 2013 iki 2023 metų sukurtų kriptovaliutų projektų skaičius išaugo net 141 kartą. Šiam staigiam naujų kriptovaliutų atsiradimui didelę įtaką turėjo ir atsiradęs naujas sutelktinio finansavimo būdas, vadinamas „ICO“ (pirminis monetų siūlymas). Šie projektai naudoja blokų grandinės technologiją, kad sukurtų žetonus, suteikiančius investicines galimybes į naujai į rinką išleistą potencialų projektą (Zetzsche, 2019). Didėjant kriptovaliutų projektų skaičiui, kai kurie kūrėjai pradėjo inicijuoti fiktyvius projektus, kurių pagrindinis tikslas buvo neteisėtai pasisavinti investuotojų kapitalą, taip įgyvendinant finansinius nusikaltimus. Dėl rinkos nestabilumo ir nepakankamos reguliacinės priežiūros šis investavimo metodas tapo itin rizikingu (Karpenko, 2021). Nors decentralizuotos finansinės sistemos siekia užtikrinti didesnę skaidrumą, tyrimų pavyzdžiai, tokie kaip (ICO) projektai – „Onecoin“, „AnubisDAO“, „Squid Game (SQUID) token“, – rodo, kad šioje rinkoje vis dar egzistuoja reikšminga aukštos rizikos projektų koncentracija. Šie projektai, kuriuose dėl lėšų pasisavinimo nukentėjo didelė dalis investuotojų, atspindi bendrą ICO rinkos situaciją, kur nepakankamas reguliavimas ir kontrolė sudaro sąlygas tokiems sukčiavimo atvejams (Cernera, 2023). Pateiktoje lentelėje (5 priedas) pastebimas naujai į rinką išleistų „ICO“ ir jų surinktų lėšų nepastovumas. Nors pastaraisiais laikotarpiais pastebimas naujai išleidžiamų „ICO“ projektų sumažėjimas, kriptovaliutų rinka yra cikliška, lygiagrečiai mokslininkai (Adhami ir kt. (2018), Karpenko ir kt. (2021), McGee ir Conlon (2021), Agarwal ir kt. (2023) (Trozze, 2023), ir kt.) savo darbuose pateikia ICO rinkos vertinimą, kaip gana mažai ištirtos ir neaiškos, rizikingos, be vieningų išvadų, metodinių nurodymų investuotojams ir įmonėms, siekiantiems efektyviai pasinaudoti pirminiu viešu žetonų siūlymu kaip investavimo ar finansavimo priemone. Todėl šiuo metu rinkai rodant teigiamas tendencijas svarbu ištirti kokią įtaką rinkos veiksniai tokie kaip ICO projekto rizikos balas arba populiarumas gali turėti projekto kapitalizacijai bei atliekam nusikaltimui joje, siekiant ateityje mažinti nekikrų projektų skaičių bei didinant skaidrumą ne tik ICO, bet ir visoje decentralizuotų finansų rinkoje.

Darbo naujumas. Analizuojant su nusikaltimais ICO projektuose susijusius tyrimus buvo pastebėta, jog egzistuoja trūkumas tyrimų, kurie tirtų butent finansinių nusikaltimų dydžio priklausomybę nuo ICO populiarumo, rizikos balo arba keityklos tipo kur bus listinama moneta.

Darbo problema. Ar egzistuoja nusikaltimo dydžio pirminiuose monetų siūlymuose priklausomybė nuo projekto populiarumo ir projekto turimo rizikos balo, ar keityklos kurioje bus listinamą moneta?

Darbo tikslas - nustatyti, ar egzistuoja nusikaltimo dydžio pirminiuose monetų siūlymuose priklausomybė nuo projekto populiarumo, projekto turimo rizikos balo ir keityklos tipo, kurioje listinama moneta, bei pateikti išvadas ir pasiūlymus investuotojams, siekiantiems efektyviai pasinaudoti pirminiu viešu žetonų siūlymu kaip investavimo ar finansavimo priemone

Darbo uždaviniai:

1. **Išanalizuoti** decentralizuotų ekosistemų ir ICO projektų sampratą, jų reikšmę bei atsiradimo priežastis, identifikuojant pagrindinius veiksnius, darančius įtaką finansinių nusikaltimų mastui. Aptarti teorinius ir praktinius aspektus, susijusius su rizikos balo, projekto populiarumo ir keityklos tipo įtaka finansiniams nusikaltimams bei įvertinti decentralizuotų ir centralizuotų keityklų vaidmenį šioje ekosistemoje.
2. **Parengti** empyrinio tyrimo metodologiją, kuri leistų analizuoti finansinių nusikaltimų ICO projektuose ryšius su jų populiarumu, rizikos balu ir keityklos tipu.
3. **Atlikti** empyrinį tyrimą, siekiant nustatyti, kaip keityklos tipas, projekto populiarumas ir rizikos balas lemia ICO projektuose surinktą sumą kaip finansinio nusikaltimo masto rodiklį.
4. **Pateikti** empyrinio tyrimo išvadas ir rekomendacijas investuotojams bei įmonėms dėl efektyvesnių rizikos valdymo strategijų ICO projektuose, siekiant sumažinti finansinių nusikaltimų riziką.

Tyrimo metodai:

1. **Mokslinės literatūros analizės metodas:** Šis metodas naudojamas atskleisti darbo metodiką ir uždavinius remiantis moksline literatūra.
2. **Lyginamosios analizės metodas:** Šis metodas naudojamas lyginant įvairius mokslinius tyrimus apie finansinius nusikaltimus ICO projektuose.
3. **Atvejų analizė:** Šis metodas naudojamas pateikiant konkrečius finansinių nusikaltimų ICO projektuose pavyzdžius juos aprašant analizuojant ir pateikiant autorių vertinimus.

4. **Statistinė analizė:** Atliekama aprašomoji statistika siekiant geriau įvertinti gautus empyrinio tyrimo rezultatus.
5. **Regresinė analizė:** Regresijos analizė leidžia atlikti statistinę reikšmingumo analizę, nustatant, ar įvertinti regresijos koeficientai yra statistiškai reikšmingi. Tai leidžia sužinoti, ar kintamieji, tokiu kaip listingo platforma, populiarumas ir rizikos balas, turi tikrąjį poveikį finansinių nusikaltimų nutikimui.

Darbo pradžioje remiamasi mokslinės literatūros analize ir autorių atliktais tyrimais, siekiant išsamiai suprasti decentralizuotų ekosistemų ir ICO projektų sampratą, jų reikšmę bei atsiradimo priežastis. Analizuojami įvairių autorių darbai, kurie nagrinėja ICO projektų populiarumo, rizikos balo ir keityklos tipo įtaką finansinių nusikaltimų mastui. Šis teorinis pagrindas leidžia identifikuoti pagrindinius veiksnius, darančius įtaką finansiniams nusikaltimams, ir atskleisti decentralizuotų bei centralizuotų keityklų vaidmenį šioje ekosistemoje. Literatūros analizė suteikia pagrindą tolesniems empyrinio tyrimo etapams, užtikrinant, kad tyrimo metodologija ir pasirinkti kintamieji atitinka jau atliktus mokslinius tyrimus ir jų išvadas. Atlikus empyrinį tyrimą, įvertinama, kaip šie veiksniai lemia surinktą sumą kaip finansinio nusikaltimo masto rodiklį. Galiausiai pateikiamos išvados ir rekomendacijos investuotojams bei įmonėms dėl efektyvesnių rizikos valdymo strategijų, siekiant mažinti finansinių nusikaltimų riziką ICO projektuose.

1. FINANSINIŲ NUSIKALTIMŲ ICO PROJEKTUOSE

LITERATŪROS APŽVALGA

1.1. Decentralizuotų ekosistemų bei ICO projektų samprata

Šiuolaikinėje pasaulio ekonomikoje tampa įprasta įsigyti prekes iš įvairių šalių: elektroniką iš Taivano, daržoves iš Meksikos, drabužius iš Kinijos, automobilius iš Pietų Korėjos ir taip toliau. Šis reiškinys yra tiesioginė globalizacijos proceso išdava ir puikus pavyzdys, iliustruojantis dabartinės pasaulinės ekonomikos funkcionavimo modelį (Dicken, 2014). Globalizacija apibrėžiama kaip „perėjimas prie vis labiau tarpusavyje susijusios ir integruotos pasaulio ekonomikos, kuri suteikia platesnes galimybes tiek verslo įmonėms, tiek individams“ (Gary, 2014). Globalizacijos kontekste atsiveria erdvės ir sąlygos finansinių technologijų evoliucijai, kurios viena reikšmingiausių naujovių – decentralizuotų finansų (angl. *Decentralized Finance, DeFi*) atsiradimas. Ši koncepcija, pagrįsta blokų grandinės (angl. *blockchain*) technologija, radikaliai keičia tradicines finansines sistemas, atsisakydama tarpininkų, tokių kaip bankai. Decentralizuoti finansai siekia užtikrinti tiesioginius, be tarpininkų vykdomus sandorius, kas reikšmingai keičia ekonominių santykių struktūrą. Tačiau, nors decentralizuotų finansų technologijos atveria naujas galimybes, jos taip pat kelia rimtų iššūkių, ypač susijusių su finansinių nusikaltimų prevencija. DeFi ekosistemos atsiradimas leidžia analizuoti jų skirtumus nuo tradicinių finansinių sistemų, įskaitant standartines valiutas ir įprastus ekonominius modelius. Decentralizuoti finansai apima:

- Įvairias technologijas ir procesus, kurie iš esmės keičia tradicinių valiutų ir finansinių institucijų veikimo principus, tačiau kartu kelia riziką dėl mažesnės reguliavimo kontrolės ir didesnės galimybės neteisėtiems veiksams.
- Veiklą decentralizuotuose blokų grandinės tinkluose, todėl nebereikia centrinių institucijų ar tarpininkų. Išmaniosios sutartys savarankiškai vykdo sandorius.
- Minimizuoja arba panaikina tarpininkus, leisdamą naudotojams tiesiogiai kontroliuoti savo turtą ir sandorius per išmaniuosius kontraktus.
- Skatina finansinę įtraukti, suteikdama galimybę naudotis finansinėmis paslaugomis asmenims, neturintiems galimybės naudotis tradicinėmis bankų paslaugomis. Dalyvauti gali visi, turintys interneto ryšį.
- Veikia pasauliniu mastu, todėl vartotojai visame pasaulyje gali dalyvauti be geografinių apribojimų. Sandoriai neturi sienų.

Tradicioniai finansai ir jų ypatybės:

- Centralizuotos sistemos, kuriose tarpininkai, tokie kaip bankai ir finansų įstaigos, palengvina sandorius. Remiasi centralizuota kontrole ir reguliavimo institucijomis.
- Tradiciniuose finansuose vykdoma stipri veiklos bei sandorų kontrolė.
- Prieigą prie jų gali riboti geografinė padėtis, finansinis statusas arba reguliavimo kliūtys, o tai riboja dalyvavimą finansinėje ekosistemoje.
- Susiduria su tokia rizika kaip sukčiavimas, kibernetinės atakos ir sisteminės klaidos. Saugumo priemonės dažnai įgyvendinamos per centralizuotus subjektus.

DeFi apima įvairias technologijų, verslo modelių ir organizacinių struktūras, paprastai pakeičiančias tradicines finansinio tarpininkavimo formas. Pasirinkimas tarp DeFi ir tradicinio finansavimo priklauso nuo individualių pageidavimų, tolerancijos rizikai ir pageidaujamo finansinių ir naujovių pažinimo lygio (Zetzsche, 2020). Pažymėtina ir tai, kad DeFi remiasi technologijomis, o ne tradicine bankininkyste, taip iš esmės palengvindamas sandorių tarp dviejų šalių sudarymą. Atvirojo kodo protokolai, sukurti viešosiose blokų grandinėse, sudaro decentralizuotos finansinės veiklos pagrindą. Dėl didėjančios duomenų apdorojimo galios, duomenų saugojimo, mažėjančių sąnaudų ir ryšio pralaidumo, DeFi tapo itin plačiai naudojamas visame pasaulyje (Chen, 2018). Kriptovaliuta – tam tikri skaitmeniniai failai, užpildyti informacija ir užkoduoti kriptografijos būdu. Tai failai, kurie yra sukurti naudojant viešojo bei privačiojo raktų poras, sukurtas aplink konkretų šifravimo algoritmą (Nakamoto, 2008). Taip pat tai apima du pagrindinius veikiančios finansų sistemos komponentus – infrastruktūrą ir valiutą. DeFi, siekiant pašalinti centralizuotų komponentų poreikį, dažniausiai remiamasi „Ethereum“ blokų grandinės protokolu, kuris tarnauja kaip decentralizuota platforma programų kūrimui. „Ethereum“ technologija suteikia galimybę kurti ir naudoti išmaniąsias sutartis (angl. *smart contracts*) – programinį kodą, kuris automatizuoja finansinių paslaugų teikimą ir valdymą, užtikrinant didesnę efektyvumą, skaidrumą bei sandorių saugumą be tarpininkų įsikišimo. Stabilios monetos, pavyzdžiui, DAI, atlieka svarbų vaidmenį DeFi sistemoje, atspindėdamos standartinės valiutos, tokios kaip euras ar doleris, vertę ir palaikydamos decentralizuotą finansų sistemą stabilesne. DeFi privalumai neapsiriboja vien mokėjimais internetu, bet apima įvairius finansinius aspektus, pavyzdžiui, valiutų keitimą, paskolas, draudimą ar netgi taupymo planus (Wronka, 2023). Decentralizuotas kriptovaliutų pobūdis, pagrįstas paskirstytųjų registrų technologija, suteikia galimybę vykdyti sandorius tarp pseudoniminių naudotojų, nereikalaujant patikimo tarpininko. Naudojant tokias kriptovaliutas kaip „Bitcoin“, papildomai gali būti

taikomos pagalbinės technologijos, kurios maišo norimą kriptovaliutos kiekį su kitomis valiutomis rinkoje prieš atliekant sandorį (Mackenzie, 2022). Tokie metodai dar labiau sustiprina sandorių anonimiškumą ir užtikrina aukštesnį privatumo lygį. Privatumo poreikis skatina naujų projektų, tokių kaip „Zerocoin Project“, kūrimą. Projektas „Zerocoin“ siūlo privatumo didinimo protokolą, kuris veikia per dviejų etapų procesą, įtraukiantį depozitinę sąskaitą ir laikiną valiutą „Zerocoin“. Pirmiausia siuntėjas perveda savo turimą „Bitcoin“ į depozitinę sąskaitą, kur sukuriamą lygiavertę „Zerocoin“ valiutos sumą. Vėliau ši laikina valiuta persiunčiama gavėjui. Kadangi „Zerocoin“ sandoriai nėra registruojami „Bitcoin“ blokų grandinėje, jie tampa sudėtingiau atsekami (Naganuma, 2017). Gavėjas gali išpirkti „Zerocoin“ valiutą naudodamas nulinio žinojimo įrodymus (angl. *zero-knowledge proof*), kurie išsaugo sandorio privatumą, nes tarp siuntėjo ir gavėjo nėra tiesioginio ryšio. „Zerocoin“ technologija pašalina poreikį naudoti valiutų maišymo paslaugas, nes konvertavimo procesas vykdomas tiesiogiai protokolo lygyje. Šis protokolas buvo iš pradžių pasiūlytas pritaikyti „Bitcoin“ valiutai, tačiau šiuo metu naudojamas alternatyviose kriptovaliutose, tokiose kaip „Zcash“, „Dash“ ir „Monero“ (Hendrickson, 2022). Dėl savo anonimiškumo ir privatumo užtikrinimo šios technologijos tampa patrauklios naudotojams, siekiantiems išvengti tradicinių mokėjimo sistemų stebėsenos. Jeigu ateityje gryniesi pinigai būtų uždrausti, naudotojai, kurie pirmenybę teikia anonimiškiems sandoriams, greičiausiai rinktųsi kriptovaliutas kaip alternatyvą finansiniam privatumui išlaikyti (Hendrickson, 2022). Toks pokytis neabejotinai skatintų kriptovaliutų rinkos plėtrą. Naujų finansinių technologijų pažanga ir anonimiškumo užtikrinimas prisideda prie to, kad vis daugiau žmonių renkasi kriptovaliutas kasdieniams mokėjimams ir investicijoms. Tačiau kartu su šių technologijų populiarumu auga ir jų naudojimas neteisėtoms veikloms. Ši beveik visiškai nekontroliuojama ir anonimiška decentralizuotų finansų ekosistema sudaro sąlygas finansiniams nusikaltimams, didindama jų riziką ir sudėtingumą.

Kriptovaliutų skaičius pasaulyje sparčiai auga (žr. 1 paveiksl.), šis staigus augimas buvo nulemtas, to jog privatūs ir juridiniai investuotojai šią naują vertiną teigiamai. Kriptovaliutos laikui bėgant tapo ne tik investicinis turtas, tačiau ir atsiskaitymo priemone (Boyko, 2020). Pastebima, jog buvo sukurta daug naujų projektų susijusių su kriptovaliutomis ir valiutų skaičius nuo 2013 iki 2023 metų išaugo net 141 kartą. Prie tokio staigaus naujų kriptovaliutų skaičiaus augimo stipriai prisidėjo ir naujai atsiradę sutelktinio finansavimo būdai ICO, IDO IEO. ICO, IDO, IEO kurie paprastai naudoja blokų grandinės technologiją, kad pasiūlytų žetonus, kurie suteikia įvairias teises mainais už sukurtą ir naujai į rinką išleistą kripto valiutą. Tokie projektai gali būti laikomi sutelktinio finansavimo ir blokų grandinės jungtimi (Zetzsche, 2019). Šie sutelktinio finansavimo

būdai sparčiai prisidėjo prie kriptovaliutų kiekio augimo, tiek prie populiarinimo, kadangi fiziniai investuotojai investavę į ateityje sėkmingą projektą gaudavo didelius investicinius pelnus, o sėkmingi projektai toliau tęsdavo veiklą kripto srityje (Howell, 2019). Tačiau dėl aukšto anonimiškumo ir žemo kontrolės lygio projektų kūrėjai pradėjo piknaudžiauti esama situacija ir pasitaikydavo atvejų kai projektų kūrėjai išsvaistydavo arba nusišavindavo investuotojų pinigus taip atlikdami finansinį nusikaltimą (Mackenzie, 2022). Todėl nesant realiai kripto turto kontrolei šie investavimo būdai tapo aukštos rizikos investuotojams ir investuotojai pradėjo stipriau vertinti projektų rizikingumą ir atsižvelgti į platesnę spektą veiksnių (Karpenko, 2021). Nors pastebima (Priedas nr. 5), jog tokia investicinė rinka kaip ICO šiuo metu yra ženkliai susitraukusi, tačiau lygiagrečiai vertinama, jog kriptovaliutų rinka yra cikliška ko pasekoje įvairių veiksmų populiarumas priklauso nuo bendros rinkos situacijos, taip pat galima pastebėti rinkos cikliškumą, todėl yra prielaidų teigti, jog ICO rinka turi galimybių atsistatyti ir ateityje projektų apimtys didės. Šiuo metu daugiausiai ICO vyksta Jungtinėse Amerikos Valstijose, kurios yra ICO palanki šalis. Amerikos teisės aktai yra gana detalūs kripto atžvilgiu. 2017 m. JAV Vertybinių popierių komisija pripažino, kad galiojantys teisės aktai turėtų būti taikomi ir žetonams ir ICO. Vienas iš pastaruoju metu daugiausiai dėmesio sulaukusių reguliavimo veiksmų yra JAV Vertybinių popierių ir biržos komisijos (SEC) gruodžio mėn. 2020 m. ieškinys prieš "Ripple" ir du jos vyresnius vadovus dėl to, kad jie tariamai vykdė JAV dolerių 1,3 mlrd. vertės neregistruotą XRP žetonų siūlymą. Po šio pranešimo "Ripple" prekyba buvo sustabdyta, o XRP vėliau atpigė 31 proc. (Karpenko, 2021).

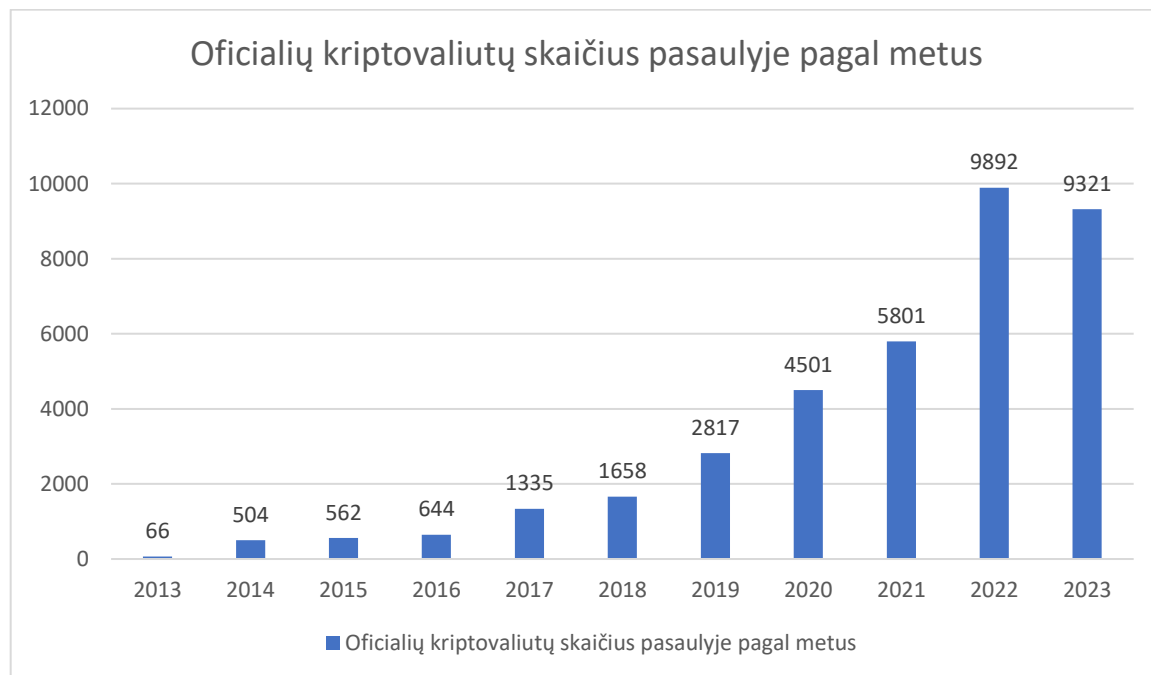
Globalizacijos procesai ir finansinių technologijų plėtra reikšmingai transformuoja šiuolaikinę pasaulinę ekonomiką, atveriant naujas galimybes ir kartu keliant naujus iššūkius. Decentralizuoti finansai (DeFi), pagrįsti blokų grandinės technologija, keičia tradicinę finansų sistemą, pašalindami tarpininkus, didindami finansinę įtrauktį bei suteikdami galimybę naudotis finansinėmis paslaugomis pasauliniu mastu. Tačiau DeFi ir susijusių inovacijų, tokių kaip pirminiai monetų siūlymai (ICO), ekosistemos pasižymi aukštu anonimiškumo lygiu ir nepakankamu reguliavimu, kas skatina finansinių nusikaltimų plitimą. Nors ICO rinka patyrė susitraukimą dėl sukčiavimo atvejų ir reguliavimo trūkumo, ji išlieka perspektyvi dėl savo cikliškumo ir galimų reguliacinių patobulinimų, ypač rinkose, kuriose teisinė aplinka yra palanki inovacijoms. Todėl siekiant suderinti finansinių technologijų pažangą su saugumo ir reguliavimo poreikiais, būtina gilinti supratimą apie decentralizuotų finansų keliamus iššūkius bei stiprinti reguliavimo priemones.

1.2 Decentralizuotų ekosistemų raida ir nusikaltimai ICO projektų kontekste

Kriptovaliutų atsiradimas siejamas su Bitcoin kriptovaliuta sukurta 2008 metais, ši valiuta labai greitai įgavo populiarumą ir jau 2011 metais pradėjo reguliariai fiksuoti daugiau nei 1000 sandorių per dieną. Privačių subjektų sukurtas kripto turtas tapo plačiai paplitusiu ir lengvai prieinamu tarpvalstybiniu reiškiniu (Stunžinas, 2018).

1 paveikslas.

Oficialių kriptovaliutų skaičius pasaulyje pagal metus (2013-2023m.)



Šaltiniai: Skaičiavimai atlikti autoriaus remiantis duomenų bazės „Statista“ duomenimis.

Pateiktame paveiksle galima pastebėti, jog oficialių rinkoje esančių kriptovaliutų skaičius per pastaruosius 10 metų išaugo daugiau kaip 141 kartų. Su kriptovaliutomis susiję reguliavimo iššūkiai įvairiose šalyse skiriasi, todėl atsiranda reguliacinis arbitražas. Legalios ir nelegalios kriptovaliutų rinkos egzistuoja kartu, legali veikla, ypač kriptovaliutų, daugiausia vykdoma kriptovaliutų biržose spekuliaciniais tikslais. Neteisėta veikla apima juodojo interneto rinkas, pinigų plovimą, išpirkos mokėjimus ir vagystes, naudojant kriptovaliutas kaip mokėjimo priemones (Houben., 2020). Vieni iš pirmųjų bitkoinų naudotojų tai darė neteisėtais būdais; JAV kovos su narkotikais tarnybos analizė administracijos (DEA) duomenimis, 2013 m. apie 90 % "Bitcoin" sandorių buvo susiję su nusikalstama veikla, galimu narkotikų platinimu (Butler, 2019). O pagal Foley ir Karlsen (2019) atliktą tyrimą apie kriptovaliutas ir per jas atliekamą nusikaltimų finansavimą pastebima, kad beveik pusė metinių bitkoinų sandorių iki 2016 metų buvo susiję su

neteisėta veikla. Siekiant kovoti su nusikaltimais decentralizuotoje sistemoje šiais laikais daug dėmesio skiriama kovos su finansiniais nusikaltimais ir teisės aktų, nukreiptų prieš neteisėtą kriptovaliutų naudojimą tobulimą (Yadav, 2022). Be to, pabrėžtina, jog reikšmingas privačių kripto monetų, skirtų lėšų rinkimui, skaičiaus augimas ir stabilijų monetų bei centrinio banko skaitmeninių valiutų (CBDC) atsiradimas yra labai svarbūs žingsnis siekiant nustatyti ribojimus kripto turtui (Bindseil, 2020).

