

VILNIAUS UNIVERSITETAS

EKONOMIKOS IR VERSLO ADMINISTRAVIMO FAKULTETAS

FINANSAI IR BANKININKYSTĖ

Beatričė Panavienė

MAGISTRO BAIGIAMASIS DARBAS

FINANSINIŲ NUSIKALTIMŲ DECENTRALIZUOTOJE FINANSŲ EKOSISTEMOJE VERTINIMAS	ASSESING FINANCIAL CRIMES IN DECENTRALIZED FINANCIAL EKOSYSTEM
---	---

Darbo vadovė prof. dr. Alfreda Šapkauskienė

Vilnius, 2025

TURINYS

LENTELĖS	3
PAVEIKSLAI	4
ĮVADAS	5
1. FINANSINIŲ NUSIKALTIMŲ DECENTRALIZUOTOJE FINANSŲ EKOSISTESMOJE TEORINIAI ASPEKTAI	9
1.1 Decentralizuotų finansų samprata	9
1.2 Virtualių valiutų rinkų nepastovumo ypatybės	16
1.3 Finansinių nusikaltimų samprata ir tipologija decentralizuotų finansų kontekste	18
1.4 „Rug pull“ decentralizuotų finansų nusikaltimo savybės ir atpažinimas	25
2. „RUG PULL“ FINANSINIO NUSIKALTIMO VERTINIMO METODOLOGIJA	29
2.1 Eterio kainų ir finansinių nusikaltimų lyginamoji analizė	30
2.2 Eterio kainų ir pervedimų į žetonus, susijusius su „Rug pull“, atvejo analizė bei modelio kūrimas	31
3. „RUG PULL“ FINANSINIO NUSIKALTIMO VERTINIMAS	37
3.1 Eterio kainų ir finansinių nusikaltimų palyginimas	37
3.2 „Rug pull“. Konkretaus virtualaus žetono nusikaltimo atvejis ir jo palyginimas su Eterio virtualios valiutos verte	39
3.3 Modelis, skirtas investuotojams įsitikinti, kad žetonas nėra susijęs su „Rug pull“ finansiniu nusikaltimu	56
IŠVADOS IR PASIŪLYMAI	61
LITERATŪRA IR ŠALTINIAI	64
SANTRAUKA	76
SUMMARY	78
PRIEDAI	80

LENTELĖS

1 lentelė. Blokų antraštės komponentai	10
2 lentelė. Tradicinių ir decentralizuotų finansų skirtumai	15
3 lentelė. Antruoju tyrimo analizuojamu laikotarpiu 2020-11-03 – 2021-11-08 nagrinėjami žetonai	41
4 lentelė. Žetono T.testo reikšmė ir kritinė t-reikšmė analizuojamu 2020-11-03 – 2021-11-08 laikotarpiu	43
5 lentelė. Trečiuoju tyrimo analizuojamu laikotarpiu 2021-11-09 – 2022-06-18 nagrinėjami žetonai	45
6 lentelė. Žetono T.testo reikšmė ir kritinė t-reikšmė analizuojamu 2021-11-09 – 2022-06-18 laikotarpiu	47
7 lentelė. Ketvirtuoju tyrimo analizuojamu laikotarpiu 2022-06-19 – 2023-09-24 nagrinėjami žetonai	49
8 lentelė. Žetonų, kurių dabartinis likvidumas mažiau nei 0,01 Eterio, likvidumo analizė.....	50
9 lentelė. Penktuoju tyrimo analizuojamu laikotarpiu 2023-09-25 – 2024-12-02 nagrinėjami žetonai	52

PAVEIKSLAI

1 paveikslas. Grafinis blokų grandinės atvaizdavimas	11
2 paveikslas. „Rug pull“ finansinio nusikaltimo tipologija	21
3 paveikslas. Tyrimų išdėstymo pagal darbo eigą seka	29
4 paveikslas. Statistinės hipotezės patikrinimo etapai	31
5 paveikslas. Virtualių valiutų kainų kitimas nuo 2014 m. iki 2024 m. gruodžio 2 d.	3737
6 paveikslas. Gauta neteisėtais adresais bendra virtualios valiutos vertė 2018-2023 metų laikotarpiu	38
7 paveikslas. Pervedimų į „Rug pull“ nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2020-01-01 – 2020-11-02	40
8 paveikslas. Pervedimų į „Rug pull“ nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2020-11-03 – 2021-11-08	44
9 paveikslas. Pervedimų į „Rug pull“ nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2021-11-09 – 2022-06-18	48
10 paveikslas. Pervedimų į „Rug pull“ nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2022-06-19 – 2023-09-24	51
11 paveikslas. Pervedimų į „Rug pull“ nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2023-09-25 – 2024-12-02	54
12 paveikslas. Apsisaugojimo modelis nuo su „Rug pull“ finansiniu nusikaltimu susijusio žetono	57

IVADAS

Darbo temos aktualumas. Beveik kiekvienas asmuo šiame pasaulyje nori ir norėtų turėti daugiau finansinio turto. Tam, kad finansiniai pajėgumai leistų išpildyti savo svajones, žmonės atranda įvairių būdų užsidirbti pinigų ar pakelti savo turimo turto vertę. Dalis žmonių renkasi dirbti per du darbus, dalis žmonių renkasi nuosavo turto nuomos galimybes, o dalis investuoja į finansines priemones. Visose išvardintose srityse yra galimybė ne tik uždirbti pinigų tačiau ir juos prarasti. Ne išimtis ir investavimas. Nuo 2014 metų išpopuliarėjo nauja galimybė – investuoti į decentralizuotų finansų rinką Anna Fleck (2022), Consensus (2019), Gandal ir kt. (2014). Tai yra rinka, kuri veikia 7 dienas per savaitę, 24 valandas per parą, rinka, kurioje investuojant yra galimybė greitai praturtėti, bet taip pat ir greitai prarasti pinigus, dėl didelių kainų pokyčių į investuojamus vienetus – virtualią valiutą. Virtuali valiuta – skaitmeninė finansinė priemonė, kurios disponuojamos blokų grandinėse bei kurių apsigėrimui nėra reikalingi tarpininkai, tokie kaip finansinės institucijos (Tierno, 2023). Tačiau kaip ir tradiciniai finansai, taip ir decentralizuoti finansai susiduria su sukčiavimo ir apgaulės rizikomis. Decentralizuotuose finansuose, kaip ir visur kitur, kartu su išpopuliarėjimu padaugėjo ir sukčiavimo, apgavystės bei nusikaltimų apraiškų dėl savo ypatingų decentralizuotų finansų savybių, tokių kaip - pseudonimiškumas ir tarpininkų nebuvimas (Marc Truchet, 2022; Zheng ir kt., 2023). Dabartiniai investuotojai, o ypač „mėgėjai“ investuotojai, kurie investuodami į virtualias valiutas ar jų pagrindu kurtus žetonus, mažai domisi ar net nesupranta kokių pagrindų jos yra pagamintos, dažnu atveju nukenčia ir taip kelia nepasitikėjimą decentralizuota finansų rinka (Chainalysis, 2022). Būtent dėl to šiame darbe pasirinkta išnagrinėti šiuos nusikaltimus, jiems būdingus bruožus, dažnumą, išsirinkti populiariausią bei didžiausią žalą nešantį nusikaltimą, jį ištirti bei pateikti būdus kaip nuo to apsisaugoti. Šiame magistro darbe ne vien pateikiama kaip veikia decentralizuota finansų rinka ar joje vykstantys nusikaltimai, tačiau ir šių nusikaltimų požymiai. Darbe detaliai išnagrinėtas ir pasirinktas dar neseniai, 2021 metais, išpopuliarėjęs „Rug pull“ decentralizuotų finansų finansinis nusikaltimas, kurio metu investuotojai gali prarasti visas savo investuotas lėšas Crystal Blockchain's Analytics Team (2023), Sharma ir kt. (2024), Stangl ir Neumann (2024). Taip pat, darbe pastebėjus, jog šiam nusikaltimui neturint susistemintų prevencinių priemonių, o jos yra reikalingos, siekiant netapti sukčiavimo auka, buvo nuspręsta sukurti modelį, kuriuo remiantis ir įvykdžius visus modelio žingsnius investuotojas galėtų atsidurti etape, kur lieka tik pačiam apsispręsti ar tikrai jis nori investuoti į norimą virtualų vieneta, nes galiausiai investuotojas investuoja tam, kad praturtėti ir

išpildyti savo svajones, o ne tam, kad prarasti lėšas ir taip pat prarasti pasitikėjimą tuo, kas šiuo metu pasaulyje ne vieną žmogų padarė milijonieriumi ar net milijardieriumi – decentralizuota finansų rinka.

Analizuojamos temos ištirimo lygis – mokslininkai tirdami finansinius nusikaltimus decentralizuotų finansų ekosistemoje yra ištyrę ir aprašę šių nusikaltimų naujumą, metodus, sampratas bei sąvokas. Nors decentralizuoti finansai yra gana nauja tema, tačiau teoriniu aspektu mokslininkai yra detalčiai išanalizavę didžiąją dalį finansinių nusikaltimų. Remiantis šio darbo tolimesne eiga, buvo pastebėta, kad 2021 metais atsiradusio „Rug pull“ decentralizuotų finansų finansinio nusikaltimo aspektas per tokį trumpą laiką teoriškai yra išanalizuotas detalčiai, tačiau duomenų ir atliktų tyrimų kiekis šia tema, tikėtina kol kas, yra minimalus ir pagrindiniai šaltiniai duomenims rinkti yra didelių kompanijų, kurios tiria virtualias valiutas, internetiniai tinklapiai. Pavyzdžiui, Cernera ir kt. (2022) autoriai atliko mokslinį tyrimą susijusį su virtualiais žetonais ir likvidumo fondais esančiais Eterio bei „BNB Smart Chain“ blokų grandinėse. Šio tyrimo tikslas buvo palyginti žetonų bei tų žetonų kūrėjų gyvavimo trukmę. Galiausiai buvo sukurtas robotas, kuris turėjo pirkti žetonus, tačiau jis tapo pačios nagrinėjamos temos auka, tai yra, įsigijo žetonų, susijusių su „Rug pull“. Xia ir kt. (2021) savo moksliniame darbe analizuoja žetonus, susijusius su „Rug pull“ finansiniu nusikaltimu, „Uniswap V2“ likvidumo fonde. Tyrimui atlikti duomenys buvo surinkti iš internetinės svetainės „The Graph“ (The Graph, 2024), tačiau šiuo atveju, siekiant surinkti duomenis iš šio puslapio privalu žinoti - konkretų žetoną (žetono adresą). Taip pat atliekant išsamią mokslinių tyrimų analizę, pastebėta, kad yra nagrinėjami realūs įvykė „Rug pull“ atvejai. Rahmanda (2024) moksliniame straipsnyje atliekama teisinės literatūros apžvalga, kurios metu apžvelgiama kaip į „Rug pull“ atvejus reaguoja teisinė aplinka. Zhou ir kt. (2024) moksliniame tyrime taip pat tiria įvykusius „Rug pull“ atvejus, kurių dėka investuotojai patyrė didelius nuostolius. Šio tyrimo metu duomenys buvo surinkti remiantis finansinių nusikaltimų analizės ataskaitomis bei pranešimais, tokiais kaip Chainalysis (2023). Tyrimo metu buvo identifikuotos keturios „Rug pull“ rizikos, nusakančios kas galėtų parodyti, kad žetonas yra susijęs su „Rug pull“ nusikaltimu, tačiau tyrime nėra nurodyta, kaip šias rizikas gali pasitikrinti investuotojas, kad neinvestuotų pinigų, į su „Rug pull“ nusikalstama veikla susijusį žetoną.

Darbo naujumas – Šiame magistro darbe atliekamas pervedimų į decentralizuotų finansų finansinių nusikaltimų „Rug pull“ virtualių žetonų kiekio ir Eterio to meto vertės palyginimas, nes išnagrinėjus mokslinius tyrimus, nustatyta, kad tyrimai yra atlikti tik koncentruojantis į „Rug pull“ atvejus, tačiau nėra analizuojama, kas lemia, jog „Rug pull“ finansiniai nusikaltimai įvyksta. Taip pat pateikiamas dar neegzistuojantis modelis apsaugojimui nuo investavimo į „Rug pull“ finansinio

nusikaltimo tipo sukurtus virtualius žetonus, nes išanalizavus mokslinius tyrimus pastebėta, kad iki šiol nėra pateikta būdų, kuriais būtų galima išvengti „Rug pull“, taip pat pastebėta, kad kuriami modeliai identifikuoja, jog įvyko „Rug pull“, remiantis tik istoriniais duomenimis, ir galiausiai identifiukuota, kad nors ir yra pateikiami „Rug pull“ rizikos faktoriai, kurie parodo, kad žetonas gali būti susijęs su „Rug pull“, tačiau nėra atskleidžiama kaip investuotojas žinodamas minėtus rizikos faktorius, gali pats pasitikrinti žetoną.

Darbo problema – investavimas šiais laikais labai populiarus būdas pakelti savo turimo turto vertę. Ne išimtis yra ir investavimas į decentralizuotų finansų rinką bei jos siūlomus vienetus. Nesvarbu ar tai būtų virtuali valiuta ar virtualus žetonas, tačiau ar decentralizuotų finansų rinką yra saugi?

Darbo tikslas – išnagrinėjus finansinių nusikaltimų decentralizuotų finansų ekosistemoje teorinius aspektus, atlikti finansinių nusikaltimų decentralizuotoje finansų ekosistemoje vertinimą.

Darbo uždaviniai:

1. Išnagrinėjus mokslinę literatūrą, išryškinti finansinių nusikaltimų decentralizuotų finansų ekosistemoje ir „Rug pull“ finansinio nusikaltimo nagrinėjimo aktualumą, bei pateikti „Rug pull“ finansinio nusikaltimo tipologiją;
2. Parengti metodologiją decentralizuotų finansų finansinių nusikaltimų ir virtualių valiutų palyginimui, „Rug pull“ finansinio nusikaltimo vertinimui ir atpažinimui, bei modelio, skirtam apsisaugojimui nuo „Rug pull“ decentralizuotų finansų finansinio nusikaltimo, kūrimui;
3. Palyginti decentralizuotų finansų finansinių nusikaltimų aktyvumą su Eterio verte pasirinktais laikotarpiais bei ištirti kaip pasirinktais laikotarpiais Eterio kainų kitimas koreliuoja su investuotojų pervedimais į decentralizuotų finansų finansinio nusikaltimo „Rug pull“ virtualius žetonus;
4. Sukurti modelį apsisaugojimui nuo „Rug pull“ decentralizuotų finansų finansinio nusikaltimo.

Darbe taikyti metodai. Mokslinės literatūros šaltinių nagrinėjimas bei informacijos susistemimas, komparatyvinės analizės, inferencinės statistikos, T.testo, Pearsono koreliacijos metodai.

Darbo struktūra. Magistro darbą sudaro trys dalys. Pirmoje darbo dalyje pateikiama decentralizuotų finansų samprata bei skirtumai ir panašumai lyginant tradicinius ir bei decentralizuotus finansus. Taip pat yra apžvelgiamos virtualių valiutų nepastovumo ypatybės ir

identifikuojama, kad viena iš nepastovumą lemiančių priežasčių yra įtartini sandoriai. Šioje darbo dalyje yra išryškinamas „Rug pull“ finansinio nusikaltimo aktualumas bei pateikiama detali „Rug pull“ finansinio nusikaltimo analizė ir nustatoma, jog nėra sukurta jokio modelio apsaugojimui nuo šio nusikaltimo. Antrojoje darbo dalyje pateikiama Eterio kainų ir finansinių nusikaltimų su tuometinėmis Eterio virtualios valiutos kainomis lyginamosios analizės, detali kiekvieno virtualaus žetono susijusio su „Rug pull“ decentralizuotų finansų finansiniu nusikaltimu ir Eterio kainomis koreliacijos bei modelio kūrimo metodologija. Trečioji darbo dalis apima Eterio kainų ir finansinių nusikaltimų su tuometinėmis Eterio virtualios valiutos kainomis lyginamąją analizę, „Rug pull“ decentralizuotų finansų finansinio nusikaltimų vertinimą, bei pervedimų, į tokių nusikaltimų žetoną, skaičių palyginimą su tuometinėmis Eterio kainomis pasirinktais laikotarpiais. Taip pat, remiantis atlikta mokslinės literatūros analize, įgyta patirtimi atliekant magistro darbo tyrimo dalį, sukuriamas modelis, skirtas apsaugoti investuotojus nuo investavimo ar lėšų praradimo investuojant į decentralizuotų finansų finansinių nusikaltimo „Rug pull“ virtualius žetonus. Magistro darbo apimtis – 79 puslapiai, į kuriuos įeina: įvadas, trys skyriaai, suformuluotos išvados ir pasiūlymai, baigiamajame magistro darbe naudoti literatūros šaltiniai, santrauka parašyta lietuvių bei anglų kalbomis, 9 lentelės, 12 paveikslų bei 8 priedai.

1. FINANSINIŲ NUSIKALTIMŲ DECENTRALIZUOTOJE FINANSŲ EKOSISTESMOJE TEORINIAI ASPEKTAI

Pirmojoje magistro darbo dalyje pateikiamas yra decentralizuotų finansų apibrėžimas, samprata bei skirtumai ir panašumai lyginant tradicinius bei decentralizuotus finansus. Taip pat yra apžvelgiamos virtualių valiutų nepastovumo ypatybės ir identifikuojama, kad viena iš nepastovumą lemiančių priežasčių yra įtartini sandoriai. Be to yra analizuojami decentralizuotų finansų finansiniai nusikaltimai bei išryškinamas „Rug pull“ finansinio nusikaltimo nagrinėjimo aktualumas. Galiausiai, yra pateikiama detali „Rug pull“ finansinio nusikaltimo analizė, atskleidžiama kokie yra kriterijai siekiant nustatyti, kad žetonas yra susijęs su finansiniu nusikaltimu „Rug pull“ bei identifikuojama, kad modelio, kuriuo remiantis asmenys gali apsisaugoti nuo investavimo į žetonus, susijusius su „Rug pull“ nusikalstama veika, nėra.

1.1 Decentralizuotų finansų samprata

Siekiant aiškiau suprasti decentralizuotus finansus, pirmiausia svarbu suprasti jų sąvoką. Mokslinėje literatūroje pastebima, kad decentralizuoti finansai (santrumpa – DeFi) siejami su blokų grandinėmis (angl. *blockchain*) (Beinke ir kt., 2024; Bekemeier, 2023; Marc Truchet, 2022; OJOG, 2021; Ozili, 2022; Schuler ir kt., 2024). Blokų grandinė yra sukurta technologija, kurios pagalba istoriniai duomenys yra saugojami. Pačios blokų grandinės sąvoka apibūdina jos veikimą, tai yra, informacija yra kaupiama į duomenų rinkinius, kurie decentralizuotoje duomenų sistemoje yra sujungiami (Firdaus ir kt., 2019; Katina ir kt., 2019; Lewis ir kt., 2017; Valiente ir Tschorsch, 2021). Duomenų rinkiniai (blokai) apima dvi dalis: bloko antraštę (angl. *block header*) ir bloko duomenis. Bloko antraštę sudaro šeši komponentai: bloko versija, Merkle medžio šaknies (angl. *Merkle tree root*) maišos kodas, ankstesnio bloko maišos kodas, laiko žyma, nbitai ir unikalūs skaičius vadinamas „*Nonce*“ (Dong ir kt., 2023; Moosavi ir kt., 2024; Two Hop Ventures, 2017). Blokų antraštės komponentai aprašyti 1 lentelėje.