Realios priežiūros nebuvimas kelia susirūpinimą dėl didelio daugelio kriptografinių aktyvų kintamumo ir neįrodyto atsparumo (Hauben, 2020). Vienas iš garsiausių tokių projektų, kuris buvo didelio masto finansinis nusikaltimas yra „OneCoin“. Šis projektas veikė finansinės piramidės principu ir buvo reklamuojamas tinklinio marketingo sistema. Kiekvienas „OneCoin“ investuotojas buvo įtraukiamas į tam skirtos socialinės medijos grupę, kurioje buvo skelbiama, jog už kiekvieną atvestą papildomą investuotoją esami investuotojai gaus dalį nuo naujo investuotojo į kriptovaliutą investuotų lėšų. Todėl „OneCoin“ grupės nariai-investuotojai buvo suinteresuoti, jog į šį projektą būtų pritraukta kaip galima daugiau žmonių. Ši tinklinio marketingo sistema gana sėkmingai veikė ir nuo 2014 metų ketvirtojo ketvirčio iki 2016 metų ketvirtojo ketvirčio investicijos į „OneCoin“ projektą sudarė maždaug 300 milijonus dolerių. Nuo pat „OneCoin“ įkūrimo pradžios, šio kripto projekto įkūrėjai Ruja Ignatova ir Sebastianas Grienwoodas naudojos „Bitcoin“ žinomumu, kad įtikintų investuotojus, jog „OneCoin“ yra kita „nepraleidžiama“ investavimo galimybė. Sebastianas Grienwoodas parengtame „OneCoin PowerPoint“ pristatyme: „OneCoin“ projektas buvo apibūdinamas kaip unikalus ir novatoriškas kripto projektas, kuris yra pateikiamas į kripto investicijų rinką garsiosios kriptovaliutos „Bitcoin“ sėkmės pagrindu. Sekančioje skaidrėje „OneCoin“ pabrėžė staigų „Bitcoin“ augimą, teigdama, kad „2013 metais „Bitcoin“ vertė padidėjo 75 kartus“. Tačiau skirtingai nuo tokių kriptovaliutų kaip „Bitcoin“ ar „Ethereum“, „OneCoin“ realios vertės neturėjo ir projekto kūrėjų: Rujos Ignatovos ir Sebastiano Greenwoodo buvo sugalvotas tam, jog galutinėje projekto stadijoje išvilioni iš investuotojų pinigus bei pasisavinti juos. „OneCoin“ projekto steigėjai melavo savo nariams apie tai, kaip vertinama jos kriptovaliuta, teigdami, kad „OneCoin“ kaina pagrįsta rinkos kapitalizacija bei pasiūla ir paklausa, nors iš tikrųjų patys „OneCoin“ įkūrėjai savavališkai programuotojų pagalba nustatydavo monetos vertę, neatsižvelgdama į rinkos jėgas. Tariamą „OneCoin“ vertę nuo 2019 metų sausio mėnesio augo nuo 0,50 euro iki 29,95 eurų už monetą. „OneCoin“ monetos kaina visą projekto veikimo laikotarpį niekada nemažėjo, tokie rezultatai investuotojus įkvėpė sparčiai investuoti (Sapkota, 2020). Pirmoji pradėjusi skelbti apie tai, jog šis projektas yra finansinio sukčiavimo Ponzi schema buvo „Norvegijos tiesioginės

prekybos asociacija“. Ji pirmoji detaliau išnagrinėjo „OneCoin“ kriptovaliutos kodą ir paskelbė, jog šis projektas yra niekuo nepagrįstas, jog nėra atskiros šio projekto blokų grandinės bei paneigė Rujos Ignatovos ir Sebastiano Greenwoodo skelbtas žinias, jog šią kriptovaliutą kaip ir kitas didžiasias kripto valiutas galima „kasti“. Kaip savo tinklaraštyje rašo „Niujorko pietinės apygardos JAV prokuratūra“ bendrai apie 4 milijardai dolerių iš skirtingų investuotojų buvo investuota į šią apgaulišką kriptovaliutą. Patys šios finansinės schemos kūrėjai iš investuotojų pavogė daugiau nei 500 milijonų dolerių ir ši finansinė schema iki šiol yra laikoma viena didžiausių finansinių apgaulių kripto decentralizuotoje ekosistemoje.

Pagal „CryptoVantage“ duomenis antras pagal dydį bei nukentėjusių investuotojų skaičių yra „AnubisDAO“ šis projektas buvo sukurtas 2021 metų spalį, po to kai rinkoje stipriai pradėjo populiarėti tokios niekuom neparemtos kriptovaliutos kaip „Dogecoin“ ir „Shiba Inu“. „AnubisDA“ kriptovaliuto valiuta iš kriptovaliutų investuotojų surinko 13 556 ETH. Tačiau praėjus vos 20 valandų nuo lėšų surinkimo, ETH buvo išsiųsti į skirtingus adresų pinigines taip pasisavinant investuotojų lėšas. Tinklaraščio „CryptoNews“ duomenimis po dvejų metų blokų analitikai pastebėjo tendenciją, kad lėšos (13 556 ETH) buvo konvertuotos į „Polygon“ kriptovaliutą, o tada išsiųstos į du skirtingus „Polygon“ adresus. Šios lėšos buvo pervestos per „Tornado Cash“ - kriptovaliutų skirstytuvą, kurio viena iš pagrindinių funkcijų yra visiškai nuasmeninti sandorius. 2022 metų rugpjūčio 8 dieną Jungtinių Amerikos Valstijų Izdo departamento Užsienio turto kontrolės biuras (OFAC) pritaikė sankcijas virtualios valiutos maišytuvui „Tornado Cash“ už tai, kad nuo 2019 metų jis leido nesąžiningiems kriptovaliutos turėtojams legalizuoti apie 7 milijardus dolerių. Šios kriptovaliutų platformos veikimas stipriai prisidėjo prie to, jog dalis naujai į rinką išleistų bei sutelktinio investavimo ieškančių projektų lėšų būtų nusisavinta. Kadangi decentralizuotoje finansų sistemoje daugelis transakcijų yra anonimiškos ir transakcijos yra vykdomos blokų grandinėje, o ne per patvirtintas mokėjimų sistemas. Daugeliu atvejų nėra įmanoma kontroliuoti lėšų, kurias investuotojai yra investavę į tam tikrą projektą, kadangi atlikus investiciją į pirminį monetų siūlymą (ICO), lėšos surinktos iš investuotojų per monetų siūlymą turi būti skirtos projekto vystymui – tai reiškia, jog galią disponuoti lėšomis įgauna projekto savininkas (Wilson., 2022).

Remiantis tinklaraščiu „Washington Post“ trečias pagal dydį ir aktualumą finansų iš investuotojų įsisavinimas naudojant pirminį monetų siūlymą yra pagal „Netflix“ serialą sukurta kripto moneta „SQUID token“. Šios monetos kūrėjų tikslinė auditorija buvo jaunieji investuotojai, kurie siekia maksimaliai greitos gražos trumpuoju laikotarpiu. Šio projekto idėja buvo paremta novatorišku „Žaisk kad uždirbtum“ sprendimu. Pagal projekto

„Baltąjį lapą“ investuotojai galėjo žaisti vaizdo žaidimus, taip virtualioje erdvėje uždirbti kriptovaliutą, kurią ateityje per CEX bus galima konvertuoti į standartines valiutas tokias kaip eurai ar doleriai. Toki „Žaisk kad uždirbtum“ kripto projektai 2021 metais traukė didelį investuotojų dėmesį ir šiam projektui tik patėkus į rinką jis pritraukė didelį investuotojų susidomėjimą. Pagrindiniai šio projekto investuotojai buvo nuo 16 iki 30 metų turintys asmenys. Šiam projektui populiarėjant augo ir projekto kaina bei kapitalizacija. Pastebima (6 Priedas), jog vos atsiradus „SQUID“ kripto valiutai, jos kaina siekė vos 0.04405 dolerio. Tačiau iškart pradėjus pirmuosius prieš projektinius monetų siūlymus paklausa šia moneta buvo tokia didelė, jog didėjant kapitalizacijai šios kriptovaliutos kaina per 4 dienas išaugo beveik 874 kartus. Toks spartus augimas dažnai atkreipia didelį investuotojų dėmesį, todėl šios kriptovaliutos paklausa augant kainai vis didėjo. Pasiekus piko kainos tašką – 38.48 dolerius už vieną „SQUID“ skaitmeninę monetą. Projekto organizatoriai pasinaudodami tyčinėmis spragomis sukurtos monetos kode pasisavino investuotojų investuotas lėšas. Atliekant šio finansinio nusikaltimo tyrimą per „Binance Smart Chain“ blokų grandinės naršyklę, buvo nustatyti aštuoni su sukčiavimu susijusieji piniginių adresai. Vienas iš adresų, kuriam priklauso penki procentai visų apyvartoje esančių „SQUID“ monetos, iškeitė 3,38 milijono dolerių vertės „SQUID“ monetų į „BNB“ monetas, prieš išsiųsdamas lėšas per kriptovaliutų maišytuvą „Tornado Cash“.

Vertinant darbe pateiktus finansinius nusikaltimus, pastebima, kad „OneCoin“, „AnubisDAO“ ir „SQUID“ yra trys skirtingos kriptovaliutų projektų kategorijos, kurios išsiskiria savo bruožais. „OneCoin“ veikė kaip finansinė piramidė su socialinio tinklinio marketingo strategija pritraukiant investuotojus. Ši schema sukėlė iliuzijas apie unikalumą ir didelę investicinę galimybę, naudojant tinklo narių prisitraukimą. Rezultatas – didelis investicijų surinkimas, neparemtas jokia realia verte, sukeldamas milžinišką nuostolį investuotojams. „AnubisDAO“ buvo naujas projektas, kuris pasinaudojo populiarėjančiomis „Meme“ tipo jokių projektu neparemtomis kriptovaliutomis. Sukurtas kaip kriptovaliutų investicinis fondas, jis naudojo „Polygon“ ir „Tornado Cash“ nusišavinant investuotojų lėšas ir taip pat išlaikant anonimiškumą. „SQUID token“ atveju buvo pasinaudota tuo metu populiariu „Netflix“ serialu taip pritraukiant jaunuosius investuotojus, o lėšos taip pat buvo nusišavintos naudojant „Tornado Cash“ kriptovaliutų maišytuvą. Abu atvejai taip pat parodo, kad decentralizuotos finansinės sistemos anonimiškumas ir technologinės spragos gali leisti organizatoriams nelegaliai pasisavinti investuotojų pinigus. Šie įvykiai taip pat padėjo atskleisti decentralizuotų projektų saugumo spragas ir skatinti Europos sąjungos teisės aktų griežtinimą dėl decentralizuotų sistemų reguliavimo. Siekiant sumažinti su pinigų plovimu ir teroristų finansavimo rizika, susijusia

su krypto turtu, ES teisės aktų leidėjas į Kovos su pinigų plovimu ir teroristų finansavimu (AML/CFT) sistemą įtraukė „piniginių paslaugų teikėjus“ ir „paslaugų teikėjus, teikiančius virtualiųjų valiutų ir fiat valiutų mainų paslaugas“. Šiuo įtraukimu jie priskiriami prie įpareigotųjų subjektų pagal 2018 m. gegužės 30 d. priimtą Penktąją kovos su pinigų plovimu direktyvą. Šis žingsnis buvo vienas pirmųjų, kurie gana ženkliai prisidėjo prie skaidresnės keityklų veiklos. Sustiprinti subjektų užsiimančių krypto turto veikla „Pažink savo klientą“ standartų vykdymas verčia rinkos dalyvius elgtis skaidriau decentralizuotų finansų rinkoje.

1.3 Pirminio viešo žetonų siūlymo nusikaltimo masto įtakos veiksnių nustatymo ir tyrimo teoriniai aspektai

Finansiniai nusikaltimai kriptovaliutų sektoriuje yra sparčiai augantis ir ypač svarbus klausimas tiek reguliatoriams, tiek investuotojams. Skaitmeninės valiutos, tokios kaip Bitcoin, Ethereum ir kitos, sukūrė naujas galimybes finansų rinkose, tačiau kartu atvėrė daug pažeidžiamumų, kurie gali būti išnaudojami neteisėtiems tikslams. ICO (pirminiai skaitmeninių monetų pasiūlymai) yra svarbi rinkos struktūra, kuri susijusi su finansiniais nusikaltimais. ICO, kaip vienas iš būdų pritraukti kapitalą kriptovaliutų projektams, pasižymi dideliu rizikos lygiu dėl trūkstamos reguliacijos ir kontrolės, o tai suteikia galimybes sukčiams pasinaudoti neskaidriais ir apgaulingais metodais. Taigi, nagrinėjant šiuos finansinius nusikaltimus, labai svarbu analizuoti įvairius kriterijus, kurie sąveikauja ir kartu sudaro pažeidžiamą sistemą, kurioje gali įvykti nusikaltimai (Grobys, 2022).

Atlikus literatūros analizę, buvo išskirtos trys pagrindinės su finansiniais nusikaltimais susijusios rinkos: decentralizuotos kriptovaliutų keityklos, centralizuotos kriptovaliutų keityklos ir ICO projektai. Visos šios rinkos yra tarpusavyje susijusios, tačiau ICO kaip pagrindinė rinka išsiskiria dėl savo ypatumų. ICO projektai dažnai veikia silpnos reguliacijos sąlygomis, o tai sukelia didelę riziką tiek investuotojams, tiek pačioms platformoms. Tyrimai rodo, kad ICO projektai dažnai naudojami apgaulingoms praktikoms ir neskaidriais investiciniais vertinimais, o tai gali turėti didelių finansinių nuostolių investuotojams. Tokie autoriai kaip Agarwal ir kt. (2023), Ante ir Meyer (2021), Anson (2021) pabrėžia, kad ICO projektuose gali įvykti finansiniai nusikaltimai dėl neskaidrių praktikų ir netinkamo rizikos valdymo. Taip pat, nors decentralizuotos ir centralizuotos kriptovaliutų keityklos dažnai turi griežtesnes saugumo priemones, jos vis tiek gali paveikti finansinių nusikaltimų mastą, kai kriptovaliutos yra listinamos ir prekiaujama šiose rinkose.

Xia ir kt. (2020), Akyildirim ir kt. (2023), Yousaf ir kt. (2023) atlikti tyrimai rodo, kad tiek decentralizuotos, tiek centralizuotos keityklos gali būti pažeidžiamos įsilaužimų, pažeidimų ir kitų nusikaltimų. Todėl būtina išsamiai tirti visas šias rinkas, kad būtų galima geriau suprasti, kaip finansiniai nusikaltimai įtakoja ICO projektų sėkmę ir saugumą skaitmeninėje finansų ekosistemoje.

1 lentelė.

Pagrindinės su finansiniais nusikaltimais decentralizuotoje ekosistemoje susijusios autorių tiriamos rinkos.

Decentralizuotos ekosistemos rinka	Tiriantys autoriai
Decentralizuotos kriptovaliutų keityklos	Xia ir kt, (2020), Aspris ir kt (2021), Xia ir kt (2021), Pengcheng ir kt (2023) Erdinc ir kt (2020)
Centralizuotos kriptovaliutų keityklos	Akyildirim ir kt (2023), Naganuma ir kt (2017), Yousaf ir kt (2023), Akanksha ir kt (2023), Imran ir kt (2022), Gao ir kt (2021)
Pirminiai monetų siūlymai (ICO)	Agarwal ir kt, (2023), Ante ir Meyer (2021), Anson (2021), De Andrés ir kt (2021), Conlon ir McGee (2021), Fu (2022), Gurrea-Martínez ir Nydia (2019), Grobys ir kt. (2022), Hornuf ir kt (2021), Swartz (2022), Zetsche (2018), Tronnier ir kt (2023)

Šaltiniai: Lentelė sukurta autoriaus remiantis 1 lentelėje nurodytų autorių tyrimais

„Coinweb“ duomenimis šiuo metu pasaulyje veikia 1492 kriptovaliutų keityklos, taip pat yra 18 998 rinkos, kuriose galima vykdyti prekybą kriptovaliutomis (2 priedas). Tai reiškia, kad 1492 biržų platformose galima prekiauti 18 998 skirtingomis prekybos poromis (pvz., USDT/BTC arba XRP/ETH). Vidutiniškai biržos platforma turi 73 rinkas, kuriose jos naudotojai gali prekiauti. Vertinant tai, jog kriptovaliutų keityklų skaičius pasaulyje sparčiai auga, o kriptovaliutų keityklos yra vieni pagrindinių skaitmeninių monetų distribucijos abjektų svarbu ištirti ir jų specifikas siekiant plačiau siekiant atlikti detalesnę analizę apie ICO projektuose atliekamus finansinius nusikaltimus. Remiantis „CoinGecko“ duomenimis yra trys pagrindiniai kriptovaliutų keityklų tipai:

- Centralizuotos kriptovaliutų keityklos
- Decentralizuotos kriptovaliutų keityklos
- Kriptovaliutų išvestinių finansinių priemonių keityklos

Decentralizuotos biržos (DEX) leidžia naudotojams pirkti, parduoti ir prekiauti kriptovaliutomis „Ethereum“ tinkle nedalyvaujant centralizuotam biržos operatoriui. Sandoriai vykdomi autonomiškai, juos reglamentuoja išmaniosios sutartys, kurios diktuoja sąlygas ir procesus. Tai reiškia, kad naudotojams nereikia registruotis, tikrinti tapatybės ar

mokėti mokesčių atsiimant lėšas (Falker, 2021). Tai leidžia asmenims visame pasaulyje jungtis su kitais asmenimis, norinčiais apdrausti savo turtą decentralizuotoje finansų sistemoje (Wronka, 2023). Lygiagrečiai norint listinguoti savo tokenus decentralizuotoje biržoje (DEX). Pirmiausia, reikia sukurti tokeną, atitinkantį pasirinktos blockchain platformos standartus, pavyzdžiui, ERC-20 Ethereum tinkle (Aspris, 2021). Taip pat parengti ir įdiegti išmaniąją sutartį (smart contract), kuri valdys tokenų emisiją, platinimą ir kitas funkcijas. Siekiant užtikrinti sklandžią prekybą, reikia sukurti likvidumo porą, tarp siūlomo tokeno ir ETH, ir įnešti pradinį likvidumą į likvidumo fondą. Pasirinkus tinkamą decentralizuotą biržą, tokią kaip „Uniswap“, „SushiSwap“ ar „PancakeSwap“, reikia pridėti tokeną, sukuriant prekybos porą ir įnešant likvidumą, kad vartotojai galėtų pradėti prekiauti tokenu. Atlikti išsamų išmaniosios sutarties auditą, siekiant identifikuoti ir pašalinti galimas saugumo spragas. Informuoti bendruomenę apie tokeno listingavimą DEX platformoje, kad jie galėtų pradėti prekybą ir prisidėti prie likvidumo didinimo. Atlikus šiuos žingsnius, bus listinguoti decentralizuotoje biržoje, suteikiant vartotojams galimybę prekiauti tokenais be tarpininkų (Andres, 2022).

Centralizuotose biržose (CEX), kuriose taikomi aukštesni mokesčiai taip pat kiekvienas klientas turi atitikti „Pažink savo klientą“ standartus. Lygiagrečiai norint listinguoti savo tokeną centralizuotoje biržoje (CEX), būtina paruošti reikalingą dokumentaciją, įskaitant išsamią baltąją knygą (whitepaper), kurioje detalai pristatomas projekto tikslas, technologija, komanda ir verslo modelis. Reikia atlikti teisinį auditą, siekiant užtikrinti, kad projektas atitinka visus taikomus teisės aktus ir reguliavimo reikalavimus, įskaitant vertybinių popierių įstatymus ir pinigų plovimo prevencijos taisykles (Hägele, 2024). Pateikus paraišką biržai ir sumokėjus listingo mokestį, reikia atlikti techninę integraciją (API) su biržos platforma, įskaitant tokenų pervedimo mechanizmų nustatymą ir piniginių adresų generavimą. Prieš pradėdant prekybą, vykdoma rinkodarą ir įtraukiama bendruomenė, informuojant apie artėjantį listingavimą, siekiant pritraukti daugiau dėmesio ir padidinti prekybos apimtis. Galiausiai, birža paskelbs prekybos pradžios datą, nuo kurios vartotojai galės pradėti prekiauti jūsų tokenais (Li, 2022). Atlikus šiuos žingsnius, tokenai bus listinguoti centralizuotoje biržoje, suteikiant vartotojams galimybę prekiauti tokenais. Toks reguliavimas skatina decentralizuotų kriptovaliutų keityklų naudojimą ypač ICO projektų, kurie planuoja įgyvendinti finansinį nusikaltimą (Wronka, 2023).

„CoinGecko“ atliktas kripto valiutų keityklų tipų vertinimas ir pagal numatytas metrikas nustatytas kriptovaliutų keityklos patikimumas bei populiarumas esamuoju

momentu. Vertinant centralizuotas kriptovaliutų keityklas, kriptovaliutų keityklos patikimumo balas yra nustatomas pasitelkiant šiuos duomenis:

- Bendras likvidumas
- Operacijų kiekis
- API aprėptis
- Kibernetinis saugumas
- Veikimo laikotarpis
- Komandos buvimas
- Ankstesni incidentai
- Turto įrodymas
- Įsipareigojimų įrodymas (2024 m. II ketv.)

Patikimumo balas yra nustatinėjamas didžiajai daliai pasaulyje esančių keityklų, šis balas gali svyriuoti atitinkamai nuo 1 iki 10. Esant 1 patikimumo balui kriptovaliutų keityklą galima laikyti nepatikima – rizikinga, galimai galinčia susidurti su problemomis ateityje. Esant 10 patikimumo balui kriptovaliutos keityklą galima vadinti saugia, aukšto likvidumo. Patikimumo balas nustatomas remiantis kriptovaliutų keityklos duomenimis apie einamosios veiklos rezultatus (Priedas nr. 10). Šiai dienai remiantis „CoinGecko“ duomenimis pagal patikimumo balą lyderiaujančios kriptovaliutų keityklos yra „Bybit“, „OKX“, „Coinbase Exchange“ ir „Kraken“ šios kriptovaliutų keityklos yra laikomos saugiausiomis atžvelgiant į joms suteiktą 10 iš 10 patikimo balą, mažesnio saugumo kriptovaliutos keityklomis laikomos „WEEX“, „Coinone“, „Fairdesk“ joms yra suteiktas 5 iš 10 patikimumo balas. Pats žemiausias patikimumo balas yra suteiktas tokioms keitykloms kaip „Aprobit“, „Purcow“, „FinanceX“, joms yra suteiktas 1 iš 10 patikimumo balas. Tačiau vertinant duomenis buvo pastebėta, jog net ir aukščia patikimumo balą turinčios kriptovaliutų keityklos susiduria su finansiniais nusikaltimais (Priedas nr. 10).

Atliekant finansinių nusikaltimų ICO projektuose tyrimą ir analizuojant autorių literatūra buvo pastebėti skirtinti lėšų surinkimo būdai ir pagrindinės sritys, kuriomis naudojasi finansinai nusikaltėliai siekiant atlikti finansinius nusikaltimus (žr. 2 lent.).

2 lentelė.

ICO, IDO ir IEO: Savybių ir Rizikų Palyginimo Lentelė.

Savybė	ICO (Initial Coin Offering)	IDO (Initial DEX Offering)	IEO (Initial Exchange Offering)
Platforma	Įmonės nuosava svetainė ar platforma	Decentralizuota birža (DEX)	Centralizuota birža (CEX)
Paleidimo kontrolė	Projektų komanda valdo visą paleidimą	Atvira ir be leidimų; dalyvauti gali visi	Valdoma biržos, reikalingas atrankos procesas
Saugumas	Santykinai didelė rizika; galimi sukčiavimai	Vidutiniškai saugu; už sandorius atsako DEX	Aukštesnis saugumas dėl biržos priežiūros
Mokesčiai	Maži mokesčiai, tačiau reikalingas rinkodaros biudžetas	Dažniausiai maži mokesčiai, bet taikomi DEX sandorių mokesčiai	Didesni mokesčiai dėl įtraukimo į biržą ir administravimo
Likvidumas	Kintamas; priklauso nuo projekto ir vartotojų paklausos	Momentinis likvidumas, nes tokenai iškart įtraukiami į DEX	Didesnis pradinis likvidumas dėl įsitvirtinusios vartotojų bazės
Prieinamumas	Globalus, nereikalauja platformos, bet rizikingesnis	Atviras visiems, turintiems prieigą prie DEX	Ribotas iki konkrečios biržos vartotojų
Pasitikėjimo lygis	Žemas, nes yra minimali priežiūra	Vidutinis, priklauso nuo DEX reputacijos	Aukštas, nes birža atlieka išsamų patikrinimą

Šaltiniai: Lentelė sukurta autoriaus remiantis „Techopedia“ bei autorių tokių kaip Agarwal ir kt. (2023), Ante ir Meyer (2021), Anson (2021), De Andrés ir kt. (2021), Conlon ir McGee (2021), Fu (2022), Gurrea-Martínez ir Nydia (2019), Grobys ir kt. (2022), Hornuf ir kt. (2021), Swartz (2022), Zetsche (2018) bei Tronnier ir kt. (2023) duomenimis.

Vertinant pateiktą lentelę galima pastebėti, jog iš pateiktų sutelktinio finansavimo per kriptovaliutų keityklas būdų tokių kaip ICO (Initial Coin Offering), IDO (Initial DEX Offering) IEO (Initial Exchange Offering), pats rizikingiausias yra ICO, kadangi būtent jis yra mažiausiai kontroliuojamas ir palieka daugiausiai laisvės projekto komandai, lygiagrečiai per ICO ir buvo atlikta daugiausiai finansinių nusikaltimų. Dauguma autorių savo darbuose analizuodmi nusikaltimus kriptovaliutų rinkose taip pat išskyrė ICO, kaip vieną iš pagrindinių instrumentų su kuriuo buvo atliekami finansiniai nusikaltimai decentralizuotose ekosistemose. Jie pabrėžė, kad toks sutelktinio finansavimo tipas pasižymi specifinėmis savybėmis, kurios lemia ne tik jų populiarumą, bet ir riziką, ypač kalbant apie sukčiavimą, reguliavimo spragas ir investuotojų apsaugos trūkumą. ICO projektai išsiskiria

mažu pasitikėjimo lygiu ir beveik visišku reguliavimo bei priežiūros nebuvimu, todėl jie tampa pagrindiniu sukčiavimo taikiniu (Cernera, 2023). Šio tipo projektai leidžia, bet kam rinkti lėšas globaliu mastu, nekeliant aukštų įėjimo barjerų ar reikalaujant patikrinimų, būdingų IEO (Initial Exchange Offering) ar IDO (Initial DEX Offering) projektų tipams. Dėl to ICO yra labiausiai rizikingas ir nesaugus investavimo objektas, į kurį investuojant dažnai pasitaiko finansinių nusikaltimų, tokių kaip „rug pull“ schemos, apgaulingos iniciatyvos su melagingomis komandos ar projektų idėjomis bei lėšų pasisavinimas (Arner, 2018). Tačiau lygiagrečiai pirminis monetų siūlymas (ICO) taip pat tapo svarbia lėšų rinkimo priemone įmonėms ar projektams, kurie neturi pakankamo kapitalo kiekio įgyvendinti projektus arba startuoliams, kurie ieško finansavimo tam tikros idėjos kūrimui (Miglo, 2022).

2017 metais per ICO Jungtinėse Valstijose surinkta maždaug 4 milijardai JAV dolerių, o 2018 metais ICO pritraukė daugiau kaip 21 milijardus dolerių, iš dalies pakeisdami tradicinį rizikos kapitalą kaip svarbų lėšų rinkimo būdą. Atsižvelgiant į sparčiai besikeičiančią informacinių technologijų sritį, pirminiai monetų siūlymai tapo tiek vidaus, tiek tarptautinių reguliavimo institucijų dėmesio centre. Pirminis monetų siūlymas (ICO) yra naujas lėšų rinkimo būdas, išsiskiriantis trim pagrindiniais aspektais:

Pirma, siekiant pritraukti kapitalo neišleidžiama tradicinių finansinių produktų, tokių kaip akcijos ar obligacijos, vietoj to jie naudojama kriptovaliutos, vadinamas žetonais, suteikiančiais savininkams įvairias teises.

Antra, kitaip nei tradicinio lėšų rinkimo atveju, emitentas gauna ne įprastą valiutą, o kriptografinius aktyvus, pavyzdžiui, bitkoinus ar eterius, kurie plačiai pripažįstami visuomenėje.

Trečia, išleidžiant žetonus apeinami tradiciniai kanalai, nes naudojama blokų grandinės technologija. Galiausiai, skirtingai nuo tradicinių vertybinių popierių emisijų, ICO dažnai nereikia rengti ir registruoti pasiūlymo Vertybinių popierių ir biržų komisijai (SEC), nebent žetonai pagal atitinkamus vertybinių popierių įstatymus priskiriami vertybinių popierių kategorijai (Dean, 2020). Pakanka paprasto dokumento, vadinamo "baltąja knyga", kaip pagrindinės informacijos atskleidimo prievolės, kuriai netaikoma priežiūra ar privalomų sąlygų nustatymas (Remolina, 2018). Vertinant pateiktus duomenis (žr. 3 pried.) pastebima, jog 2016 metais ICO rinka buvo palyginti nauja, per metus buvo išleisti vos 29 nauji projektai, dauguma žmonių dar nebuvo susipažinę su šiuo finansavimo modeliu. Tai buvo laikotarpis, kai kriptovaliutų populiarumas sparčiai didėjo, kadangi jau esamos kriptovaliutos tokios kaip „Bitcoin“ ir „Ethereum“ indikavo kilimo tendenciją ir

teikė didelį pozityvą rinkoje investuotojai ieškojo kitų decentralizuotų investavimo būdų. Coindesk duomenimis vienais sėkmingiausių tais metais išleistų projektų buvo:

„ICONOMI“ - (10 mln. JAV dolerių): Šis projektas orientuotas į kriptoindeksų ir rizikos draudimo fondų kūrimą, taip pat į atvirų fondų platformą, leidžiančią kitiems investuotojams valdyti savo fondus.

„SingularDTV“ - (7,5 milijonų JAV dolerių): Kaip pristatomasis "ConsenSys" ICO, „SingularDTV“ siekia pristatyti dokumentinius filmus ir televizijos serialus, tuo pat metu suteikiant skaitmeninių teisių valdymo platformą.

„The DAO“ - buvo paleista 2016 metais balandžio 30 dieną, o finansavimo langas truko 28 dienas. Ir iki gegužės 15 dienos buvo surinkta daugiau kaip 100 milijonų dolerių, o iki finansavimo laikotarpio pabaigos „The DAO“ buvo didžiausias tuo metu ICO, surinkęs daugiau kaip 150 milijonus dolerių iš daugiau kaip 11 000 asmenų. Per sutelktinį pardavimą keli žmonės išreiškė susirūpinimą, kad kodas yra pažeidžiamas. Klaida pasinaudojo įsilaužėlis, kuris iki birželio vidurio pasisavino daugiau nei 3,6 mln. dolerių vertės „Ethereum“ kriptovaliutos. Taip pat tuo laikotarpiu „Ethereum“ kaina nukrito nuo daugiau nei 20 iki mažiau nei 13 dolerių. Dėl šios situacijos projektas buvo baigtas (Remolina, 2018). „The DAO“ pavyzdys parodė, kad nesąžiningi programuotojai gali pasinaudoti kodo spragomis ir trūkumais siekdami pavogti dalį disponuojamų lėšų.

2017 metais ICO buvo pastebimas didelis susidomėjimas ICO rinka (žr. 3 pried.), o tai paskatino vis daugiau žmonių steigti savo projektus, tam, kad įgyvendintų savo idėjas ar užsidirbtų pinigų. Investuotojai buvo entuziastingi dėl galimybės gauti ankstyvąją prieigą prie projektų, o optimistinė kriptovaliutų rinkos atmosfera ir gana aukštos grąžos iš esamų investicijų į kriptovaliutas skatino žmones ieškoti naujų investavimo galimybių (Swartz, 2022). Kadangi ICO yra decentralizuotas finansavimo mechanizmas, kuris suteikia naujiems kriptovaliutų projektams galimybę pritraukti finansavimą, daugeliu atvejų yra susietas su dideliais iššūkiais ir rizikomis investuotojams (Howell, 2019). Viena iš pagrindinių to priežasčių yra ta, jog ICO vyksta decentralizuotoje blokų grandinės sistemoje kurioje trūksta reguliavimo, dauguma ICO vyksta be tiesioginės valstybės ar tarptautinių finansinių institucijų priežiūros. Tai lemia mažesnę projektų išipareigojimą laikytis griežtų taisyklių, atveria duris piktnaudžiavimui ir nesąžiningoms praktikoms (Zetsche, 2017). Teikiant išankstinio monetų siūlymo projektai dažnai nereikalaujama praeiti griežtų vertinimo procedūrų, kurias taiko tradiciniai investiciniai projektai. Dėl to rinkoje atsirado prastos kokybės ar net netikri projektai, kurie buvo skirti nusišavinti investuotojų pinigus. Dėl decentralizuoto pobūdžio ICO dalyviai susiduria su dideliu rizikos lygiu, nes projektai gali žlugti dėl nepalankių rinkos sąlygų, valdymo klaidų arba

tiesiog dėl sukčiavimo. Nepakankamas skaidrumas ir teisiniai neaiškumai, taip pat jog nemaža dalis ankstyvųjų investuotojų investuodami į ICO patyrė nuostolių, nulėmė tai, jog investavimas į ICO projektus tapo vertinamas kaip rizikingas. Investuotojai pradėjo vertinti ne tik pačią idėją tačiau ir pagrindimą, buvo stengiamasi suprasti kas stovi už projekto, koks yra praktinis baltojo lapo pagrindimas (Buckley, 2017). Po 2017 metų kai didelė dalis išleistų ICO, dėl centralizuotos kontrolės trūkumo buvo išvaistyti arba tiesiog nusišavinti, valstybinių organizacijų požiūris į ICO 2018 metais pasikeitė. Šiame etape prasidėjo keletas svarbių pokyčių. Pirma, reguliavimo institucijos pradėjo aktyviau stebėti ir reguliuoti ICO, siekdamos apsaugoti investuotojus nuo galimų sukčiavimų ir netikrų projektų. Antra, kriptovaliutų kainų kritimas ir bendra rinkos nuotaika priverčia investuotojus būti atsargesniems (Buckley, 2017). 2019 metais ICO rinkoje prasidėjo „Meškų“ laikotarpis (Haffke, 2020). Pagrindinės kriptovaliutos „Bitcoin“ kaina nukrito iki 5 tūkstančių eurų, investuotojai tapo atsargesni ir mažiau linkę rizikuoti, atsižvelgdami į ankstesnius nesėkmes ir sukčiavimo atvejus. Pagal (5 Priedas) pastebimą, jog naujai į rinką leidžiamų projektų skaičius sumažėjo beveik 12 kartų, o surinktų lėšų suma sumažėjo net 20 kartų. 2020 m.: pastebimas dar ženklesnis ICO populiarumo smukimas, vertinant 5 priede pateiktą informaciją, pastebimą, jog 2020 metai ICO buvo rekordiskai prasti, vos 14 naujų projektų pasiekė rinką ir buvo surinkta tik 55,6 milijonai dolerių. Vyraujant „Meškų“ rinkai Investuotojai išliko atsargūs dėl kriptovaliutų investicijų, taip pat ICO jau buvo įgavęs nepatikimos investicijos vardą (Agarwal, 2023). Nors kai kurie projektai vis dar pritraukdavo finansavimą, jų skaičius ir surinktų lėšų suma buvo santykinai nedidelė (žr. 3 pried.). 2021 metais naujas pasitikėjimas kriptovaliutomis ir palanki rinkos situacija „Jaučių“ rinka sukėlė prielaidų steigtis naujiems ICO. Projektai pradėjo vėl pritraukti dėmesį, o investuotojai buvo linkę rizikuoti siekdami pelno. Tačiau prieš atliekant investicijas į tam tikrą projektą investuotojai pradėjo vertinti daugiau aspektų susijusių su projektu. Buvo vertinami tokie dalykai, kaip projektų narių pajėgumas įgyvendinti projektą, kuo yra grįstas projekto „Baltas lapas“, ar projekto sukurtos valiutos kodui yra atliktas auditas ir kas yra auditorius (Ante, 2021). Buvo siekiama, jog projekto savininkai negalėtų laisvai disponuoti investuotomis lėšomis ir nebūtų galimybės perkelti arba pavogti lėšų. 2022 metais stipriai išpopuliarėjo projektai susiję su virtualia realybe arba dirbtiniu intelektu, tačiau lyginant su ankstesniais metais projektų skaičius ir surinktų lėšų suma lieka santykinai nedidelė. Investuotojai yra atsargesni, bet dar yra tam tikras susidomėjimas šia finansavimo forma.

Apibendrinant ICO yra svarbi šiuolaikinės finansų ekosistemos dalis, atspindinti decentralizuotų finansų (DeFi) inovacijas ir jų keliamus iššūkius. Ši finansavimo forma,

suteikianti galimybę pritraukti kapitalą be tradicinių finansinių tarpininkų, tapo reikšminga alternatyva startuoliams ir technologijų projektams, tačiau kartu kelia didelę riziką dėl reguliavimo spragų, anonimiškumo ir didelio sukčiavimo atvejų skaičiaus (Zetsche, 2017; Arner, 2018). ICO svarbu tirti dėl jo globalios reikšmės finansų rinkoms ir didėjančio naudojimo technologiniuose sektoriuose, taip pat dėl nusikaltimų susijusių su ICO, pagal pateikiamas rinkos tendencijas galima pastebėti, jog ICO rinka yra cikliška, ko pasekoje investuotojai su kiekvienu nauju ciklu vis konservatyviau vertina ICO projektus bei prieš atliekant investicijas į projektą vertina vis platesnį ratą kintamųjų, ko pasekoje šiame darbe bus atlikta detali analizė kaip konkretūs kintamieji daro įtaką finansinio nusikaltimo mastui ICO projektuose. ICO tyrimas yra būtinas, norint sukurti tvarią reguliavimo struktūrą, geriau suprasti jo naudojimo dinamiką ir užtikrinti saugesnį jo taikymą kaip inovatyvią finansavimo priemonę.

1.3.1 Pagrindinės finansinių nusikaltimų sritys ICO projektuose

Kadangi daugelis kriptovaliutų veikia decentralizuotuose blokų grandinės tinkluose ir nėra centrinės institucijos, prižiūrinčios sandorius (Wronka, 2023). Vartotojai gali susikurti kelis adresus ir naudoti juos skirtingoms operacijoms, todėl sudėtingiau atsekti dalyvaujančių šalių tapatybę. Kai kurios kriptovaliutos, dažnai vadinamos privatumo monetomis tokios kaip: „Monero“, „Zcash“ ir „Dash“, yra specialiai sukurtos naudotojų privatumui didinti (Hendrickson, 2022). Jose naudojami pažangūs kriptografiniai metodai, kuriais siekiama užmaskuoti sandorių duomenis, todėl sunkiau atsekti lėšų srautus. Visiško konfidencialumo išlaikymas prisideda prie to, jog visoje decentralizuotoje finansų sistemoje yra beveik neįmanoma atsekti transakcijų ir pinigų srautai yra nusisavinami taip ir nesurandant tikrojo nusisavinimo kaltininko (Swartz, 2022). Decentralizuotos biržos, tokios kaip „Uniswap“, tapo pagrindiniu atakų vykdytojų taikiniu. Viena iš labiausiai paplitusių taktikų, kuri yra taikoma siekiant nusisavinti lėšas, yra anglišku terminu „Rug pull“ vykdymas (Cernera, 2023). „Rug pull“ tinklaraštis „Kriptologija“ apibūdina kaip: „kenkėjiškas sukčių veiksmas, kuomet išnaudojant saugumo spragas pasisavinamos visos projekto kainą palaikiusios lėšos – likvidumas. Po šio veiksmo projekto žetonai nebeturi jokios vertės, o investuotojai praranda visą kapitalą“. Šis veiksmas yra kūrėjų sąmoningas projekto nevykdymas, nusisavinus investuotojų investuotas lėšas taip ir neįvykdžius projektas. Tokiose platformose kaip „Uniswap“ sukuriamas ERC-20 žetonas (Ethereum Request for Comments 20), už numatytą suma įtraukiamas į kriptovaliutų biržos sąrašą ir susiejamas su garsia kriptovaliuta, pavyzdžiui, Ethereum kriptovaliuta tam, kad suteikti

sukurtai monetai tikrumo bei patikimumo įvaizdį. Pagal tinklaraštį „CryptoVantage“ yra penki pagrindiniai tipai, kuriais naudojantis kripto projektų kūrėjai pasisavina lėšas iš investuotojų ir panaikina projektą:

1. „Likvidumo praradimas, kuri įvyksta, kai žetonų kūrėjai pašalina lėšas iš likvidumo fondo.
2. Pardavimo pavedimų ribojimas, kai kūrėjai koduoja žetonus taip, kad jie yra vienintelė šalis, galinti juos parduoti, ir, atsiradus pakankamai teigiamam kainos pokyčiui, jie atsisako savo pozicijų, palikdami bevertį žetoną.
3. Dėmpingavimas, tai įvyksta tada kai projekto kūrėjai pamato, jog jų sukurtos valiutos rinkos kapitalizacija yra išaugusi ir pačios valiutos kaina yra gerokai pakilusi, kūrėjai greitai išparduoja didelę žetonų dalį, taip sumažindami monetos kainą. Tai dar angliškai vadinama „Pump and Dump“ schema
4. Įvairios „exit scam“ schemas – Tai kai projektų kūrėjai apgaulingai sudaro įspūdį apie projekto potencialą, pasiekia tam tikrą investicijų sumą ir po to visiškai nutraukia veiklą. Tokių projektų kūrėjai dažnai dingsta su visomis investuotojų lėšomis, palikdami be nieko.
5. ICO "pyramid scheme" – Kai ICO projektai remiasi įprastomis piramidės schemas idėjomis, kur naujų investuotojų pinigai yra naudojami senesniems investuotojams atsiskaityti. Tokių projektų tvarumas priklauso tik nuo to, kiek naujų investuotojų įsigyja žetonus, o kai šis srautas užgęsta, projektas subliūkšta, palikdamas senus investuotojus bevertėmis monetomis“

SATISGROUP pateiktoje 2018 metų ataskaitoje „CRYPTOASSET MARKET COVERAGE INITIATION: NETWORK CREATION“, kurią galima rasti Bloomberg tyrimų terminale, nustatyta daugybė sukčiavimo atvejų susijusių ICO. Šioje ataskaitoje atskleista, kad iki 2018 m. liepos mėn. apie 78 proc. visų pradėtų ICO buvo susiję su sukčiavimais, o tai sudarė 11 proc. visos rinkos kapitalizacijos.

Apibendrinant, decentralizuota finansų ekosistema, įskaitant ICO projektus, suteikia vartotojams anonimiškumą ir autonomiją, tačiau kartu kelia riziką prarasti investuotą turtą. ICO projektai, veikdami decentralizuotuose tinkluose, dažnai neturi centrinės institucijos, prižiūrinčios sandorius, todėl dalyvių tapatybė sunkiai atsekama. Dėl to kyla pavojus finansiniams nusikaltimams, tokiems kaip „Rug pull“, likvidumo praradimas, pardavimo ribojimas ir „pump and dump“ schemas. Šios schemas, naudojamos tiek decentralizuotose, tiek centralizuotose biržose, sukelia didelę riziką investuotojams, nes kūrėjai gali pasisavinti lėšas, palikdami investuotojus bevertėmis monetomis.

1.3.2 Decentralizuotų ir centralizuotų keityklų vaidmuo ICO projektuose bei finansinių nusikaltimų analizė

Laikui bėgant, decentralizuotos finansų ekosistemos ir finansinių nusikaltimų sąsajos tapo itin sudėtingos. Tyrimai rodo, kad pagrindinės sritys, kurias tyrinėja akademinė bendruomenė, yra pirminių monetų siūlymai (ICO) ir kriptovaliutų keityklos – šie komponentai yra glaudžiai susiję ir ilgalaikėje perspektyvoje praktiškai negali veikti vienas be kito (Anson, 2021). Centralizuotos keityklos (CEX) ir decentralizuotos keityklos (DEX) yra pagrindinės ICO projektų listingo platformos, o jų veikimo skirtumai lemia ne tik ICO sėkmę, bet ir pažeidžiamumą finansiniams nusikaltimams. Šiame kontekste svarbu vertinti, ar pasirinkta listingo platforma gali turėti įtakos finansiniams nusikaltimams (Hägele, 2024). Decentralizuota ekosistema, kuri anksčiau buvo vertinama kaip patikima nuo pažeidžiamumo, dabar susiduria su neteisėtos veiklos mažinimo iššūkiais. Pinigų plovimo prevencijos ir sukčiavimo reguliavimo klausimai yra labai svarbūs, todėl reikia taikyti teisingą požiūrį, kad būtų pasiekta pusiausvyra tarp decentralizacijos ir reguliavimo priežiūros (Zetzsche, 2018). Kadangi decentralizuota aplinka toliau vystosi, siekiant skatinti inovacijas ir kartu apsisaugoti nuo finansinių nusikaltimų šioje dinamiškoje ekosistemoje, būtinos bendros akademinės bendruomenės, pramonės ir reguliavimo institucijų pastangos. Todėl akademinėje bendruomenėje yra atlikta nemažai tyrimų kurie tiria nusikaltimus bei jų prielaidas tiek pirminiuose monetų siūlomuose, tiek kriptovaliutų keityklose.

Pagal 7 priede pateiktus duomenis, lyginant juos su 8 priede pateiktais duomenimis apie kriptovaliutų keityklas galima pastebėti, jog finansinių nusikaltimų kiekis, mastas ir būdai dažnai skiriasi, taip pat skiriasi ir keityklų kurioms jie buvo atlikti dydžiai bei žinomumas. Per pastaruosius kelerius metus kriptovaliutų keityklos susidūrė su daugybe saugumo pažeidimų, įsilaužimų ir kitų finansinių nusikaltimų, tačiau dauguma didžiausių keityklų, nepaisant šių incidentų, sugebėjo atsigauti ir išlikti veikiančios. Keityklos kaip Binance, Crypto.com, KuCoin ir Gate.io patyrė didelių nuostolių dėl įsilaužimų, tačiau jų gebėjimas investuoti į saugumo priemones ir greitai reaguoti į situaciją leido atkurti vartotojų pasitikėjimą ir užtikrinti tolesnę veiklą. Pavyzdžiui, Binance, kuri patyrė įsilaužimą 2019 m., praradusi daugiau nei 7 000 BTC, po šio incidento stipriai atnaujino savo saugumo sistemas ir tapo viena iš didžiausių ir labiausiai patikimų keityklų pasaulyje. Crypto.com, po 2021 m. įvykusio įsilaužimo, taip pat sugebėjo išspręsti savo saugumo problemas ir išlaikyti aukštą patikimumo balą. KuCoin, patyrusi 280 milijonų dolerių nuostolį dėl kibernetinio įsilaužimo, taip pat sugebėjo atstatyti savo veiklą, tapdama viena

iš populiariausių keityklų. Šios keityklos pavyzdys rodo, kad net po rimtų finansinių nusikaltimų ir įsilaužimų, didžiosios keityklos su stipriomis saugumo priemonėmis ir atstatymo strategijomis gali sugrįžti ir išlikti konkurencingos kriptovaliutų rinkoje. Kita vertus, keityklos, turinčios mažesnę rinkos kapitalą arba silpnesnę saugumą, gali nesugebėti atsigauti po tokių incidentų, dėl ko jos gali susidurti su didesniais iššūkiais norėdamos išlaikyti vartotojų pasitikėjimą ir užtikrinti stabilumą. Vis dėlto šios didžiosios keityklos rodo, kad net ir esant rimtiems iššūkiams, sugebėjimas greitai reaguoti į incidentus ir investuoti į saugumo priemones yra būtinas norint išlikti ir sėkmingai veikti šioje dinamiškoje ir nuolat besikeičiančioje rinkoje. Pastebima, jog pagal pateiktus duomenis mažiausios apimties finansinis nusikaltimas buvo fiksuotas 2015 metais kai jėga buvo atimti prisijungimai prie pagrindinės keityklos „AllCrypt“ piniginių ir išvesti ten buvę žetonai, keityklos patirtas nuostolis sudarė – 9,7 tūkstančius dolerių, ši keitykla turėjo 2 patikimumo balą. Didžiasias fiksuotas finansinis nusikaltimas buvo atliktas 2022 metais. kai viena saugiausių ir žinomiausių, 9 patikimumo balą turėjusi, „FTX“ kriptovaliutų keitykla prarado 600 milijonų dolerių investuotojų lėšų. Vertinant šiuos duomenis galima pastebėti, jog finansiniai nusikaltimai įvyksta tiek didžiausiose ir galingiausiose bei aukštą patikimo balą turinčiose keityklose tokiose kaip: „Crypto.com“, „Uniswap“, „FTX“ tiek ir smulkiose, žemą patikimumo balą turinčiose keityklose tokiose kaip: „BitPoint“, „Altsbit“, „Lendf.me“. Kadangi pastebima tendencija, jog finansiniai nusikaltimai gali būti atliekami nepriklausomai nuo kriptovaliutų keityklos apyvartų ar patikimumo balo (žr. 8 pried.). Todėl šiame darbe kaip vienas iš svarbių kintamųjų siekiant įvertinti finansinio nusikaltimo dydį bus vertinamas, ICO projekto planuojamo arba jau esamo listinimo platforma.

2022 metais lapkričio mėnesį įvykęs vienos iš pagrindinių kriptovaliutų biržų „FTX“ žlugimas sulaukė didelio dėmesio ne tik dėl investuotojų nuostolių dydžio, bet ir įžūlumo – finansinių struktūrų kuriose jis veikė (Roy, 2023). Dėl veikiančių įmonių valdymo ir visuomenės pasitikėjimo pažeidimų taip pat dėl jos plataus masto priklausomybės nuo kriptovaliutų rinkos kilimo faktoriaus. FTX, viena didžiausių pasaulyje kriptovaliutų biržų, kuri buvo vertinama 32 milijardų dolerių, per naktį žlugo dėl to, jog „The Wall-Street Journal“ skaičiavimais, 2022 metų lapkričio mėnesį FTX trūko apie 8 milijardų dolerių grynujų pinigų- likvidumo. 2022 metų lapkričio 2 dieną „CoinDesk“ paskelbė straipsnį, kuriame teigiama, kad su FTX susijusi prekybos įmonė „Alameda Research“, priklausanti FTX vadovui Samui Bankmanui-Friedui, Nuo 2022 metų birželio 1 dienos. iki 2022 metų liepos 22 dienos žinomos „Alameda“ piniginių buvo didžiausi stabiliųjų kripto valiutų indėlininkai laikė didelę dalį FTT ir kad šie FTT indėliai

sudarė didelę jų turto dalį. „CoinDesk“ pranešė, kad apyvartoje buvo 5,1 milijardų dolerių vertės FTT žetonų, o „Alameda“ balanse buvo 3,66 milijardų dolerių „atrankintos FTT“, 2,16 milijardai dolerių „FTT užstato“ ir 292 milijardai dolerių „užrankintos FTT“. Straipsnis sukėlė pinigų išėmimo iš FTX bangą, tačiau galiausiai, dėl likvidumo trūkumo klientai nebegalėjo atgauti biržoje įmokėtų pinigų. Investuotojų pinigų atsiėmimo sustabdymas sukėlė kitų prekybos įmonių, investavusių į FTX pavyzdžiui, „BlockFi“ ir „Voyager“, bankrotus, jau nekalbant apie didžiulius skolų nurašymus „BlackRock“ ir „Sequoia“. Niujorko pietinės apygardos prokuroras, federalinio teismo, kuriame buvo nagrinėjama byla buvusiai biržos vadovybei, FTX įvykį apibūdino kaip „vieną didžiausių sukčiavimų finansų istorijoje“. Žiniasklaidoje vis dažniau pabrėžiamas šios rinkos tarpusavio sąsajų pobūdis ir jos pažeidžiamumą dėl užkrato ir išplitimo poveikio (Jalan, 2023). Pastebėta, jog būtent po „FTX“ žlugimo 2022 metais lapkričio mėnesį didžiųjų kripto valiutų tokių kaip „Bitcoin“, „Ethereum“, „Solana“ kapitalizacija sumažėjo apie 15 procentų (žr. 2 pried.). Pastebima, jog būtent 2022 metų lapkričio 10 dieną „Bitcoin“ kriptovaliutos, kuri yra tiesiogiai susieta su kitomis kriptovaliutomis ir yra laikoma vienu iš pagrindinių rinkos rodiklių, „Bitcoin“ kaina nukrito beveik 18 procentų. Šis reiškinys buvo tiesiogiai susijęs su FTX keityklos žlugimu. Šis reiškinys aiškiai parodo, jog kriptovaliutų valiutų rinka yra labai jautri naujienoms, jog investuotojai tiek smuklieji, tiek stambieji aktyviai seka rinkoje vykstančius dalykus ir reaguoja į teigiamą arba neigiamą informaciją. Šiuo atveju „FTX“ bankrotas rinkoje sukėlė didelį nepasitikėjimą rinka, kas nulėmė, jog investuotojai ženkliai dalį kapitalo perkėlė iš kripto turto rinkas į kitas finansų rinkas. Toks staigus perkėlimas kripto valiutų rinkoje momentaliai sukėlė kainų kritimą (Fu, 2022). 2023 metais Yousaf ir Goodell atliktame tyrime susijusiame su „FTX“ pasitelkiant mažiausių kvadratų (OLS) metodą buvo vertinamos 29 tuo metu populiariausių kriptovaliutų gražos. Tyrimo metu pastebėta, jog 26 iš 29 vertintų kriptovaliutų generavo neigiamą gražą. Sekantis 2023 Jalan ir Matkovskyy tyrimas atliktas naudojant CoVar siekiantis įvertinti „FTX“ bankroto įtaką 100 populiariausių kriptovaliutų kainoms, nurodė, jog bendra rinkos kapitalizacija ir kriptovaliutų kainos bankroto metu ir po jo buvo žemesnės nei prieš tai. „Žmonės nori kontroliuoti savo lėšas, net daugelis mūsų klientų prašė atsiimti lėšas iš centralizuotos biržos ir perkelti jų žetonų rinkos kontrolę tik į DEX“, - sako „Gotbit“ generalinis direktorius Aleksas Andrijuninas. „FTX“ bankrutavimas sukeltas finansinių nusikaltimų padarė ženkliai įtaką visam decentralizuotam pasauliui, pradedant nuo kapitalizacijos sumažėjimo, baigiant pasitikėjimu centralizuotomis valiutų keityklomis. Vertinant šiuos įvykius svarbu pabrėžti, jog decentralizuotoje ekosistemoje, kaip ir įprastose finansų rinkos yra labai greita informacijos sklaida, kadangi žmonės kurie investuoja į kriptovaliutas

dažnai yra pažengę technologijų srityje, taip pat aukštesnio išsilavinimo lygio. Šie veiksniai bei žmonių elgesio specifika daro įtaką stiprią įtaką ir rinkai. Kadangi aukštesnio išsilavinimo investuotojai greičiau suranda apdoroja bei tiksliau reaguoja į gautą informaciją (Jalan., 2023). Tačiau kaip rodo autorių Akyildirim ir kiti (2023) atliktas tyrimas, kuris pateikė detalią informaciją apie „FTX“ kriptovaliutų keityklos balanso duomenis 2022 metų laikotarpiu. „FTX“ kontroliavo nemažą dalį ir kitų kriptovaliutų tokių kaip „Bitcoin“ ir „GBTC“ todėl šios kriptovaliutos žlugimas turėjo ne tik netiesioginį poveikį rinkai, tačiau ir kapitalizacijos prasme padarė neigiamą įtaką pačiai rinkai.