Antroji bloko dalis apima visų įvykusių operacijų skaičių bei konkrečias įvykusias operacijas (Dong ir kt., 2023; Moosavi ir kt., 2024; Two Hop Ventures, 2017). Siekiant suprasti kas yra blokų grandinės operacijos, svarbu išsiaiškinti, kaip jos sudaromos. Blokų grandinės naudotojai, į kuriuos įeina įrenginiai, pavyzdžiui, kompiuteriai ar serveriai, yra vadinami mazgais (Askar ir kt., 2021; Islam

ir Apu, 2024; Moosavi ir kt., 2024; Tmeizeh ir kt., 2023). Blokų grandinės naudotojai blokų grandinėje atlieka sandorius. Sandoriai vykdomi naudojant skaitmeninį parašą (angl. *digital signature*). Skaitmeninis parašas apima dviejų tipų kriptografinius raktus: viešąjį (angl. *public key*) ir privatųjį (angl. *private key*). Viešasis raktas yra matomas ir žinomas visiems mazgams, tačiau privatųjį raktą žino tik atitinkamas mazgas. Tai reiškia, kad žinant viešąjį raktą galima atsekti, kas atliko pasirašymą, tačiau nežinant privačiojo (unikalaus asmeninio) rakto neįmanoma atlikti pasirašymo funkcijos (Abdelrahman, 2022; Moosavi ir kt., 2024). Svarbu paminėti, kad tiek viešas, tiek privatus raktas yra sudaromas arba sugeneruojamas iš atsitiktinių simbolių sekos. Šiuo atveju tarpusavio sandoriai, patvirtinami pačių mazgų skaitmeniniais parašais, nereikalauja finansinių institucijų, kaip tarpininko, įsitraukimo todėl šis modelis vadinamas lygiarangis ryšys (angl. *peer-to-peer network*, santrumpa *P2P*) (Sarode ir kt., 2021). Sandorių informacija yra paskleidžiama visiems mazgams ir šis procesas yra vadinamas paskalų protokolu (angl. *Gossip protocol*) (Shaleva ir Korkhov, 2021).

1 lentelė

Blokų antraštės komponentai

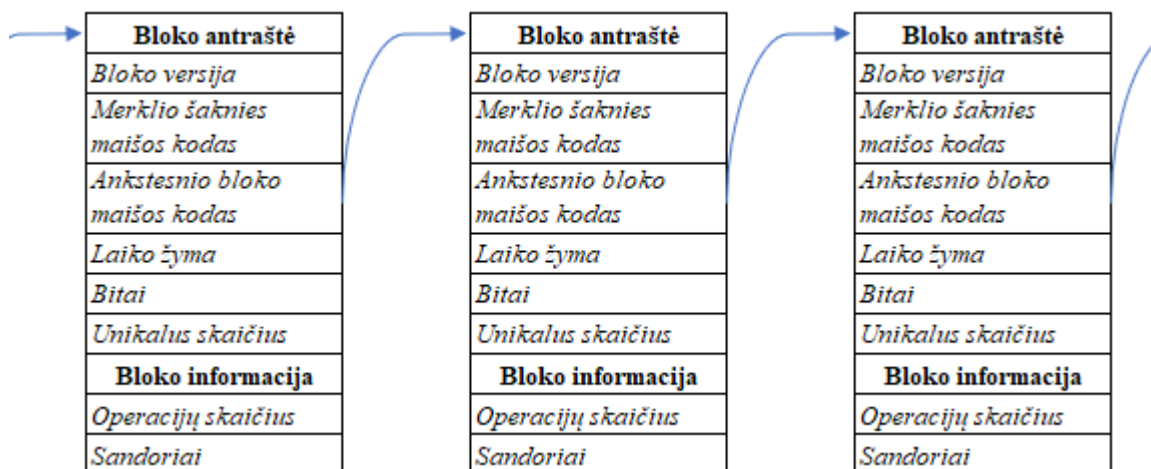
Blokų antraštės komponentas	Komponento aprašymas	Šaltinis
Bloko versija	Pateikiama informacija, kuri nurodo, kokia taisyklė (kaip skaičiuojamas unikalus skaičius) naudojama konkrečiam blokui.	(Dong ir kt., 2023; Moosavi ir kt., 2024; Two Hop Ventures, 2017)
Merkle šaknies maišos kodas	Visų ankstesnių blokų operacijų maiša.	(Dong ir kt., 2023; Moosavi ir kt., 2024; Two Hop Ventures, 2017)
Ankstesnio bloko maišos kodas	Ankstesniojo bloko operacijų maiša.	(Dong ir kt., 2023; Moosavi ir kt., 2024; Two Hop Ventures, 2017)
Laiko žyma	Informacija, kada naujas duomenų rinkinys buvo prijungtas prie ankstesnio duomenų rinkinio	(Dong ir kt., 2023; Moosavi ir kt., 2024; Two Hop Ventures, 2017)
nBitai	Naujai sudaryto (einamojo) bloko maišos kodo sutrumpinta versija	(Dong ir kt., 2023; Moosavi ir kt., 2024; Two Hop Ventures, 2017)
Unikalus skaičius	Unikalus skaičius (angl. <i>number used once</i> , santrumpa <i>Nonce</i>), kuris prasideda nuliu. Šiuo skaičiumi yra sukuriamas kiekvieno bloko duomenų maišos kodas.	(Dong ir kt., 2023; Moosavi ir kt., 2024; Two Hop Ventures, 2017)

Šaltinis: sudarytas autorės, remiantis lentelėje nurodytais autoriais

Duomenų vientisumui, užtikrinimui, kad egzistuoja sandoriai, naudojamas Konsensuso protokolas (angl. *Consensus Protocol*) (Rahmani, 2022). Decentralizuotose finansuose protokolas yra laikomas taisyklių ar standartų rinkinys, kuris naudojamas blokų grandinėse (Metelski ir Sobieraj, 2022). Konsensuso protokolas naudoja 3 metodus: darbo įrodymas (angl. *Proof of Work*. Toliau – PoW), dalyvavimo įrodymas (angl. *Proof of Stake*. Toliau – PoS) ir deleguoto dalyvavimo įrodymas (angl. *Delegated Proof of Stake*. Toliau – DpoS). Dažniausiai naudojamas PoW. Šiuo atveju mazgai turi išsiaiškinti unikalų skaičių (*Nonce*), kuriuo patvirtintų, kad blokas ir jame pateikiama informacija yra teisingi. Alternatyvūs mechanizmai yra PoS ir DPoS. Šiuo atveju bloko teisingumą tikrina mazgai, kurie atrenkami pagal turimą virtualios valiutos kiekį. Galiausiai DPoS, tai mechanizmas, kurio metu yra balsuojama ir išrenkami blokų tvirtintojai ir naujų blokų kūrėjai (Dong ir kt., 2023; Moosavi ir kt., 2024; Two Hop Ventures, 2017).

1 paveikslas

Grafinis blokų grandinės atvaizdavimas



Šaltinis: sudarytas autorės, remiantis Moosavi ir kt. (2024)

Išsiaiškinus, ką apima vienas blokas, svarbu suprasti kaip ankstesnis blokas sujungiamas su naujuoju bloku. Taigi, blokų grandinės rinkiniai tarpusavyje yra sujungiami į naujausio bloko antraštę įrašant ankstesniojo bloko maišos kodą (angl. *hash codes*). Šie maišos kodai yra pseudoatsitiktiniai ir generuojami naudojant kriptografinę maišos funkciją. Kriptografinės maišos funkcija tai yra algoritmas, kuris sudarytas iš atsitiktinių simbolių (raidžių ir skaičių) (Kuznetsov ir kt., 2023; Long ir kt., 2023). Atkreiptinas dėmesys, kad kriptografinė maišos funkcija užtikrina duomenų nekintamumą. Siekiant pakeisti tam tikros operacijos turinį ar norint įterpti naująją operaciją, tektų pakeisti ne tik atitinkamą bloką, tačiau ir visus vėlesnius blokų grandinės blokus, o tai pareikalautų

didelių skaičiavimo pastangų (Felix Adebayo Bakare ir kt., 2024). Blokų grandinės sudarymas pateikiamas 1 paveiksle.

Taip pat decentralizuotų finansų neatsiejama dalis yra išmaniosios sutartys (angl. *smart contracts*) (Albina Hysaj, 2023; Beinke ir kt., 2024; Marc Truchet, 2022). Mokslinėje literatūroje išmanioji sutartis yra apibrėžiama kaip blokų grandinėje suformuotas kodas, kuris užtikrina, kad sutarties sąlygos automatiškai būtų įvykdytos, tai yra, įpareigoja sutarties šalis įvykdyti savo įsipareigojimus (Massimo Doria ir kt., 2024; Moosavi ir kt., 2024; Savelyev, 2016; Taherdoost, 2023; Wu ir kt., 2022). Išmaniosios sutartys bei finansinių institucijų tarpininkavimo nebuvimas yra decentralizuotų finansų esminės savybės, kurios identifikuoja, kad tai nėra tradiciniai finansai (Marc Truchet, 2022). Taigi, išanalizavus mokslinius šaltinius, galima apibrėžti, kad decentralizuoti finansai tai yra finansų rinkų dalis, kurie sukuria galimybę tam tikras finansines operacijas atlikti naudojantis automatiškai vykdomais programiniais kodais blokų grandinėje be finansinių institucijų įsitraukimo (Auer ir kt., 2024; Bourveau ir kt., 2024; Wieandt ir Heppding, 2023).

Decentralizuotose programose yra disponuojama virtualiomis valiutomis (angl. *cryptocurrencies*). Virtuali valiuta apibūdinama kaip skaitmeninė finansinė priemonė, kurios disponuojamos blokų grandinėse bei kurių apsisiekimui nėra reikalingi tarpininkai, tokie kaip finansinės institucijos (Tierno, 2023). Virtualios valiutos gali būti suskirstytos į du tipus: stabilias monetas (angl. *stablecoins*) ir nestabilias monetas (angl. *non-stablecoins*). Stabilios monetas yra apibrėžiamos kaip monetas, kurios yra susietos su „fiat“ valiutomis, o tai lemia jos stabilumą (Makarov ir Schoar, 2022; Tierno, 2023). Stabilios monetas išsaugo savo vertę tol, kol galima ją iškeisti į „fiat“ valiutą. „Fiat“ valiuta tai fizinė valiuta, kuri dažniausiai apibūdina eurą ar JAV dolerį (Makarov ir Schoar, 2022). Mokslinėje literatūroje Makarov ir Schoar (2022) yra nurodoma, kad pagrindinės stabilios monetas susietos su „fiat“ valiuta yra „Tether“, „Binance USD“ ir „USD Coin“. Kalbant apie nestabilias monetas, jos sudaro didelę grupę visų virtualių valiutų. Nestabilių monetų kainos labai svyruoja ir priklauso nuo investuotojų nuotaikų. Pirmiausia, kaip nestabilias monetas galima laikyti virtualias valiutas, kurios turi tik vertę, tačiau jokios kitos funkcijos neatlieka. Šiai nestabilių monetų grupei priskiriamos paplitusios valiutos kaip „Bitcoin“ (toliau – Bitkoinas), „Litecoin“. Kita, taip didelę rinkos dalį užimanti grupė, yra nestabilios monetas, kurios disponuojamos išmaniųjų sutarčių programose. Tokias nestabilias monetas galima laikyti kaip „Binance Smart Chain“, „Solana“, „Ethereum“ (toliau – Eteris). Šios nestabilios monetas programos tipo vertė priklauso nuo decentralizuotoje programoje veikiančių programinės įrangos apimties ir jų skaičiaus. Kitas nestabilių monetų tipas yra apibūdinamas kaip decentralizuoto finansavimo

programos, kurios apima decentralizuotus virtualių valiutų mainus, skolinimą ir skolinimąsi. Decentralizuota birža arba decentralizuoti mainai (angl. *decentralized exchange, DEX*) apibūdinami kaip P2P rinka, kurioje sandoriai yra vykdomi be tarpininkų. Skirtingai nuo centralizuotų biržų, decentralizuoti mainai suteikia teisę savo privačius raktus kontroliuoti patiems rinkos dalyviams. Išmaniųjų sutarčių technologija decentralizuotoje biržoje panaikina rinkos dalyviams sandorio šalies riziką. Decentralizuotos biržos pagrinde naudoja automatinius rinkos formuotojo (angl. *automated market maker, AMM*) protokolus, kurie sukuria galimybę keistis vienu metu dvejomis virtualios valiutos monetomis. Decentralizuotų biržų pavyzdžiai galėtų būti „Uniswap“, „Sushiswap“ ar „PancakeSwap“. Skolinimosi ir skolinimo rinkos, kuriose yra naudojami decentralizuoti protokolai kontroliuojami išmaniųjų sutarčių pagalba, leidžia rinkos dalyviams skolinti arba pasiskolinti virtualų turtą. Išmaniųjų sutarčių pagalba yra nustatomos rinkos palūkanų normos, skolos grąžinimo sąlygos, paskolos sumos bei trukmė. Skolinimo ir skolinimosi rinkos apima tokias decentralizuotas programas kaip „Aave“, „MakerDAO“ ar „Compound“. Galiausiai, trečiasis nestabilių valiutų tipas yra nepakeičiamieji žetonai (angl. *Non-fungible tokens, NFT*). Nepakeičiamieji žetonai yra apibūdinami kaip vienetinis, unikalus blokų grandinės skaitmeninis, fizinis turtas arba teisė naudotis tam tikru turtu. Vienas iš nepakeičiamų žetonų pavyzdžių galėtų būti skaitmeninis koliažas, apimantis penkis tūkstančius vaizdų, kuris buvo parduotas 2021 metų kovo mėnesį. „Beeple“ pseudonimu pasivadinęs menininkas minėtą meno kūrinį pardavė už šešiasdešimt devynis milijonus JAV dolerių (Makarov ir Schoar, 2022). Svarbu atkreipti dėmesį, kad aukščiau minimų monetų pagrindu yra sukuriami žetonai (angl. *tokens*). Eteris yra labiausiai paplitusi žetonų kūrimo programinė įranga dėl joje egzistuojančios išmaniosios sutarties funkcijos. Eterio blokų grandinėje sukurti žetonai vadinami „ERC-20“ standarto žetonais, o nepakeičiamieji žetonai – „ERC-721“ ir „ERC-1155“. Pagrindinis skirtumas yra jų struktūra ir paskirtis. Monetos veikia savo blokų grandinėje ir jos yra laikomos kaip mainų priemonė, tačiau žetonai veikia jau sukurtose blokų grandinėse, tokiose kaip Eterio, ir siūlo daugiau funkcijų. Šie žetonai yra susieti su atitinkamu protokolu ar projektu blokų grandinėje (Huang ir kt., 2023; Schueffel ir kt., 2019).

Pasitelkiant blokų grandinės technologiją bei P2P yra sukurtos decentralizuotos programos (angl. *decentralized application*. Toliau – *dApp*) (Garg Aakash ir kt., 2023; Zheng ir kt., 2023). Išnagrinėjus mokslinius šaltinius pastebėta, kad yra išskiriami keturi dApp tipai: vietinis klientas (angl. *native client*), išmaniosios sutartys, naršyklės ir sutarčių bendras veikimas bei visiškai decentralizuota programa. Vietinio kliento decentralizuotos programos pavyzdys būtų virtuali valiuta Bitkoinas. Siekiant atlikti operacijas susijusias su Bitkoinais reikalinga lokali mobili programa, tai

yra, operacijos atliekamos mobilios programinės įrangos pagalba, tačiau operacijų atlikimas nėra pasiekiamas naršyklėje. Tokį mechanizmą taip pat naudoja ir kitos ankstyvosios virtualios valiutos tokios kaip „Litecoin“ ar „PPcoin“. Vietinio kliento decentralizuotoje programoje naudojama tik blokų grandinė. Išmaniosios sutarties decentralizuota programa papildo vietinio kliento programą. Šiuo atveju blokų grandinė pasipildo nauju aspektu – išmaniąja sutartimi. Programos vartotojai atlikdami operacijas gali naudotis išmaniosios sutarties naršykle, tačiau tai reikalauja programavimo žinių, nes nedaugelis išmaniųjų sutarties naršyklių turi grafinę sąsają (angl. *graphical user interface*), kuriomis būtų galima naudotis neturint programavimo žinių. Išmaniosios sutarties dApp pavyzdys būtų virtuali valiuta Eteris. Trečioji decentralizuota programa papildo antrąją dApp tipą grafinę sąsają, kuri vartotojams palengvina naudojimąsi decentralizuotomis programomis bei prieigą prie virtualių valiutų. Minėtosios decentralizuotos programos pavyzdžiai būtų „MakderDAO“, „Uniswap“, „Curve“ ir kiti. Ketvirtoji decentralizuota programa skiriasi nuo trečiosios dApp tuo, jog ji naudoja ne centralizuotus serverius, tai reiškia, kad naršyklės grafinė sąsaja saugoma ne vienoje vietoje. Šios ketvirtosios dApp pavyzdys būtų „TornadoCash“ (Zheng ir kt., 2023).

Išsiaiškinus, kas yra decentralizuoti finansai yra svarbu suprasti kokie yra skirtumai tarp decentralizuotų finansų ir centralizuotų finansų. Kaip ir buvo minėta anksčiau vienas iš pagrindinių skirtumų tarp tradicinių ir decentralizuotų finansų yra tarpininkai. Tradiciniuose finansuose tarpininkai yra finansų institucijos, kurių yra atliekamos operacijos. Tuo tarpu decentralizuotuose finansuose tarpininkų nėra, juos pakeičia išmaniosios sutartys, kurių dėka sandoriai yra patvirtinami automatiškai. Kitas aspektas yra komponavimas. Decentralizuoti finansai leidžia skirtingoms paslaugoms ar produktams bei skirtingoms programinėms įrangoms veikti vienoje vietoje blokų grandinės principu, tačiau tradiciniai finansai tokių galimybių neturi, nes viena iš priežasčių yra tai, jog sistemos yra uždaros (Aramonte Sirio ir kt., 2021; Autorité des Marchés Financiers (AMF), 2023; Hazim ir kt., 2022). Dar vienas reikšmingas skirtumas tarp tradicinių ir decentralizuotų finansų yra „pažink savo klientą“ (angl. *Know your customer*. Toliau – KYC) procesas. Tradicinių finansų atveju klientas norėdamas atidaryti sąskaitą banke, pagal įstatymus, turi pateikti tapatybę patvirtinančius dokumentus, tačiau decentralizuotų finansų atveju, KYC nėra reguliuojamas, todėl programinės įrangos naudotojas dažnu atveju neturi patvirtinti savo tapatybės, o taip pat jo asmeniniai duomenys, pavyzdžiui, vardas ir pavardė, gali skirtis. Kalbant apie apribojimus, tai decentralizuotuose finansuose nėra kontroliuojančios institucijos, nėra ribojimų kokie veiksmai programinėse įrangose gali būti atliekami bei taip pat nėra apribojimų, kurie nustatytų kokiomis sumomis galima disponuoti programinėse įrangose (Hazim ir kt., 2022). Tradiciniuose finansuose, subjektai vykdančys paslaugas,

susijusias su finansinėmis priemonėmis, yra atskaitingi tik atitinkamoms institucijoms, tačiau decentralizuotuose finansuose blokų grandinės principas užtikrina, tokiais mechanizmais kaip duomenų nekintamumas, kriptografija bei konsensuso protokolai, aukštą duomenų skaidrumo bei saugumo lygį (Felix Adebayo Bakare ir kt., 2024; Hazim ir kt., 2022). Taip pat ir tarpininkavimo mokesčiai skiriasi tarp tradicinių ir decentralizuotų finansų. Tradicinių finansų tarpininkų siekis yra gauti pelno iš įvykusių sandorių, tačiau decentralizuotuose finansuose tarpininkavimas yra automatizuotas, todėl tarpininkavimo mokesčiai yra patrauklesni nei tradiciniuose finansuose (Hazim ir kt., 2022). Skirtumai tarp tradicinių ir decentralizuotų finansų pateikiami 2 lentelėje.