Apibendrinant, kriptovaliutų keityklos yra svarbi sparčiai augančios kriptovaliutų ekosistemos dalis, kurios tikslas – sumažinti priklausomybę nuo tradicinių centralizuotų valiutų keityklų. Standartiškai centralizuotos keityklos (CEX) laikomos saugesnėmis ir patikimesnėmis nei decentralizuotos (DEX) dėl didesnio likvidumo, reguliavimo priemonių ir platesnio vartotojų pasiekiamumo, ko pasekoje daugiau ICO projektų renkasi CEX (5 lentelė). CEX, tokios kaip Binance ar Coinbase, siūlo patikimesnes prekybos sąlygas, griežtesnį reguliavimą, taip pat didesnę vartotojų ir rinkos pasitikėjimą (Hägele, 2024). Tačiau, remiantis FTX pavyzdžiu, matome, kad net ir didžiausiose, centralizuotose keityklose gali kilti rimtų finansinių nusikaltimų ir neskaidrumo problemų. FTX žlugimas, kuris įvyko dėl neskaidraus valdymo, netinkamų finansinių struktūrų ir vidinių klaidų, parodė, kad CEX nėra visiškai apsaugotos nuo pažeidžiamumo ir finansinių nusikaltimų (Akyildirim, 2023). Tai rodo, kad nors CEX dažnai laikomos patikimomis ir saugiomis dėl jų reguliavimo ir stebėsenos priemonių, jos taip pat gali būti pažeidžiamos vidinių klaidų, sukčiavimo ir manipuliavimo. Šiuo atveju, FTX, kaip viena iš didžiausių pasaulyje centralizuotų keityklų, ne tik sukėlė didžiulius investuotojų nuostolius, bet ir pavertė šią keityklą pavyzdžiu, kad net ir reguliuojamos centralizuotos keityklos gali tapti saugumo ir finansinių nusikaltimų šaltiniu (Akyildirim, 2023). Todėl labai svarbu atlikti išsamų tyrimą apie keityklas, kuriose bus listinami ICO žetonai, ir vertinti, kaip šios keityklos gali paveikti nusikaltimų mastą ir jų poveikį visam projektui.

1.4 Finansinių nusikaltimų pirminiuose monetų siūlymuose tyrimų vertinimas ir pavyzdžiai

Mokslinėje literatūroje, analizuojant finansinius nusikaltimus ICO projektuose, dažnai nagrinėjami įvairūs kintamieji, galintys turėti įtakos šių projektų patikimumui ir jų tapimui nusikalstamos veiklos objektu, taip pat vertinant finansinių nusikaltimų mastą (žr. 3 lent.). Nemaža dalis tyrėjų savo darbuose vertina keletą skirtingų kintamųjų, siekdami

atskleisti, kaip šie veiksniai veikia finansinių nusikaltimų atsiradimo riziką ir ICO projekto rezultatus. Kaip pastebi Adhami ir kt. (2018) bei De Andrés ir kt. (2021), projekto populiarumas gali būti lemiamas veiksnys, rodantis investuotojų pasitikėjimą ir projekto sėkmės potencialą. Tuo tarpu kiti tyrėjai, tokie kaip Dean ir kt. (2020) bei Grobys ir kt. (2022), pabrėžia rizikos balo svarbą – jis leidžia įvertinti projekto galimą saugumą ir patikimumą. Be to, tyrimai atskleidžia, kad pasirinktas keityklos tipas (centralizuota, decentralizuota ar visai nenaudojama) taip pat daro įtaką projekto likvidumui ir nusikalstamos veiklos rizikai (Agarwal ir kt., 2023, Han ir kt., 2024). Svarbus aspektas tyrimuose yra ir ICO metu surinkta lėšų suma. Kaip nurodo Agarwal ir kt. (2023) bei Ante ir Meyer (2021), didesnė pritraukta suma gali reikšti didesnę investuotojų pasitikėjimą, tačiau kartu gali tapti pritraukiančiu taikiniu finansiniams nusikaltimams, taip pat pritrauktų lėšų suma indukuoja apie numatomo finansinio nusikaltimo dydį. Šių kintamųjų nagrinėjimas leidžia mokslininkams geriau suprasti finansinių nusikaltimų ICO projektuose priežastis ir dinamiką.

3 lentelė.

Pagrindiniai su finansiniais nusikaltimais ICO projektuose autorių tiriama kintamieji.

Tirti kintamieji	Autoriai
ICO populiarumas	Adhami ir kiti, 2018; De Andrés ir kiti, 2021; Grobys, King ir Sapkota 2022.
ICO Rizikos balas	Dean ir kiti, 2020; Grobys, King, T; Sapkota, 2022.
Keitykla (CEX/DEX/N/A)	Agarwal ir kiti, 2023; Akyildirim ir kiti, 2023, (Aspris, ir kiti, 2021, Han, Huang ir Zhong, 2024, Hägele, 2024.
Surinkta suma (tūkst. USD)	Agarwal ir kiti 2023; Ante, Meyer, 2021, Grobys, King, Sapkota, 2022, (Ante, Sandner, Fiedler, 2018.

Šaltiniai: Lentelė sukurta autoriaus remiantis lentelėje pateiktų autorių tyrimais.

Lentelėje pateikiami pagrindiniai kintamieji, kurie buvo tiriama autorių atliktuose tyrimuose, siekiant įvertinti finansinių nusikaltimų tikimybę bei mastą ICO projektuose. Šie kintamieji buvo vertinami analizuojant ICO projekto riziką ir sukčiavimo atvejus, nes jie daugeliu atvejų būtent nuo šių veiksnių priklausydavo projekto surinkta suma;

Populiarūs ICO projektai dažnai pritraukia didesnę investuotojų auditoriją, kas gali padidinti finansinių nusikaltimų riziką, ypač jei projektas nėra pakankamai skaidrus ir nėra užtikrinamas tinkamas reguliavimas. Populiarumas gali taip pat sukelti rinkos

manipuliavimo riziką, kadangi didesnė suma gali būti lengviau manipuluojama nepatikimų subjektų.

ICO rizikos balas. Tai rodiklis, kuris įvertina rizikos lygį, konkrečiam ICO projektui, atsižvelgiant į 1.3.1 darbo dalyje pateiktus faktorius, tokius kaip projekto komanda, technologijos, teisinė bazė ir finansinė struktūra. Aukštas rizikos balas paprastai reiškia mažesnę finansinių nusikaltimų pavojų investuotojams.

Keityklos tipas kurioje listintas/bus listinamas žetonas. ICO projektų listinimas tiek decentralizuotose (DEX), tiek centralizuotose (CEX) keityklose gali turėti reikšmingą įtaką projektų saugumui ir finansinių nusikaltimų rizikai. Centralizuotos keityklos dažnai turi griežtesnę reguliaciją ir saugumo priemones, tačiau jos taip pat gali tapti taikiniais įsilaužėlių atakoms. Decentralizuotos keityklos, nors ir suteikia didesnę anonimiškumą ir mažesnę reguliavimą, gali būti mažiau saugios ir dažnai pasitaiko, kad jose vykdomi finansiniai sukčiavimai.

Surinkta lėšų suma per ICO gali turėti tiesioginę įtaką finansinių nusikaltimų mastui. Didelė surinkta suma gali rodyti didesnę investuotojų pasitikėjimą, tačiau ji taip pat gali sukurti prielaidas neteisėtai veiklai, nes didesni projektai gali turėti daugiau galimybių paslėpti sukčiavimus. Šis kintamasis buvo buvo naudojamas nustatyti finansinio nusikaltimo dydžiui.

Apibendrinant, autorių tyrimai atskleidžia pagrindinius kintamuosius, galinčius turėti reikšmingą įtaką finansinių nusikaltimų mastui ICO projektuose, įskaitant ICO populiarumą, rizikos balą, keityklos tipą ir surinktą lėšų sumą. ICO populiarumas, yra lemiamas veiksnys, rodantis investuotojų pasitikėjimą ir potencialiai didinantis nusikaltimų riziką dėl rinkos manipuliacijos galimybių. Rizikos balas įvertina projekto saugumo ir patikimumo lygį, o žemi balai gali signalizuoti didesnę riziką. Keityklos tipas, ar tai būtų decentralizuota (DEX), ar centralizuota (CEX), daro tiesioginę įtaką projektų saugumui. Surinkta suma atspindi projekto sėkmę ir investuotojų pasitikėjimą, tačiau didelės sumos taip pat gali tapti taikiniu nusikalstamai veiklai. Tyrimai rodo, kad šie kintamieji, analizuojami tiek atskirai, tiek jų sąveikoje, suteikia vertingų įžvalgų apie ICO projektų riziką ir finansinių nusikaltimų potencialą, padedant identifikuoti galimus rizikos veiksnius ir gerinti reguliacinę aplinką.

1.4.1 ICO rizikos balo kaip kintamojo naudojimas finansinių nusikaltimų ICO projektuose tyrimuose

Projekto sėkmė renkant finansinavimą dažnai priklauso nuo marketingo strategijos, turimos komandos, jau esamo kapitalo bei projektų kūrėjų istorijos (Sassi., 2023). Nuo to priklauso projektui suteikiamas rizikingumo vertinimas. Remiantis „ICOMARKS“ duomenimis didžioji dalis leidžiamų ICO turi sau nustatytą rizikingumo reitingą. Reitingas svyruoja nuo 1 – labai rizikingas projektas iki 10 – žemo rizikingumo projektas. Šis reitingas apskaičiuojamas remiantis:

- Bendra informacija (aprašymas, vaizdo įrašas, baltoji knyga ir kt.)
- Finansinė informacija (platforma, žetono tipas, kaina, ribinė vertė, maža ribinė vertė ir kt.)
- Projekto etapai
- Nuorodos ir veikla socialiniuose tinkluose
- Vieša informacija apie komandą ir patarėjus

Šie reitingai yra skirti padėti investuotojam susidaryti pirminį vaizdą apie projektą ir jo patikimumą (Boreiko, 2019). ICO vertinimas susiduria su reikšmingais iššūkiais, kuriuos lemia nepakankamas reguliavimas, neapibrėžtos informacijos pateikimo standartai ir duomenų trūkumas. Šiuos trūkumus iš dalies sprendžia nepriklausomos platformos, kuriose pateikiama statistinė informacija apie ICO, jų reitingai ir kiti svarbūs duomenys. Šių platformų nustatyti rizikos balai ilgainiui pradėjo daryti poveikį ICO projektų patikimumui ir jų sėkmei, ko pasekoje ir finansinio nusikaltimo dydžiui. Todėl šis kintamasis tapo daugelio mokslinių tyrimų objektu (Adhami ir kt., 2018; De Andrés ir kt., 2021; Grobys ir kt., 2022; Agarwal ir kt., 2023; Ante ir kt., 2018). Grobys ir kt. (2022) tyrimai išryškina ICO rizikos balą kaip svarbų rodiklį, kuris gali padėti įvertinti projekto patikimumą ir išskirti potencialiai sėkmingus projektus. Dean ir kt. (2020) akcentuoja, kad rizikos balai yra ne tik vertingi rodikliai investuotojams, bet ir padeda identifikuoti projektus, kurie ateityje gali būti siejami su finansiniais nusikaltimais.

Apibendrinant, nepaisant ekspertų pateikiamų vertinimų ir reitingų, Adhami ir kt. (2018) bei Boreiko ir Vidusso (2018) pastebi, kad kai kurie projektai vengia detaliai viešinti savo techninę informaciją arba ją pateikia sunkiai suprantamu formatu. Tai gali apsunkinti investuotojų galimybes objektyviai įvertinti projektą. Tokiais atvejais, pasak Albrecht ir kt. (2019), platformų teikiami ICO reitingai tampa pagrindiniu investuotojų informacijos šaltiniu, kuris padeda atskirti patikimus projektus nuo abejotinų.

1.4.2 Populiarumo kaip kintamojo naudojimas finansinių nusikaltimų ICO projektuose tyrimuose

Taip pat yra labai svarbu įvertinti ir esamą projekto populiarumą, kadangi daugeliu atvejų, būtent nuo to priklauso investicijos dydis ir kaina (Kethineni, 2020). Grobys ir kt. (2022), De Andrés ir kt. (2022) bei Adhami ir kt. (2018) tyrimuose nagrinėjamas ICO populiarumas kaip reikšmingas veiksnys, galintis daryti įtaką finansinių nusikaltimų atvejų dažnumui ir mastui ICO projektuose. Šiuose tyrimuose populiarumas buvo vertinamas pagal tokius kaip: socialinės medijos veiklą, diskusijas internetiniuose forumuose, „hype“ ir rizikos balas, investuotojų įsitraukimą bei bendrą rinkos susidomėjimą projektais. Tyrimai atskleidė, kad populiarumas gali būti svarbus indikatorius analizuojant sukčiavimo riziką ICO rinkoje. Viena vertus, didelis populiarumas padidina projekto matomumą ir patrauklumą investuotojams, tačiau tuo pačiu pritraukia ir didesnę sukčių dėmesį. Grobys ir kt. (2022) pastebėjo, kad labiau matomi projektai dažniau tampa manipuliacinių schemų, tokių kaip „pump and dump“, arba kitų sukčiavimo atvejų taikiniais. Panašiai De Andrés ir kt. (2022) pabrėžė, kad didelis ICO projektų populiarumas prisidėda ne tik prie rinkos augimo, bet ir prie spekuliacinio elgesio bei sukčiavimo masto didėjimo. Adhami ir kt. (2018) savo tyrime akcentavo, kad populiarumas yra ne tik sėkmingo finansavimo rodiklis, bet ir veiksnys, kuris gali atskleisti projekto riziką. Jie nustatė, kad nors populiarius projektai dažniau pritraukia investuotojus ir sėkmingai pritraukia finansavimą, pernelyg didelis dėmesys gali kelti papildomas grėsmes, pavyzdžiui, didesnę kibernetinių atakų ar manipuliacijų riziką.

Populiarumas, kaip kintamasis, mokslinėje literatūroje yra laikomas svarbiu įrankiu finansinių nusikaltimų ICO projektuose analizei. Autoriai pabrėžia, kad populiarumo analizė padeda identifikuoti rizikingus projektus ir geriau suprasti rinkos dinamiką, kuri gali skatinti nusikalstamą veiklą, tokią kaip likvidumo ištraukimas ar apgaulės. Be to, šis kintamasis gali būti naudingas reguliavimo strategijų tobulinimui, nes jo integravimas į rizikos vertinimo modelius leidžia efektyviau apsaugoti investuotojus ir užtikrinti rinkos stabilumą. Aukštas projekto populiarumas, nors ir demonstruoja gebėjimą pritraukti investicijas, gali kelti papildomą riziką, nes tokie projektai neretai tampa sukčiavimo taikiniais. Todėl populiarumo rodikliai yra reikšmingi ne tik nusikalstamų veikų prevencijai, bet ir ilgalaikio projekto patikimumo bei vertės vertinimui.

1.4.3 Projekto surinktos sumos kaip priklausomojo kintamojo naudojimas finansinių nusikaltimų ICO projektuose tyrimuose

Atliekant finansinių nusikaltimų analizę ICO rinkoje, vienas iš svarbiausių kintamųjų yra projekto surinkta suma. Šis kintamasis leidžia įvertinti ne tik projekto sėkmę, bet ir galimų finansinių nusikaltimų mastą. Straipsnyje "A Fractal View on Losses Attributable to Scams in the Market for Initial Coin Offerings" autoriai King ir Sapkota (2022) detaliai analizuoja surinktą sumą kaip pagrindinį tyrimo objektą, siekdami identifikuoti ir įvertinti nuostolius, kuriuos patiria investuotojai dėl apgaulės ICO projektuose.

Autoriai remiasi daugiau nei 5000 ICO projektų, vykdytų laikotarpiu nuo 2014 m. rugpjūčio iki 2019 m. gruodžio, duomenų analize. Iš šios imties buvo surinkta informacija apie 1014 projektų, kuriuose buvo užfiksuota informacija apie surinktas lėšas. Straipsnyje pateikiama, kad 56,80% šių projektų buvo susiję su apgavystėmis, o tai sudarė 65,80% visos rinkos kapitalizacijos, arba maždaug 10,12 milijardo JAV dolerių. Grobys ir kiti nurodo, kad surinkta suma kaip kintamasis ne tik atspindi projekto mastą, bet ir leidžia įvertinti potencialų rizikos lygį. Tyrimo metu buvo pastebėta, kad didesnės surinktos sumos dažnai susijusios su didesniais nuostoliais sukčiavimo atveju. Pavyzdžiui, didžiausias nuostolis, užfiksuotas Petro projekto, siekė 735 mln. JAV dolerių, o tai sudaro reikšmingą visų sukčiavimo atvejų dalį. Ši tendencija rodo, kad sukčiavimo mastą galima tiesiogiai sieti su surinkta suma kaip matavimo vienetu. Be to, autoriai pastebėjo, kad ICO rinkoje galioja stipriai išreikštas „80/20“ principas (Pareto dėsnis), pagal kurį 20% projektų sukelia 80% visų nuostolių.

Analizuojant ICO projektų rinką, surinkta suma dažnai traktuojama kaip reikšmingas rodiklis, atspindintis projekto sėkmę ir investuotojų pasitikėjimą. Tačiau moksliniuose tyrimuose taip pat pabrėžiama, kad surinktos sumos dydis gali būti susijęs su finansinių nusikaltimų mastu. Pasak Ante ir Meyer (2021), surinkta suma ICO projektuose gali būti vertinama kaip signalas apie projekto kokybę, tačiau kartu šis signalas gali būti iškreiptas manipuliacijų, sukčiavimo ar kitų neteisėtų veiklų. Autoriai nurodo, kad ICO rinkose, kuriose nėra centralizuotų reguliacinių mechanizmų, surinktos lėšos gali būti panaudotos neteisėtoms veikloms, įskaitant pinigų plovimą, "pump-and-dump" schemas ar kitas manipuliacijas. Ante ir Meyer (2021) aptaria, kad surinkta suma dažnai tampa pagrindiniu tikslu manipulatoriams, kurie siekia pasinaudoti projekto viešumu ir investuotojų susidomėjimu. Jie taip pat pažymi, kad neteisėtos veiklos mastą gali rodyti išankstiniai prekybos apimtys pokyčiai arba rinkos segmentacija. Šiame kontekste

„Blockchain-Based ICOs: Pure Hype or the Dawn of a New Era of Startup Financing?“ (Ante, Sandner, Fiedler, 2018) tyrimas atskleidžia keturis pagrindinius sėkmės aspektus, kurie taip pat gali būti susiję su finansiniais nusikaltimais: žmogiškąjį kapitalą, verslo modelio kokybę, projekto aprašymą ir socialinę mediją. Autoriai pastebi, kad aukštos kokybės infrastruktūros ir „whitepaper“ dokumentų egzistavimas didina projekto sėkmės galimybes, tačiau taip pat gali būti išnaudojami manipuliacijoms. Surinktos lėšos dažnai tampa rodikliu, naudojamu kaip signalas investuotojų pritraukimui, tačiau tuo pat metu gali būti susijusios su sukčiavimu.

Atsižvelgiant į šiuos rezultatus, surinkta suma yra itin tinkamas kintamasis, vertinant finansinio nusikaltimo mastą ICO projektuose. Šis kintamasis leidžia ne tik identifikuoti rizikingus projektus, bet ir kiekybiškai įvertinti sukčiavimo pasekmes rinkai. Naudojant galios dėsnių modelius, galima numatyti, kokios ekstremalios vertės gali būti pasiekiamos, ir identifikuoti kritines sritis, kuriose reikia papildomos reguliacinės priežiūros. Todėl būsimas tyrimas, kuriame surinkta suma bus analizuojama kaip finansinio nusikaltimo masto rodiklis, gali prisidėti prie platesnio supratimo apie ICO rinkos problemas bei pateikti praktines rekomendacijas reguliavimo institucijoms ir investuotojams.

1.5 Finansinių nusikaltimų pirminiuose monetų siūlymuose tyrimo metodų identifikavimas

Siekiant efektyviai analizuoti ir vertinti finansinius nusikaltimus, susijusius su pirminiais monetų siūlymais (ICO), svarbu identifikuoti ir suprasti taikomus tyrimo metodus bei jų efektyvumą. Tai apima kruopščią esamų mokslinių darbų ir empirinių tyrimų analizę, leidžiančią detaliai įvertinti finansinių nusikaltimų mastą ir jų poveikį decentralizuotoms finansų sistemoms (4 lentelė).

4 lentelė.

Autorių tyrimų metodai tiriant didžiausius pirminiuose monetų siūlymuose atliktus finansinius nusikaltimus

Tyrimo metodas	Tyrimo metodas	Autoriai, metai
Kokybiniai tyrimo metodai	Literatūros analizė, Atvėjų analizė	Trozze ir kt. (2022), Karpenko ir kt. (2020)
Kiekybiniai tyrimo metodai	Statistinių duomenų rinkimas ir analizė (regresinė analizė, įvairūs testai, aprašomoji statistika)	Adhami ir kt. (2018), Zheng ir Wang (2022) Ante ir kt. (2018), Boreiko ir Vidusso (2018), Hornuf ir kt. (2021), Lars Hornuf ir kt. (2021), Ante ir Meyer (2021), Lee ir kt. (2018), Fu ir kt. (2022), Liebau ir Schueffel (2019), Agarwal, ir kiti (2023).

Šaltiniai: Lentelė sukurta autoriaus remiantis lentelėje pateiktų autorių tyrimais.

Vertinant autorių Trozze ir kiti (2022) atliktą literatūros analizę „Cryptocurrencies and future financial crime“ kurioje nagrinėjami tiriamieji darbai kurie yra susiję su nusikaltimais decentralizuotoje rinkoje ir pirminiais monetų siūlymais. Galima įvertinti padarytą išvadą, jog sukčiavimo kriptovaliutomis tyrimų skaičius didėja, tačiau siekiant šią rinką padaryti kaip galima skaidresnę reikalingas didesnis kiekis tyrimų, kuris apimtų epmyrinius finansinių nusikaltimų tyrimus. Siekiant skaidrinti konkrečiai pirminių monetų siūlymų rinką Karpenko, Blokhina ir Chebukhanov (2020) atliko tyrimą, kurio tikslas buvo išnagrinėti ICO plėtrą ir jos įtaką kriptovaliutų rinkai, identifikuoti pagrindines plėtros tendencijas bei įvertinti dalyvaujančių įmonių ir išleistų finansavimo sumų mastą. Tyrimo rezultatai parodė, jog kad ICO rinka sparčiai augo 2016–2019 metais, pritraukdama dėmesį iš daugelio pasaulio šalių. Išskirtinai daug ICO vyko Jungtinėse Valstijose ir Singapūre, kurios pasižymi aukštu finansinės infrastruktūros lygiu, plačia skaitmenizacija ir pakankamu teisiniu reglamentavimu. Tyrimo metu identifikuotos rizikos kategorijos - finansinės, techninės ir analitinės, o siūlomos riziką mažinančios priemonės apėmė baltojo popieriaus publikavimą, KYC procedūrą ir užstato agentų įtraukimą. Be to, nustatyta, kad ICO projektų sėkmė arba nesėkmė dažnai priklauso nuo teisinio reglamentavimo, bendradarbiavimo su potencialiais investuotojais ir tinkamos ICO reklamos strategijos. Būtent pirminių monetų siūlymų rinkoje yra vykdoma daug finansinių nusikaltimų kurie yra susiję su pinigų nusiavinimu - „Rug pull“. Šis finansinio nusikaltimo būdas buvo naudojamas darbe jau minėtuose „Onecoin“, „AnubisDAO“ ir „SQUID“ projektuose. Ši

finansinių nusikaltimų būdą savo tyrime „Short Paper: DeFi Deception – Uncovering the prevalence of rugpulls in cryptocurrency projects“ išnagrinėjo autoriai: Agarwal, Atondo-Siu, Ordekian ir kiti (2023). Atlikus kiekybinį tyrimą paaiškėjo, jog visos šešios „Rug pull“ sritys veikė panašiu principu. Autoriai pateikė išvadas, kurios nurodė, jog „Rug pull“ projektai dažnai naudoja finansinius, laiko ir kainų principus, kad pritrauktų investuotojus, bet retai naudoja klastojimo, atitraukimo ar melagysčių principus. Taip pat atlikta empirinė analizė rodo, kad ilgai veikiantys projektai linkę palaukti palankaus „Ethereum“ kursų ir tik tada įgyvendinti „Rug pull“. Kursų ir „Rugpull“ projektų skaičiaus mėnesio koreliacija palaiko šią hipotezę. Analizuojant finansinių nusikaltimų ICO projektuose tyrimus pastebima, tyrinėjimo metodai ir sritys gana stipriai skiriasi. Liebau ir Schueffel (2019) tyriamajame darbe buvo atlikta duomenų bazių analizė siekiant nustatyti, kokią dalį bendros pirminių monetų siūlymų rinkos sudaro finansiniai nusikaltimai, kurių metu buvo pasisavintos investuotojų lėšos. Pirma, naudojant „Lexis Nexis“ duomenų bazę, buvo vertinami naujienų straipsniai, susijusę su tyrinėjamos imties ICO, medžiaga. Antrame žingsnyje buvo atliktas išsamus paieškos proceso tyrimas, siekiant surasti galimus teisinius procesus ar teismo bylas, kilusias iš pasirinktos imties ICO. Trečia, jeigu buvo pradėtos teisėsaugos procedūros, buvo tiriama, ar jau priimtas teismo sprendimas ir, jeigu taip, kokios buvo sprendimo detalės. Atlikus tyrimą nustatyta, jog apie 10 procentų 2016 metais išleistų ICO projektų baigėsi finansiais nusikaltimais, kai buvo nusisavintos investuotojų lėšos. Atsižvelgiant į tai, jog 2016 metais ICO rinka buvo sąlyginai maža ir rinkos kapitalizacija sudarė 90 milijonų dolerių (žr. 5 pried.), 10 procentų nuo visos rinkos sudarė 9 milijonus dolerių. (žr. 6 pried.) 5-8 numeriu pažymėti empiriniai tyrimai rėmėsi duomenimis apie konkrečių ICO prekiavimo duomenis, kapitalizaciją, likvidumą, dienos kainas bei laikotarpį kurį buvo prekiaujama siūloma moneta. Tai padėjo indikuoti, jog keityklų kuriose parduodama skaitmeninė moneta dydis bei likvidumas daro stiprią įtaką ICO sėkmei jei baltajama lape nurodo, jog bus ten listinguotas ir nurodoma, jog mažesnės keityklos dažniau susiduria su sukčiavimo atvejais (žr. 7 pried.). (žr. 6 pried.) pateiktas 7 tyrimas, atliktas taikant Mann-Whitney U testą ir mažos imties T testą taip pat ir Kolmogorov-Smirnov testą parodė, jog siūlomi rodikliai ir prognozavimo modeliai nepademonstravo statistinio skirtumo tarp piramidinių schemų ICO ir sėkmingų ICO žetonų platinimo modelių. Išvadose nurodyta, kad daugiapakopės rinkodaros (MLM) ir piramidinių schemų modelių paplitimas ICO platinimo yra gana didelis, o tai rodo, kad ICO dažniausiai naudojamos į MLM panašios strategijos, sukeliant papildomą riziką investuotojams. Straipsnyje pripažįstami trūkumai ir raginama tęsti teisės, politikos ir sociologijos mokslinius tyrimus, kad būtų galima geriau nustatyti piramidines schemas

kripto valiutų rinkoje, kartu pabrėžiant reguliavimo pastangų poreikį, siekiant užtikrinti šios finansinės inovacijos klestėjimą ateityje.

Pirminio viešo žetonų siūlymo rinka, nors ir yra nuosmukio periode tiek išleistų projektų skaičiaus, tiek surinktų lėšų kiekiu, išlieka svarbi decentralizuotų finansų rinkų dalis (3 priedas.). Decentralizuota ekosistema, kurioje vykdomi ICO, yra itin dinamiška ir stipriai priklausoma nuo bendros rinkos tendencijų. Analizuojant finansinius nusikaltimus ICO projektuose, svarbu pastebėti, kad ši tema dar nėra iki galo išnagrinėta, todėl nuodugnių tyrimų poreikis išlieka aktualus. Daugelis autorių, tokių kaip Adhami ir kt. (2018), Zheng ir Wang (2022), Boreiko ir Vidusso (2018), Hornuf ir kt. (2021), dažniausiai renkasi kiekybinius tyrimo metodus, pavyzdžiui, regresinės analizės, statistinių duomenų vertinimo ar testų taikymą, siekdami išsamiau suprasti veiksnius, darančius įtaką ICO projektų sėkmei ir finansinių nusikaltimų mastui. Šių metodų taikymas leidžia gauti aiškius ir pagrįstus rezultatus, kurie padeda identifikuoti svarbiausius rizikos veiksnius ir tendencijas. Tęsiant tokio pobūdžio tyrimus, galima užtikrinti, kad ICO rinka taptų skaidresnė ir mažiau pažeidžiama finansinių nusikaltimų, ypač rinkos pakilimo laikotarpiais. Mokslinių tyrimų rezultatai, įskaitant atliktą regresinę analizę, taip pat padeda formuoti praktines rekomendacijas, kurios gali būti naudingos tiek investuotojams, tiek įmonėms, planuojančioms naudoti ICO kaip finansavimo priemonę.

2. FINANSINIŲ NUSIKALTIMŲ ICO PROJEKTUOSE EMPYRINIO TYRIMO METODOLOGIJA

2.1 Tyrimo tikslas, modelis ir hipotezės

Šio tyrimo tikslas yra ištirti finansinius nusikaltimus ICO projektuose, analizuojant pagrindinius veiksnius, turinčius įtakos šiems nusikaltimams, tokius kaip: ICO populiarumas, ICO rizikos balas, keityklos tipas bei surinkta suma (tūkst. USD). Šie kintamieji padės įvertinti, kaip skirtingos ICO projekto charakteristikos gali turėti įtakos finansinių nusikaltimų mastui. Remiantis duomenimis iš „Coinmarketcap.com“, šiuo metu pasaulyje yra daugiau nei 23000 skirtingų kriptovaliutų, kurių bendra kapitalizacija siekia \$1,751 trilijoną. Norint įvertinti šį dydį, galima palyginti su Niujorko vertybinių popierių biržos kapitalizacija, kuri sudaro apie 30,1 trilijonus dolerių, ir NASDAQ kapitalizacija, kuri siekia 17 trilijonų dolerių. Kriptovaliutų kapitalizacija yra ženkli net dviejų didžiausių akcijų biržų kontekste. Todėl supratimas apie finansinius nusikaltimus decentralizuotoje ekosistemoje yra išties esminis, siekiant užtikrinti finansinių rinkų stabilumą ir investuotojų kapitalo saugumą. Tai tampa dar aktualesniu diskusijų objektu, ypač atsižvelgiant į tai, kad įvairios šalys nagrinėja galimybes taikyti kriptovaliutas nacionaliniu mastu (Bindseil, 2020). Šiame bus aprašoma empirinio tyrimo metodologija, kuri bus taikoma gauti išsamesnių įžvalgų apie finansinius nusikaltimus ICO projektuose.

Analizuojant ICO projektus, susijusius su finansiniais nusikaltimais, pastebėta, jog dauguma tyrimų kurie tyrė finansinius nusikaltimus ICO projektuose (4 lentelė) yra buvo atlikti naudojant kiekybinius tyrimo metodus tokius kaip statistinių duomenų rinkimas ir analizė, todėl šiame tyrime remiantis (3 lentelė) pateiktais tyrimais šio darbo pradinis etapas apėmė literatūros analizę, siekiant identifikuoti pagrindinius veiksnius, darančius įtaką finansiniams nusikaltimams ICO projektuose. Šis žingsnis leido aiškiai apibrėžti tyrimo kintamuosius, tokius kaip ICO populiarumas, rizikos balas, keityklos tipas ir surinkta suma, ir formuluoti hipotezes, kurios bus empiriškai tikrinamos. Tyrimas bus atliekamas siekiant nustatyti, kaip šie veiksniai daro įtaką finansinio nusikaltimo dydžiui – matuojamam surinktų lėšų dydžiui. Finansinio nusikaltimo dydis yra svarbus rodiklis, kadangi jis leidžia įvertinti, kokią riziką investuotojams ir rinkai gali kelti ICO projektas (Swartz, 2022). Šio tyrimo rezultatai prisidės prie giliau suprantamos ICO projektų specifikos, padės geriau vertinti riziką ir tobulinti reguliavimo mechanizmus.

Šiame tyrime bus naudojami duomenys, kurie buvo atrinkti remiantis pateiktais autoriais ir jų atliktais tyrimais, siekiant įvertinti, kaip ICO projektų populiarumas, rizikos balas, listinimo tipas ir surinktos sumos dydis gali paveikti finansinių nusikaltimų mastą. Pateikti duomenys apima šiuos kintamuosius:

1. **ICO populiarumas** – Klasifikuotas į keturias kategorijas: Žemas, Vidutinis, Aukštas, Labai aukštas.
2. **ICO rizikos balas** – Klasifikuotas į keturias kategorijas: Neįvertinta, Žemas, Vidutinis, Aukštas.
3. **Keityklos tipas**– Nurodo, ar ICO projektas buvo listintas centralizuotoje (CEX) ar decentralizuotoje (DEX) keitykloje, jei nepavyko gauti duomenų N/A.
4. **Surinkta suma (tūkst. USD)** – Tai priklausomas kintamasis, kuris matuoja finansinio nusikaltimo mastą.

Kiekvienam iš šių kintamųjų darbe yra keliamos H0 ir H1 hipotezės:

- **Hipotezė H0:** ICO listinimo būdas (CEX ar DEX) neturi reikšmingos įtakos finansinio nusikaltimo mastui .
- **Hipotezė H1:** ICO listinimo būdas (CEX ar DEX) turi reikšmingą įtaką finansinio nusikaltimo mastui

Ši hipotezė buvo keliamą remiantis autorių Agarwal ir kt. (2023), Aspris ir kt. (2021), Han, Huang ir Zhong (2024) bei Hägele (2024) tyrimais, kuriuose buvo analizuojamas keityklos tipo (CEX ar DEX) poveikis ICO projektų veiklai ir finansinio nusikaltimo mastui. Šie tyrimai pabrėžė, kad centralizuotos keityklos (CEX) dažnai turi griežtesnius reguliavimo reikalavimus ir geriau užtikrina projektų skaidrumą, tačiau jos taip pat gali būti patrauklesnės taikiniai nusikalstamoms veikoms, tokioms kaip likvidumo vagystės. Tuo tarpu decentralizuotos keityklos (DEX), nors ir užtikrina didesnę anonimiškumą, dažnai yra mažiau reguliuojamos, o tai gali sudaryti palankesnes sąlygas finansiniams nusikaltimams, tokiems kaip sukčiavimas ar neteisėtas lėšų pervedimas. Atsižvelgiant į šiuos aspektus, hipotezė buvo formuluojama siekiant empiriškai įvertinti, ar keityklos tipas reikšmingai įtakoja finansinio nusikaltimo mastą ICO projektuose.

- **Hipotezė H0:** ICO rizikos balas (aukštas, vidutinis, žemas) neturi reikšmingos įtakos finansinio nusikaltimo mastui.
- **Hipotezė H1:** ICO rizikos balas (aukštas, vidutinis, žemas) turi reikšmingą įtaką finansinio nusikaltimo mastui.

Ši hipotezė buvo keliama remiantis Dean ir kt. (2020) bei Grobys, King ir Sapkota (2022) tyrimais, kuriuose buvo nagrinėjamas ICO rizikos balo poveikis projektų saugumui ir jų ryšiui su finansinio nusikaltimo mastu. Autoriai pabrėžė, kad rizikos balas yra svarbus rodiklis, leidžiantis įvertinti projekto patikimumą ir galimas rizikas. Aukštas rizikos balas paprastai siejamas su didesniu skaidrumu ir mažesne finansinių nusikaltimų tikimybe, tuo tarpu žemas balas gali indikuoti padidėjusią riziką, įskaitant sukčiavimo ar neteisėtų veiklų galimybę. Atsižvelgiant į šiuos aspektus, hipotezė buvo suformuluota siekiant empiriškai įvertinti, ar rizikos balas turi reikšmingą įtaką finansinio nusikaltimo mastui ICO projektuose, ir nustatyti, kurios rizikos kategorijos labiausiai veikia šią priklausomybę.

- **Hipotezė H0:** ICO populiarumas (labai aukštas, aukštas, vidutinis, žemas) neturi reikšmingos įtakos finansinio nusikaltimo mastui.
- **Hipotezė H1:** ICO populiarumas (labai aukštas, aukštas, vidutinis, žemas) turi reikšmingą įtaką finansinio nusikaltimo mastui.

Ši hipotezė buvo keliama remiantis Adhami ir kt. (2018), De Andrés ir kt. (2021), bei Grobys, King ir Sapkota (2022) tyrimais, kuriuose buvo analizuojamas ICO projektų populiarumo poveikis finansiniams rezultatams ir nusikaltimų mastui. Autoriai teigia, kad ICO populiarumas, matuojamas investuotojų įsitraukimu, viešumu ir rinkodaros kampanijų sėkme, gali turėti reikšmingą įtaką projekto sėkmei ir jo potencialiam tapimui nusikalstamos veiklos taikiniu. Labai aukšto ar aukšto populiarumo projektai dažniau pritraukia didesnes investicijas, tačiau kartu ir padidina riziką, susijusią su finansinėmis apgaulėmis ar manipuliacijomis rinkoje. Hipotezė buvo suformuluota siekiant empiriškai įvertinti, ar populiarumas gali būti laikomas reikšmingu veiksniu, lemiančiu finansinio nusikaltimo mastą ICO projektuose, ir nustatyti, kaip skirtingi populiarumo lygiai paveikia šį santykį.

2.2 Empyrinio tyrimo modelis

Darbe keliamos hipotezės bus tikrinamos remiantis 1 darbo dalyje analizuotų autorių tyrimo metodais. Šio tyrimo empirinis modelis bus atliekamas visų pirma patikrinant ar duomenys tolygiai pasiskirstę atliekant Shapiro-Wilk testą, pateikiama modelio lygtis:

(1 formulė)

$$W = \frac{(\sum_{i=1}^n a_i x_{(i)})^2}{\sum_{i=1}^n (x_i - \bar{x}_{(i)})^2}$$

Shapiro-Wilk testas atliekamas siekiant įvertinti, ar kiekvienos kategorijos duomenys (ICO populiarumas, ICO rizikos balas ir Keityklos tipas) yra normaliai paskirstyti. Šio testo tikslas yra patikrinti, ar duomenų paskirstymas atitinka normalumo prielaidą, kuri būtina tolesnei analizei. Kur:

$x_{(i)}$: i-asis stebėjimas, išrikiuotas didėjančia tvarka,

$\bar{x}$: Stebėjimų vidurkis,

a_i : Svoriniai koeficientai, apskaičiuoti remiantis tikėtinomis koreliacijomis su normaliojo pasiskirstymo eilute,

n : Imties dydis.

Šio testo formulė analizuoja kiekvienos kategorijos duomenų simetriškumą, apskaičiuodama statistiką W , kuri lygina duomenų stebėjimus su tikėtinu normaliu pasiskirstymu. Testo rezultatai leidžia nustatyti, ar normalumo prielaidos yra tenkinamos, o tai būtina sprendžiant, ar naudoti parametrinius metodus, tokius kaip ANOVA, ar pereiti prie neparametrinių metodų šiuo atveju Kruskalio–Walliso testo. Lygiagrečiai papildomam patikrinimui buvo atliktas Levene'o testas, kuris parodė ar skirtingų grupių (šiuo atveju – ICO populiarumo, rizikos balo ir keityklos tipo kategorijų) kintamasis turi vienodą dispersiją, formulė pateikiama:

(2 formulė)

$$F = \frac{\sum_{g=1}^k N_g (\bar{z}_g - \bar{z})^2}{\sum_{g=1}^k \sum_{i=1}^{N_g} (z_{gi} - \bar{z}_g)^2}$$

Levene'o testas parodė, kad visų analizuojamų kintamųjų grupių dispersijos yra homogeniškos $p > 0$. Tai indikavo, kad duomenys skirtingose grupėse yra pakankamai vienodai paskirstyti, todėl galima naudoti parametrinius metodus, tokius kaip ANOVA, siekiant toliau analizuoti šių kintamųjų įtaką surinktos sumos dydžiui.

(3 formulė)

$$F = \frac{\frac{\sum_{g=1}^k N_g (\bar{y}_g - \bar{y})^2}{k - 1}}{\frac{\sum_{g=1}^k \sum_{i=1}^{N_g} (y_{gi} - \bar{y}_g)^2}{N - k}}$$

Kur:

k: grupių skaičius (pvz., „Žemas“, „Vidutinis“, „Aukštas“, „Labai aukštas“).

N: visų stebėjimų skaičius.

Ng: stebėjimų skaičius kiekvienoje grupėje.

$\bar{Y}_g$: kiekvienos grupės vidurkis.

$\bar{Y}$: bendras vidurkis.

Y_{gi} : individuali stebėjimo reikšmė g-toje grupėje.

ANOVA analizė yra esminė siekiant įvertinti, ar ICO populiarumas, rizikos balas ir keityklos tipas reikšmingai veikia ICO projektų surinktą sumą, kuri yra finansinio nusikaltimo masto rodiklis. Ši analizė leidžia patikrinti, ar vidutinės surinktos sumos statistiškai skiriasi tarp skirtingų grupių, nustatyti, kuris iš kintamųjų turi stipriausią poveikį, bei įvertinti galimus sąveikos efektus tarp jų. ANOVA testas suteikia galimybę statistiškai pagrįstai patvirtinti arba atmesti tyrime iškeltas hipotezes, padedant identifikuoti reikšmingus skirtumus tarp populiarumo, rizikos balų ir keityklos tipų grupių. Lygiagrečiai siekiant papildomai patikrinti ANOVA testus buvo pasirinkta Spearman koreliacijos analizė kaip papildomas tyrimo metodas, nes pradinuose analizės etapuose nustatyta, kad kintamųjų tokių kaip keityklos tipas duomenų paskirstymas neatitinka normalumo prielaidų. Šis metodas leidžia įvertinti ryšį tarp ranginių kintamųjų, todėl jis yra tinkamas analizuojant nenormaliai paskirstytus duomenis arba duomenis su kategoriniais kintamaisiais, kaip šiuo atveju – ICO populiarumas, ICO rizikos balas ir keityklos tipas.

(4 formulė)

$$p = 1 - \frac{6 \sum d_i^2}{n(n^2 - 1)}$$

Jei koreliacijos koeficientas (p) yra artimas 1 arba -1, tai leistų daryti išvadą, kad tarp nagrinėjamų kintamųjų egzistuoja stiprus teigiamas arba neigiamas ryšys. Tokiu atveju galima būtų tiksliau prognozuoti, kaip tam tikri veiksniai, pavyzdžiui, didelis populiarumas arba žemas rizikos balas, paveikia projektų gebėjimą pritraukti finansavimą. Jei koreliacijos koeficientas būtų artimas 0, tai reikštų, kad ryšys tarp kintamųjų yra silpnas arba jo visai nėra, ir būtina apsvarstyti kitus galimus veiksnius. Šis metodas svarbus kadangi gali įvertinti monotoninius ryšius, net jei jie nėra linijiniai. Jei būtų pastebėta stipri teigiama koreliacija tarp ICO populiarumo ir surinktos sumos, tai leistų nustatyti, jog investuotojai

teikia pirmenybę gerai žinomiems projektams. Tuo tarpu silpnas ryšys galėtų rodyti, kad kiti veiksniai, tokie kaip rizikos balas ar keityklos tipas yra svarbesni pritraukiant lėšas.

Siekiant nustatyti, ar aukštesnis rizikos balas daro įtaką ICO projekto finansinio nusikaltimo dydžiui. Šio tyrimo modelis remiasi standartine regresijos lygtimi:

(5 formulė)

$$y = a + \beta_1 x_1 \cdots + \beta_k x_k + \varepsilon$$

Lygtyje priklausomas kintamasis y žymi sąlygą, kurią modelis siekia įvertinti. a – konstanta, kurios reikšmė nurodo, kur regresijos tiesė kerta y ašį. β – koeficientas, nurodantis regresijos tiesės statumą ir atitinkamai regresoriaus jautrumą pokyčiams. ε – žymi liekamąją paklaidą, o k – nepriklausomų kintamųjų skaičių. x žymi nepriklausomą kintamąjį, kuris siekia paaiškinti priklausomąjį kintamąjį y .

Šio tyrimo atveju kintamieji bus:

- y – finansinio nusikaltimo mastas,
- x_2 – ICO rizikos balas,

Modelio postūmis žymimas kaip β_0 , β_1 ir β_2 – regresijos koeficientai, kurie nurodo kiekvieno nepriklausomo kintamojo įtaką priklausomajam kintamajam. ε – paklaidą, kuri atsiranda dėl neįvertintų faktorių. Regresijos analizė leis įvertinti ne tik kiekvieno kintamojo įtaką atskirai, bet ir jų tarpusavio sąveiką, leidžiančią geriau suprasti, kaip visi veiksniai kartu daro įtaką finansinių nusikaltimų dydžiui.

Tyrimo esmė - išsiaiškinti, ar projekto populiarumas, rizikos vertinimas gali būti naudingi vertinant finansinio riziką ICO projektuose. Šis tyrimas yra skirtas gilinti supratimą apie tai, kaip šie veiksniai gali turėti įtakos finansinių nusikaltimų tikimybei ICO projektuose. Galutinėje stadijoje pateikiamos rekomendacijos, kurios padės sumažinti finansinio nusikaltimo riziką šio tipo projektuose. Tai leis įgyti išsamų supratimą apie rizikos veiksnius ir padės įgyvendinti praktines priemones siekiant saugumo ir patikimumo ICO projektų rinkoje.

3. FINANSINIŲ NUSIKALTIMŲ ICO PROJEKTUOSE EMPYRINIS TYRIMAS

Šiame skyriuje, remiantis 2 skyriuje apibrėžta metodologija, bus pristatomas empyrinis tyrimas, kuriuo siekiama įvertinti finansinių nusikaltimų mastą ICO (pirminių monetų siūlymų) projektuose. Tyrimo pagrindą sudaro analizuojami duomenys apie ICO projektus, kurie atliko finansinį nusikaltimą, vertinant - ICO populiarumą, rizikos balus, listinimo tipus ir surinktas lėšas, siekiant nustatyti, kaip šie kintamieji gali būti susiję su nusikalstama veikla šiame decentralizuotame finansavimo modelyje. Naudojant logistinę regresiją, bus įvertinta, kurie kintamieji reikšmingai prisideda prie nusikaltimų tikimybės, ir pateiktos įžvalgos apie rizikos valdymo ir reguliavimo galimybes ICO rinkoje.

3.1 Finansinių nusikaltimų pirminiuose monetų siūlymuose empyrinis tyrimas

Norint atlikti finansinių nusikaltimų analizę ICO projektuose, pirmiausia būtina nustatyti tyrimo imtį. Atsižvelgiant į tai, kad pagrindinis priklausomas kintamasis šiame tyrime yra ICO projekto surinktos lėšos, kurios dažniausiai tampa žinomos tik užbaigus projektą, tyrimo imtis apima tik tuos ICO, kurių veikla jau yra pasibaigusi. Siekiant užtikrinti tyrimo rezultatų patikimumą ir surinkti kuo didesnę duomenų bazę, į analizę įtraukiami visi pasibaigę ICO projektai kuriuose buvo atliktas finansinis nusikaltimas nuo jų atsiradimo pradžios 2015 m. iki 2023m.. Remiantis „ICOMARKS“ ir „Foundico“ platformų pateiktais duomenimis, per šį laikotarpį buvo identifikuota 95 ICO projektai, kuriuose nustatyti finansiniai nusikaltimai. Šie projektai sudaro tyrimo pagrindą ir leidžia analizuoti įvairius veiksnius, tokius kaip ICO populiarumas, rizikos balas, keityklos tipas (CEX/DEX) ir surinktų lėšų dydis. Toks tyrimo imties pasirinkimas suteikia galimybę įvertinti galimus ryšius tarp šių veiksnių ir finansinių nusikaltimų masto, taip pat pateikti rekomendacijas dėl ICO rinkos reguliavimo ir rizikos mažinimo priemonių.

5 lentelė.

Duomenys apie didžiausius pirminius monetų siūlymus, kuriuose buvo atlikti finansiniai nusikaltimai .

Nr.	Projekto pavadinimas	ICO populiarumas	ICO Rizikos balas	Keitykla (CEX/DEX)	Surinkta suma (tūkst. USD)
1	Petro	Žemas	Aukštas	CEX	735,000
2	Pincoin	Žemas	Neįvertinta	N/A	660,000

3	TaTaTu	Vidutinis	Neįvertinta	CEX	575,000
4	Filecoin	Aukštas	Žemas	CEX	257,000
5	Tezos	Vidutinis	Neįvertinta	CEX	232,000
6	Polymath	Labai aukštas	Neįvertinta	CEX	207,326
7	SIRINLABS	Labai aukštas	Žemas	CEX	157,886
8	Bankera	Labai aukštas	Žemas	CEX	151,800
9	Neluns	Vidutinis	Neįvertinta	CEX	136,000
10	Orbs	Vidutinis	Neįvertinta	CEX	118,000
11	Envion	Aukštas	Aukštas	CEX	100,000
12	Comsa	Vidutinis	Vidutinis	CEX	95,000
13	OKOIN	Žemas	Aukštas	DEX	80,000
14	Tenx	Aukštas	Žemas	CEX	80,000
15	Flashmoni	Žemas	Vidutinis	CEX	72,000
16	Bankex	Aukštas	Žemas	CEX	70,600
17	Hycon	Vidutinis	Neįvertinta	CEX	68,000
18	Zeepin	Aukštas	Neįvertinta	DEX	62,600
19	ACChain	Labai aukštas	Aukštas	CEX	60,000
20	WPP	Aukštas	Aukštas	N/A	59,780
21	Tron	Žemas	Vidutinis	N/A	58,098
22	Elastos	Aukštas	Neįvertinta	CEX	57,891
23	Alchemy	Vidutinis	Aukštas	CEX	57,000
24	MobileGo	Vidutinis	Neįvertinta	CEX	53,000
25	Nexo	Vidutinis	Neįvertinta	DEX	52,500
26	Neuromation	Aukštas	Vidutinis	N/A	51,835
27	Crypterium	Aukštas	Vidutinis	CEX	51,657
28	Swissborg	Aukštas	Vidutinis	CEX	50,890
29	Odyssey	Vidutinis	Aukštas	CEX	50,000
30	Savedroid	Vidutinis	Aukštas	CEX	50,000
31	BlockStack	Vidutinis	Žemas	CEX	50,000
32	Celsius	Labai aukštas	Vidutinis	CEX	50,000
33	HybridBlock	Aukštas	Vidutinis	DEX	47,830
34	GoNetwork	Aukštas	Vidutinis	CEX	46,790
35	Iungo	Aukštas	Neįvertinta	CEX	45,979
36	NAGACoin	Vidutinis	Aukštas	CEX	45,319
37	Loopring	Aukštas	Vidutinis	N/A	45,000
38	ArcBlock	Aukštas	Vidutinis	CEX	45,000
39	Fresco	Žemas	Aukštas	CEX	45,000
40	IndaHash	Aukštas	Žemas	CEX	42,716
41	Fusion	Vidutinis	Vidutinis	CEX	42,200
42	Consentium	Vidutinis	Aukštas	CEX	42,000
43	SONM	Aukštas	Neįvertinta	CEX	42,000
44	Finom	Vidutinis	Vidutinis	DEX	41,285
45	Electroneum	Vidutinis	Žemas	CEX	40,000
46	Datawallet	Aukštas	Žemas	DEX	40,000
47	Yggdrash	Vidutinis	Aukštas	CEX	40,000
48	Hurify	Vidutinis	Žemas	CEX	40,000
49	WePower	Aukštas	Vidutinis	DEX	40,000
50	FANTOM	Aukštas	Vidutinis	CEX	39,400
51	0chain	Vidutinis	Neįvertinta	DEX	39,000
52	Stellar	Aukštas	Neįvertinta	CEX	39,000
53	Ripio	Vidutinis	Neįvertinta	CEX	37,800
54	Crypto20	Aukštas	Vidutinis	CEX	37,698
55	Kelta	Vidutinis	Aukštas	CEX	37,378
56	MoneyToken	Aukštas	Aukštas	CEX	37,189

57	Monetha	Aukštas	Labai žemas	CEX	37,000
58	Wanchain	Aukštas	Žemas	DEX	35,658
59	PundiX	Aukštas	Neįvertinta	CEX	35,000
60	Agrello	Aukštas	Vidutinis	CEX	35,000
61	BasicAttentionToken	Labai aukštas	Neįvertinta	CEX	35,000
62	SHIVOM	Aukštas	Vidutinis	CEX	35,000
63	Stox	Aukštas	Vidutinis	CEX	33,000
64	BackToTheFuture	Vidutinis	Vidutinis	CEX	33,000
65	Civic	Aukštas	Neįvertinta	CEX	33,000
66	SingularityNET	Aukštas	Neįvertinta	CEX	32,848
67	JET8	Vidutinis	Vidutinis	CEX	32,700
68	Qlink	Žemas	Žemas	CEX	32,000
69	Polybius	Vidutinis	Neįvertinta	DEX	31,000
70	CyberMiles	Labai aukštas	Vidutinis	DEX	30,882
71	STORMToken	Aukštas	Vidutinis	CEX	30,716
72	Play2Live	Vidutinis	Žemas	CEX	30,000
73	ShipChain	Aukštas	Neįvertinta	CEX	30,000
74	DigitalTicks	Vidutinis	Neįvertinta	CEX	30,000
75	Havven	Vidutinis	Vidutinis	CEX	30,000
76	JioCoin	Žemas	Aukštas	DEX	30,000
77	Fitrova	Žemas	Neįvertinta	CEX	29,028
78	Faceter	Vidutinis	Žemas	CEX	28,610
79	Universa	Aukštas	Žemas	CEX	28,559
80	AirCoin	Žemas	Neįvertinta	CEX	27,988
81	Refereum	Aukštas	Žemas	CEX	27,800
82	SentinelProtocol	Aukštas	Vidutinis	CEX	27,700
83	Eidoo	Vidutinis	Neįvertinta	CEX	27,423
84	AION	Aukštas	Neįvertinta	CEX	27,000
85	OmiseGO	Vidutinis	Neįvertinta	CEX	27,000
86	UserVice	Vidutinis	Aukštas	CEX	26,893
87	Monaco	Vidutinis	Žemas	CEX	26,700
88	Pchain	Vidutinis	Neįvertinta	N/A	26,674
89	SENSE	Vidutinis	Vidutinis	CEX	26,000
90	PowerLedger	Aukštas	Vidutinis	CEX	26,000
91	Essentia	Labai aukštas	Vidutinis	CEX	25,500
92	Aitheon	Vidutinis	Neįvertinta	CEX	25,353
93	Bitdepository	Žemas	Neįvertinta	CEX	25,000
94	Storiqa	Aukštas	Žemas	DEX	25,000
95	APEX	Vidutinis	Neįvertinta	CEX	25,000

Šaltiniai: Lentelė sukurta autoriaus remiantis „ICOMARKS“ ir „Foundico“ duomenimis.