2 lentelė

Tradicionių ir decentralizuotų finansų skirtumai

	Tradicioniai finansai	Decentralizuoti finansai
Tarpininkai	Finansinės institucijos	Išmaniosios sutartys
Lėšų laikymas	Lėšos laikomos finansinėse institucijose	Lėšos laikomos skaitmeninėse piniginėse, kurias valdo programinės įrangos naudotojai
Ar yra galimybė komponuoti	Ne	Taip
Pinigų srautas	Pinigų srautų valdymą užtikrina finansinės institucijos	Pinigų srautų valdymą užtikrina programinės įrangos naudotojai
Operacijų įvykdymas	Operacijų įvykdymas gali užtrukti	Greitas operacijų įvykdymas
Pažink savo klientą	Reikalinga tapatybė ir naudotojo asmeniniai duomenys	Pseudonimiškumas
Apribojimai	Egzistuoja	Neegzistuoja
Prieinamumas	Prieinama tik tiems asmenims, kurie turi sąskaitą finansinėje institucijoje	Neribojama, jei vartotojai turi interneto prieigą
Lėšų prieinamumas	Darbo valandomis	Lėšų prieinamumas 24 valandas per parą
Duomenų skaidrumas	Ne	Taip
Duomenų pasiekiamumas	Apribotas	Visuotinis
Naudos gavėjai	Finansinės institucijos	Programinės įrangos naudotojai

Šaltiniai: sudaryta remiantis Hazim ir kt. (2022), The European Union Blockchain Observatory (2022)

Apibendrinant skirtumus tarp tradicinių ir decentralizuotų finansų, galima teigti, kad decentralizuoti finansai vartotojams suteikia didesnę finansų sistemos efektyvumą ir lankstumą, didesnę prieinamumą skirtingiems vartotojams bei skaidrumą (Marc Truchet, 2022). Tačiau kaip ir tradiciniuose finansuose, decentralizuotų finansų veikla susijusi su rizikomis. Viena iš decentralizuotų

finansų rizikų yra finansinė rizika. Šiuo atveju finansinė rizika yra susijusi su nepastovumu bei likvidumu. Decentralizuotuose finansuose pagrindu operacijų turinys yra susijęs su virtualiomis valiutomis, kurios iš savęs yra nepastovios, todėl decentralizuotų programų naudotojai gali patirti nuostolių. Taip pat virtualios valiutos tarpusavyje yra susijusios, todėl staigus dominuojančios skaitmeninės valiutos kainos pasikeitimas gali reikšmingai paveikti koreliuojančias virtualias valiutas. Likvidumo rizika šiuo atveju pasireiškia tuo, kad decentralizuotų finansų dalyviams nėra galimybės atsiimti savo turto bei juo disponuoti. Tai gali įvykti tuomet kai programinėje įrangoje nebėra pakankamai turto (Hafner ir kt., 2023; Marc Truchet, 2022; Zheng ir kt., 2023). Kita decentralizuotų finansų rizika yra susijusi su neteisėta veikla. Pseudonimiškumas turi įtakos didesnio masto nusikaltimams, nes asmenys gali pasislėpti po anonimiškumu. Be to, finansinių institucijų, kaip tarpininko, kurie užtikrintų reguliavimą, nebuvimas – paskatina neteisėtos veiklos tankį. Galiausiai, galima būtų išskirti technologinę riziką. Šiuo atveju ji gali būti susijusi su išmaniųjų sutarčių pažeidžiamumu. Nors išmaniosios sutartys yra automatizuotos, tačiau jų programinis kodas gali turėti klaidų, kuriais gali pasinaudoti neteisėta veikla užsiimančios asmenys (Marc Truchet, 2022; Zheng ir kt., 2023).

1.2 Virtualių valiutų rinkų nepastovumo ypatybės

Kaip ir buvo aptarta 1.1 skyriuje decentralizuoti finansai susiję su nepastovumu (angl. *market volatility*). Svarbus aspektas yra tas, kad didesnis nepastovumas yra spekuliacijų ir padidėjusių įtartinų sandorių priežastis (Cheraghali ir kt., 2024; Khan ir Ali Hakami, 2022). Rinkos nepastovumas yra apibūdinamas kaip tam tikro turto kainos staigūs svyravimai per atitinkamą laiko tarpą. Didesnis bei dažnesnis kainos kitimas lemia didesnę rinkos nepastovumą. Didesnis nepastovumas indikuoja, kad atitinkamas turtas yra rizikingesnis palyginus su kitais ir tai reiškia, kad jis gali lemti galimybę patirti didesnius nuostolius arba grąžą (De Silva ir kt., 2017; International Monetary Fund, 2003; Kissell, 2014; Raimond James, 2023). Kalbant apie tradicinių bei decentralizuotų finansų priemones, moksliniuose šaltiniuose pabrėžiama, kad nepastovumas yra didesnis skaitmeninių valiutų rinkose. Azar ir kt. (2022) teigimu virtualios valiutos, lyginant su tradicinėmis finansinėmis priemonėmis, patiria didesnę svyravimą finansų rinkų normalaus veikimo laikotarpiais, tradicinių rinkų sutrikimo laikotarpiais skaitmeninės valiutos gali būti tokios pat nepastovios kaip ir tradicinės finansinės priemonės, o decentralizuotų rinkų sutrikimo laikotarpiais virtualios valiutos svyravimai yra kur kas

didesni nei tradicinių finansinių priemonių. Mehdi Manaa ir kt. (2019), Sila ir kt. (2024) taip pat pabrėžia, kad tradicinės finansinės priemonės pasižymi mažesniu kintamumu nei virtualios valiutos.

Virtualių valiutų nepastovumą gali lemti keletas aspektų. Viena iš priežasčių, kodėl skaitmeninės valiutos patiria svyravimus, yra kainos nustatymas (Brini ir Lenz, 2024). Decentralizuotų finansų rinka yra ganėtinai nauja, pavyzdžiui, Bitkoinas, pirmoji virtuali valiuta, egzistuoja tik 15 metų (Campbell-Verduyn, 2018). Tai reiškia, kad skaitmeninių valiutų rinka laikui bėgant vis daugiau sulauks susidomėjimo, ir naujų rinkos dalyvių atsiradimas darys įtaką svyravimams. Kaip ir buvo paminėta prieš tai, skaitmeninių valiutų rinka yra vis dar formavimosi stadijoje. Nors ji susilaukė didelio susidomėjimo, tačiau jos dydis palyginti su tradicinėmis finansų priemonėmis yra ganėtinai mažas. Khan ir Ali Hakami (2022) teigimu, virtualių valiutų mažas rinkos dydis lemia didesnius kainų svyravimus. Dar viena priežastis, lemianti skaitmeninių valiutų svyravimus yra pasiūlos ir paklausos dinamika. Virtualių valiutų pasiūla yra ribota, nes jų kiekis rinkoje priklauso nuo skaitmeninės valiutos „kasėjų“ (angl. *miners*), o tai sudaro sąlygas kainų nepastovumui, nes reikšmingai išaugusi paklausa gali lemti kainų padidėjimą (Zhang ir kt., 2024). Kitas aspektas, kuris turi įtakos virtualių valiutų kainų nepastovumui, yra rinkos sentimentas arba kitaip dar vadinamas - rinkos nuotaikomis. Rinkos sentimentas tai rinkos dalyvių požiūris į atitinkamą finansų rinką. Rinkos nuotaikos daro įtaką kainų pokyčiams, nes jos paskatina pasiūlą ir paklausą. Kainų kilimas sukuria pakilias rinkos nuotaikas, kurios dar labiau didina kainas ir atvirkščiai (Aggarwal, 2022). Rinkos sentimentų įtakos kainų nepastovumui pavyzdys būtų įmonės „Tesla“ Bitkoino įsigijimas 2021 metų sausio mėnesį. Šios įmonės Bitkoino įsigijimas lėmė optimistišką rinkos sureagavimą ir Bitkoino kainos vėlesniais mėnesiais išaugo rekordiškai – maždaug iki 69 000 JAV dolerių (Mironeanu ir kt., 2021). Be abejo, virtualių valiutų rinkų reguliavimo neegzistavimas, taip pat lemia jų nepastovumą. Autorius Chokor ir Alfieri (2021) pabrėžia, kad virtualių valiutų rinkos reguliavimo pagrindinis tikslas yra užtikrinti kainų stabilumą dėl dviejų aspektų: augantis investuotojų susidomėjimas nauja spekuliacine priemone, tai yra, blokų grandinės technologija, bei taip pat pinigų judėjimo spartumui daranti įtaka virtuali valiuta. Galiausiai, taip pat svarbus aspektas yra virtualios valiutos rinkos veikimas 24 valandas per parą, 7 dienas per savaitę. Priešingai vyksta tradicinėse rinkose, kuomet ten yra prekiaujama nuo pirmadienio iki penktadienio nustatytomis valandomis. Tai reiškia, kad nėra nustatytų mechanizmų, kurie priverčia sustoti prekybinę veiklą ir taip apsaugoti rinką nuo per didelio nepastovumo, rinkos manipuliavimo ar turto pardavimo, kuris lemia paniką (BIS, 2023). Minimi mechanizmai vadinami automatiniu pertraukikliu (angl. *circuit-breaker*).

Išanalizavus virtualias valiutas buvo pastebėta jog naujai susiformavę decentralizuoti finansai yra itin nepastovūs dėl kelių aspektų – pirma dėl kainų nustatymo, antra dėl pasiūlos ir paklausos dinamikos bei trečia – rinkos sentimentų (rinkos nuotaikų). Didelį virtualių valiutų kainų svyravimą taip pat lemia 24/7 rinka, kuri niekada nesustoja ir neatitinka įprastos tradicinės rinkos tvarkos, kurioje priverčiama sustabdyti prekybinę veiklą kas apsaugoja tradicinę rinką nuo nepastovumo, manipuliavimo ja ar rinkos ir turto pardavimo taip sustabdant paniką. Asmenys lydimi šios panikos dažnai priima skubotus sprendimus investuojant ar parduodant savo virtualų turtą ir tokiais momentais dėl neapdairumo bei skubotumo papuola į nusikaltėlių rankas taip tapdami nukentėjusiais finansų nusikaltimų decentralizuotuose finansuose statistikos dalimi.

1.3 Finansinių nusikaltimų samprata ir tipologija decentralizuotų finansų kontekste

Dėl decentralizuoto veikimo, trūkstamo reguliavimo bei anonimiškumo - decentralizuotų finansų sritis tampa vis patrauklesnė nusikalstamai veiklai. Todėl yra svarbu ir aktualu analizuoti finansinius nusikaltimus decentralizuotų finansų ekosistemoje, tam kad žinoti kaip juos atpažinti ir kaip nuo jų apsisaugoti. Siekiant suprasti finansinius nusikaltimus, svarbu aptarti kokių tipų decentralizuotuose finansuose jų galima sutikti. Finansinis nusikaltimas gali būti apibrėžiamas kaip asmenų grupės ar vieno asmens neteisėti veiksmai, kuriais siekiama gauti finansinės naudos pasinaudojant egzistuojančiomis finansų rinkų ar paslaugų priemonėmis (Reagan Ronald, 2023).

Viena iš labiausiai paplitusių virtualių valiutų nusikaltimo temų yra „pinigų plovimas“ (angl. *money laundering*). „Pinigų plovimas“ apibūdinamas kaip veiksmas, kurio metu yra siekiama integruoti į teisėtą ekonomiką neteisėtu būdu gautus pinigus (Murphy, 2024). Taigi, decentralizuotose finansų rinkose pasinaudodami blokų grandinės anonimiškumo galimybėmis nusikalstama veikla užsiimantys asmenys siekia gautus neteisėtus pinigus perkelti į reguliuojamą ir teisėtą bankinę sistemą. Vienas iš pinigų plovimo pavyzdžių, yra pinigų plovimo įgyvendinimas per decentralizuotas biržas. Nusikalstama veikla užsiimantis asmuo įsilaužimo į biržą būdu gauna Eterio arba juo pagrindu sukurtas monetas tokias kaip – „Tether“, „USD Coin“, „Uniswap“ ar „Arbitrum“, tuomet asmuo minėtas monetas perkelia į savo turimą decentralizuotos biržos piniginę. Nelegaliu būdu gautos monetas yra keičiamos į kitas monetas, kurios tampa teisėtos ir legalios. Siekdamas išvengti nereikalingo susidomėjimo, nusikalstama veikla užsiimantis asmuo, dažnai naudoja „maišytuvų“ (angl. *mixer*) programine įranga. Virtualios valiutos „maišytuvas“ apibūdinama kaip paslauga, kurios metu skaitmeninių valiutų jungimo būdu yra paslepiama informacija, tokia kaip virtualios valiutos

savininkas ar lėšų kilmė (World economic forum, 2023). Viena iš paplitusių maišymo programinių įrangų yra „Tornado Cash“ dApp. Minėta paslauga leidžia apjungti tiek neteisėtu būdu, tiek teisėtu būdu gautas lėšas ir šios paslaugos pagalba neteisėtos lėšos tampa sunkiau atsekamos (Elliptic, 2020). Mokslinėje literatūroje pateikiama keletas pavyzdžių, susijusių su „pinigų plovimu“. Vienas iš žinomų „pinigų plovimo“ atvejų, susijęs su virtualiomis valiutomis, įvyko 2017 metais. Larry Harmon buvo apkaltintas „išplovus“ daugiau nei 354 tūkstančius Bitkoinų, kurių tuo metu vertė siekė 311 milijonų JAV dolerių. Šis asmuo sukūrė „Coin Ninja“ programinę įrangą bei virtualią piniginę „DropBit“. Larry Harmon „pinigų plovimą“ atliko naudojantis „Helix“ programine įranga, kuomet šios programos naudotojai atlikdavo pervedimus per tamsųjį tinklą (angl. *dark net*). 2020 metais vasario mėnesį minėtas asmuo buvo suimtas ir jam buvo pareikšti kaltinimai, dėl „pinigų plovimo“. Teigiama, kad Larry Harmon grėsia 20 metų kalėjimas bei 500 tūkstančių JAV dolerių bauda (Homeland Security, 2022). Kitą atvejį, susijusį su „pinigų plovimu“, aptaria „Elliptic“ blokų grandinės analizuotojų komanda, kuri tiria finansinius nusikaltimus, susijusius su virtualiomis valiutomis. Elliptic (2020) ataskaitoje nurodomas „pinigų plovimo atvejis, susijęs su virtualių valiutų birža „RG Coins“. Ataskaitoje nurodoma, kad 2020 metų rugsėjį buvo nuteistas „RG Coins“ įkūrėjas, dėl „pinigų plovimo“. Savo biržoje jis leido veikti nusikalstamai organizacijai ir atlikti „pinigų plovimo“ operacijas. Nusikalstama organizacija siūlydama patrauklias, tačiau netikras, prekes internetinėje svetainėje „eBay“, pasisavindavo asmenų pinigus, kuriuos vėliau pervedavo į virtualių valiutų biržą „RG Coins“. Nurodoma, kad padaryta žala siekė 4,9 milijonus JAV dolerių.

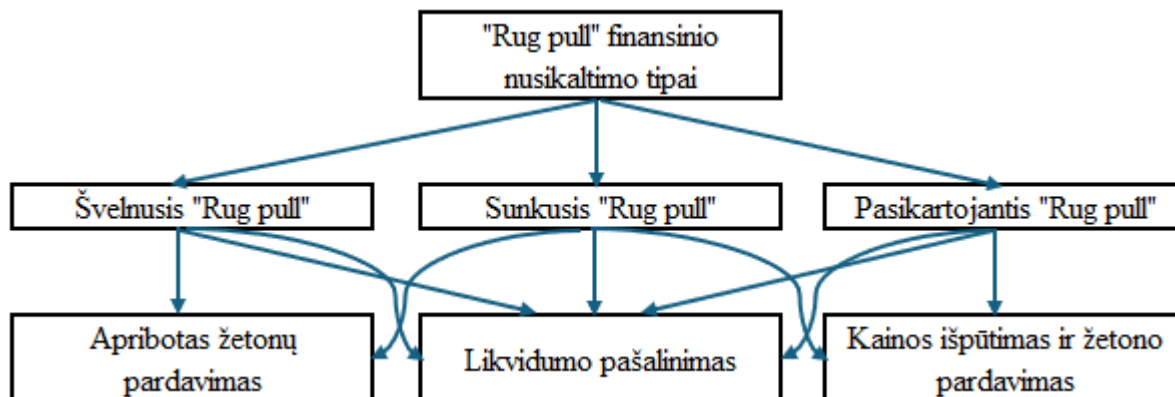
Kitas finansinių nusikaltimų tipas yra „rug pull“ metodas arba lietuviškai vadinamas „kilimo patraukimas“. „Rug pull“ tai yra metodas, kurio metu asmenys įgyvendina naują virtualios valiutos projektą, kurio metu įnirtingai bando pritraukti investuotojus. Virtualiai valiutai pasiekus aukščiausią vertę, asmenys sukūrę naująjį virtualios valiutos projektą, likviduoja savo lėšas, o visų investuotojų lėšos tampa bevertės (Sun ir kt., 2024). Sun ir kt. (2024) moksliniame straipsnyje identifikuoja, kad „Rug pull“ veikia dviem principais: pirmuoju atveju sukuriamos monetos ir užprogramuojamos taip, kad tik monetos kūrėjas turi teisę parduoti turimas monetas, antrasis, kuomet agresyvios rinkodaros pagalba yra išpučiama monetos kaina ir kainai pasiekus aukščiausią tašką monetos kūrėjai pasitraukia su visomis lėšomis palikdami kitus investuotojus su bevertėmis monetomis. Kitame Zhou ir kt. (2024) moksliniame šaltinyje nurodoma, kad „Rug pull“ gali pasireikšti keturiais būdais. Pirmasis būdas apibūdinamas kaip juodasis sąrašas (angl. *Black list*). Šiuo atveju, žetono kūrėjai gali apriboti atlikti pervedimų operacijas konkreitiems adresams, tai reiškia kad žetono pradininkai gali neleisti investuotojams atlikti žetonų pardavimų. Taip pat nurodoma, kad šiuo atveju žetonų kūrėjai be

apribojimų gali sumažinti žetono likvidumą parduodant žetonus, kas lemtų žetono nulinę vertę. Panašiu principu veikia ir kitas „Rug pull“ būdas, kuomet žetono kūrėjai neteisėtai pakeičia žetono pardavimo laiko tarpą, kas lemia, jog investuotojas laiku neatlikęs žetono pardavimo prarandą teisę į žetoną. Šis būdas vadinamas laiko apribojimu (angl. *time limit*). Kitas „Rug pull“ būdas apibrėžiamas kaip balanso pakeičiamumas (angl. *Modifiable balance*). Šiuo atveju žetono kūrėjai turi galimybę pakeisti piniginės likutį. Tokie pakeitimai nėra teisėti. Šiuo „Rug pull“ procesu yra pašalinamas didelis kiekis virtualių žetonų iš apyvartos, kas lemia likvidumo sumažėjimą. Galiausiai tai sukelia greitą žetono kainos žlugimą. Taip pat atkreipiamas dėmesys, kad šiuo atveju žetonų kūrėjai gali neteisėtai pasisavinti investuotojų žetonus, tai yra, perkelti juos į savo pinigines. Ketvirtasis, paskutinis, „Rug pull“ metodas yra apibūdinamas kaip išorinė priklausomybė (angl. *alien depend*). Šiuo atveju į pagalbą yra pasitelkiamos išorinės programos, kurios gali padėti atlikti „Rug pull“ finansinį nusikaltimą per laiko apribojimą, balanso pakeitimą ar juodąjį sąrašą (Zhou ir kt., 2024). Išanalizavus Zhou ir kt. (2024) mokslinio straipsnio tipus, pastebėta, kad ketvirtasis autorių pateikiamas „Rug pull“ tipas yra labiau kaip įrankis, padedantis kitiems „Rug pull“ tipams veikti, o ne „Rug pull“ rūšis. Sharma ir kt. (2024) moksliniame straipsnyje nurodomos trys „Rug pull“ finansinio nusikaltimo rūšys. Pirmoji rūšis yra apibrėžiama kaip sunkusis (angl. *hard*) „Rug pull“, kurio metu žetono kūrėjai pasisavinę lėšas nebereaguoja į investuotojų žinutes arba panaikina paskyras per internetines svetaines tokias kaip „Discord“ ar „Twitter“. Kitas „Rug pull“ metodas, kurio metu žetono kūrėjai panaikina likvidumą, tačiau palieka projektą aktyviu, vadinamas švelniu (angl. *soft*) „Rug pull“. Trečiasis „Rug pull“ finansinio nusikaltimo metodas apibrėžiamas kaip išplėstinis „Rug pull“ (angl. *rug pull by extension*), kuomet kūrėjai tuo pačiu piniginės adresu sukuria kelis žetonus, susijusius su „Rug pull“ finansiniu nusikaltimu. Taip pat nagrinėjant mokslinę literatūrą pastebėta, kad sukčiavimo metodas „kainos išpūtimas ir žetono išpardavimas“ (angl. *pump and dump scam*) yra tas pats „Rug pull“ finansinis nusikaltimas, nes kainos išpūtimas ir žetono išpardavimo sukčiavimas apibūdinamas kaip žetonų kūrėjų staigus žetonų pardavimas, prieš tai šį žetoną išreklamavus, kuris lemia žetonų kainos kritimą iki nulio ir investuotojų lėšų praradimą (Chainalysis, 2024). Taigi, išnagrinėjus mokslinę literatūrą susijusią su „Rug pull“ finansinio nusikaltimo rūšimis ir pastebėjus jog skirtingi autoriai aprašo „Rug pull“ tipologiją skirtingai buvo nuspręsta apibendrinti šių autorių pateikiamus „Rug pull“ tipus. Taigi, susisteminus informaciją identifikuota, kad „Rug pull“ finansinis nusikaltimas gali būti susiskirstomas į tris tipus, remiantis Sharma ir kt. (2024): švelnųjį „Rug pull“, kuomet žetono kūrėjai pasisavinę investuotojų lėšas nedingsta ir palieka žetoną rinkoje, sunkųjį „Rug pull“, kuomet žetono kūrėjai pasisavinę investuotojų lėšas – pradingsta ir

nebereguoja ir pasikartojantis „Rug pull“, kuomet tas pats adresas (žetono kūrėjas) sukuria kelis žetonus, susijusius su „Rug pull“ nusikalstama veika. Taip pat nustatyta, kad pats finansinis nusikaltimas „Rug pull“ gali įvykti trejomis kryptimis, remiantis Chainalysis (2024), Sun ir kt. (2024), Zhou ir kt. (2024) autoriais. Pirmasis kryptis - apribojant žetonų pardavimą, kuomet žetono kūrėjas užprogramuoja žetoną arba nustato žetono pardavimo laiką, kas lemia kad abiem atvejais investuotojas praranda teisę parduoti žetoną. Antrąja kryptimi galima būtų įvardinti staigų likvidumo pašalinimą, kas lemia kainos kritimą. Likvidumas yra pašalinamas tuomet, kai kaina pasiekia aukščiausią tašką arba žetono kūrėjas pakeičia piniginių likutį. Galiausiai tai lemia kainos kritimą, o žetonai tampa beverčiais. Paskutinė, trečioji kryptis – kainos išpūtimas ir žetono pardavimas, kurios metu, žiniasklaidos ir socialinės medijos pagalba, išpučiama žetono kaina ir žetono kainai pasiekus piką, jis yra parduodamas žetonų kūrėjų, taip paliekant žetonus beverčiais. Grafinė „Rug pull“ tipologijos vizualizacija pateikiama 2 paveiksle.

2 paveikslas

„Rug pull“ finansinio nusikaltimo tipologija



Šaltinis: sudarytas autorės, remiantis Chainalysis (2024), Sharma ir kt. (2024), Sun ir kt. (2024), Zhou BNRist ir kt. (2024)

Išnagrinėjus mokslinę literatūrą, nustatyta, kad „Rug pull“ yra vienas žiauriausių decentralizuotų finansų finansinių nusikaltimų. Teigiama, kad „Rug pull“ yra viena iš žalingiausių skaitmeninių valiutų sukčiavimo atvejų, kuris padaro įtaką ne tik individualiems investuotojams, bet ir stipriai mažina pasitikėjimą decentralizuotų finansų sektoriumi (Chainalysis, 2022). Taip pat moksliniuose straipsniuose nurodoma, kad po 2020 metais išpopuliarėjusių decentralizuotų finansų ir nepakeičiamųjų žetonų 2021 metais, „Rug pull“ tapo vienas iš pagrindinių finansinių nusikaltimų schemų, atsižvelgiant į pasisavintų lėšų kiekį bei nusikaltimų dažnumą (Crystal Blockchain’s

Analytics Team, 2023; Sharma ir kt., 2024; Stangl ir Neumann, 2024). Taip pat identifikuota, kad kol kas nėra sukurto metodo, kaip užkirsti kelią „Rug pull“ finansinio nusikaltimo įvykimui (Cernera ir kt., 2022). Vienas iš žinomiausių sukčiavimo „Rug pull“ atvejų yra su „SQUID“ moneta, kurio metu šių monetų kaina per kelias savaites išaugo daugiau nei keturiasdešimt tūkstančių procentų. Investuotojai pastebėję išaugusias kainas suskubo parduoti savo turimas „SQUID“ monetas, tačiau paaiškėjo, kad pardavimo teisę turėjo tik šios virtualios valiutos kūrėjai. Virtualios valiutos kūrėjai išmaniųjų sutarčių pagalba apribojo visus „SQUID“ valiutos turėtojus tik jos pirkimu, bet ne pardavimu. „SQUID“ valiutos kūrėjams išsigyrinus lėšas, virtualios valiutos kaina nukrito iki mažiau nei cento (SharkTeam, 2021). Kitas „Rug pull“ nusikalstamos veikos atvejis, kurio metu buvo pasisavinta 2 milijardai JAV dolerių, yra susijęs su „Thodex“ virtualių valiutų birža, kuri dingo iš rinkos 2021 metų balandžio mėnesį. Šios biržos savininkas viešai paskelbė, kad „Thodex“ veiklą turėjo nutraukti, kad apsaugotų investuotojų lėšas, tačiau paaiškėjo, kad tokiu principu buvo įvykdyta, ne kas kita kaip „Rug pull“. „Thodex“ savininkui bei visoms susijusioms šalims, kurios prisidėjo prie šios nusikalstamos veikos, siekiama skirti laisvės atėmimo bausmę iki gyvos galvos, nes nusikaltimo aukomis tapo daugiau nei 2000 asmenų. Šis „Rug pull“ nusikaltimas laikomas didžiausiu 2021 metų nusikaltimu (Botha ir kt., 2023; Chainalysis, 2022). Dar vienas, laikomas antruoju didžiausiu, pagal pasisavintų lėšų dydį, „Rug pull“ nusikaltimų atvejis yra susijęs su „AnubisDAO“. Šis projektas reklamavosi kaip alternatyva, kuri teiks laisvai plaukiojančią, decentralizuotą valiutą. Atkreiptinas dėmesys, kad „AnubisDAO“ projektas neturėjo sukurtos internetinės svetainės, ataskaitos, kuri aprašo šį naująjį projektą (angl. *white paper*). Šis projektas sulaukė didžiulio susidomėjimo ir mažiau nei per parą surinko daugiau nei 58 milijonus JAV dolerių vertų virtualių valiutų. Praėjus 20-čiai valandų po lėšų surinkimo žetono kūrėjai, persivedė likvidumo lėšas į savo privačias pinigines, kas lėmė žetono kainos kritimą iki nulio, tai reiškia, kad investuotojai prarado visas savo suinvestuotas lėšas (Botha ir kt., 2023; Chainalysis, 2022). Chainalysis (2022) teigimu, „AnubisDAO“ yra geras pavyzdys, kaip svarbu yra įvertinti ar investuoti naujus žetonus, jeigu jiems nebuvo atliktas kodo auditas.

Dar viena finansinių nusikaltimų rūšis yra greitųjų paskolų (angl. *flash loans*) atakos. Decentralizuotuose finansuose greitoji paskola yra apibūdinama kaip virtualios valiutos pasiskolinimas ir grąžinimas per tą patį bloko grandinės sandorį nenaudojant savo lėšų kaip užstato. Išpuoliai yra vykdomi remiantis greitųjų paskolų teikiamu likvidumu, nes nusikalstama veikla užsiimantiems asmenims suteikiama galimybė išnaudoti išmaniosios sutarties pažeidžiamumą,

manipuliuoti virtualios valiutos kainomis ar neteisėtai pasisavinti protokolo lėšas (Aramonte Sirio ir kt., 2021).

Išanalizavus finansinius nusikaltimus, kurie vyksta pačiose decentralizuotų finansų rinkose, svarbu atkreipti dėmesį ir į tai, kad finansiniai nusikaltimai gali būti susiję virtualiomis valiutomis, tačiau nevykti pačiose blokų grandinėse. Toliau pateikiami finansiniai nusikaltimai, kuriems įgyvendinti pasinaudojama virtualių valiutų erdve.

Vienas iš tokių finansinių nusikaltimų yra išpirkos reikalaujanti kenkėjiška programa (angl. *Ransomware*). Tai yra kenkėjiška programa, kuri nelegaliu būdu įsilaužia į fizinio ar juridinio asmens kompiuterį, kompiuterių sistemą, serverius, užšifruoja asmeniui svarbius dokumentus, panaikina prieigą prie atitinkamų programų, internetinių puslapių, pradeda kasti virtualią valiutą naudojantis asmens ar įmonės kompiuteriais ir galiausiai prašo išpirkos, kad asmenims būtų sugrąžinta prieiga prie norimų dokumentų ar duomenų. Taip pat, tokia kenkėjiška programa gali sudaryti visą tinklą kompiuterių skaičiuojant juos tūkstančiais ar net dešimtimis tūkstančių. Minima kenkėjiška programa į kompiuterį gali patekti įvairiais būdais: per apgaulingas internetines nuorodas, kurios siunčiamos elektroniniais paštais naudojant socialinę inžineriją, per netikrus internetinius puslapius, atsisiųstas programas, o ypač per nelegaliai atsisiųstas programas, tiesiogiai tinklu ar prisijungus prie atviro tinko viešojoje erdvėje, per namų internetą, kuris yra gan atvirai prieinamas iš išorės bei daugybės kitų būdų, kurie priklauso nuo įsilaužėlio sukurto kodo ar vaizduotės bei sugebėjimų. Nusikaltėliai dažnai iš anksto naudodami atvirus šaltinius ar atvirais šaltiniais prieinama informacija pasidomi apie įmonę ir jų vidinę infrastruktūrą. Atsižvelgiant į įmonės įrangos saugumą ar personalo kompiuterinį raštingumą yra pasirenkama koku būdu kompiuteriai ar įmonės serveriai bus infekuojami – tiesiogiai tinklu ar naudojantis socialine inžinerija per neišsilavinusius asmenis. Infekavus kompiuterius bei užblokavus duomenis ir prieigas prie jų, dažnu atveju, nusikaltėliai kaip išpirkos mokėjimo būdą pasirenka - virtualias valiutas, tokias kaip Bitkoinas ar Eteris, atsižvelgiant į tai, kad virtualių valiutų sandoriai yra pseudoniminiai (lėšų gavėjo atsekamumo nebuvimas), sandoriai įvyksta greitai, nes jiems patvirtinti nereikia tarpininkų paslaugų, tai yra, bankų, o ir pinigų gavimas yra tarptautinis, tai reiškia, kad šioms neteisėtoms operacijoms įvykti nereikalinga ta pati dviejų asmenų lokacija (Aurangzeb ir kt., 2017; Hoseini, 2022; Simoiu ir kt., 2017). Chainalysis (2022) virtualių valiutų nusikaltimų ataskaitoje yra nurodoma, kad 2020 metais buvo atlikta apie 692 milijonų JAV dolerių, o 2021 metais daugiau nei 602 milijonai JAV dolerių pervedimų, kurie buvo susiję su išpirkos reikalaujančiu kenkėjiškos programos finansiniu nusikaltimu. Nustatyta, kad vieno pervedimo vidurkis, susijęs su išpirkos reikalaujančiu kenkėjiškos programos finansiniu nusikaltimu, 2020

metais siekė 88 tūkstančius JAV dolerių, o 2021 metais – 118 tūkstančius JAV dolerių. Teigiama, kad vidutinį pervedimų dydį išaugino nukreiptas nusikaltėlių dėmesys nebe į pavienius asmenis, o didelis apyvartas turinčias organizacijas (Chainalysis, 2022).

Kitas finansinių nusikaltimų tipas yra terorizmo finansavimas. Terorizmo finansavimas apibrėžiamas kaip procesas, kurio metu lėšos yra surenkamos ir kuriomis yra remiamos teroristinės veiklos, teroristinės grupuotės ar pavieniai asmenys. Pirminis pinigų gavimas gali apimti tiek legalius, tiek nelegalius pinigų šaltinius, tačiau galutinis finansavimas yra susijęs su neteisėta veikla (FATF, 2019). Virtualių valiutų erdvė nusikalstama veikla užsiimantiems asmenims yra patogi dėl kelių aspektų. Vienas tokių aspektų yra anonimiškumas, kuris leidžia nusikaltėliams atlikti virtualių valiutų pervedimus neatskleidus savo tapatybės. Nors sandoriai yra viešai skelbiami blokų grandinėse, tačiau nusikaltimą vykdantys asmenys, naudodami papildomas priemones ir programas, gali paslėpti savo tikrąją tapatybę. Kaip ir išpirkos reikalaujančios kenkėjiškos programos finansinis nusikaltimas, terorizmo finansavimas naudoja virtualių valiutų erdvę dėl greito ir lengvo pinigų pervedimo, kuris nereikalauja tarpininkų patvirtinimo atlikti sandorį. Taip pat terorizmo finansavimas virtualiomis valiutomis gali vykti tamsiajame tinkle, kuriame yra parduodamos teroristinei veiklai naudojamos priemonės, tokios kaip ginklai, suklastoti dokumentai, kurių pagalba nusikaltėliai gali paslėpti savo tikrąją tapatybę. Jog sandoriai būtų kuo mažiau atsekami, nusikalstama veikla užsiimantys asmenys gali naudoti „maišytuvus“, kurie padėtų jiems paslėpti tikrąją pinigų kilmę (Congressional Research Service, 2024; Egmont group, 2023). Tačiau įsitraukus teisėsaugos institucijoms, galima atrasti atvejų, kuomet teroristinė veikla yra sustabdoma. Pavyzdžiui, 2019 metais ir 2020 metais federalinių tyrimų biuras ir kitos teisėsaugos institucijos konfiskavo daugiau nei 1 milijoną JAV dolerių virtualios valiutos formatu iš grupuotės „AI-Qaeda“, kurie savo veiklą reklamavo tokiose programose kaip „Telegram“ ir „Facebook“. Kitas pažymėtinas atvejis, kuris buvo pirmasis skaitmeninės valiutos, kuri susijusi su terorizmo finansavimu, konfiskavimas, yra susijęs su „Hamas“ nusikalstama grupuote. Izraelio Nacionalinis kovos su terorizmu finansavimo biuras (angl. *Israel's National Bureau for Counter Terror Financing (NBCTF)*) 2021 metų birželio 30 dieną spaudos konferencijoje paskelbė, kad buvo konfiskuota virtuali valiuta, padalinta per kelias asmenų pinigines, susijusi su „Hamas“ nusikalstamos veikos rėmimu. Tyrimo metu buvo konfiskuotos įvairios skaitmeninės valiutos tokios kaip Bitkoinas, Eteris, „Tether“ (Chainalysis, 2022; Congressional Research Service, 2024).

Dar vienas paplitęs finansinis nusikaltimas, tačiau neišsiskiriantis didelėmis sumomis, yra romantinis sukčiavimas (angl. *romance scam*) arba dabartiniais laikais žinomas kaip „kiaulės skerdimo“ (angl. *pig butchering*) sukčiavimas. Šį pavadinimą sugalvojo nusikaltėliai, kurie savo

aukas vadina „kiaulėmis“, nes aukos yra „penimos“ iki tol, kol jos gali būti „paskerdžiamos“ (Acharya ir Holz, 2024). Taigi, romantinis sukčiavimas apibrėžiamas kaip sukčiavimo schema, kurios metu nusikalstama veika užsiimantis asmuo apsimeta, kad ieško romantinio ryšio ir emocinio manipuliavimo metu išvilioja pinigus iš aukos. Ryšys tarp aukos ir apgaviko yra užmezgamas įvairiais internetiniais kanalais – per socialinius tinklus, pažinčių svetaines. Kuomet nusikaltėlis užmezga romantinį ryšį su auka, jis pateikia aukai įtikinamą priežastį, kodėl jam yra reikalinga tam tikra pinigų suma, ir kaip pinigų pervedimo būdą aukai pasiūlo virtualių valiutų erdvę. Skaitmenines valiutas kaip pinigų alternatyvą nusikaltėliai, susiję su romantiniu sukčiavimu, renkasi dėl tų pačių priežasčių kaip ir buvo minėta anksčiau. Viena iš priežasčių yra anonimiškumas, nes nusikaltėlis tiek sukčiavimo metu, tiek virtualių valiutų sandorių metu neatskleidžia savo tapatybės, todėl atsekamumas yra beveik neįmanomas. Taip pat greitas sandorio įvykimas, be tarpininkų, irgi lemia tai, kodėl nusikaltėliai išvilioja pinigus virtualių valiutų forma, nes asmuo pakliuvęs į tokią situaciją neturi laiko susivokti, jog jis tapo sukčiavimo auka, o sandorio atšaukimas šiuo atveju nėra galimas (Acharya ir Holz, 2024). Chainalysis (2022) virtualių valiutų nusikaltimų ataskaitoje yra nurodoma, kad nusikaltimų, susijusių su romantiniais sukčiavimais, kiekis išaugo 85 kartais nuo 2020 metų iki 2023 metų.

Taigi, siekiant atskirti ir suprasti, kuris sandoris yra susijęs su nusikalstama veikla, svarbu suprasti kokie yra įtartinų sandorių bruožai. Įtartinas pervedimas apibrėžiamas kaip finansinė operacija, kuri yra susijusi su nusikalstamos veiklos metu gautomis lėšomis (Financial Intelligence Unit, 2022). Decentralizuotų finansų ekosistemoje įtartinai sandoriai gali būti siejami su neįprastu vieno pervedimo dydžiu, dažnesniu sandorių kiekiu per ganėtinai trumpą laiko tarpą, gautų lėšų padalinimu per skirtingas pinigines ar maišymo programinių įrangų naudojimas tolimesnėms finansinėms operacijoms atlikti (Elliptic, 2020). Atsižvelgiant į tai, kad nagrinėjant mokslinę literatūrą buvo nustatyta, jog „Rug pull“ po decentralizuotų finansų išpopuliarėjimo tapo viena iš žiauriausių ir pagrindinių nusikalstamos veikos schemų iki pat šių dienų, taip pat šio nusikaltimo aukos praranda negrįžtamai savo lėšas, o ir būdų kaip laiku užkirsti kelią „Rug pull“ finansiniam nusikaltimui nėra. Vertinant visus šiuos išvardintus aspektus apie „Rug pull“ finansinį nusikaltimą buvo nuspręsta detaliau nagrinėti šį ir šiomis dienomis aktualų finansinį nusikaltimą.