Finansinių nusikaltimų rizika ICO projektuose gali priklausyti nuo daugybės veiksnių, kai kurie projektai, kaip „Petro“, „Pincoin“ ir „TaTaTu“, kurie turėjo žemą populiarumą, tačiau aukštą rizikos balą, įvykdė finansinius nusikaltimus, kas sukėlė investuotojų nuostolius. Tai rodo, kad net ir mažiau žinomi projektai, turintys didelį rizikos balą, gali tapti taikiniu finansinių nusikaltimų. Kita vertus, kai kuriuose projektuose, pavyzdžiui, „Filecoin“ ir „Tezos“, kurių ICO populiarumas buvo aukštas, o rizikos balas žemas, nors ir surinkta didelė suma, taip pat buvo atlikta finansinių nusikaltimų. Tai rodo, kad net ir gerai žinomi ir sėkmingi projektai, turintys didelę surinktą sumą, gali būti siejami su finansiniais nusikaltimais, kurie daro įtaką investuotojų pasitikėjimui ir rinkos

stabilumui. Tai pabrėžia, kad didelis ICO populiarumas ir suma ne visada garantuoja saugumą, nes ne visos problemos yra susijusios tik su valdymo kokybe ar projekto sėkme. Šie duomenys rodo, kad finansinių nusikaltimų atsiradimas ICO projektuose gali priklausyti nuo daugelio veiksnių, įskaitant ICO populiarumą, rizikos balą ir surinktą sumą. Dėl šios priežasties svarbu atlikti empirinį tyrimą, siekiant nustatyti, ar egzistuoja ryšys tarp šių veiksnių ir finansinių nusikaltimų. Toks tyrimas padės geriau suprasti, kokie rizikos veiksniai lemia finansinių nusikaltimų tikimybę ICO sektoriuje ir kokių priemonių reikėtų imtis, siekiant užtikrinti saugesnę kriptovaliutų rinką.

6 lentelė.

Duomenų apie didžiausius pirminius monetų siūlymus, kuriuose buvo atlikti finansiniai nusikaltimai aprašomojoji statistika.

Statistika	Vertė
Iš viso projektų	95
Bendra surinkta suma (tūkst. USD)	5,444,015
Vidutinė surinkta suma (tūkst. USD)	57,305
Mediana (tūkst. USD)	40,000
Didžiausia surinkta suma (tūkst. USD)	735,000
Mažiausia surinkta suma (tūkst. USD)	25,000
Standartinis nuokrypis (tūkst. USD)	86,166

Šaltiniai: Lentelė sukurta autoriaus remiantis „ICOMARKS“ duomenimis.

Iš viso pateikta informacija apie 95 projektus, kurie bendrai surinko 5,444,015 tūkst. USD. Didžiausia surinkta suma siekia 735,000 tūkst. USD (Petro projektas), o mažiausia surinkta suma yra 25,000 tūkst. USD, kurią surinko Bitdepository, Storiqa ir APEX projektai. Vidutinė surinkta suma yra 57,305 tūkst. USD, o mediana - 40,000 tūkst. USD, standartinis nuokrypis sudaro 86,166 tūkst. USD. Bendras didelis standartinis nuokrypis rodo, kad yra didelis skirtumas tarp surinktų sumų tarp įvairių projektų. Pagal šiuos duomenis galima matyti, jog ICO sėkmė gali priklausyti nuo skirtingų faktorių, todėl yra svarbu įvertinti kas konkrečiai gali turėti įtakos projektų sėkmei.

3.1.1 Keityklos tipo kaip kintamojo įtaka ICO projektų finansinio nusikaltimo mastui empirinis tyrimas

Šiame poskyryje analizuojama keityklos tipo įtaka ICO projektų surinktai sumai, kuri yra vertinama kaip finansinio nusikaltimo masto rodiklis. Keityklos pasirinkimas gali atspindėti projekto patikimumą, skaidrumą ir rizikos lygį, taip pat turėti reikšmingos įtakos investuotojų elgsenai.

7 lentelė.

Duomenų apie didžiausius pirminius monetų siūlymus, kuriuose buvo altikti finansiniai nusikaltimai, vertinant pagal projekto pasirinktą keityklos tipą listingui, aprašomojoji statistika.

Keityklos tipas	Projektų skaičius	Vidutinė surinkta suma (tūkst. USD)	Mediana (tūkst. USD)	Bendra surinkta suma (tūkst. USD)
CEX	76	88,470	50,000	6,721,720
DEX	11	47,873	39,000	526,600
N/A	8	120,548	58,098	964,385

Šaltiniai: Lentelė sukurta autoriaus remiantis „ICOMARKS“ duomenimis.

Lentelėje pateikiami duomenys atspindi ICO projektų surinktos sumos statistinius rodiklius pagal keityklos tipą: centralizuotas keityklas (CEX), decentralizuotas keityklas (DEX) ir neapibrėžtą keityklos tipą (N/A). Didžiausias projektų skaičius (76) buvo arba pateikė, jog bus listinguotas CEX keityklose, kuriose vidutinė surinkta suma siekė 88,470 tūkst. USD, o mediana – 50,000 tūkst. USD. DEX keityklose, kuriose buvo arba pateikė, jog bus listinguotas listinguoti 11 projektų, vidutinė surinkta suma buvo 47,873 tūkst. USD, o mediana – 39,000 tūkst. USD. Projektai, kurių keityklos tipas nenurodytas (N/A), pasižymėjo didžiausia vidutine surinkta suma – 120,548 tūkst. USD, o mediana siekė 58,098 tūkst. USD. Šie duomenys indikuoja, jog didžioji dalis ICO projektų renkasi CEX kaip potencialaus listingo keityklą, daroma išvada, jog CEX dėl griežtesnės kontrolės ir reikalavimų suteikia investuotojams pasitikėjimo jausmą, ko pasekoje daugiau ICO projektų rinkosi būtent CEX. Lygiagrečiai tyrimo tikslas buvo įvertinti, ar keityklos tipas (CEX, DEX, N/A) turi reikšmingą įtaką ICO projektų surinktai sumai. Tyrime buvo atlikas duomenų normalumo tikrinimas, dispersijos homogeniškumo vertinimas ir, jei prielaidos buvo tenkinamos, variacinės analizės (ANOVA) taikymą. Gauti rezultatai pateikiami ir interpretuojami pagal kiekvieną analizės etapą. Shapiro-Wilk testas buvo naudojamas įvertinti, ar surinktos sumos kiekvienoje keityklos grupėje (CEX, DEX, N/A) yra paskirstytos normaliai. Šio testo reikšmės pateikiamos (žr. 8 lent.).

8 lentelė.

Normalumo prielaidos tikrinimas Shapiro-Wilk testo rezultatai

Keitykla	p reikšmė
CEX	4.37e-13
DEX	0.0351
N/A	3.85e-10

Šaltiniai: Lentelė sukurta autoriaus naudojant RSTUDIO.

Visų trijų grupių p reikšmės yra mažesnės nei 0.05, o tai rodo, kad duomenų paskirstymas nėra normalus. Kadangi ANOVA reikalauja normalumo prielaidos, ši sąlyga

nėra visiškai tenkinama. Dėl to Levene'o testas buvo atliktas siekiant patikrinti, ar grupių dispersijos yra homogeniškos – tai svarbi prielaida ANOVA taikymui.

9 lentelė.

Dispersijos homogeniškumo tikrinimas Leveno testas rezultatai

Df	F reikšmė	p reikšmė
2	0.6557	0.5215

Šaltiniai: Lentelė sukurta autoriaus naudojant RSTUDIO.

Levene'o testo p reikšmė (0.5215) yra didesnė nei 0.05, o tai rodo, kad dispersijos tarp grupių yra homogeniškos. Tai reiškia, jog ši ANOVA prielaida yra tenkinama, todėl buvo galima tęsti analizę nepaisant netenkinamo normalumo. Variacinė analizė buvo atlikta siekiant nustatyti, ar keityklos tipas turi reikšmingą įtaką ICO projektų surinktai sumai. ANOVA rezultatų santrauka pateikta 10 lentelėje.

10 lentelė.

Variacinės analizės ANOVA rezultatai

Terminas	Kvadratų suma	Laisvės laipsniai	Vidutinė kvadratų reikšmė	F reikšmė	p reikšmė
Keitykla	2.28e+10	2	1.14e+10	0.87	0.423
Rezidualai	1.21e+12	92	1.32e+10	-	-

Šaltiniai: Lentelė sukurta autoriaus naudojant RSTUDIO.

ANOVA rezultatai rodo, kad p reikšmė (0.423) yra didesnė nei 0.05. Tai reiškia, jog nėra statistiškai reikšmingų skirtumų tarp grupių (CEX, DEX, N/A) surinktų sumų atžvilgiu. Todėl tyrimas nepatvirtina, kad keityklos tipas daro reikšmingą įtaką ICO projekto surinktai sumai. Todėl darbe buvo atlikta regresinė analizė siekiant papildomai įvertinti ar keityklos, kurioje turėto būti listinguotas projektas turi įtaką surinktai sumai. Prieš atliekant koreliacinę analizę, iš duomenų rinkinio buvo pašalintos eilutės su „N/A“ reikšme keityklos tipo kintamajame, nes ši reikšmė reiškia, kad nėra duomenų apie tai, kur buvo listinguotas projektas. Kadangi tyrimo tikslas buvo įvertinti, ar keityklos tipas turi reikšmingą ryšį su ICO projektuose surinkta suma, nepakankami arba nežinomi duomenys galėjo iškraipyti rezultatus ir sumažinti analizės patikimumą. Keityklos tipas buvo kintamasis: CEX priskirta reikšmė 1, o DEX – reikšmė 0.

11 lentelė.

Spearman koreliacijos su rezultatų santrauka.

Testas	Statistika	p reikšmė
Shapiro-Wilk normalumo testas	W = 0.383	p < 2.2e-16
Spearman koreliacija	rho = 0.211	p = 0.079

Šaltiniai: Lentelė sukurta autoriaus naudojant RSTUDIO.

Spearman koreliacijos analizė parodė, kad egzistuoja silpnas ryšys tarp keityklos tipo ir ICO projekto surinktos sumos ($\rho = 0.211$), tačiau šis ryšys nėra statistiškai reikšmingas ($p = 0.079$). Rezultatai rodo tendenciją, kad CEX yra susijusios su didesnėmis surinktomis sumomis, palyginti su DEX. Tai leidžia dalinai patvirtinti hipotezę, kad egzistuoja ryšys tarp keityklos tipo ir finansinio nusikaltimo dydžio. CEX keityklų gebėjimas pritraukti didesnes sumas galimai kyla dėl jų struktūrinių ir funkcinių pranašumų, tokių kaip didesnis patikimumas, reguliavimo užtikrinimas ir patrauklesnės rinkodaros strategijos. Šie aspektai gali pritraukti daugiau investuotojų ir sudaryti palankesnes sąlygas ICO projektams surinkti didesnes sumas, o tai savo ruožtu gali turėti įtakos finansinių nusikaltimų mastui, kai surinktos lėšos yra panaudojamos neteisėtiems tikslams.

Apibendrinant, šio tyrimo rezultatai rodo tendenciją, kuri leidžia dalinai patvirtinti iškeltą hipotezę apie ryšį tarp keityklos tipo ir finansinio nusikaltimo dydžio. Tai pabrėžia CEX keityklų svarbą ICO projektų finansavimo ekosistemoje, siekiant plačiau ištirti rodiklius kurie daro įtaką finansiniams nusikaltimams ICO projektuose, toliau bus atliekamas tyrimas ar projekto populiarumas turi įtakos finansinio nusikaltimo mastui ICO projektuose.

3.1.2 Projekto populiarumo kaip kintamojo įtaka ICO projektų finansinio nusikaltimo mastui empirinis tyrimas

Finansinių nusikaltimų prevencija ir analizė ICO projektuose yra aktuali tema šiuolaikiniame finansų sektoriuje, ypač atsižvelgiant į didėjančią „blockchain“ technologijų ir kriptovaliutų rinkos svarbą. ICO projektų populiarumas gali būti svarbus veiksnys, nulemiantis finansinių nusikaltimų mastą, nes aukštas populiarumas dažnai siejamas su didesniu investuotojų dėmesiu ir reikšmingomis surinktomis sumomis. Šioje tyrimo dalyje bus tiriama, kaip ICO projekto populiarumas susijęs su surinkta finansavimo suma, remiantis tuo, kad surinktos lėšos gali būti naudojamos kaip finansinių nusikaltimų mato rodiklis. X lentelėje pateikiama turimų duomenų apie ICO projektus susijusius su finansiniais nusikaltimais aprašomoji statistika, vertinant pagal projekto populiarumą (žr.12 lent.)

12 lentelė.

Duomenų apie didžiausius pirminius monetų siūlymus, kuriuose buvo altikti finansiniai nusikaltimai, vertinant pagal projekto populiarumą, aprašomojoji statistika.

ICO populiarumas	Projektų skaičius	Vidutinė surinkta suma (tūkst. USD)	Mediana (tūkst. USD)	Bendra surinkta suma (tūkst. USD)
Labai aukštas	12	162,901	60,000	1,954,816
Aukštas	32	60,528	40,000	1,936,899
Vidutinis	35	52,579	35,000	1,840,263
Žemas	16	113,866	45,000	1,821,037

Šaltiniai: Lentelė sukurta autoriaus remiantis „ICOMARKS“ duomenimis.

Analizuojant ICO populiarumo kategorijas - labai aukšto populiarumo kategorijoje yra 12 projektų, aukšto - 32 projektai, vidutinio - 35 projektai, žemo - 16 projektų. Projektai, turintys labai aukštą populiarumą, vidutiniškai surinko 162,901 tūkst. USD, o mediana siekia 60,000 tūkst. USD, bendra šios kategorijos projektų surinkta suma - 1,954,816 tūkst. USD. Aukšto populiarumo kategorijoje vidutinė surinkta suma yra 60,528 tūkst. USD, o mediana - 40,000 tūkst. USD, bendras surinktas suma - 1,936,899 tūkst. USD. Vidutinio populiarumo projektai vidutiniškai surinko 52,579 tūkst. USD, o mediana siekia 35,000 tūkst. USD, bendras surinktas suma - 1,840,263 tūkst. USD. Žemo populiarumo projektai vidutiniškai surinko 113,866 tūkst. USD, o mediana siekia 45,000 tūkst. USD, bendras surinktas suma - 1,821,037 tūkst. USD. Labai aukšto populiarumo projektai surinko didžiausias vidutines sumas, o bendra šios kategorijos projektų surinkta suma yra didžiausia. Aukšto populiarumo kategorijos projektai surinko mažesnes vidutines sumas nei labai aukšto populiarumo projektai, tačiau jų bendra surinkta suma yra beveik lygiavertė, tai indikuoja, jog net ir žemesnį populiarumą turintys projektai gali surinkti ženklas sumas.

Vidutinio populiarumo projektai surinko mažiausias vidutines sumas, kas gali rodyti mažesnę investuotojų susidomėjimą arba atsargesnę požiūrį į šiuos projektus. Tačiau ši kategorija turi daugiausiai projektų, todėl bendra surinkta suma vis dar yra reikšminga.

Žemo populiarumo projektai, nors ir surinko mažiau nei labai aukšto populiarumo projektai, vis dėlto vidutiniškai surinko didesnes sumas nei vidutinio populiarumo projektai. Tai gali rodyti, kad nors šie projektai turi mažesnę viešą profilį, jie sugebėjo pritraukti reikšmingas investicijas kaip specifinių nišų projektai. Atliekant empirinį tyrimą buvo atliktas Shapiro-Wilk testas, siekiant patikrinti, ar ICO surinktos sumos yra normaliai paskirstytos skirtingose populiarumo kategorijose. Kadangi p reikšmė yra mažesnė nei 0.05, galime atmesti hipotezę, kad duomenys yra normaliai paskirstyti. Tai rodo, jog

surinktų sumų pasiskirstymas nėra normalus. Todėl buvo pasirinktas Kruskalio–Valio testas, testų reikšmės pateiktos (žr. 13 lent.).

13 lentelė.

Lentelė su pagrindiniais testo statistiniais rezultatais.

Testas	Statistika	p reikšmė
Shapiro-Wilk testas	$W = 0.38$	< 0.001
Kruskalio–Valio testas	$\text{Chi-sq} = 7.94$	0.047
Spearman koreliacija	$\rho = 0.312$	0.005

Šaltiniai: Lentelė sukurta autoriaus naudojant RSTUDIO.

Kruskalio–Valio testo rezultatai rodo, kad p reikšmė yra mažesnė nei 0.05, o tai leidžia daryti išvadą, kad egzistuoja statistiškai reikšmingi skirtumai tarp skirtingų ICO populiarumo kategorijų. Tai patvirtina, kad populiarumo lygis daro įtaką projektų gebėjimui pritraukti finansavimą. Siekiant nustatyti tiesioginį ryšį tarp ICO populiarumo ir surinktos sumos, buvo atliktas Spearman koreliacijos testas. Koreliacijos koeficientas $\rho = 0.312$ rodo teigiamą, nors ir silpną ryšį tarp ICO populiarumo ir surinktos sumos. Kadangi p reikšmė yra mažesnė nei 0.05, šis ryšys yra statistiškai reikšmingas, o tai leidžia teigti, kad didėjant populiarumo lygiui, projektai vidutiniškai pritraukia didesnes investicijas. Labai aukšto populiarumo projektai surinko didžiausias vidutines sumas, atspindinčias stiprų investuotojų pasitikėjimą ir gebėjimą pritraukti lėšas, dažnai dėl platesnės rinkodaros ir marketingo. Žemo populiarumo projektai, nors vidutiniškai surinko mažiau nei labai aukšto populiarumo projektai, dažnai demonstruoja reikšmingus rezultatus, kas gali reikšti jų sėkmę dėl nišinių privalumų ar specifinio rinkos segmentavimo. Tuo tarpu vidutinio populiarumo projektai surinko mažiausias vidutines sumas, kas gali rodyti investuotojų atsargesnį požiūrį, tačiau, turėdami daugiausiai projektų, šie vis tiek reikšmingai prisideda prie bendros surinktos sumos.

Apibendrinant, tyrimo rezultatai atskleidė, kad ICO populiarumas yra svarbus, lemiančių surinktų lėšų dydį, ir turi reikšmingą įtaką finansinio nusikaltimo ICO projekte mastui. Nors koreliacinė analizė parodė silpną, tačiau statistiškai reikšmingą ryšį tarp ICO populiarumo ir surinktos sumos, tendencijos išryškina svarbius skirtumus tarp populiarumo kategorijų. Labai aukšto populiarumo projektai aiškiai dominuoja, surinkdami didžiausias vidutines sumas. Ši sėkmė gali būti siejama su stipresnėmis rinkodaros strategijomis, didesniu visuomenės dėmesiu ir investuotojų pasitikėjimu, kurį šie projektai geba sukurti. Jie dažniausiai veikia kaip aukštos kokybės projektai, pritraukiantys reikšmingą dalį investicijų rinkos.

3.1.3 Projekto rizikos balo kaip kintamojo įtaka ICO projektų finansinio nusikaltimo mastui empirinis tyrimas

Rizikos balas dažnai naudojamas įvertinti tokio tipo investicijų saugumą ir galimą grąžą, todėl svarbu ištirti, kaip šis balas gali paveikti surinkto finansavimo dydį (Zhang, 2020). Todėl atliekant tyrimą buvo analizuojami ICO projektų kurie atliko finansinį nusikaltimą rizikos balo duomenys (žr. 14 lent.).

14 lentelė.

Didžiausių finansinių nusikaltimų pirminiuose monetų siūlymuose duomenų, vertinant pagal rizikingumą, aprašomojoji statistika.

ICO reitingo rizikos balas	Projektų skaičius	Vidutinė surinkta suma (tūkst. USD)	Mediana (tūkst. USD)	Bendra surinkta suma (tūkst. USD)
Labai aukštas	8	157,039	60,000	1,256,314
Aukštas	16	79,612	45,000	1,273,795
Vidutinis	36	46,218	40,000	1,663,852
Žemas	20	63,640	40,000	1,272,799
Neįvertinta	15	86,293	42,000	1,292,755

Šaltiniai: Lentelė sukurta autoriaus remiantis „ICOMARKS“ duomenimis.

Pagal ICO rizikos balą, labai aukšto rizikos balo projektai vidutiniškai surinko 157,039 tūkst. USD, o mediana siekia 60,000 tūkst. USD, bendra surinkta suma 1,256,314 tūkst. USD. Aukšto rizikos balo projektai vidutiniškai surinko 79,612 tūkst. USD, o mediana siekė 45,000 tūkst. USD, bendra surinkta suma - 1,273,795 tūkst. USD. Vidutinio rizikos balo projektai vidutiniškai surinko 46,218 tūkst. USD, o mediana siekia 40,000 tūkst. USD, bendra surinkta suma - 1,663,852 tūkst. USD. Žemo rizikos balo projektai vidutiniškai surinko 63,640 tūkst. USD, o mediana siekė 40,000 tūkst. USD, bendrai surinkta suma - 1,272,799 tūkst. USD. Neįvertinti projektai vidutiniškai surinko 86,293 tūkst. USD, o mediana siekia 42,000 tūkst. USD, bendra surinkta suma - 1,292,755 tūkst. USD. Projektai su labai aukštu rizikos lygiu surinko didžiausias sumas, tai parodo, jog investuotojai yra linkę prisiimti didesnę riziką tikėdamiesi didesnės grąžos.

Rizikingų projektų surinkto finansavimo apimties mediana yra didesnė taip pat bendra surinkta suma yra didelė, kas indikuoja, jog didelį finansavimą gali surinkti net rizikingi ir daugeliu atvejų nieko nepagrįsti projektai. Aukšto rizikos lygio projektai vidutiniškai surinko mažesnes sumas nei labai aukšto rizikos projektai, tačiau vis tiek surinko dideles sumas, tai nurodo, kad investuotojai gali prisiimti didesnę riziką už atitinkamą grąžą ir daugeliu atvejų investuotojai neįvertina visų rizikų susijusių su projektu, tačiau aklaiai remiasi projekto kūrėjų pateiktą informacija bei reklama. Vidutinio rizikos

lygio projektai sudaro didžiausią bendrą surinktą sumą, rodančią, kad ši rizikos kategorija yra patraukliausia daugumai investuotojų dėl subalansuoto rizikos ir grąžos santykio. Žemo rizikos lygio projektai vidutiniškai surinko didesnes sumas nei vidutinės rizikos projektai, tačiau jų bendra surinkta suma yra panaši į aukšto rizikos projektų surinktą sumą, tai indikuoja, kad atsargesni investuotojai, taip pat investuoja reikšmingas sumas. Neįvertinti projektai vidutiniškai surinko nemažas sumas, rodydami, kad nepaisant neapibrėžtumo, investuotojai yra pasirengę finansuoti ir tokius projektus, remdamiesi kitais kriterijais. Tačiau ši teorija dar bus tikrinama atliekant koreliacinę analizę. Rizikos balas dažnai naudojamas įvertinti tokio tipo investicijų saugumą ir galimą grąžą, todėl svarbu ištirti, kaip šis balas gali paveikti surinkto finansavimo dydį (Zhang, 2020). Tyrimui atlikti buvo naudojama tiesinė regresija kurios rezultatai pateikiami (žr. 2 paveiksl.).

2 paveikslas

Tiesinės regresijos modelio rezultatai įvertinti kokią įtaką rizikos balas turi ICO projekto surinktai sumai.

Residuals:

Min	1Q	Median	3Q	Max
-337500	-13861	-3261	4539	337500

Coefficients:

	Estimate	Std. Error	t value	Pr(> t)
(Intercept)	68051	16478	4.130	0.000106 ***
ICO_Rizikos_baluŽemas	-22591	20085	-1.125	0.264832
ICO_Rizikos_baluVidutinis	-16018	24068	-0.666	0.508071
ICO_Rizikos_baluAukštas	329449	50789	6.487	1.39e-08 ***

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 67940 on 65 degrees of freedom

Multiple R-squared: 0.4411, Adjusted R-squared: 0.4153

F-statistic: 17.1 on 3 and 65 DF, p-value: 2.707e-08

Šaltiniai: Paveikslas sukurtas autoriaus remiantis „ICOMARKS“ duomenimis.

Statistinė analizė indikuoja, jog ICO projektai su aukštu rizikos balu pritraukė vidutiniškai 329,449 tūkst. USD. didesnes finansines sumas, palyginti su kitomis rizikos kategorijomis. Kitos kategorijos (žemas, vidutinis, aukštas) neturėjo statistiškai reikšmingos įtakos. Tiesinė regresija paaiškino 44.11% dispersijos duomenų. F-statistika $F = 17.1$ ir $p = 2.707e-08$ patvirtina modelio statistinį reikšmingumą. Todėl daroma išvada, jog ICO rizikos balas gali įtakoti surinktą finansavimo sumą. Kadangi projektai su aukštensiu rizikos balu dažniausiai pritraukė didesnes lėšas.

Siekiant sumažinti riziką prarasti investicijas ICO projektuose, investuotojai turi atlikti išsamų tyrimą apie kiekvieną projektą ir jo komandą. Tai apima dokumentacijos analizę, kurioje būtina išnagrinėti projekto baltoją knygą, techninę dokumentaciją ir verslo

modelį, siekiant suprasti projekto tikslus, technologiją ir įgyvendinimo planą. Taip pat svarbu patikrinti projekto komandos narių patirtį, reputaciją ir ankstesnius projektus, užtikrinant, kad komanda turi patirties ir sėkmingų projektų istoriją (Zhang, 2020). Analizė parodė, kad ICO projektai gali pritraukti investicijas nepriklausomai nuo rizikos lygio, tačiau mažesnė rizika dažnai siejama su didesnėmis potencialiomis investicijomis, todėl daroma išvada, jog investuotojai reaguoja tik į pačius aukščiausius rizikos balus – skaidriausius projektus.