1.4 „Rug pull“ decentralizuotų finansų nusikaltimo savybės ir atpažinimas

Taigi, atsižvelgus į „Rug pull“ finansinio nusikaltimo decentralizuotoje finansų sistemoje nagrinėjimo aktualumą, toliau yra analizuojami kokie moksliniai tyrimai buvo atlikti atsižvelgus į

„Rug pull“. Atkreiptinas dėmesys, kad „Rug pull“ finansinio nusikaltimo tyrimų atlikta ganėtinai mažai, nes tai nauja finansinių nusikaltimų sfera. Cernera ir kt. (2022) autoriai atliko mokslinį tyrimą susijusį su virtualiais žetonais ir likvidumo fondais esančiais Eterio bei „BNB Smart Chain“ blokų grandinėse. Šio tyrimo tikslas buvo palyginti žetonų bei tų žetonų kūrėjų gyvavimo trukmę. Galiausiai buvo sukurtas robotas, kuris turėjo pirkti žetonus, tačiau jis tapo pačios nagrinėjamos temos auka, tai yra, įsigijo žetonų, susijusių su „Rug pull“. Taip pat savo moksliniame darbe pabrėžia, kad „Rug pull“ yra nauja ir mažai išnagrinėta tema, todėl iki šiol nėra pateikta būdų, kuriais būtų galima išvengti „Rug pull“ finansinio nusikaltimo. Xia ir kt. (2021) savo moksliniame darbe analizuoja žetonus, susijusius su „Rug pull“ finansiniu nusikaltimu, „Uniswap V2“ likvidumo fonde. Tyrimui atlikti duomenys buvo surinkti iš internetinės svetainės „The Graph“ (The Graph, 2024), tačiau šiuo atveju, siekiant surinkti duomenis iš šio puslapio privalu žinoti - konkretų žetoną (žetono adresą). Šio tyrimo autorius identifikuoja, kad sukurtas modelis aptikti „Rug pull“ nusikaltimus, remiasi tik istoriniais duomenimis. Taip pat atliekant išsamią mokslinių tyrimų analizę, pastebėta, kad yra nagrinėjami realūs įvykė „Rug pull“ atvejai. Rahmanda (2024) moksliniame straipsnyje atliekama teisinės literatūros apžvalga, kurios metu apžvelgiama kaip į „Rug pull“ atvejus reaguoja teisinė aplinka. Zhou ir kt. (2024) moksliniame tyrime taip pat tiria įvykusius „Rug pull“ atvejus, kurių dėka investuotojai patyrė didelius nuostolius. Šio tyrimo metu duomenys buvo surinkti remiantis finansinių nusikaltimų analizės ataskaitomis bei pranešimais, tokiais kaip Chainalysis (2023). Tyrimo metu buvo identifiкуotos keturios „Rug pull“ rizikos, nusakančios kas galėtų parodyti, kad žetonas yra susijęs su „Rug pull“ nusikaltimu (jos analizuojamos 1.3 magistro darbo skyriuje), tačiau tyrime nėra nurodyta, kaip šias rizikas gali patikrinti investuotojas, kad neinvestuotų pinigų, į su „Rug pull“ nusikalstama veikla susijusį žetoną. Taigi, išnagrinėjus mokslinius tyrimus, nustatyta, kad tyrimai yra atlikti tik koncentruojantis į „Rug pull“ atvejus, tačiau nėra analizuojama, kas lemia, jog „Rug pull“ finansiniai nusikaltimai įvyksta. Todėl šio magistro darbo tyrime siekiama atskleisti, kad „Rug pull“ finansiniams nusikaltimams turi įtakos virtualių valiutų kainos, konkrečiai analizuojant Eterio pagrindu sukurtus žetonus. Išnagrinėjus mokslinę literatūrą ir juose nurodomus tyrimus, buvo pastebėta, kad viešuose internetiniuose puslapiuose, kuriuose pateikiama informacija susijusi su blokų grandinėmis, nėra galimybės atrinkti duomenų, kurie susiję su decentralizuotų finansų nusikalstama veikla, kaip ir buvo aprašyta analizuojant Xia ir kt. (2021) mokslinį tyrimą. Minimuose puslapiuose yra galimybė informaciją atrūšiuoti pagal adresus, žetonus, vardo korteles (angl. *name tags*), domenų pavadinimus, internetinius puslapius, tai reiškia, kad siekiant atrūšiuoti tokią informaciją, privalu žinoti adresus, žetonus ar kitus minėtus aspektus, pagal kuriuos galima būtų išrūšiuoti informaciją susijusią su

nusikalstama veika. Išnagrinėjus mokslinius šaltinius, Garin ir Gisin (2023) moksliniame straipsnyje pastebėtas sukurtas internetinis puslapis, kuriame identifikuojami adresai, susiję su nusikalstama veika. Minimas puslapis vadinasi „BitcoinAbuse“, kurio analizuojamu laikotarpiu pavadinimas yra pakeistas į „Chainabuse“. Todėl tyrimui atlikti buvo analizuojami atvejai, pateikiami (Chainabuse, 2024). Išanalizavus mokslinius tyrimus ir atsižvelgus į tai, kad iki šiol nėra pateikta būdų, kuriais būtų galima išvengti „Rug pull“, taip pat atsižvelgus į tai, kad kuriami modeliai identifikuoja, jog įvyko „Rug pull“, remiantis tik istoriniais duomenis, ir atsižvelgus į tai, kad nors ir yra pateikiami „Rug pull“ rizikos faktoriai, kurie parodo, kad žetonas gali būti susijęs su „Rug pull“, tačiau nėra atskleidžiama kaip investuotojas žinodamas minėtus rizikos faktorius, gali pats pasitikrinti žetoną, trečiojoje magistro darbo dalyje nuspręsta sukurti modelį, kuriuo remiantis investuotojas galėtų pasitikrinti, kad žetonas yra susijęs su nusikalstama veika „Rug pull“.

Siekiant suprasti, kad žetonas yra susijęs su „Rug pull“ decentralizuotų finansų finansiniu nusikaltimu, buvo nuspręsta išnagrinėti mokslinius šaltinius ir nustatyti, kokie yra galimi „Rug pull“ „susijusio su žetonu, kriterijai. Pirmiausia, svarbu suprasti ar žetono kūrėjas yra žinomas ir ar žetoną reklamuojantys asmenys yra patikimi (Sharma ir kt., 2024). Kitas aspektas yra staigus kainos pakylimas. Žetono kūrėjai, siekdami gauti maksimalų neteisėtą pelną, yra suinteresuoti, kad jų sukurtas žetonas atrodytų patrauklus – dirbtinai išpučiama kaina atliekant žetonų pirkimus iš asmeninių piniginių (Huang ir kt., 2023). Chainalysis (2022) virtualių valiutų nusikaltimų ataskaitoje nurodoma, kad žetonas tapo populiarus ir buvo pasiektas susidomėjimas juo tuomet, kai asmenys, nesusiję su didžiausiais žetono turėtojais, įsigijo žetoną daugiau nei penkis kartus. Taip pat moksliniuose straipsniuose nurodoma, kad dažnu atveju „Rug pull“ yra atliekami per pirmąją žetono sukūrimo dieną. Cernera ir kt. (2022) moksliniame straipsnyje yra nurodoma, kad tyrimo metu buvo išsiaiškinta, jog 81,2 procentai sukurtų naujų žetonų, kurie buvo susiję su „Rug pull“ finansiniu nusikaltimu, egzistavo vieną dieną. Kitas aspektas, rodantis „Rug pull“ nusikalstamos veikos tikimybę, yra neužrakintas likvidumas. Neužrakintas likvidumas rodo, kad bet kuriuo momentu, žetono kūrėjai gali pasisavinti visas investuotojų lėšas. Nurodoma, kad likvidumas turi būti užrakintas ir galioti mažiausiai tris metus (Stangl ir Neumann, 2024; Sun ir kt., 2024; Xia ir kt., 2021). Taip pat yra moksliniuose šaltiniuose nurodoma, kad „Rug pull“ nusikaltimas gali pasireikšti ir tuomet kai yra nepakankamas likvidumas. Teigiama, kad nepakankamas likvidumas yra tuomet, kai likvidumas siekia mažiau nei 95 procentus (Stangl ir Neumann, 2024; Sun ir kt., 2024; Xia ir kt., 2021). Chainalysis (2022) virtualių valiutų nusikaltimų ataskaitoje yra taip pat identifikuojama, kad „Rug pull“ nusikaltimas įvyko tuomet, kai daugiau nei 70 procentų likvidumo buvo pašalinta iš likvidumo

fondo, o likęs likvidumas siekia 300 JAV dolerių ar net mažiau. Taip pat, kaip ir buvo minėta 1.3 magistro darbo dalyje, dar vienas būdas įsitikinti, kad žetonas gali būti susijęs su „Rug pull“ finansiniu nusikaltimu yra patikrinimas ar žetonu galima prekiauti, tai yra, įsigijus jį ar bus galimybė minėtą žetoną parduoti (Sun ir kt., 2024). Analizuojant mokslinę literatūrą taip pat pastebėta, kad žetonai susiję su nusikalstama veikla, pasižymi tokiais savybėmis kaip trumpalaikis prekybos ciklas, tai reiškia, kad operacijos susijusios su žetonu pagrinde įvyksta per pirmąsias žetono sukūrimo dienas. Taip pat žetonai kūrėjams duoda didelę grąžą, neskaitant investicijų, kuriomis siekiama padidinti žetono žinomumą ir patrauklumą (Jelesković, 2024).

Taigi, išnagrinėjus mokslinę literatūrą identifikuota, kad decentralizuoti finansai suteikia vartotojams ne tik didesnę finansų sistemos efektyvumą lankstumą, prieinamumą skirtingiems vartotojams bei skaidrumą, tačiau kaip ir tradiciniai finansai, patiria rizikas, tokias kaip finansinė rizika. Decentralizuotų finansų atveju finansinė rizika yra susijusi su dideliu nepastovumu, kurį lemia spekuliacijos ir daugėjantys įtartini sandoriai. Mokslinės literatūros analizės metu nustatyta, kad nusikalstamų atvejų skaičių didina – decentralizuotas veikimas, trūkstamas reguliavimas bei anonimiškumas. Taip pat buvo identifikuota, kad „Rug pull“ yra viena iš žalingiausių skaitmeninių valiutų sukčiavimo atvejų, kuris padaro įtaką ne tik individualiems investuotojams, bet ir stipriai mažina pasitikėjimą decentralizuotų finansų sektoriumi. Atsižvelgus į aukščiau minimus faktus ir taip pat atsižvelgus į tai, kad tik nuo dabar yra stiprinamas virtualių valiutų kontroliavimas, parodžius, kokie aspektai gali parodyti, kad žetonas yra susijęs „Rug pull“ finansiniu nusikaltimu, trečiojoje darbo dalyje yra analizuojami pervedimai į žetonus, susijusius su vienu iš finansinio nusikaltimo tipų „Rug pull“. Atsižvelgus į tai, kad sukčiavimas neįvyksta be operacijų, kurias atlieka aukos (investuotojai) ir į tai, kad Eteris yra labiausiai paplitusi žetonų kūrimo programinė įranga dėl joje egzistuojančios išmaniosios sutarties funkcijos, nuspręsta trečiojoje darbo dalyje palyginti Eterio kainas su pervedimų skaičiumi į žetonus, susijusius su nusikalstama veika „Rug pull“. Taip pat siekiant apsaugoti investuotojus nuo pinigų praradimo ir identifikavus, kad modelio, kuris pateiktų žingsnius kaip patikrinti ar žetonas nesusijęs su „Rug pull“ finansiniu nusikaltimu, nėra, trečiojoje magistro darbo dalyje yra sukuriamas modelis žingsnis po žingsnio ką daryti investuotojui, kuris nori patikrinti ar žetonas nesusijęs su „Rug pull“ finansiniu nusikaltimu.

2. „RUG PULL“ FINANSINIO NUSIKALTIMO VERTINIMO METODOLOGIJA

Antrojoje magistro darbo dalyje yra pateikiama tyrimo metodologija, kuria remiantis atlikta vienos iš žinomiausių virtualios valiutos – Eterio – kainų ir decentralizuotų finansų finansinių nusikaltimų palyginimas, kuris buvo atliktas lyginamosios analizės principu. Išanalizavus decentralizuotų finansų bruožus, parodžius skirtingus galimus decentralizuotų finansų nusikalstamos veiklos tipus, atskleidus, kad viena iš finansinių nusikaltimo kategorijų „Rug pull“ yra susijusi su rimtais investuotojų lėšų praradimais ir siekiant parodyti, kad pagrindinių virtualių valiutų kainos daro įtaką į Eterio pagrindu sukurtų žetonų, kurie susiję su „Rug pull“ finansiniu nusikaltimu, pervedimų skaičiui, inferencinės statistikos metodo pagalba, buvo nuspręsta parodyti, kad – Eterio kainoms kintant (didėjant arba mažėjant) įvyksta daugiau „Rug pull“ finansinių nusikaltimų, susijusių su virtualiomis valiutomis. Patvirtinus hipotezę, yra sukuriamas modelis, kuris padės išvengti pinigų praradimo investuojant į virtualius žetonus susijusias su nusikalstama veikla (žr. 3 pav.).

3 paveikslas

Tyrimų išdėstymo pagal darbo eigą seka

Virtualių valiutų ir finansinių nusikaltimų palyginimas

Eterio kainų ir į Eterio pagrindu sukurtų žetonų, kurie susiję su „Rug pull“ finansiniu nusikaltimu, pervedimų skaičiaus palyginimas

Sukurto modelio, kuris padės išvengti įsitraukimo į "Rug pull" nusikalstamą veiklą, apibendrinimas

Šaltinis: sudarytas autorės

Tyrimo tikslas – patvirtinus hipotezę, jog Eterio kainų kitimas lemia į Eterio pagrindu sukurtų žetonų, kurie susiję su „Rug pull“ finansiniu nusikaltimu, pervedimų skaičių padidėjimą, sukurti modelį, kuris padėtų investuotojams apsisaugoti įsitraukimo į "Rug pull" nusikalstamą veiklą.

Tyrimo objektas – į Eterio pagrindu sukurtų nestabilių monetų, kurios susijusios su „Rug pull“ finansiniu nusikaltimu, pervedimų skaičius.

Tyrimo uždaviniai:

1. Palyginti Eterio kainų kitimus su decentralizuotų finansų finansinių nusikaltimų skaičiumi.
2. Išanalizuoti į Eterio pagrindu sukurtų žetonų, susijusių su „Rug pull“ finansiniu nusikaltimu, pervedimų skaičių.
3. Sukurti modelį, kuriuo galėtų remtis investuotojai, kad įsitikinti žetono patikimumu.

2.1 Eterio kainų ir finansinių nusikaltimų lyginamoji analizė

Siekiant atlikti Eterio kainų kitimo ir finansinių nusikaltimų, susijusių su virtualiomis valiutomis, skaičiaus palyginimą, yra pasirenkamas lyginamosios (komparatyvinis) analizės metodas, kuris apima kokybinio tyrimo surinktus duomenis. Šis metodas yra priskiriamas prie neeksperimentinių tyrimo būdų. Lyginamasis metodas apibrėžiamas kaip atvejų ir jų savybių, kurios įvardinamos kaip lyginamieji objektai, sociologinis tyrimas. Komparatyvinis metodas taikomas tais atvejais, kai tyrimui skirtų atvejų skaičius yra per mažas, kad būtų galima naudoti statistinius metodus. Šį metodą galima pradėti naudoti tuomet, kai yra bent du tiriami atvejai (Gudavičiūtė, 2021; Zenonas, 2008).

Šia lyginamąja analize siekiama parodyti, kad Eterio kainos kylimas bei kritimas turi įtakos finansinių nusikaltimų skaičiaus didėjimui. Lyginamajai analizei atlikti buvo naudojami duomenys iš tokių viešai prieinamų šaltinių kaip, internetinio puslapio CoinGecko (2024) bei ataskaitos Chainalysis (2024). Tam, kad būtų lengviau apsibrėžti bei analizuoti pateiktus duomenis, virtualių valiutų gyvavimas ir vertingumas buvo suskirstytas į penkis etapus – pirmasis etapas – pradžia (nuo 2014 metų iki pat 2020 metų galo), antrasis etapas – pirmasis pakilimas (nuo 2021 metų iki 2021 metų pabaigos), trečiasis etapas – pirmasis kritimas (nuo 2021 metų galo iki 2022 metų vidurio), ketvirtasis etapas – stagnacija (nuo 2022 metų vidurio iki 2024 metų pradžios) ir penktasis etapas – antrasis pakilimas (nuo 2024 metų pradžios iki šių dienų). Etapai atvaizduojami pažymint atitinkamus laikotarpius spalvomis: pirmasis etapas – pažymėta žaliu stačiakampiu, antrasis etapas pažymėtas oranžiniu stačiakampiu, trečiasis etapas – pažymėtas geltonu stačiakampiu, ketvirtasis etapas – pažymėtas mėlynu stačiakampiu ir penktasis etapas – pažymėtas raudonu stačiakampiu. Siekiant atvaizduoti tinkamai, kad Eterio kainų pasikeitimas koreliuoja su finansinių nusikaltimų skaičiumi, informacija pateikiama paveikslų forma. Įrodžius, kad Eterio kainų pasikeitimas koreliuoja su finansinių nusikaltimų skaičiumi, o taip pat ir „Rug pull“ finansinio nusikaltimo kiekiams turi įtakos

Eterio kaina, toliau yra atliekamas Eterio kainos palyginimas su pervedimais, kurie buvo atlikti į žetonus, susijusius su „Rug pull“ nusikalstama veikla.

2.2 Eterio kainų ir pervedimų į žetonus, susijusius su „Rug pull“, atvejo analizė bei modelio kūrimas

Siekiant parodyti, kad virtualių valiutų kainų kilimas bei kritimas daro įtaką „Rug pull“ nusikalstamos veiklos padidėjimui, pirmiausia buvo atliekamas pervedimų skaičiaus į Eterio pagrindu sukurtus žetonus, susijusius su „Rug pull“ finansiniu nusikaltimu vertinimas, remiantis inferencine statistika, kuri yra vienas iš kiekybinės analizės būdų tyrimui gautiems duomenims nagrinėti. Pastaroji statistika (statistinės išvados), gali būti apibrėžiama kaip tyrimas, nagrinėjantis tam tikrą imtį respondentų, o gauti rezultatai gali būti pritaikomi populiacijai visa apimtimi (Gudavičiūtė, 2021; LiDA, 2020). Statistinės išvados metodas buvo pasirinktas atlikti tyrimui atsižvelgiant į tai, kad jos leidžia suformuluoti išvadas iškeltam tikslui, tai yra, hipotezės patikrinimui (Gudavičiūtė, 2021; Kern, 2013). Hipotezės tikrinimo procesas yra padalijamas į keturis nuoseklius etapus (žr. 4 pav.).

4 paveikslas

Statistinės hipotezės patikrinimo etapai



Šaltinis: sudarytas autorės, remiantis Gudavičiūtė (2021), LiDA (2020)

Tyrimo hipotezė, apibūdinama kaip tikslus problemos teiginys, kuris gali būti patikrinamas tiesiogiai empiriniu tyrimu, tai yra, tyrimu, kuri išvados yra pagrįstos gautais įrodymais (Lazar ir kt., 2017). Parodžius, kad virtualių valiutų kainų kitimas daro įtaką decentralizuotuose finansuose vykstantiems finansiniams nusikaltimams, atsižvelgus į tai, kad investuotojai įsitraukę į „Rug pull“ nusikalstamą veiklą negrįžtamai praranda savo lėšas, ir identifikavus, kad į žetonus, susijusius su sukčiavimu pervedimai, atliekami didžiausia apimti pirmosiomis žetono sukūrimo dienomis, suformuluojama hipotezė ir teigiama, kad Eterio kainos kylimas ar kritimas lemia išaugusį sukurtų žetonų, susijusių su „Rug pull“, kiekį, o tai reiškia, kad pervedimų skaičius koreliuoja atvirkščiai

(kuomet Eterio kaina kyla arba krenta, pervedimų skaičius į atskirą žetoną, susijusį su „Rug pull“ nusikalstama veika, mažėja):

$$\begin{cases} H_0: \text{Eterio kainos žymus pokytis lemia pervedimų skaičiaus } \textit{mažėjimą} \text{ į daugumą žetonų, susijusių} \\ \text{su „Rug pull“ nusikaltimu} \\ H_1: \text{Eterio kainos žymus pokytis lemia pervedimų skaičiaus } \textit{didėjimą} \text{ į daugumą žetonų, susijusių} \\ \text{su „Rug pull“ nusikaltimu} \end{cases} \quad (1)$$

Antrajame etape pateikiama statistinė hipotezė, kuri apibūdinama kaip teiginys apie populiacijos prigimtį, kuris išreiškiamas skaitine išraiška (Čekanavičius ir Murauskas, 2001; Gudavičiūtė, 2021; Ross, 2017):

$$\begin{cases} H_0: p \geq \mu \\ H_1: p < \mu \end{cases} \quad (2)$$

kur:

H_0 – sąlyga patvirtinanti hipotezę;

H_1 – sąlyga nepatvirtinanti hipotezės;

p – žetonų, susijusių su „Rug pull“ nusikalstama veika, skaičius, į kuriuos atliekami investuotojų pervedimai, statistiškai reikšmingai neigiamai koreliuoja su Eterio virtualios valiutos kainos augimu ir teigiamai koreliuoja su Eterio kainos kritimu;

μ - žetonų, susijusių su „Rug pull“ nusikalstama veika, skaičius, į kuriuos atliekami investuotojų pervedimai, turėtų statistiškai reikšmingai neigiamai koreliuoti su Eterio virtualios valiutos kainos augimu ir teigiamai koreliuoti su Eterio kainos kritimu.

Norint šiame etape išreikšti statistinę hipotezę skaitine išraiška, būtina nustatyti duomenų analizės imties dydį, kuris padės pagrįsti tyrimo patikimumą. Apskaičiuoti imties dydžiui yra pasitelkiama Paniotto formulė, kurią pateikia Ruževičius (2016):

$$n = \frac{1}{\Delta^2 + \frac{1}{N}} \quad (3)$$

kur:

n – imties dydis;

Δ – ribinė atrankos paklaida (nuo 5 procentų iki 10 procentų socialiniuose moksluose galima naudoti paklaida);

N – tyrėjo numatyta visuma.

Kaip teigiama moksliniame šaltinyje Vaghela (2024) atsižvelgus į ribotą imties prieinamumą bei tyrimo pobūdį socialiniuose moksluose galima naudoti 90 procentų pasiklivimo lygį, tai yra, 10 procentų ribinę atrankos paklaidą. Atsižvelgus į tai, kad peržiūrėjus visus pranešimus susijusius su „Rug pull“ nusikaltimu ir atmetus netinkamus duomenis, tyrimui atlikti buvo galima pasinaudoti tik 146 sukurtų žetonų, susijusių su „Rug pull“ nusikaltama veikla, duomenimis, pasirenkamas 10 procentų imties paklaidos dydis. Taigi tam, kad parodyti, jog tyrimas yra patikimas, buvo apskaičiuotas 85 žetonų, kurie susiję su finansiniu nusikaltimu „Rug pull“, imties dydis:

$$n = \frac{1}{0,1^2 + \frac{1}{583}} \sim 85 \quad (5)$$

kur:

n – imties dydis;

Δ – 0,1;

N – 2024 metų gruodžio 2 dienos Chainabuse (2024) duomenimis 583 pranešimai susiję su „Rug pull“ nusikalstamos veikos atvejais.

Taigi, norint parodyti, jog žetonų, susijusių su „Rug pull“ nusikalstama veika, skaičius, į kuriuos atliekami investuotojų pervedimai, statistiškai reikšmingai koreliuoja su Eterio virtualios valiutos žymiais kitimais ir nustatius, kad imties dydis turėtų apimti 85 žetonus, susijusius su „Rug pull“ nusikalstama veika, daroma išvada, jog anksčiau minėta hipotezė patvirtinama tuomet, kai daugiau nei pusės į žetonus, susijusius su „Rug pull“ nusikalstama veikla, pervedimų skaičius mažėjo, kuomet Eterio kainos kilo ir mažėjo kuomet Eterio kaina krito. Žemiau pateikiama statistinė hipotezė:

$$\begin{cases} H_0: p \geq 43 \\ H_1: p < 43 \end{cases} \quad (6)$$

Duomenų analizės etapu (žr. 3 pav.) atliekama surinktų duomenų apie pervedimus į žetonus, susijusius su nusikalstama veika – „Rug pull“. Kaip ir buvo minėta anksčiau, peržiūrėti visi pranešimai, kurie susiję su vienu iš finansinių nusikaltimų kategorijų – „Rug pull“ ir atsižvelgus į atrinktus pranešimus, iš viso buvo paimta 146 žetonų, kurie susiję su „Rug pull“, operacijos (žr. 1 priedą).

Siekiant parodyti, kad egzistuoja ryšys tarp Eterio kainų kitimo ir pervedimų skaičiaus, kurie atliekami į su „Rug pull“ nusikalstama veika sukurtus žetonus, atliekamas T.testas. Pasirenkamas T.testas, nes tyrimo metu norime įvertinti ar tarp dviejų kintamųjų, tai yra pervedimų skaičiaus į žetonus, susijusius su nusikalstama veikla „Rug pull“, ir Eterio kainų, egzistuoja ne atsitiktinis ryšys,

tai reiškia, kad siekiama parodyti, jog Eterio kainų kylimas ar kritimas daro įtaką pervedimų skaičiaus mažėjimui į žetonus, susijusius su „Rug pull“ nusikalstama veikla. Atkreipiamas dėmesys, kad skaičiuojamas dvipusis T.testas, nes yra tikimasi, kad koreliacija tarp anksčiau paminėtų kintamųjų gali būti tiek teigiama, tiek neigiama (Allua ir Thompson, 2009; Marshall ir Jonker, 2011).

$$t = \frac{r\sqrt{n-2}}{\sqrt{1-r^2}} \quad (7)$$

kur:

t – T.testo apskaičiuota reikšmė;

r – koreliacijos koeficientas apskaičiuotas tarp pervedimų skaičiaus į žetonus, susijusius su nusikalstama veikla „Rug pull“, ir Eterio kainų;

n – pervedimų skaičius į žetonus, susijusius su nusikalstama veikla „Rug pull“.

Tam kad išsiaiškinti ar egzistuoja reikšmingas ryšys, papildomai apskaičiuota kritinė t-reikšmė ir palyginta su T.testo apskaičiuota reikšme (T.testo reikšmė turi būti didesnė nei kritinė t-reikšmė). Kritinė t-reikšmė, naudojama teiginio ar hipotezės pagrįstumui patikrinti, šiuo atveju padės įvertinti ar ryšys tarp pervedimų skaičiaus į žetonus, susijusius su nusikalstama veikla „Rug pull“, ir Eterio kainų yra statistiškai reikšmingas. Kritinė t-reikšmė gaunama iš t skirstinio, kuris yra tikimybių skirstinio tipas. Tikimybių skirstinys apibūdinamas kaip grafikas, rodantis visus galimus konkrečios situacijos padarinius ir kiekvieno rezultato tikimybę (Elst, 2019). Šiuo atveju yra pasinaudojama Microsoft Excel 2016 programinės įrangos teikiama formule, kuri apskaičiuoja kritinę t-reikšmę:

$$\text{kritinė t-reikšmė} = T.INV.2T(\text{reikšmingumo lygis, laisvės laipsniai}) \quad (8)$$

Kur:

Reikšmingumo lygis – 0,05 (Elst, 2019);

Laisvės laipsniai - pervedimų skaičius į žetonus, susijusius su nusikalstama veikla „Rug pull“ minus 2.

Apskaičiuojant koreliaciją tarp pervedimų, kuriuos atlieka investuotojai, į žetonus, susijusių su „Rug pull“ nusikalstama veika, ir Eterio virtualios valiutos žymių kitimų pasirenkama skaičiuoti labiausiai paplitusį Pearsono koreliacijos koeficientą (Marshall ir Jonker, 2011). Šiuo atveju yra taip pat pasinaudojama Microsoft Excel 2016 programinės įrangos teikiama formule, kuri apskaičiuoja Pearsono koreliacijos koeficientą:

$$=CORREL(\text{pirmasis masyvas, antrasis masyvas}) \quad (9)$$

kur:

pirmasis masyvas – Eterio kainos;

antrasis masyvas - pervedimų skaičius į žetoną, susijusį su nusikalstama veikla „Rug pull“.

Taigi, aprašius tyrimo etapus, toliau yra nurodoma, kokie duomenys ir kokiais būdais duomenys yra atrenkami tyrimui. Atliekant tyrimą buvo naudojami duomenys iš Chainabuse (2024). Internetinis puslapis, kuriame galima rasti pranešimus, susijusius su įvairiomis decentralizuotų finansinių nusikaltimų kategorijomis, buvo pasirinktas remiantis Garin ir Gisin (2023) moksliniu straipsniu. Šiame internetiniame puslapyje galima rasti pranešimus, susijusius su įvairiomis decentralizuotų finansinių nusikaltimų kategorijomis, tame tarpe ir pranešimus apie „Rug pull“. Peržiūrėjus visus pranešimus, susijusius su viena iš decentralizuotų finansų finansinių nusikaltimų „Rug pull“ rūšių, buvo atmetami pranešimai, tokie kaip: pranešimai, kurie šiuo metu saugumo sumetimais ir siekiu neatskleisti nusikaltimo tyrimo eigos yra neprieinami, pranešimai, pagal kuriuos žetonai ir su juo susijusios operacijos yra panaikintos ir neprieinamos, pranešimai, kuriuose pateikiami tik internetinių puslapių nuorodos, pranešimai, kurie susiję su žetonais susietais ne su Eterio moneta ir todėl nėra galimybės pamatyti bei pasiimti operacijų iš „Eterio blokų grandinės nagrinėjimo“ internetinio puslapio (Etherscan, 2024). Taigi, duomenims sisteminti yra pasirenkami pranešimai, kuriuose pateikiami konkrečių asmenų piniginių adresai, kurie sukūrė žetonus, susijusius su „Rug pull“ finansiniu nusikaltimu bei pačių žetonų, kurie susiję su „Rug pull“, adresai. Atrinkus piniginių bei žetonų adresus, buvo atliekama paieška Etherscan (2024) internetiniame puslapyje. Pirmiausia buvo peržiūrėti asmenų piniginių adresų, susijusių su „Rug pull“ nusikaltimu, operacijos. Operacijų peržiūra buvo atliekama tam, kad būtų identifikuoti šių asmenų sukurti žetonai, kurie operacijų įrašų visumoje pateikiami kaip operacija „Contract Creation“. Identifikavus konkrečių asmenų sukurtus žetonus bei atsirinkus konkretų žetono adresą tyrimui buvo ištraukiama visa egzistavusių operacijų informacija iš Etherscan (2024) internetinio puslapio. Papildomai, kad įsitikinti, jog žetonai yra susiję su „Rug pull“ nusikalstama veikla, atliekama kiekvieno žetono analizė internetiniame puslapyje Solidus Labs (2024) atsižvelgus į nurodytus kriterijus 1.4 magistro darbo dalyje. Kaip ir buvo paminėta anksčiau, tyrimui buvo atrinkti 146 žetonai. Iš surinktų duomenų sudaroma duomenų bazė naudojant Microsoft Excel 2016 programinę įrangą. Surinkus visu šiuos duomenis į bendrą analizę, padarytų pervedimų į žetonus, sukurtus atlikti „Rug pull“ finansinį nusikaltimus, kiekis buvo palygintas su Eterio virtualios valiutos kainos kilimo bei kritimo etapais. Taip pat, renkant duomenis, buvo pastebėta jog Eterio kainai kylant minimų žetonų sukuriamas skaičius irgi kyla, dėl investuotojų poreikio greičiau pakelti savo portfelio vertę arba Eterio kainai

krentant virtualių žetonų skaičius kyla dėl noro investuotojams kompensuoti prarastą valiutos vertę, kol suinvestuotų pinigų į Eterį vertė krito. Taip pat, verta paminėti, jog kai kurie tiriami žetonai tiriamų etapų metu persikerta su etapų pabaigos ir pradžios laikais. Šie etapai plačiau aprašyti 3.1 magistro darbo dalyje. Nagrinėjamas laikotarpis taip pat pasirinktas atsižvelgus į sukurtų pranešimų datas, tai yra nuo 2020-07-24 iki 2024-12-02. Atsižvelgus į iškeltą hipotezę bei nagrinėjamus laikotarpius, minimus 2.1 magistro darbo dalyje, detaliau nagrinėjami trys laikotarpiai: antrasis laikotarpis – 2020-11-03 – 2021-11-08, trečiasis laikotarpis – 2021-11-09 – 2022-06-18 bei penktasis laikotarpis – 2023-09-25 – 2024-12-02, nes šiais laikotarpiais Eterio kaina krito arba kilo. Apžvelgiami, tačiau detaliau nenagrinėjami du laikotarpiai: pirmasis laikotarpis – 2020-01-01 – 2020-11-02 ir ketvirtasis laikotarpis – 2022-06-19 – 2023-09-24, nes pirmuoju laikotarpiu Eterio kaina nebuvo populiari, o ketvirtuoju laikotarpiu identifikuota, kad kaina vyraavo panašiam lygyje. Eterio istorinės kainos buvo paimtos iš internetinio puslapio Investing.com (2024).

Galiausiai, 3.3 darbo dalyje pateikiamas modelis, kuris parodo kaip pasitikrinti, jog žetonas susijęs su „Rug pull“ nusikalstama veikla. Modelis, kuris pateikiamas 3.3 magistro darbo dalyje yra kurtas paprasčiausiu būdu vadinamu žingsnis po žingsnio (angl. *step-by-step*). Šis būdas nurodo asmeniui žingsnis po žingsnio, etapas po etapo, ką reikia padaryti ar pasitikrinti prieš investuojant į Eterio pagrindu kurtą žetoną. Kuriant modelį buvo remtasi 1.4 magistro darbo dalyje nurodytais aspektais bei patirtimi, kuri buvo sukaupta atliekant 3.2 magistro darbo dalies tyrimą.

3. „RUG PULL“ FINANSINIO NUSIKALTIMO VERTINIMAS

Trečioji darbo dalis apima Eterio kainų ir finansinių nusikaltimų su tuometinėmis Eterio virtualios valiutos kainomis lyginamąją analizę, „Rug pull“ decentralizuotų finansų finansinio nusikaltimų vertinimą, bei pervedimų, į tokių nusikaltimų žetoną, skaičių palyginimą su tuometinėmis Eterio kainomis pasirinktais laikotarpiais. Taip pat, remiantis atlikta mokslinės literatūros analize, įgyta patirtimi atliekant magistro darbo tyrimo dalį, sukuriamas modelis, skirtas apsaugoti investuotojus nuo investavimo ar lėšų praradimo investuojant į decentralizuotų finansų finansinių nusikaltimo „Rug pull“ virtualius žetonus.

3.1 Eterio kainų ir finansinių nusikaltimų palyginimas

Remiantis atlikta literatūros analize pirmoje darbo dalyje buvo nuspręsta atlikti lyginamąją analizę ir įsitikinti, jog virtualių valiutų ir finansinių nusikaltimų kiekis yra koreliuojantys dydžiai. Kadangi skaitmeninės valiutos yra labai nauja decentralizuota finansinė rinka, tyrimui naudojami internetiniai šaltiniai bei jų pateikiami duomenys. Toliau pateikiama bendra virtualių valiutų vertė nuo 2014 metų iki dabar, remiantis CoinGecko (2024) (žr. 5 pav.). Analizei pasirinktas laikotarpis dėl išaugusio populiarumo, kurį teigia - Anna Fleck (2022), Consensus (2019), Gandal ir kt. (2014).

5 paveikslas

Virtualių valiutų kainų kitimas nuo 2014 m. iki 2024 m. gruodžio 2 d.

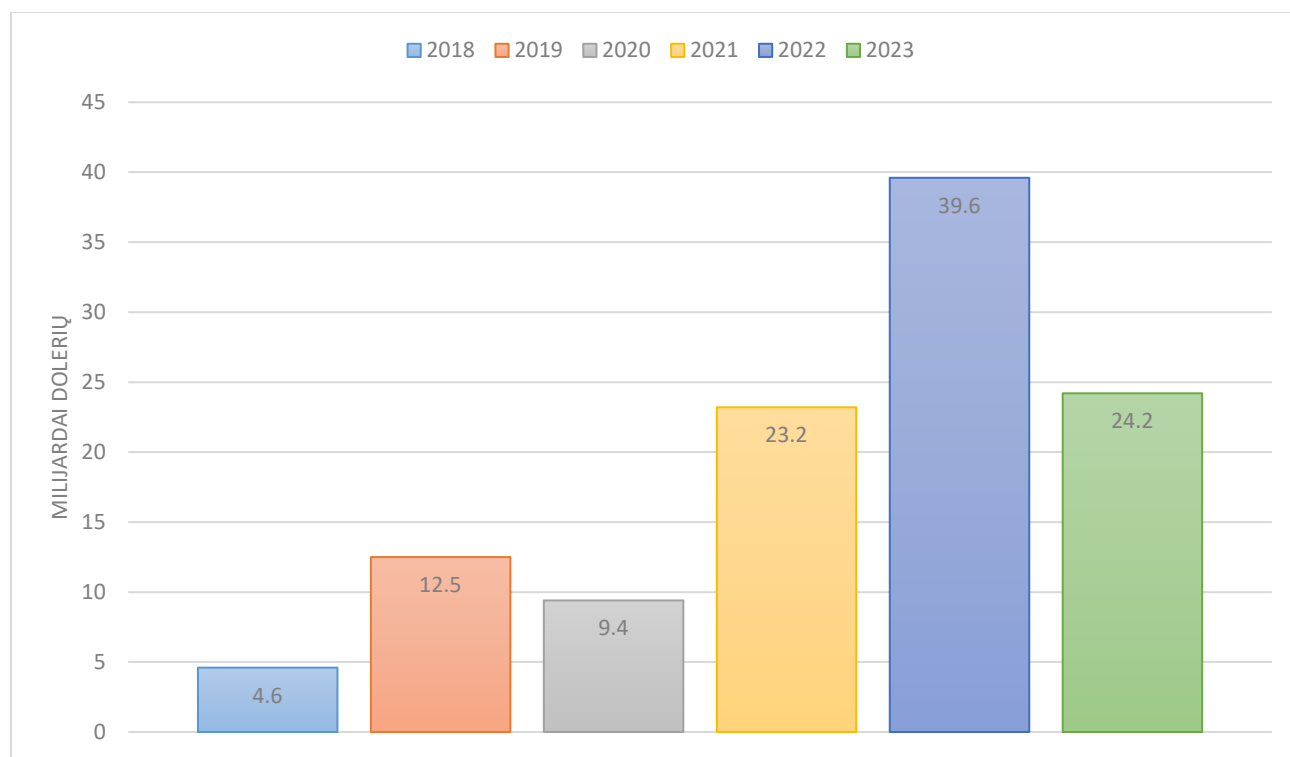


Šaltinis: Sudaryta autorės, remiantis CoinGecko (2024) šaltiniu

Įvertinus pateiktus duomenis ir tam, kad būtų lengviau apsibrėžti bei analizuoti pateiktus duomenis, virtualių valiutų gyvavimas ir vertingumas buvo suskirstytas į penkis etapus – pirmasis etapas – pradžia (nuo 2014 metų iki pat 2020 metų galo (pažymėta žaliu stačiakampiu)), antrasis etapas – pirmasis pakilimas (nuo 2021 metų iki 2021 metų pabaigos (pažymėtas oranžiniu stačiakampiu)), trečiasis etapas – pirmasis kritimas (nuo 2021 metų galo iki 2022 metų vidurio (pažymėtas geltonu stačiakampiu)), ketvirtasis etapas – stagnacija (nuo 2022 metų vidurio iki 2024 metų pradžios (pažymėtas mėlynu stačiakampiu)) ir penktasis etapas – antrasis pakilimas (nuo 2024 metų pradžios iki šių dienų (pažymėtas raudonu stačiakampiu)) (žr. 5 pav.).

6 paveikslas

Gauta neteisėtais adresais bendra virtualios valiutos vertė 2018-2023 metų laikotarpiu



Šaltinis: sudarytas autorės, remiantis Chainalysis (2024)

Remiantis pateikta 2 darbo dalyje hipoteze nutarta pateikti decentralizuotų finansų finansinių nusikaltimų grafiką tais pačiais laikotarpiais tam, kad nustatyti koreliaciją tarp skaitmeninių valiutų kainų kilimo ir nusikaltimų kiekio susijusių su virtualiomis valiutomis bei investavimu į jas. Kadangi skaitmeninėmis valiutomis atliekamus nusikaltimus susekti neįmanoma arba itin sudėtinga yra pateikiamas virtualių valiutų vertės gavimas naudojantis nelegaliais adresais. Remiantis Chainalysis

(2024) duomenimis nuo 2018 metų iki 2023 metų atlikta analize (žr. 6 pav.) galima atkreipti dėmesį, jog antrojo etapo metu – pirmojo pakilimo virtualios valiutos vertės gavimas yra smarkiai pakilęs ir išsiskiria iš gautų verčių pradžios ar stagnacijos etapų metu ir sudaro 39,6 milijardus dolerių. Kadangi antrojo etapo pradžia buvo 2021 metais tai paaiškina dar palyginus su 2022 metais ne tokią didelę rodomą reikšmę, tačiau tai jau buvo gan aktyvus procesas, dėl to sutampa su stagnacijos etapo duomenimis. 2021 metais neteisėtais virtualių valiutų adresais nelegalių sandorių vertė siekė 23,2 milijardus dolerių, o 2023 metais 24,2 milijardus dolerių. Įvertinus šiuos duomenis galima teigti, jog kylant virtualių valiutų vertei atsiranda naujų būdų ir daugiau asmenų norinčių pavogti, gauti, apgauti asmenis turinčius ar investuojančius į virtualias valiutas ir taip praturtėti.