IŠVADOS IR PASIŪLYMAI

1. Tyrimas atskleidė, kad finansinių nusikaltimų ICO projektuose mastą lemia daugybė veiksnių, tokių kaip projekto populiarumas, rizikos balas bei keityklos, kurioje projektas listinamas, tipas. ICO rinka, nors ir siūlo gero potencialaus uždarbio galimybes investuotojams ir įmonėms, susiduria su finansiniais nusikaltimais dėl menko reguliavimo, informacijos asimetrijos ir galimų apgavysčių.
2. Dauguma sukčiavimo atvejų decentralizuotose finansų sistemose susiję su pirminiais monetų siūlymais (ICO). Pastebima, jog ICO sritis yra linkusi į pažeidimus ir manipuliacijas, trūksta teisinės reguliavimo kontrolės.
3. Projekto populiarumas yra svarbus veiksnys, darantis įtaką surinktai sumai. Labai populiarūs projektai dažniausiai pritraukia didesnę investuotojų pasitikėjimą ir surenka daugiau lėšų, tačiau taip pat tampa labiau pažeidžiami finansiniams nusikaltimams. Tai rodo, jog populiarumas gali būti susijęs tiek su projekto sėkme, tiek su didesne rizika.
4. Atliekant empyrinį tyrimą buvo nustatyta, kad ICO projektai su aukštu rizikos balu (mažesnio rizikingumo) pritraukė vidutiniškai 329,449 tūkst. USD didesnes investicijas, palyginti su kitomis rizikos kategorijomis. Statistinė analizė parodė, kad tik ši kategorija turėjo statistiškai reikšmingą poveikį pritrauktoms lėšoms (F-statistika $F = 17.1$, $p = 2.707e-08$), o kitos kategorijos, tokios kaip „vidutinis“ ar „žemas“ rizikos balas, neturėjo reikšmingos įtakos. Todėl daroma išvada, kad investuotojai labiau pasitiki skaidriais, aukšto rizikos balo projektais, kurie yra patikimesni ir potencialiai mažiau linkę į nusikalstamą veiklą.
5. Siekiant sumažinti riziką prarasti investicijas ICO projektuose, investuotojams būtina atlikti nuodugnų kiekvieno projekto ir jo komandos tyrimą. Tai apima išsamią projekto dokumentacijos peržiūrą, įskaitant baltoją knygą (whitepaper), techninę dokumentaciją ir verslo modelį, siekiant pilnai suprasti projekto tikslus, technologinį pagrindą ir įgyvendinimo planus. Ypač svarbu įvertinti komandos narių patirtį, reputaciją ir ankstesnius projektus, siekiant užtikrinti, kad jie turi reikiamą kompetenciją ir sėkmingų projektų istoriją. Taip pat rekomenduojama analizuoti projekto populiarumą, stebint socialinių tinklų aktyvumą, bendruomenės įsitraukimą ir sekėjų skaičių, kad būtų galima įvertinti bendruomenės palaikymą. Be to, svarbu peržiūrėti nepriklausomų ekspertų atliktas audito ataskaitas ir rizikos vertinimus.
6. Tam, kad rizika susijusi su ICO projektais būtų mažinama, būtina stiprinti teisinį reguliavimą, įdiegti veiksmingas saugumo priemones ir atlikti tyrimus kurie pateiktų

detalią informaciją apie nusikaltimus ICO. Tai padėtų užtikrinti, kad investuotojai būtų apsaugoti nuo potencialių finansinių nusikaltimų.

7. Atliekant ICO rinkos nusikaltimų analizę, jos rezultatai ir metodologijos ateityje galėtų būti pritaikytos ir kitiems sutelktinio finansavimo metodams, tokiems kaip „Security Token Offerings“ (STO), „Initial Exchange Offerings“ (IEO). Tyrimai leistų geriau suprasti šių inovatyvių finansavimo modelių rizikas, padėtų kurti universalius rizikos valdymo sprendimus ir skatintų skaidrumo didinimą visame decentralizuotų finansų sektoriuje.

LITERATŪROS IR ŠALTINIŲ SĄRAŠAS

- Agarwal, S., Atondo-Siu, G., Ordekian, M., Hutchings, A., Mariconti, E., and Vasek, M. (2023). "DeFi Deception – Uncovering the prevalence of rugpulls in cryptocurrency projects." University College London, University of Cambridge.
- Akyildirim, E., Conlon, T., Corbet, S., Goodell, J. W. (2023). Understanding the FTX exchange collapse: A dynamic connectedness approach. *Finance Research Letters*, 53, 103643. <https://doi.org/10.1016/j.frl.2023.103643>
- Anson, M. (2021). "Initial Exchange Offerings: The Next Evolution in Cryptocurrencies." *The Journal of Alternative Investments*, 10.3905/jai.2021.1.127.
- Adhami, S., Giudici, G., & Martinazzi, S. (2018). "Why do businesses go crypto? An empirical analysis of initial coin offerings." *Journal of Economics and Business*, 100, 64–75. <https://doi.org/10.1016/j.jeconbus.2018.04.001>
- Aspris, A., Foley, S., Svec, J., Wang, L. (2021). Decentralized exchanges: The “wild west” of cryptocurrency trading. *International Review of Financial Analysis*, 77, 101845. <https://doi.org/10.1016/j.irfa.2021.101845>
- Agarwal, U., Rishiwal, V., Tanwar, S., Yadav, M. (2022) "Blockchain and crypto forensics: Investigating crypto frauds." Correspondence: Vinay Rishiwal, Department of Computer Science and Engineering. <https://doi.org/10.1002/nem.2255>
- Ante, L., Meyer, A. (2021). "Cross-listings of blockchain-based tokens issued through initial coin offerings: Do liquidity and specific cryptocurrency exchanges matter?" *Decisions in Economics and Finance*, 44, 957–980. <https://doi.org/10.1007/s10203-021-00323-0>.
- Ante, L., Sandner, P., Fiedler, I. (2018). "Blockchain-Based ICOs: Pure Hype or the Dawn of a New Era of Startup Financing?" *Journal of Risk and Financial Management*, 11(4), 80. <https://doi.org/10.3390/jrfm11040080>.
- Brown, S. D. (2016). "Cryptocurrency and criminality: The Bitcoin opportunity." *The Police Journal: Theory, Practice and Principles*, 89(4), 327–339. <https://doi.org/10.1177/0032258X16658927>
- Boreiko, D., Vidusso, G. (2019). New Blockchain Intermediaries: Do ICO Rating Websites Do Their Job Well? *The Journal of Alternative Investments*, 21(4), 67–79. <https://doi.org/10.3905/jai.2019.21.4.067>
- Bindseil, U. (2020). "Tiered CBDC and the Financial System." European Central Bank (ECB). <http://dx.doi.org/10.2139/ssrn.3513422>.

- Boyko, A., Dotsenko, T., Dolia, Yu. (2020) "Patterns of financial crimes using cryptocurrencies." Sumy State University, Sumy, Ukraine. DOI: 10.55643/ser.2.44.2022.454.
- Butler, S. (2019). Criminal use of cryptocurrencies: a great new threat or is cash still king? *Journal of Cyber Policy*, 4(3), 326-345. <https://doi.org/10.1080/23738871.2019.168072>
- Cavusgil, S. T., Knight, G. ir Riesenberger, J. R. (2016). *International business*. London: Pearson,
- Conlon, T., McGee, R. (2021). *ICO Fraud and Regulation*. Batten-Corbet-Lucey Handbooks in Alternative Investments, Forthcoming. <https://ssrn.com/abstract=3770659>
- Cernera, F., La Morgia, M., Mei, A., and Sassi, F. (2023). "Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens in Ethereum and in the Binance Smart Chain (BNB)." Sapienza University of Rome. In *Proceedings of the 32nd USENIX Security Symposium*, August 9–11, 2023, Anaheim, CA, USA. 978-1-939133-37-3.
- Chen, Y. (2018). "Blockchain tokens and the democratization of entrepreneurship and innovation." *Business Horizons*, 61(4), 567–575. <https://doi.org/10.1016/j.bushor.2018.03.006>
- De Kluyver, C. (2017). *A Primer on Corporate Governance*. Business Expert Press.
- Dean, T., Daluwathumullagamage, D. J., Marsden, A. (2020). "Predictability of ICO Success and Returns." *The Journal of Applied Business and Economics*, 22(13), 20–36.
- De Andrés, P., Arroyo, D., Correia, R., & Rezola, A. (2021). Challenges of the market for initial coin offerings. *International Review of Financial Analysis*,. <https://doi.org/10.1016/j.irfa.2021.101966>
- Daniels, J. D., Radebaugh, L. H. ir Sullivan, D. P. (2017). *International business*. London: Pearson.
- Dicken, P. (2014). *Global Shift: Mapping the Changing Contours of the World Economy*. United states: Guilford Publications.
- ElBahrawy, A., Alessandretti, L., Kandler, A., Pastor-Satorras, R., Baronchelli, A. (2017). Evolutionary dynamics of the cryptocurrency market. *Royal Society Open Science*, 4, 170623. <http://dx.doi.org/10.1098/rsos.170623>

- Foley, S., Karlsen, J. R., Putniņš, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798–1853. <https://doi.org/10.1093/rfs/hhz015>
- Fu, Z., Gu, W., Fang, Z., Yan, J., & Liu, X. F. (2022). Pyramid Scheme Prevails in ICO: Evidence from Primary Market Token Transaction Analyses. <http://dx.doi.org/10.2139/ssrn.4225546>.
- Gurrea-Martínez A., Nydia R. (2019) "The Law and Finance of Initial Coin Offerings." Ibero-American Institute for Law and Finance, Working Paper Series 4/2018. Oxford University Press. <http://dx.doi.org/10.2139/ssrn.3182261>
- Grobys, K., King, T., Sapkota, N. (2022). "A Fractal View on Losses Attributable to Scams in the Market for Initial Coin Offerings." *J. Risk Financial Manag.*, 15(12), 579. <https://doi.org/10.3390/jrfm15120579>.
- Gujarati, Damodar N. (2004) *Basic Econometrics*. 4th ed. New York: McGraw-Hill
- Mankiw, N. G., Taylor, M. P. (2017). *Economics*. Cengage Learning. (Chapter 2: Thinking like an Economist)
- Mackenzie, S. (2022). "Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial." *The British Journal of Criminology*, 62(6), 1537–1552. <https://doi.org/10.1093/bjc/azab118>
- Miglo, A. (2022). "Choice between IEO and ICO: Speed vs. Liquidity vs. Risk." *FinTech*, 1, 276–293. <https://doi.org/10.3390/fintech1030021>.
- Naganuma, K., Yoshino, M., Sato, H., Suzuki, T. (2017). "Auditable Zerocoin." Hitachi, Ltd. Research and Development Group, Kanagawa, Japan. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*: 10.1109/EuroSPW.2017.51.
- Han, J., Huang, S., Zhong, Z. (2024). "Trust in DeFi: An Empirical Study of the Decentralized Exchange." <https://doi.org/10.2139/ssrn.3896461>
- Hägele, S. (2024). "Centralized exchanges vs. decentralized exchanges in cryptocurrency markets: A systematic literature review." *Electronic Markets*, 34(33). <https://doi.org/10.1007/s12525-024-00714-2>
- Hendrickson, J. R., Luther, W. J. (2022). "Cash, crime, and cryptocurrencies." *The Quarterly Review of Economics and Finance*, 85, 200–207. Oxford University Press.
- Haffke, L., Fromberger, M. (2020). "ICO Market Report 2019/2020 – Performance Analysis of 2019's Initial Coin Offerings." *SSRN Electronic Journal*. 10.2139/ssrn.3770793.

- Hornuf, L., Kück, T., Schwienbacher, A. (2021). "Initial coin offerings, information disclosure, and fraud.". Max Planck Institute for Innovation and Competition, Munich, Germany; University of Bremen, Faculty of Business Studies and Economics. <https://doi.org/10.1007/s11187-021-00471-y>.
- Howell, S. T., Niessner, M., Yermack, D. (2019). Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales. *The Review of Financial Studies*, 33(9), 3925-3974. <https://doi.org/10.1093/rfs/hhz131>
- Houben, R., Snyers, A. (2020). Crypto-assets: Key developments, regulatory concerns and responses (PE 648.793). Briefing for the Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies.
- Jalan, A., Matkovskyy, R. (2023). "Systemic risks in the cryptocurrency market: Evidence from the FTX collapse." *Finance Research Letters*, 53, 103670. Elsevier.
- Karpenko, O. A., Blokhina, T. K., Chebukhanova, L. V. (2021). The Initial Coin Offering (ICO) Process: Regulation and Risks. *Journal of Risk and Financial Management*, 14(12), 599. <https://doi.org/10.3390/jrfm14120599>
- Kethineni, S., Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, 30(3), 325-344. <https://doi.org/10.1177/1057567719827051>
- Karimov, B., Wójcik, P. (2021). Identification of Scams in Initial Coin Offerings With Machine Learning. *Frontiers in Artificial Intelligence*, Volume 4 - 2021, Article 718450. <https://doi.org/10.3389/frai.2021.718450>
- Kreminskyi, O., Kuzmenko, O., Antoniuk, A., Smahlo, O. (2021) "International Cooperation in the Investigation of Economic Crimes Related to Cryptocurrency Circulation." University of the State Fiscal Service of Ukraine, Ukraine. Vinnytsia Institute of Trade and Economics, Kyiv National University of Trade and Economics, Ukraine. 10.25115/eea.v39i6.5247.
- Laucius, G. (2023). "Naujasis kriptoturto veiklos reglamentavimas Lietuvoje ir Europos Sąjungoje." *Teisė*, 128, 115–132. <https://doi.org/10.15388/Teise.2023.128>.
- Liebau, D., Schueffel, P. (2019). "Cryptocurrencies & Initial Coin Offerings: Are they Scams? - An Empirical Study." [https://doi.org/10.31585/jbba-2-1-\(5\)2019](https://doi.org/10.31585/jbba-2-1-(5)2019).
- Li, J., Luo, M., Wang, M., Wei, Z. (2022). *Cryptocurrency listings on cryptocurrency exchanges*. Donald G. Costello College of Business at George Mason University Research Paper. <http://dx.doi.org/10.2139/ssrn.4715718>

- Mikołajewicz-Woźniak, A., Scheibe, A. (2015). "Virtual currency schemes – the future of financial services." *Foresight*, 17(4), 365-377. <https://doi.org/10.1108/FS-04-2014-0021>
- Mcgee, R., Conlon, T. (2021). ICO Fraud and Regulation. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3770659>
- Makridis, C., Froewis, M., Sridhar, K., Böhme, R. (2021). The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. <http://dx.doi.org/10.2139/ssrn.3915140>
- Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11(1), 1. <https://doi.org/10.1186/s40163-021-00163-8>
- Tronnier, F., Hamm, P., Harborth, D. (2023). The Behavioral Biases of Cryptocurrency Retail Investors – Lessons from ICOs. In S. Publisher (Ed.), *Activist Retail Investors and the Future of Financial Markets* (pp. 115-135). Routledge International Studies in Money and Banking. <https://doi.org/10.4324/9781003351085-10>
- Teichmann, F. M. J., Falker, M. C. (2021) "Cryptocurrencies and financial crime: solutions from Liechtenstein." *Journal of Money Laundering Control* 24, no. 4: 775-788. 10.1108/JMLC-05-2020-0060.
- Wronka, C. (2023). "Financial crime in the decentralized finance ecosystem: new challenges for compliance." *Journal of Financial Crime*, 30(1), 97-113. <https://doi.org/10.1108/JFC-09-2021-0218>
- Yousaf, I., Goodell, J. W. (2023). "Reputational contagion and the fall of FTX: Examining the response of tokens to the delegitimization of FTT." *Finance Research Letters*, 54, 103704. Elsevier.
- Nakamoto S. (2008). Bitcoin: Peer-to-Peer Electronic Cash System. Prieiga per internetą: https://s3.amazonaws.com/academia.edu.documents/32413652/Bitcoin_P2P_electronic_cash_system.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1544018015&Signature=v5ZXWQc7MyVhkrfqWAQnDPQo5J0%3D&responsecontentdisposition=inline%3B%20filename%3DBitcoin_A_Peer-to_Peer_Electronic_Cash_S.pdf
- Xia, P., Wang, H., Luo, X., Wu, L., Zhou, Y., Bai, G., Xu, G., Huang, G., Liu, X. (2023) , "Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams." <https://doi.org/10.1109/eCrime51433.2020.9493255>.
- Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Luo, X., Zhang, C., Xiao, X., Xu, G. (2021). "Trade or Trick?: Detecting and Characterizing Scam Tokens on Uniswap

- Decentralized Exchange." *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, Volume 5, Issue 3, Article No.: 39, pp 1–26. <https://doi.org/10.1145/3491051>.
- Swartz L. (2022). "Theorizing the 2017 blockchain ICO bubble as a network scam" *New Media & Society*, Article No.: 39, pp 1–26. <https://doi.org/10.1177/14614448221099224>
- Samieifar, S., Baur, D. G. (January 2020). Read me if you can! An analysis of ICO white papers. *Finance Research Letters*, 38(2), Article 101427. <https://doi.org/10.1016/j.frl.2020.101427>
- Stunžinas, R. (2018). Kriptografinių valiutų srities terminai: reikšmės, raida ir variantai. *Terminology / Terminologija*, 25, 128–146. ISSN: 1392-267X.
- SATISGROUP. (2018). "Cryptoasset Market Coverage Initiation: Network Creation." Bloomberg. Pasiekama per: https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ
- Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., Luo, X., Xu, G. (2020). "Characterizing cryptocurrency exchange scams" *Computers & Security* <https://doi.org/10.1016/j.cose.2020.101993>
- Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Luo, X., Zhang, C., Xiao, X., Xu, G. (2021). Trade or trick?: Detecting and characterizing scam tokens on Uniswap decentralized exchange. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, <https://doi.org/10.1145/3491051>
- Rhue, L. (2018). Trust is All You Need: An Empirical Exploration of Initial Coin Offerings (ICOs) and ICO Reputation Scores. 10.2139/ssrn.3179723
- Šapkauskienė, A., Višinskaitė, I. (2020). Initial Coin Offerings (ICOs): Benefits, Risks and Success Measures. *Entrepreneurship and Sustainability Issues*, 7(3), [http://doi.org/10.9770/jesi.2020.7.3\(3\)](http://doi.org/10.9770/jesi.2020.7.3(3)). ISSN 2345-0282.
- Zetsche, D. A., Arner, D. W., Buckley, R. P. (2020). Decentralized Finance. *Journal of Financial Regulation*, 6, 172–203. <https://doi.org/10.1093/jfr/fjaa010>
- Zetsche, D. A., Buckley, R. P., Arner, D. W., Föhr, L. (2018). The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators (University of New South Wales Law Research Series, Law Working Paper Series No. 2017-011). University of Luxembourg; University of New South Wales.

FINANSINIŲ NUSIKALTIMŲ ICO PROJEKTUOSE TYRIMAS

EDAS KARAPETJANAS

Magistro darbas

FINANSAI IR BANKININKYSTĖ

Vilniaus universiteto Ekonomikos ir verslo administravimo fakultetas

Darbo vadovė - Prof. Dr. Alfreda Šapkauskienė

Vilnius, 2025

SANTRAUKA

66 puslapiai, 14 lentelės, 2 paveikslai, 69 šaltiniai.

Šio magistro darbo tikslas yra išnagrinėti, kaip ICO projektų populiarumas, rizikos balas ir keityklos tipas lemia finansinių nusikaltimų mastą, taip pat pateikti praktines rekomendacijas, siekiant sumažinti riziką šioje rinkoje. Tyrimo aktualumą pabrėžia spartus kriptovaliutų rinkos augimas ir ICO projektų gausa, kartu su nepakankama reguliavimo sistema, kuri sudaro sąlygas finansiniams nusikaltimams. Tokie projektai kaip „Onecoin“ ar „Squid Game Token“ iliustruoja riziką, susijusią su šia finansine inovacija, kuri investuotojams gali sukelti didelių nuostolių.

Darbas grindžiamas trijų pagrindinių kintamųjų – populiarumo, rizikos balo ir keityklos tipo – analize, remiantis mokslinės literatūros apžvalga ir empiriniu tyrimu. Literatūros analizėje išryškinta decentralizuotų ekosistemų reikšmė ir pagrindiniai finansinių nusikaltimų veiksniai ICO projektuose, remiantis tokiais autoriais kaip Adhami ir kt. (2018), Karpenko ir kt. (2021), bei Agarwal ir kt. (2023). Šioje dalyje taip pat aptarta, kaip decentralizuotos ir centralizuotos keityklos gali įtakoti projekto skaidrumą ir patikimumą. Empyrinis tyrimas, pagrįstas statistiniais metodais, buvo sukurtas siekiant nustatyti ryšį tarp kintamųjų ir projekto surinktos sumos, vertinant ją kaip finansinio nusikaltimo masto rodiklį.

Tyrimo rezultatai rodo, kad ICO projektai su aukštu rizikos balu dažnai pritraukia didesnes investicijas, tačiau taip pat yra linke į nusikalstamą veiklą. Tai susiję su tuo, jog aukšto rizikos balo projektai investuotojams atrodo patikimesni, ko pasekoje investuojama didesnė suma su siekiu gauti didelę grąžą. Remiantis gautais rezultatais, pateiktos rekomendacijos investuotojams ir įmonėms, siekiant mažinti riziką ir gerinti skaidrumą ICO rinkoje. Pabrėžiama, kad išsamus projekto analizės procesas, įskaitant rizikos balo

vertinimą, galėtų padėti sumažinti finansinių nusikaltimų tikimybę ir didinti rinkos patikimumą.

INVESTIGATION OF FINANCIAL CRIME IN ICO PROJECTS

EDAS KARAPETJANAS

Master thesis

FINANCE AND BANKING

Vilnius University, Faculty of Economics and Business Administration

Supervisor - Prof. Dr. Alfreda Šapkauskienė

Vilnius, 2025

SUMMARY

66 pages, 14 tables, 2 pictures, 69 references.

The primary aim of this master's thesis is to examine how ICO project popularity, risk score, and exchange type influence the extent of financial crimes, as well as to provide practical recommendations for mitigating risks in this domain. The relevance of the research is underscored by the rapid growth of the cryptocurrency market and the abundance of ICO projects, coupled with insufficient regulatory frameworks that create opportunities for financial crimes. High-profile cases such as "Onecoin" and "Squid Game Token" exemplify the risks associated with these financial innovations, often resulting in significant losses for investors.

The thesis focuses on analyzing three key variables—popularity, risk score, and exchange type through a comprehensive review of scientific literature and an empirical study. The literature review highlights the significance of decentralized ecosystems and the main factors influencing financial crimes in ICO projects, drawing on works by Adhami et al. (2018), Karpenko et al. (2021), and Agarwal et al. (2023). This section also discusses how decentralized and centralized exchanges affect the transparency and credibility of projects. The empirical study, grounded in statistical methods, was designed to identify the relationship between these variables and the funds raised by projects, treating this as an indicator of the scale of financial crime.

The research findings indicate that ICO projects with high risk scores often attract larger investments but are also more prone to criminal activities. This can be attributed to the perception that high-risk score projects appear more reliable to investors, leading to larger investment amounts in the pursuit of substantial returns. Based on the results, recommendations have been provided for investors and companies to mitigate risks and enhance transparency in

the ICO market. It is emphasized that a comprehensive project analysis process, including the evaluation of risk scores, could help reduce the likelihood of financial crimes and increase market reliability.

PRIEDAI

1 priedas.

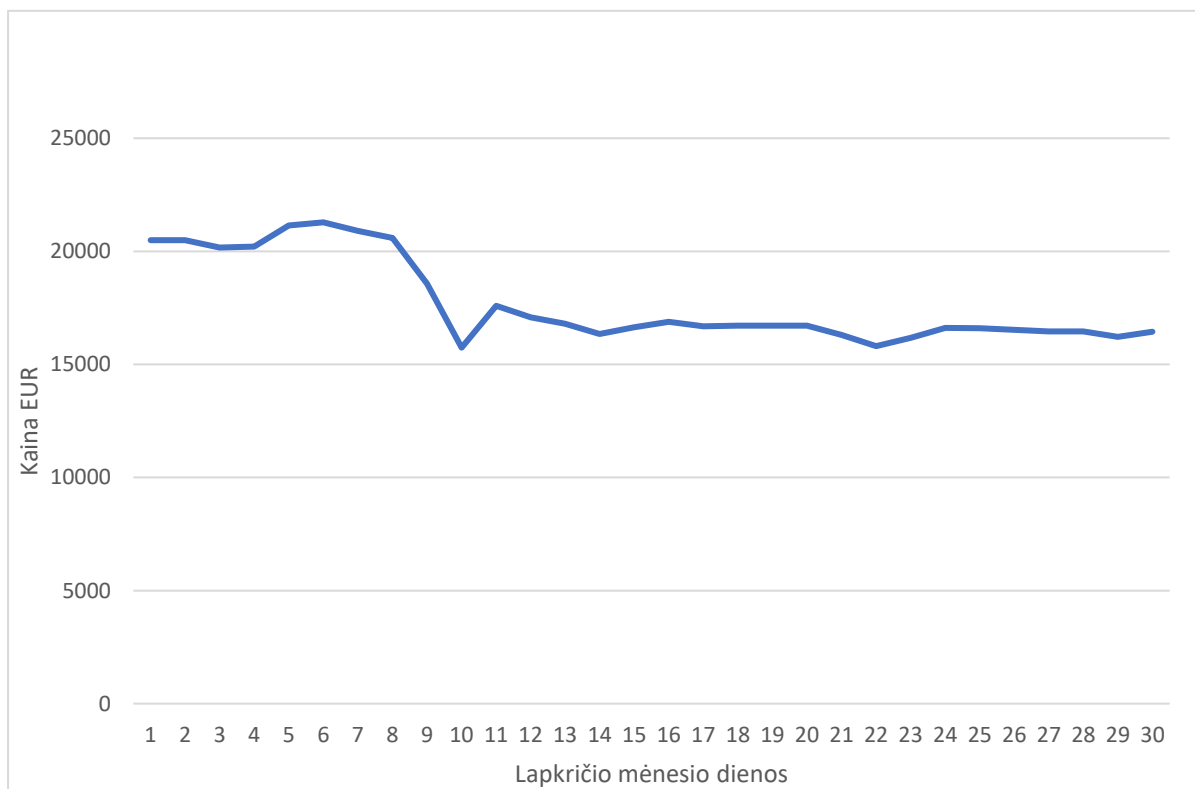
Kriptovaliutų keityklų skaičius pasaulyje

Keityklos tipas	Veikiančių platformų skaičius	Bendras egzistavusių platformų skaičius
Centralizuota	925	1,043
Decentralizuota	567	594

Šaltiniai: Lentelė sudaryta autoriaus remiantis duomenų bazės „Coinweb“ duomenimis.

2 priedas.