Atlikus aukščiau pateikiamų duomenų analizę yra matoma, jog virtualių valiutų vertė ir atliekamų finansinių nusikaltimų, susijusių su skaitmeninėmis valiutomis, kiekiai koreliuoja tarpusavyje. Analizuojant „Chainalysis“ finansinių nusikaltimų ataskaitas tarp visų populiariausių nusikaltimų rūšių egzistuojančių decentralizuotuose finansuose 2021 metais buvo pastebėta, jog nuo minimų metų į nusikaltimų, susijusių su virtualiomis valiutomis, rinką atėjo nusikaltimas vadinamas „Rug pull“ ir ypač išpopuliarėjęs tarp Eteriu pagrįstų žetonų (Chainalysis, 2022). 2021 metais „Rug pull“ tapo pagrindiniu finansiniu nusikaltimu, nes sudarė 37 procentus visų pajamų gaunamų iš virtualių valiutų sukčiavimų (Chainalysis, 2022). Chainalysis (2022) teigimu „Rug pull“ yra viena iš žalingiausių skaitmeninių valiutų sukčiavimo atvejų, kurie padaro įtaką ne tik individualiems investuotojams, bet ir stipriai mažina pasitikėjimą decentralizuotų finansų sektoriumi, todėl antrojo tyrimo metu bus atliekama statistiškai reikšmingos koreliacijos nustatymas tarp pervedimų į „Rug pull“ metodu atliktus nusikaltimus ir virtualios valiutos – Eterio – vertės kitimų.

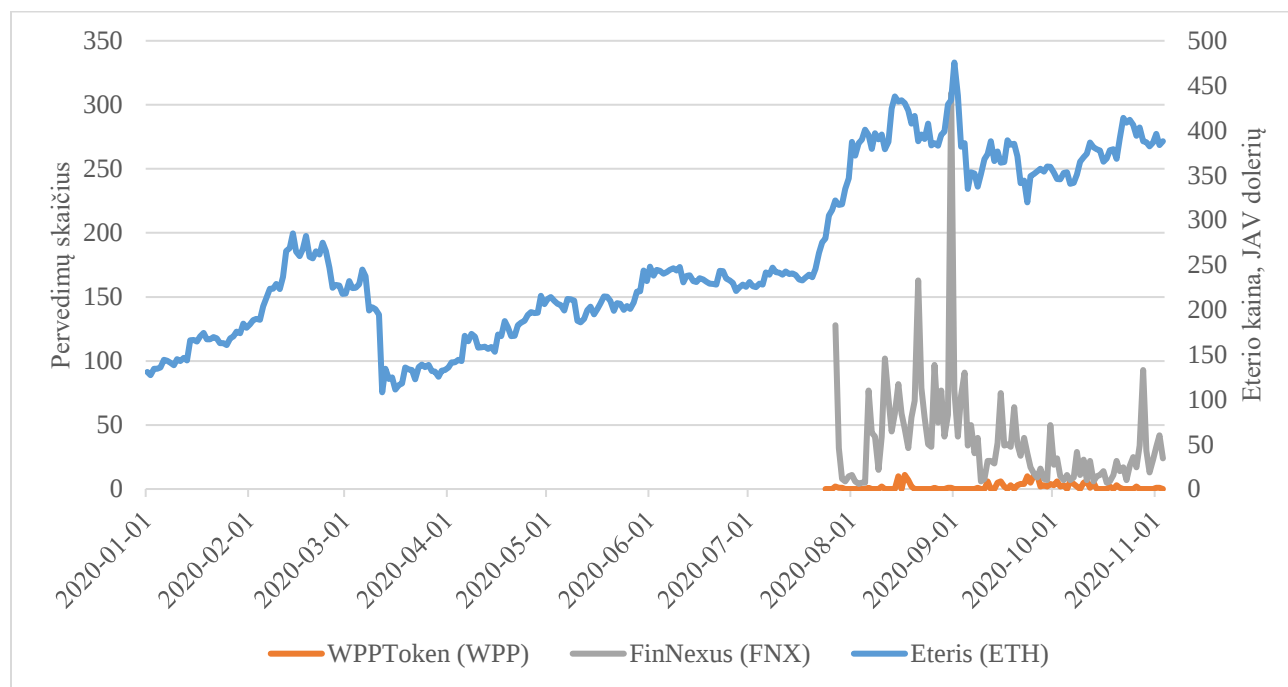
3.2 „Rug pull“. Konkretaus virtualaus žetono nusikaltimo atvejis ir jo palyginimas su Eterio virtualios valiutos verte

Kaip ir minėta anksčiau, antrame tyrime atliekama atvejo, konkrečiai „Rug pull“ metodu pavogtų pinigų analizė lyginant su virtualių valiutų vertės kitimu, t.y. kilimu ir kritimu. Atliekant tyrimą buvo naudojami duomenys iš Chainabuse (2024). Antrame priede pateikiamas visų į žetonus, kurie susiję viena iš nusikalstamos veiklos kategorijų „Rug pull“, atliktų pervedimų ir virtualios valiutos Eterio, kurio pagrindu yra daugiausiai kuriama žetonų, kainos palyginimas. Pirmasis laikotarpis, tai yra, nuo 2014 metų iki 2020 metų galo (konkrečiai lapkričio mėnesio trečios dienos) yra apžvelgiamas, tačiau nenagrinėjamas, nes nestabili moneta – Eteris – nebuvo populiarus. Taip pat

tyrimo metu pastebėta ir identifikuota, kad pranešimai, susiję su „Rug pull“ nusikalstama veikla, buvo pradėti kurti tik 2020 metų liepos mėnesio pabaigoje. Tyrimo metu nustatyta, kad nuo 2020 metų liepos dvidešimt septintos dienos iki 2020 metų lapkričio 3 dienos buvo sukurti 2 pranešimai internetiniame puslapyje Chainabuse (2024) apie 2 žetonus („FinNexus“ (FNX) ir „WPPToken“ (WPP)), kurie susiję su „Rug pull“ nusikalstama veika.

7 paveikslas

Pervedimų į „Rug pull“ nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2020-01-01 – 2020-11-02



Šaltinis: sudaryta autorės, remiantis (Etherscan, 2024; yahoo!finance, 2024; Solidus Labs, 2024)

Tam kad papildomai įsitikinti, kad šie žetonai yra susiję su neteisėta veikla, jie buvo patikrinti internetiniame puslapyje „Token Sniffer“ (Solidus Labs, 2024). „Token Sniffer“ internetiniame puslapyje nurodyta, kad „WPPToken“ žetonas buvo sukurtas – 2020-07-24, o „FinNexus“ – 2020-07-27. Nustatyta, kad „WPPToken“ (WPP) ir „FinNexus“ (FNX) žetonų įvertinimas yra nulis ir dešimt iš šimto ir viena iš priežasčių, lėmusių tokius abiejų žetonų įvertinimus yra nepakankamas ir neužrakintas likvidumas. 2024 metų gruodžio antros dienos duomenimis „WPPToken“ (WPP) likvidumas siekia 0,08 Eterio (291,48 JAV dolerių), kai pradinis likvidumas siekė 35,1 Eterio (127886,15 JAV dolerių), tai yra, likvidumas per visą žetono gyvavimo laikotarpį sumažėjo 438,75 karto. Kalbant apie „FinNexus“ (FNX), 2024 metų gruodžio antrą dieną likvidumas siekė 0,78 Eterio

(2841,91 JAV dolerių), kai pradinis likvidumas – 3902,64 Eterio (14219190,79 JAV dolerių), tai yra, likvidumas per visą žetono gyvavimo laikotarpį sumažėjo 5003,38 karto. „WPPToken“ (WPP) buvo atlikta 3642 operacijos, o „FinNexus“ (FNX) – 15407. Taigi, pagal pateiktą 7 paveikslą galima matyti, kad „FinNexus“ (FNX) operacijų kiekis, kuomet Eterio kaina 2020-09-01 pasirinktu nagrinėjamu laikotarpiu siekė aukščiausią kainos tašką (475,8 JAV dolerių) buvo atlikta daugiausiai pervedimų – 309.

Toliau yra nagrinėjamas 3.1 magistro darbo dalyje minimas antrasis laikotarpis, tai yra, nuo 2020 metų lapkričio 3 dienos iki 2021 metų lapkričio 8 dienos (imtinai). Tyrimo metu nustatyta, kad nagrinėjamu laikotarpiu buvo sukurta 16 žetonų, kurie susiję su „Rug pull“ nusikalstama veika, apie kuriuos buvo sukurti pranešimai internetiniame puslapyje Chainabuse (2024), taip pat papildomai yra nagrinėjami 2 žetonai, apžvelgti pirmuoju nagrinėjamu laikotarpiu, į kuriuos buvo atlikti pervedimai tyrimo laikotarpiu (žr. 3 lentelę, 3 priedą).

3 lentelė

Antruoju tyrimo analizuojamu laikotarpiu 2020-11-03 – 2021-11-08 nagrinėjami žetonai

Eilės numeris	Žetono pavadinimas	Žetono sukūrimo data	Pervedimų skaičius nagrinėjamu laikotarpiu
1	WPPToken (WPP)	2020-07-24	1823
2	Crypto Coven (WITCH)	2021-11-04	64
3	Emblem (EMB)	2021-02-15	8430
4	WinterBears (WB)	2021-09-18	5660
5	8 BIT UNIVERSE (8BIT)	2021-08-21	2045
6	BONEHEADS (BONE)	2021-08-20	5204
7	Buzzed Bear Hideout (BEAR)	2021-07-15	4733
8	RichKids (RKS)	2021-09-26	5068
9	TrippieHeadz (TRIPP)	2021-11-04	825
10	DAO Turtles (DTS)	2021-10-03	6293
11	Acid Apes Candy Syndicate (AACS)	2021-09-24	69
12	Trippy Ape Yacht Club (TAYC)	2021-08-16	1369
13	High Club (HC)	2021-07-19	731
14	Ethermonkeys (EB)	2021-10-11	3092
15	Etherbananas (EB)	2021-10-05	796
16	ZombieMonkeys (ZM)	2021-10-15	1082
17	FinNexus (FNX)	2020-07-27	9916
18	EvolvedApes (EVA)	2021-07-23	18005

Šaltinis: sudarytas autorės, remiantis Solidus Labs (2024)

Tam kad papildomai įsitikinti, kad 16 žetonų, nagrinėjamų antruoju laikotarpiu, yra susiję su „Rug pull“ finansiniu nusikaltimu, jie buvo patikrinti internetiniame puslapyje „Token Sniffer“ (Solidus Labs, 2024). Nustatyta, kad „Emblem“ (EMB) žetonas yra įvertintas nuliu iš šimto, nes viena

iš priežasčių, lėmusių tokį žetono įvertinimą yra nepakankamas ir neužrakintas likvidumas. 2024 metų gruodžio antros dienos duomenimis „Emblem“ (EMB) likvidumas siekė 0,01 Eterio (36,43 JAV dolerių) kai pradinis likvidumas siekė 201,95 Eterio (735800,79 JAV dolerių), tai yra, likvidumas per visą žetono gyvavimo laikotarpį sumažėjo 3902,64 karto. Kiti žetonai („Crypto Coven“ (WITCH), „WinterBears“ (WB), „8 BIT UNIVERSE“ (8BIT), „BONEHEADS“ (BONE), „Buzzed Bear Hideout“ (BEAR), „RichKids“ (RKS), „TrippieHeadz“ (TRIPP), „DAO Turtles“ (DTS), „Acid Apes Candy Syndicate“ (AACS), „Trippy Ape Yacht Club“ (TAYC), „High Club“ (HC), „Ethermonkeys“ (EB), „Etherbananas“ (EB), „ZombieMonkeys“ (ZM), „EvolvedApes“ (EVA)) yra nepakeičiamieji žetonai. Nustatyta, kad minimi nepakeičiamieji žetonai yra įvertinti nulių iš šimto, nes viena iš priežasčių, lėmusių tokius įvertinimus yra analizuojamu laikotarpiu nepakeičiamų žetonų negalimas pardavimas. Atsižvelgus į tai, kad internetiniame puslapyje „Token Sniffer“ nėra nurodoma ar nepakeičiamų žetonų likvidumas yra užrakintas, papildomai buvo peržiūrėtos nepakeičiamųjų žetonų kūrėjų piniginės, kuriose turėtų būti nurodyta ar žetono kūrėjas užrakino ar neužrakino likvidumą. Peržiūrėjus šių nepakeičiamų žetonų kūrėjų piniginių operacijas, nustatyta, kad nei vienas žetono kūrėjas nėra užrakinęs likvidumo. Taip pat svarbu paminėti, kad tyrimo metu nustatyta, kad iš šių 15 nepakeičiamų žetonų apie 3 žetonus yra sukurti straipsniai, kurių teigimu šie žetonai yra iš ties „Rug pull“ finansinio nusikaltimo atvejai. Pavyzdžiui, teigiama, kad „WinterBears“ (WB) kūrėjų komanda žadėjo prizus, tokius kaip „Pudgy Penguins“ nepakeičiamuosius žetonus pasiekus 25% pardavimų ir „Cool Cat“ nepakeičiamuosius žetonus pasiekus 50% pardavimų, tačiau šie pažadai buvo pašalinti iš „WinterBears“ (WB) internetinės svetainės 2021 metų spalį, o prizai nebuvo įteikti. Taip pat „WinterBears“ (WB) kūrėjų komanda sumokėjo nuomonės kūrėjai „ArtChick“ 5 Eterius (2024 metų gruodžio antros dienos duomenimis – 18217,4 JAV dolerių), kad ji pirktų „WinterBears“ (WB) ir taip sukurtų dirbtinį susidomėjimą projektu. Tai pritraukė daugiau investuotojų, kurie manė, kad projektas yra populiarus. Galiausiai minimo nepakeičiamo žetono kūrėjų komanda žadėjo finansuoti „DAO“ fondą su vertingais nepakeičiamais žetonais ir lėšomis, tačiau, nepaisant surinktų daugiau nei 1000 Eterių (2024 metų gruodžio antros dienos duomenimis – 3643480 JAV dolerių), šie pažadai nebuvo įgyvendinti (Kitonyi, 2022; NFT degenz, 2022). Kito „BONEHEADS“ (BONE) nepakeičiamojo žetono „Rug pull“ finansinio nusikaltimo atvejis buvo nagrinėjamas Kanadoje iškeltame kolektyviniame ieškinyje, kurio suma siekė 3,1 milijoną JAV dolerių. Teigiama, kad 2021 metų gruodžio mėnesį projektas pristatė 10000 nepakeičiamųjų žetonų rinkinį, kurio kiekvieno kaina siekė 0,1 Eterio (2024 metų gruodžio antros dienos duomenimis – 364,35 JAV dolerių). „Boneheads“ žetono kūrėjų komanda buvo apkaltinta sutarties su investuotojais pažeidimu, nes neįgyvendino

projekto plano, pasisavino lėšas, apgaulingai teikė klaidinančius duomenis. Teigiama, kad projekto įkūrėjai į asmenines sąskaitas persivedė maždaug 3,1 mln. JAV dolerių lėšų ir investavo į didelės vertės nepakeičiamus žetonus, tokius kaip „CryptoPunks“ ir „Bored Ape Yacht Club“ (NFTevening, 2023; Quarmby, 2023). Galiausiai, buvo sukurtas pranešimas apie vieną iš žinomiausių nepakeičiamų žetonų „Rug pull“ atvejų - „EvolvedApes“ (EVA). „EvolvedApes“ buvo nepakeičiamų žetonų projektas, kuris 2021 metais sulaukė daug dėmesio. Tai buvo „NFT“ kolekcija, kurią sudarė 10000 skaitmeninių paveikslų, vaizduojančių beždžiones, kurios buvo parduodamos už 0.08 Eterį (2024 metų gruodžio antros dienos duomenimis – 291,48 JAV dolerių). Projektas sulaukė didelio susidomėjimo, tačiau po to, kai visi nepakeičiamieji žetonai buvo parduoti, žetono kūrėjai pasitraukė su surinktais 2,7 milijono JAV dolerių ir nepaliko jokių žinių apie projektą. Jungtinių Amerikos valstijų institucijos pateikė ieškinį prieš 3 Jungtinės Karalystės gyventojus, kuriems gresia maksimali baudmė – 20 metų kalėjimo (Millard, 2024; United States Attorney’s Office, 2024).

Taigi, atlikus antrojo laikotarpio, tai yra, nuo 2020 metų lapkričio 3 dienos iki 2021 metų lapkričio 8 dienos (imtinai), duomenų analizę, nustatyta, kad iš 18 žetonų, susijusių su „Rug pull“ nusikalstama veikla, 17 žetonų apskaičiuotos t-testo reikšmės viršija apskaičiuotas kritines t-reikšmes, tai reiškia, kad yra statistiškai reikšminga koreliacija tarp Eterio kainos augimo ir į 17 žetonų, kurie susiję su finansiniu nusikaltimu „Rug pull“, atliktų pervedimų (žr. 4 lentelę, 4 priedą).

4 lentelė

Žetono T.testo reikšmė ir kritinė t-reikšmė analizuojamu 2020-11-03 – 2021-11-08 laikotarpiu

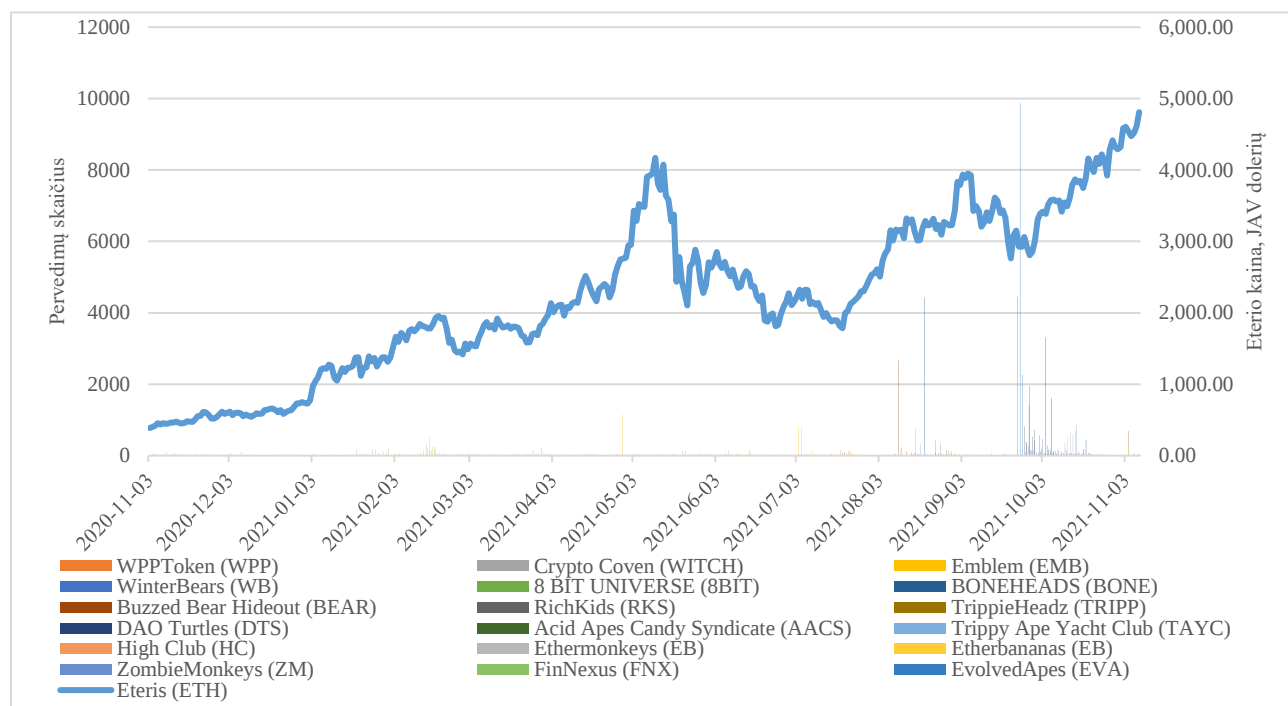
Eilės numeris	Žetono pavadinimas	T.testo reikšmė	Kritinė t-reikšmė
1	WPPToken (WPP)	-0.84	-1.96
2	Crypto Coven (WITCH)	-3.43	-2.00
3	Emblem (EMB)	-9.22	-1.96
4	WinterBears (WB)	-32.63	-1.96
5	8 BIT UNIVERSE (8BIT)	-11.42	-1.96
6	BONEHEADS (BONE)	-6.49	-1.96
7	Buzzed Bear Hideout (BEAR)	-3.02	-1.96
8	RichKids (RKS)	-49.51	-1.96
9	TrippieHeadz (TRIPP)	-6.49	-1.96
10	DAO Turtles (DTS)	-29.10	-1.96
11	Acid Apes Candy Syndicate (AACS)	-4.73	-1.99
12	Trippy Ape Yacht Club (TAYC)	-7.87	-1.96
13	High Club (HC)	-17.86	-1.96
14	Ethermonkeys (EB)	-43.76	-1.96
15	Etherbananas (EB)	-13.64	-1.96
16	ZombieMonkeys (ZM)	-9.91	-1.96
17	FinNexus (FNX)	-28.85	-1.96
18	EvolvedApes (EVA)	-51.74	-1.96

Šaltinis: sudarytas autorės

Atkreiptinas dėmesys, kad šių žetonų statistiškai reikšminga koreliacija yra neigiama, tai yra, kad kainai didėjant mažėja pervedimų skaičius. Atsižvelgus į tai, kad pervedimų skaičius į žetonus, susijusius su „Rug pull“ nusikaltimu, yra dalinamas per nagrinėjamus laikotarpius, o taip pat atskirai nagrinėjant pervedimus į žetonus galima matyti, kad pervedimų skaičius yra labai didelis, kuomet yra sukuriamas žetonas, papildomai yra apskaičiuota bendroji T.testo reikšmė nagrinėjamu antruoju laikotarpiu. Nustatyta, kad bendroji T.testo reikšmė – 51,03, o kritinė t-reikšmė – 1,96, tai reiškia, kad bendroji koreliacija teigiamai statistiškai reikšminga. Tai parodo, kad kainai pradėjus augti, padaugėjo pervedimų į žetonus, susijusius su „Rug pull“ nusikalstama veikla. Taip pat 8-jame paveiksle pateikiama grafinė vizualizacija į žetonus, susijusius su „Rug pull“ finansiniu nusikaltimu, atliktų pervedimų skaičiaus ir Eterio kainos palyginimas.