Bitcoin kainos svyravimai 2022 lapkričio mėnesį



Šaltiniai: Skaiciavimai atlikti autoriaus remiantis duomenų bazės „Statista“ duomenimis

3 priedas.

Į rinką pateiktų pirminių monetų siūlymų kiekis ir kapitalizaciją 2016 – 2022 metais

Metai	Išleista projektų	Surinkta lėšų
2016	29	\$90 milijonai
2017	875	\$6 bilijonai
2018	1,253	\$7.5 bilijonai
2019	109	\$370 milijonai
2020	14	\$55.6 milijonai
2021	320	\$378 milijonai
2022	217	\$117 milijonai

Šaltiniai: Skaičiavimai atlikti autoriaus remiantis duomenų bazės „Statista“ duomenimis

4 priedas.

Squid Game (SQUID) kriptovaliutos kaina kūrėjams nusisavinant lėšas laikotarpiu (10/27/2021-11/03/2021)



Šaltiniai: Skaičiavimai atlikti autoriaus remiantis duomenų bazės „Coinmarketcap“ duomenimis

Naudojamos formulės

1.	Tiesinės koreliacijos koeficientas (funkcija Correl)	
	$r = \frac{\overline{x_1 y_i} - \overline{x_1} \times \overline{y_i}}{\sigma_{x_1} \times \sigma_{y_i}}$	Koreliacijos koeficientas parodo dviejų kintamųjų ryšio stiprumą ir kryptį. Jis svyruoja nuo -1 iki 1, kai neigiamos reikšmės rodo atvirkštinį ryšį (kai vienas kintamasis didėja, kitas mažėja), o teigiamos reikšmės rodo tiesioginį ryšį.
2.	Regresijos koeficientas (funkcija SLOPE)	
	$b = \frac{r \cdot \hat{\sigma}_y}{\hat{\sigma}_x}$	Šis koeficientas rodo, kokio dydžio poveikį priklausomam kintamajam turės nepriklausomo kintamojo pokytis vienu vienetu, matuojamas priklausomo kintamojo vienetais.
3.	Determinacijos koeficientas (funkcija RSQ)	
	$R^2 = \frac{b_1 \sigma_{01} + b_2 \sigma_{02}}{\sigma_{00}}$	Determinacijos koeficientas yra dviejų kintamųjų tiesinio ryšio stiprumo matas. Jis parodo, kokią dalį rezultato kintamojo kintamumo galima paaiškinti veiksnio kintamojo kintamumu. Jis apskaičiuojamas kaip koreliacijos koeficiento kvadratas ir išreiškiamas procentais. Pavyzdžiui, jei determinacijos koeficientas yra 0,64, tai reiškia, kad 64 % rezultato kintamojo kintamumo galima paaiškinti veiksnio kintamojo kintamumu. Determinacijos koeficientas yra svarbus regresijos modelio prognozavimo galios matas.
4.	Statistinis patikimumas	
	$t = \left r \sqrt{\frac{n-2}{1-r^2}} \right $	Siekiant nustatyti ryšių stiprumą, vertinamas jų reikšmingumas. Koreliacijos koeficiento reikšmingumas vertinamas naudojant imties statistiką, vadinamą t. Apskaičiuota t reikšmė lyginama su kritine tkr reikšme, kad būtų galima priimti sprendimą dėl reikšmingumo.

Sudaryta autoriaus, remiantis: (Gujarati, Damodar N. (2004) *Basic Econometrics*. 4th ed. New York: McGraw-Hill)

Autorių tyrimų metodai ir rezultatai apie didžiausius pirminiuose monetų siūlymuose atliktus finansinius nusikaltimus

Autorius	Tyrimo metodai	Tyrimo rezultatai
Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., Johnson, S. D, 2022	Literatūros analizė	Tyrimai rodo, kad kriptovaliutų sukčiavimo tyrimų kiekis auga, tačiau literatūra vis dar ankstyvojoje stadijoje.
Karpenko, O. A., Blokhina, T. K., & Chebukhanova, L. V., 2020	Literatūros analizė	ICO rinka sparčiai augo 2016–2019 m. Išskirtos rizikos: finansinės, techninės, analitinės.
Agarwal, S., Atondo-Siu, G., Ordekian, M., Hutchin, A., Mariconti, E., & Vasek, M., 2021	Kiekybinė analizė, empirinis tyrimas	Rugpull dažnai susiję su Ethereum kursų svyravimais, reglamento trūkumas skatina sukčiavimų plitimą.
Adhami, S., Giudici, G., Martinazzi, S., 2018	Empirinė kiekybinė analizė, regresinė analizė, logit modelis	Šaltinio kodo prieinamumas leidžia potencialiems investuotojams patikrinti projekto patikimumą ir techninę pagrindą, todėl tai padeda ICO įgyti daugiau pasitikėjimo ir populiarumo
Ante, L., Sandner, P., Fiedler, I., 2018	Aprašomoji statistika, Regresijos analizė, Koreliacijos analizė	ICO projektų sėkmę lemiantys veiksniai yra, projekto populiarumas, socialinės medijos aktyvumas ir rizikos balas. Tyrėjai taip pat pastebėjo, kad investuotojai reaguoja į šiuos signalus, norėdami pasirinkti patikimus projektus.
Boreiko, D., & Vidusso, G. (2018).	Aprašomoji statistika, Regresijos analizė, Koreliacijos analizė	Nors ir egzistuoja rizika, susijusi su ICO vertinimu, didelis įtraukimo dažnis į vertinimo svetaines ir jų pateikti vertinimai dažnai būna naudingas indikatorius, kuris atspindi projekto tikrąją būklę ir padeda atskirti potencialiai sėkmingus projektus nuo sukčiavimo ar nesėkmingų kampanijų.
Liebau, D., & Schueffel, P., 2019	Lexis Nexis duomenų bazės analizė	10 % ICO projektų baigėsi finansiniais nusikaltimais.

Hornuf, L., Kück, T., & Schwienbacher, A., 2021	Aprašomoji statistika, regresinė analizė	ICO panašūs į kapitalo sutelktinį finansavimą reguliavimas galėtų sumažinti sukčiavimų riziką.
Ante, L., & Meyer, A., 2021	Laiko eilutės regresija, tikėtinos gražos modeliai	Keityklos dydis ir likvidumas daro stiprią įtaką ICO sėkmei; mažesnės keityklos dažniau susiduria su sukčiavimais.
Fu, Z., Gu, W., Fang, Z., Yan, J., Liu, X. F., 2022	Mann-Whitney U, Kolmogorov-Smirnov testai	Nerasta skirtumų tarp sėkmingų ir piramidinių ICO žetonų modelių; reguliavimas būtinas viešųjų investuotojų apsaugai.
Zheng, Y., & Wang, M., 2022	XGBoost algoritmas, SMOTE metodas	Dirbtinio intelekto modelis numato 80 % tikimybę, kad ICO taps finansiniu nusikaltimu.
Lars Hornuf ir kt. (2021)	Aprašomoji statistika, Regresinė analizė, P reikšmių ir hipotezių testavimas	ICO panašūs į akcijų ir kapitalo atlygio pagrįstą sutelktinį finansavimą, o informacijos atskleidimas ir reguliavimas gali sumažinti sukčiavimo riziką.

Šaltiniai: Lentelė sukurta autoriaus remiantis lentelėje pateiktų autorių tyrimais.

7 priedas.

Pagrindinių finansinių nusikaltimų kriptovaliutų keityklose (2011-2023m.) statistika.

Keityklos įsteigimas	Pažeidimas	Keityklos pavadinimas	USD	Veiksmas	Pažeidimas	Nusikaltimo metodas
2010-04	2011-08	MyBitcoin	102,500	Įsilaužimas	Piktnaudžiavimas funkcionalumu	programavimo klaida
2011-09	2012-03	Bitcoinica	213,415	Įsilaužimas	Naudojimasis pažeidžiamumu	Linode klaida
2011-09	2012-05	Bitcoinica	96,444	Įsilaužimas	Piktnaudžiavimas funkcionalumu	Rackspace PW
2011-04	2012-05	BitMarket.eu	103,896	Įsilaužimas	Pavogtų kreditų naudojimas	Įsilaužimas į SSH paskyrą
2012-02	2012-09	Bitfloor	298,666	Įsilaužimas	Pavogtų kreditų naudojimas	neužšifruota atsarginė piniginių kopija
2011-08	2013-03	BitInstant	92,907	Socialinis	Išsireikalavimas	DNS užgrobimas.
2011-01	2013-03	Mercado Bitcoin	372,000	Įsilaužimas	Piktnaudžiavimas funkcionalumu	užgrobta kupono funkcionalumas
2010-12	2013-04	Bitcoin Central	-	Įsilaužimas	Piktnaudžiavimas funkcionalumu	paskyros perėmimas, OVH pažeidimas

2011-10	2013-05	Vircorex	187,275	Įsilaužimas	Pavogtų kreditų naudojimas	PW atstatymas, debesų kompiuterijos prieglobos socialinė
2011-07	2013-11	Bitcash.cz	584,765	Įsilaužimas	Nežinomas	pažeista žiniatinklio sąsaja
2010-07	2014-02	Mt. Gox	487,815,000	-	-	įsitraukimas iš vidaus
2014-01	2014-03	Poloniex	43,136	Įsilaužimas	Piktnaudžiavimas funkcijomis	-
2013-03	2014-07	Cryptsy	5,895,000	Įsilaužimas	Antrinių durų arba C2 naudojimas	užpakalinės durys priklausomybės sistemoje
2011-01	2015-01	Bitstamp	4,122,221	Kenkėjiška programinė įranga	Parsisiuntimo programa	sudėtinga kenkėjiškos programinės įrangos ataka
2013-06	2015-01	796 Exchange	218,500	Įsilaužimas	Nežinomas	pažeista "tam tikra silpnoji vieta"
2013-01	2015-02	BTER	1,821,897	Įsilaužimas	Nežinomas	piniginės pažeidimas
2011-06	2015-02	Cavirtex	-	Įsilaužimas	Pavogtų kreditų naudojimas	atskleistos PW hash, 2FA paslaptys
2014-02	2015-03	AllCrypt	9,764	Įsilaužimas	Brutali jėga	brutaliai išviliotas techninio personalo el. paštas
2014-01	2015-03	Cryptoine	1,465	Kenkėjiška programinė įranga	Naudojimasis pažeidžiamumu	sudėtinga kenkėjiškos programinės įrangos ataka
2013-07	2016-04	BitQuick	-	Įsilaužimas	SQLi	įkėlimo funkcijos SQL injekcija
2014-07	2016-04	ShapeShift.io	141,278	Įsilaužimas	Pavogtų kreditų naudojimas	viešai neatskleistos informacijos įtraukimas
2013-07	2016-05	Gatecoin	132,225	Įsilaužimas	Nežinomas	multisig šaltoji pinigine
2012-01	2016-11	Bitcurex	1,707,750	Įsilaužimas	Nežinomas	API pasirašymo rakto išnaudojimas
2013-06	2018-04	Coinsecure	4,049,354	Piktnaudžiamas	Piktnaudžiavimas privilegijomis	įsilaužėlis, atskleista šaltoji saugykla
2014-06	2018-09	Zaif	39,585,603	Įsilaužimas	Nežinomas	Įsilaužta į 3 karštąsias pinigines
2018-05	2018-10	Maplechange	50,927	Kenkėjiška programinė įranga	Naudojimasis pažeidžiamumu	lenktynių sąlyga, išėjimo apgaulė
2013-07	2018-11	Gate.io	-	Kenkėjiška programinė įranga	Naudojimasis pažeidžiamumu	tiekimo grandinės ataka
2017-11	2019-03	DragonEx	553,811	Įsilaužimas	Nežinomas	-
2017-07	2019-05	Binance	59,908,100	Įsilaužimas	Nežinomas	API raktai ir 2FA paslaptys
2016-01	2019-07	BitPoint	12,350,450	Įsilaužimas	Nežinomas	-
2016-02	2020-02	Altsbit	70,000	Įsilaužimas	Naudojimasis pažeidžiamumu	Gauta prieiga prie karštosios pinigines
2019-02	2020-04	Lendf.me	24,500,000	Įsilaužimas	Naudojimasis pažeidžiamumu	Klaidos ir pakartotinio centravimo ataka
2016-11	2020-04	Uniswap	500,000	Įsilaužimas	Naudojimasis pažeidžiamumu	Klaidos ir pakartotinio centravimo ataka

2017-02	2020-06	Balancer	500,000	Išsilaužimas	Naudojimasis pažeidžiamumu	Protokolo pažeidžiamumas
2012-01	2020-11	Cashaa	3,100,000	Išsilaužimas	Parsisiuntimo programa	Kenkėjiška programinė įranga
2013-01	2020-09	KuCoin	275,000,000	Išsilaužimas	Nepakankama apsauga	Duomenų nutekėjimas
2013-06	2020-12	BTC Markets	270,000	Išsilaužimas	Klaida	Vidaus personalo klaida ir (arba) klaida
2012-01	2020-12	EXMO	4,000,000	Išsilaužimas	Naudojimasis pažeidžiamumu	Gauta prieiga prie karštosios piniginės
2018-05	2021-08	Hotbit	-	Išsilaužimas	Naudojimasis pažeidžiamumu	Gauta prieiga prie karštosios piniginės
2013-01	2021-12	Liquid	97,000,000	Išsilaužimas	Naudojimasis pažeidžiamumu	Gauta prieiga prie karštosios piniginės
2014-06	2022-01	BitMart	150,000,000	Išsilaužimas	Naudojimasis pažeidžiamumu	Gauta prieiga prie karštosios piniginės
2016-11	2022-02	AscendEX	80,000,000	Išsilaužimas	Naudojimasis pažeidžiamumu	Gauta prieiga prie karštosios piniginės
2017-07	2022-03	Crypto.com	34,000,000	Išsilaužimas	Nežinomas	Nežinomas
2019-02	2022-11	FTX	600,000,000	Išsilaužimas	Piktnaudžiavimas privilegijomis	Neautorizuotos operacijos
2018-05	2023-04	GDAC	13,000,000	Išsilaužimas	Naudojimasis pažeidžiamumu	Gauta prieiga prie karštosios piniginės

Šaltiniai: Lentelė sukurta autoriaus remiantis „hedgewithcrypto“ ir „Selfkey“ duomenimis.

Pagrindinių kriptovaliutų keityklų (2024m.) statistika.

Keityklos pavadinimas	Tipas	Rinkos kapitalizacija	Poros	Rinkos	Rinkos dalis	Šalis	Regionas	Veikimo pradžia	Patikimumo balas
Binance	Centralized	\$36.27B	2672	555	27%	KY Cayman Islands	Americas	07/14/2017	10
Upbit	Centralized	\$13.56B	661	379	8.20%	KR South Korea	Asia	10/31/2017	7
Bybit	Centralized	\$7.55B	686	563	5.60%	VG Virgin Islands (British)	Americas	03/17/2022	10
Crypto.com	Centralized	\$7.06B	909	415	5.30%	MT Malta	Europe	12/02/2021	9
Coinbase	Centralized	\$6.96B	606	316	5.10%	US United States	Americas	12/01/2014	10
OKX	Centralized	\$6.56B	1505	585	4.90%	SC Seychelles	Africa	11/27/2017	10
XT.com	Centralized	\$5.27B	1256	1111	3.90%	SC Seychelles	Africa	04/10/2021	8
Gate.io	Centralized	\$4.85B	3198	2043	3.60%	KY Cayman Islands	Americas	09/30/2017	9
MEXC Global	Centralized	\$4.80B	2490	2352	3.50%	SC Seychelles	Africa	10/01/2022	9
Bittrue	Centralized	\$4.71B	1008	756	3.50%	SC Seychelles	Africa	02/22/2024	6
DigiFinex	Centralized	\$4.61B	832	678	3.40%	SC Seychelles	Africa	08/13/2018	8
Bitget	Centralized	\$4.20B	931	830	3.10%	SC Seychelles	Africa	02/15/2024	8
P2B	Centralized	\$3.39B	216	134	2.50%	LT Lithuania	Europe	12/13/2023	8
Bithumb	Centralized	\$3.34B	478	399	2.20%	KR South Korea	Asia	08/26/2017	7
HTX	Centralized	\$2.75B	1737	1015	2%	SC Seychelles	Africa	03/19/2014	9
LBANK	Centralized	\$2.39B	1133	1044	1.70%	VG Virgin Islands (British)	Americas	01/11/2018	7
KuCoin	Centralized	\$1.95B	1932	1206	1.40%	SC Seychelles	Africa	11/18/2017	10
Kraken	Centralized	\$1.83B	870	328	1.30%	US United States	Americas	10/06/2013	10
Uniswap V3	Decentralized	\$1.54B	9739	1016	1%	--	Decentralized	05/04/2021	-
BigONE	Centralized	\$1.15B	300	236	0.80%	SC Seychelles	Africa	12/25/2017	8
BitMart	Centralized	\$1.13B	1727	1556	0.80%	KY Cayman Islands	Americas	05/17/2018	8
Bullish	Centralized	\$1.01B	54	35	0.80%	GI Gibraltar	Europe	04/06/2022	6
LATOKEN	Centralized	\$874M	1237	955	0.70%	KY Cayman Islands	Americas	02/08/2018	7

Raydium	Decentralized	\$860M	2757	98	0.40%	--	Decentralized	03/21/2021	-
PancakeSwap V3	Decentralized	\$679M	2789	395	0.50%	--	Decentralized	04/01/2023	-
Aerodrome	Decentralized	\$678M	819	76	0.50%	--	Decentralized	08/29/2023	-
CoinEx	Centralized	\$672M	1802	1207	0.40%	ws Samoa	Oceania	04/10/2018	7
Bitfinex8	Centralized	\$668M	891	360	0.50%	vg Virgin Islands	Americas	04/01/2013	8
BingX	Centralized	\$605M	880	870	0.40%	vg Virgin Islands	Americas	02/22/2024	9
Bilaxy	Centralized	\$586M	934	884	0.40%	sc Seychelles	Africa	12/09/2019	-
Uniswap V2	Decentralized	\$171M	10633	972	0.10%	--	Decentralized	05/05/2020	-
Curve V1	Decentralized	\$170M	375	78	0.10%	--	Decentralized	01/23/2020	-
YoBit	Centralized	\$153M	1091	284	0%	RU Russia	Europe	03/09/2016	-
bitFlyerFX	Centralized	\$121M	1	1	0.10%	JP Japan	Asia	02/21/2024	8
Gemini	Centralized	\$111M	163	126	0.10%	us United States	Americas	10/08/2015	8
bitFlyer	Centralized	\$107M	12	7	0.10%	JP Japan	Asia	07/22/2015	7
Balancer V2	Decentralized	\$81.96M	877	147	0.10%	--	Decentralized	04/22/2021	
PancakeSwap	Decentralized	\$80.24M	17340	2547	0.10%	--	Decentralized	09/19/2020	
Phoenix	Decentralized	\$76.74M	59	8	0%	--	Decentralized	02/24/2023	
Coincheck	Centralized	\$72.35M	7	7	0.10%	JP Japan	Asia	03/20/2019	6
Korbit	Centralized	\$67.41M	166	165	0%	KR South Korea	Asia	09/05/2019	7
Bitso	Centralized	\$65.22M	108	57	0%	GI Gibraltar	Europe	05/18/2017	8
bitFlyer EU	Centralized	\$62.17M	4	2	0%	LU Luxembourg	Europe	08/29/2022	7
bitFlyer US	Centralized	\$61.99M	4	2	0%	us United States	Americas	10/07/2019	7
Dcoin	Centralized	\$60.66M	148	136	0%	CH Switzerland	Europe	10/30/2018	2
Exmo	Centralized	\$58.59M	234	91	0%	PL Poland	Europe	02/21/2016	7
Binance US	Centralized	\$39.66M	381	175	0%	us United States	Americas	09/23/2019	9
Meteora	Decentralized	\$37.91M	2975	420	0%	--	Decentralized	08/04/2022	-
itBit	Centralized	\$28.23M	14	10	0%	us United States	Americas	02/14/2015	7
CEX.IO	Centralized	\$22.88M	616	222	0%	GB United Kingdom	Europe	02/09/2015	7
Raydium (stable)	Decentralized	\$22.77M	26	3	0%	--	Decentralized	01/19/2022	-
Sushiswap	Decentralized	\$21.91M	3065	523	0%	--	Decentralized	09/04/2020	-

Deribit	Centralized	\$15.20M	11	7	0%	PA Panama	Americas	04/24/2023	7
Mercado Bitcoin	Centralized	\$14.88M	199	193	0.0 ₂ 69%	BR Brazil	Americas	02/22/2024	6
Baseswap	Decentralized	\$13.01M	209	17	0.0 ₂ 95%	--	Decentralized	08/01/2023	-
Curve	Decentralized	\$11.65M	538	112	0.0 ₂ 61%	--	Decentralized	10/30/2020	-
TimeX	Centralized	\$7.79M	19	12	0.0 ₂ 31%	AU Australia	Oceania	02/18/2020	-
GOPAX	Centralized	\$6.07M	209	119	0.0 ₂ 17%	KR South Korea	Asia	01/10/2018	3
Coinjar	Centralized	\$5.97M	252	73	0.0 ₂ 21%	GB United Kingdom	Europe	05/28/2019	5
Saber	Decentralized	\$5.17M	72	22	0.0 ₂ 38%	--	Decentralized	05/28/2021	-
BitTrade	Centralized	\$5.15M	76	44	0.0 ₂ 36%	JP Japan	Asia	05/21/2019	6
Maverick Protocol	Decentralized	\$3.69M	148	36	0.0 ₂ 27%	--	Decentralized	05/08/2023	-
Luno	Centralized	\$3.33M	37	24	0.0 ₂ 22%	SG Singapore	Asia	11/14/2017	-
Integral	Decentralized	\$3.24M	14	10	0.0 ₂ 19%	--	Decentralized	03/21/2022	-
Zaif	Centralized	\$2.72M	27	15	0.0 ₂ 14%	JP Japan	Asia	05/30/2016	3
Ascendex	Centralized	\$2.62M	491	451	0.0 ₂ 16%	SG Singapore	Asia	02/22/2024	5
ShibaSwap	Decentralized	\$2.60M	332	69	0.0 ₂ 11%	--	Decentralized	07/06/2021	-
Currency.com	Centralized	\$2.43M	174	74	0.0 ₂ 13%	US United States	Americas	03/02/2020	3
Independent Reserve	Centralized	\$2.15M	36	36	0.0 ₂ 12%	AU Australia	Oceania	04/13/2018	4
Orca	Decentralized	\$2.00M	123	28	0.0 ₂ 11%	--	Decentralized	06/11/2021	-
Solidly	Decentralized	\$1.92M	58	8	0.0 ₂ 11%	--	Decentralized	09/02/2023	-
AlienBase	Decentralized	\$1.92M	80	13	0.0 ₂ 13%	--	Decentralized	08/08/2023	-
Invariant	Decentralized	\$1.84M	123	21	0.0 ₂ 12%	PL Poland	Europe	03/22/2022	-
VALR	Centralized	\$1.48M	30	21	0.0 ₃ 92%	ZA South Africa	Africa	02/27/2022	1
One Trading	Centralized	\$1.47M	34	23	0.0 ₃ 60%	IT Italy	Europe	02/17/2020	5
Btcbox	Centralized	\$1.44M	7	7	0.0 ₃ 82%	JP Japan	Asia	05/30/2016	6
Stepn	Decentralized	\$810.49K	3	1	0.0 ₃ 24%	--	Decentralized	06/09/2022	-
Apeswap	Decentralized	\$741.23K	1054	339	0.0 ₃ 45%	--	Decentralized	02/14/2021	-
Fraxswap	Decentralized	\$657.07K	15	3	0.0 ₃ 22%	--	Decentralized	05/16/2022	-
CoinMate	Centralized	\$492.67K	18	10	0.0 ₃ 30%	CZ Czech Republic	Europe	10/11/2018	-
Bancor V3	Decentralized	\$393.24K	1668	69	0.0 ₄ 15%	--	Decentralized	04/23/2022	-

Indodax	Centralized	\$388.92K	26	25	0.0484%	ID Indonesia	Asia	02/04/2020	3
Bancor	Decentralized	\$370.88K	226	82	0.0471%	--	Decentralized	01/09/2020	-
Balancer V1	Decentralized	\$317.78K	1782	266	0.0462%	--	Decentralized	03/13/2020	-
Mercurial	Decentralized	\$288.67K	33	8	0.0321%	--	Decentralized	06/24/2021	-
Clipper	Decentralized	\$287.22K	10	4	0.0321%	--	Decentralized	04/15/2022	-
DefiSwap	Decentralized	\$276.13K	90	24	0.0447%	--	Decentralized	09/10/2020	-
BitMEX	Centralized	\$211.91K	46	30	0.0315%	sc Seychelles	Africa	10/12/2017	7
DOOAR	Decentralized	\$144.22K	6	4	0.0413%	--	Decentralized	07/07/2022	-
Rocketswap	Decentralized	\$141.44K	46	8	0.0458%	--	Decentralized	07/29/2023	-
BTCMarkets	Centralized	\$133.67K	8	6	0.0724%	AU Australia	Oceania	07/31/2014	4
Nomiswap	Decentralized	\$96,370	97	21	0.0440%	--	Decentralized	12/17/2022	-
Orca V1	Decentralized	\$83,074	17	15	0.0456%	--	Decentralized	02/14/2021	-
Orion	Decentralized	\$32,589	23	4	0.0416%	--	Decentralized	06/14/2021	-
Convergence Finance	Decentralized	\$14,459	3	2	0.0556%	--	Decentralized	05/17/2021	-
SwapBased	Decentralized	\$8,069	62	8	0.0534%	--	Decentralized	08/01/2023	-
Linkswap	Decentralized	\$4,430	41	21	0.0527%	--	Decentralized	12/02/2020	-
Okcoin	Centralized	\$3,560	147	88	0.0526%	us United States	Americas	03/19/2014	4
SakeSwap	Decentralized	\$3,308	44	17	0.0616%	--	Decentralized	09/26/2020	-
ElysiumSwap	Decentralized	\$2,660	3	3	0.0623%	--	Decentralized	01/03/2022	-
WhiteSwap	Decentralized	\$1,691	13	6	0.0630%	EE Estonia	Europe	11/10/2020	5
Equalizer Finance	Decentralized	\$1,245	20	11	0.0611%	--	Decentralized	09/28/2020	-
LuaSwap	Decentralized	\$1,005	18	11	0%	--	Decentralized	10/29/2020	-
NFTX	Decentralized	\$303.80	2	2	0%	--	Decentralized	08/07/2024	-
KyberSwap	Decentralized	\$276.52	123	34	0.0720%	--	Decentralized	06/09/2022	-
SumSwap	Decentralized	\$270.53	12	4	0%	--	Decentralized	06/02/2021	-
Plasma Finance	Decentralized	-	19	13	0%	--	Decentralized	01/31/2021	-
WAGMI	Decentralized	\$8.79	12	5	0%	--	Decentralized	08/07/2024	-
SaitaSwap	Decentralized	-	15	4	0%	--	Decentralized	07/29/2022	-
CitySwap	Decentralized	-	10	7	0%	--	Decentralized	11/22/2020	-

Šaltiniai: Lentelė sukurta autoriaus remiantis „Messari“ ir „Coingecko“ duomenimis.