8 paveikslas

Pervedimų į „Rug pull“ nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2020-11-03 – 2021-11-08



Šaltinis: sudaryta autorės, remiantis Etherscan (2024), yahoo!finance (2024), Solidus Labs (2024)

Toliau yra nagrinėjamas 3.1 magistro darbo dalyje minimas trečiasis laikotarpis, tai yra, nuo 2021 metų lapkričio 9 dienos iki 2022 metų birželio 18 dienos (imtinai). Tyrimo metu nustatyta, kad nagrinėjamu laikotarpiu buvo sukurti 32 žetonai, kurie susiję su „Rug pull“ nusikalstama veika, apie

kuriuos buvo sukurti pranešimai internetiniame puslapyje Chainabuse (2024), taip pat papildomai yra nagrinėjami 2 žetonai, apžvelgti pirmuoju ir antruoju nagrinėjamu laikotarpiu, į kuriuos buvo atlikti pervedimai tyrimo laikotarpiu (žr. 5 lentelę).

5 lentelė

Trečiuoju tyrimo analizuojamu laikotarpiu 2021-11-09 – 2022-06-18 nagrinėjami žetonai

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data
1	WPPToken (WPP)	2020-07-24	26	8 BIT UNIVERSE (8BIT)	2021-08-21
2	Crypto Coven (WITCH)	2021-11-04	27	MaskBillionaireClub (MBC)	2022-02-28
3	Cookies N Kicks (CNK)	2022-02-08	28	Rich Dwarves Tribe (DWARF)	2022-02-09
4	Evolution Apes (EA)	2022-01-31	29	BONEHEADS (BONE)	2021-08-20
5	HypedHuskyMetaCityNFT (HHMC)	2022-01-25	30	Buzzed Bear Hideout (BEAR)	2021-07-15
6	Kong Ape Boss Club (KABC)	2022-12-21	31	Miss Universe NFT (MU)	2021-12-12
7	BitFrenchie (BF)	2022-12-13	32	Automated Assassins (AA)	2022-06-01
8	Metamon (METAMON)	2022-04-14	33	RichKids (RKS)	2021-09-26
9	THE HUMARS (TH)	2021-12-20	34	TrippieHeadz (TRIPP)	2021-11-04
10	Rich Jaguarz (RJ)	2022-01-25	35	Ancient Cats Club (CAT)	2021-11-27
11	Naughty Bape Club (NBC)	2021-12-20	36	Crazy Camels (CAMEL)	2021-11-14
12	Cyclops Monkey Club (CMC)	2021-12-06	37	Project Shura (SHURA)	2022-01-04
13	Empower Women Planet (EWP)	2022-01-26	38	DAO Turtles (DTS)	2021-10-03
14	Lucky Elephant Club (LEC)	2021-11-18	39	Bored Ape Tattoo Shop (BATS)	2021-11-18
15	Cyber Zombie Society (CZS)	2021-11-20	40	Trippy Ape Yacht Club (TAYC)	2021-08-16
16	Alien Alliance (AA)	2021-12-05	41	High Club (HC)	2021-07-19
17	Fud Token (FUD)	2021-11-17	42	Ethermonkeys (EB)	2021-10-11
18	Smol Boyz (SMOLBOYZ)	2022-03-07	43	Etherbananas (EB)	2021-10-05
19	Emblem (EMB)	2021-02-15	44	ZombieMonkeys (ZM)	2021-10-15
20	ToolsOfTheGreat (TOTG)	2022-05-21	45	Billionaire Dogs Club (BDC)	2021-12-11
21	TokyoClone (TOKYOCLONE)	2022-04-25	46	FinNexus (FNX)	2020-07-27
22	WinterBears (WB)	2021-09-18	47	EvolvedApes (EVA)	2021-07-23
23	The Sloth Tribe (SLOTHS)	2021-11-16	48	ThePlayBox (PLAYBOX)	2022-03-28
24	Apes In Space (AIS)	2021-12-03	49	HighRise Land (HIGHRISE)	2022-03-26
25	Clash of Shiba (COS)	2022-03-22			

Šaltinis: sudarytas autorės, remiantis Solidus Labs (2024)

Tam kad papildomai įsitikinti, kad 32 žetonai, nagrinėjamų trečiuoju laikotarpiu, yra susiję su „Rug pull“ finansiniu nusikaltimu, jie buvo patikrinti internetiniame puslapyje „Token Sniffer“ (Solidus Labs, 2024). Visi 32 žetonai yra nepakeičiamieji žetonai. Nustatyta, kad minimi nepakeičiami žetonai yra įvertinti nuliu iš šimto, nes viena iš priežasčių, lėmusių tokius įvertinimus yra analizuojamu laikotarpiu nepakeičiamų monetų negalimas pardavimas. Atsižvelgus į tai, kad

internetiniame puslapyje „Token Sniffer“ nėra nurodoma ar nepakeičiamų žetonų likvidumas yra užrakintas, papildomai buvo peržiūrėtos nepakeičiamųjų žetonų kūrėjų piniginės, kuriose turėtų būti nurodyta ar žetono kūrėjas užrakino ar neužrakino likvidumą. Peržiūrėjus šių nepakeičiamų žetonų kūrėjų piniginių operacijas, nustatyta, kad nei vienas žetono kūrėjas nėra užrakinęs likvidumo.

Tyrimo metu nustatyta, kad iš šių 32 nepakeičiamų žetonų apie 9 žetonus yra sukurti straipsniai, kurių teigimu šie žetonai susiję su „Rug pull“ finansiniu nusikaltimu. Pirmasis straipsnis susijęs su „The Naughty Bape Club“ (NBC) nepakeičiamuoju žetonu. „Rug Pull Finder“ tris mėnesius tyrė nepakeičiamųjų žetonų projektų grupę, kuri bendrai pavogė daugiau nei 40000 Eterio (2024 metų gruodžio antros dienos duomenimis – 145739200 JAV dolerių). „Rug Pull Finder“ remiasi „The Rug Busters“ darbu, kuriame atskleista, kad olandas Vasco Rouw, susijęs su daugiau nei 17 nepakeičiamųjų žetonų, tame tarpe ir „The Naughty Bape Club“ (NBC), yra pagrindinis asmuo, atlikęs „Rug pull“ finansinius nusikaltimus, susijusius nepakeičiamais žetonais. Jis sukūrė apgaulingą „XPOSE“ žetoną ir, naudodamas pseudonimus, infiltravosi į NFT rinką. Į pagalbą pasitelkęs 10 žmonių komandą, išleido didžiosios dalies projektų likvidumą ir paliko žetonus beverčius (Kar, 2022). Kitas „Rug pull“ nusikalstamos veikos atvejis susijęs su „Smol Boyz“ (SMOLBOYZ) nepakeičiamuoju žetonu. 2022 metų kovo mėnesį „OnlyFans“ modelio Vanessa Sierra pradėtas projektas iš investuotojų surinko maždaug 127 ETH (2024 metų gruodžio antros dienos duomenimis – 462721,96 JAV dolerių). Tačiau projektas buvo apkaltintas netinkamu lėšų tvarkymu, įskaitant nepakeičiamųjų žetonų prekybą, siekiant dirbtinai išpūsti kainas, ir galiausiai buvo apleistas, paliekant investuotojams bevertį turtą (Flagship Team, 2022). Trečiojo nepakeičiamojo žetono „Rich Dwarves Tribe“ (DWARF) projektas įvykdė „Rug pull“ nusikaltimą 2022 metų pradžioje, kurio metu investuotojai prarado apie 3 mln. JAV dolerių. Šis projektas buvo reklamuojamas įžymybių. Kūrėjai pardavę nepakeičiamuosius žetonus, atsisakę projekto dingo su investuotojų lėšomis (Dubey, 2022). Kitas „Rug pull“ atvejis susijęs su nepakeičiamuoju žetonu „Ancient Cats Club“ (CAT). Dėl nepakeičiamojo žetono projekto investuotojai patyrė apie 1,7 mln. JAV dolerių nuostolio. Projektą reklamavo įžymybė „Rich The Kid“, kuri prisidėjo prie pradinio minėtos monetos populiarumo. Tačiau išpardavus nepakeičiamuosius žetonus, kūrėjai dingo ir investuotojai liko su beverčiais žetonais (CoinCu, 2023). Panaši situacija įvyko su „Crazy Camels“ (CAMEL) nepakeičiamuoju žetonu, kuomet pardavus visus žetonus kūrėjai dingo. Patirta žala siekė apie 1,6 mln. JAV dolerių (Gaurav, 2024; Zmudzinski, 2023). Tokiu pačiu principu buvo įvykdyti ir „Project Shura“ (SHURA) bei „Bored Ape Tattoo Shop“ (BATS) nepakeičiamųjų žetonų projektų „Rug pull“ nusikaltimai, kurių metu investuotojai patyrė 1,7 mln. ir 2,8 mln. JAV dolerių nuostolių (Boyle, 2022;

en.ethereumworldnews.com, 2022). Galiausiai, nepakeičiamųjų žetonų „Billionaire Dogs Club“ (BDC) projektas įvykdė „Rug pull“ finansinį nusikaltimą, kurio metu kūrėjai surinkę investuotojų lėšas, pervedė jas į daugybę žetono kūrėjų piniginių taip pavogdami iš investuotojų 960000 JAV dolerių (Ahmed, 2022).

6 lentelė

Žetono T.testo reikšmė ir kritinė t-reikšmė analizuojamu 2021-11-09 – 2022-06-18 laikotarpiu

Žetono pavadinimas	T.testo reikšmė	Kritinė t-reikšmė	Žetono pavadinimas	T.testo reikšmė	Kritinė t-reikšmė
WPPToken (WPP)	4.23	1.97	8 BIT UNIVERSE (8BIT)	0.64	1.96
Crypto Coven (WITCH)	16.64	1.96	MaskBillionaireClub (MBC)	0.30	1.96
Cookies N Kicks (CNK)	6.82	1.96	Rich Dwarves Tribe (DWARF)	12.56	1.96
Evolution Apes (EA)	10.65	1.96	BONEHEADS (BONE)	0.19	1.96
HypedHuskyMetaCityNFT (HHMC)	-1.33	-1.97	Buzzed Bear Hideout (BEAR)	-0.02	-1.96
Kong Ape Boss Club (KABC)	4.79	1.97	Miss Universe NFT (MU)	10.09	1.96
BitFrenchie (BF)	34.12	1.96	Automated Assassins (AA)	18.95	1.96
Metamon (METAMON)	2.36	1.96	RichKids (RKS)	0.84	1.96
THE HUMARS (TH)	3.11	1.96	TrippieHeadz (TRIPP)	8.24	1.97
Rich Jaguarz (RJ)	-4.21	-1.98	Ancient Cats Club (CAT)	18.10	1.96
Naughty Bape Club (NBC)	7.61	1.96	Crazy Camels (CAMEL)	14.71	1.96
Cyclops Monkey Club (CMC)	27.88	1.96	Project Shura (SHURA)	17.31	1.96
Empower Women Planet (EWP)	-1.07	-1.96	DAO Turtles (DTS)	0.81	1.96
Lucky Elephant Club (LEC)	6.86	1.96	Bored Ape Tattoo Shop (BATS)	1.62	1.97
Cyber Zombie Society (CZS)	10.24	1.96	Trippy Ape Yacht Club (TAYC)	1.82	1.98
Alien Alliance (AA)	9.47	1.96	High Club (HC)	0.46	2.03
Fud Token (FUD)	6.59	1.96	Ethermonkeys (EB)	7.07	1.96
Smol Boyz (SMOLBOYZ)	-0.86	-1.96	Etherbananas (EB)	3.62	1.97
Emblem (EMB)	9.44	1.96	ZombieMonkeys (ZM)	4.26	1.96
ToolsOfTheGreat (TOTG)	4.86	1.97	Billionaire Dogs Club (BDC)	10.22	1.96
TokyoClone (TOKYOCLONE)	21.12	1.96	FinNexus (FNX)	0.49	2.00
WinterBears (WB)	6.55	1.96	EvolvedApes (EVA)	-1.08	-1.96
The Sloth Tribe (SLOTHS)	6.98	1.96	ThePlayBox (PLAYBOX)	8.46	1.96
Apes In Space (AIS)	41.41	1.96	HighRise Land (HIGHRISE)	4.81	1.97
Clash of Shiba (COS)	2.51	1.98			

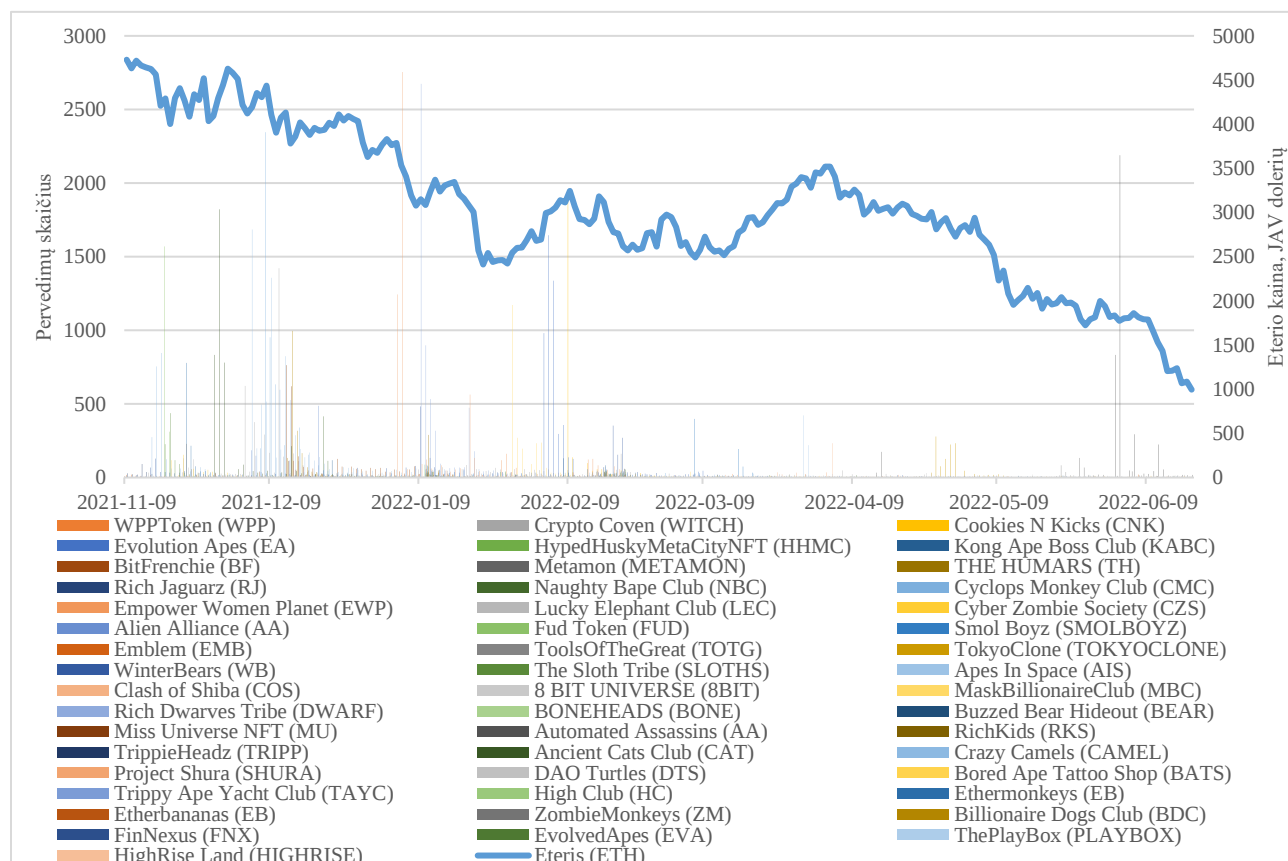
Šaltinis: sudarytas autorės

Taigi, atlikus antrojo laikotarpio, tai yra, nuo 2021 metų lapkričio 9 dienos iki 2022 metų birželio 18 dienos (imtinai), duomenų analizę, nustatyta, kad iš 49 žetonų, susijusių su „Rug pull“ nusikalstama veikla, 35 žetonų apskaičiuotos t-testo reikšmės viršija apskaičiuotas kritines t-reikšmes, tai reiškia, kad yra statistiškai reikšminga koreliacija tarp Eterio kainos augimo ir į 35 žetonus, kurie

susiję su finansiniu nusikaltimu „Rug pull“, atliktų pervedimų (žr. 6 lentelę). 34 žetonų statistiškai reikšminga koreliacija yra teigiama, tai yra, Eterio kainai mažėjant mažėja pervedimų skaičius. 1 žetono statistiškai reikšminga koreliacija yra neigiama, tai yra, kad Eterio kainai didėjant padaugėjo pervedimų skaičius. Atsižvelgus į tai, kad pervedimų skaičius į žetonus, susijusius su „Rug pull“ nusikaltimu, yra dalinamas per nagrinėjamus laikotarpius, o taip pat atskirai nagrinėjant pervedimus į žetonus galima matyti, kad pervedimų skaičius yra labai didelis, kuomet yra sukuriamas žetonas, papildomai yra apskaičiuota bendroji T.testo reikšmė nagrinėjamu trečiuoju laikotarpiu. Nustatyta, kad bendroji T.testo reikšmė – 105,34, o kritinė t-reikšmė – 1,96, tai reiškia, kad bendroji koreliacija teigiamai statistiškai reikšminga. Tai parodo, kad Eterio kainai tik pradėjus kristi, padaugėjo pervedimų į žetonus, susijusius su „Rug pull“ nusikalstama veikla ir vėliau jų kiekis palaipsniui mažėjo. Taip pat 9-jame paveiksle pateikiama grafinė vizualizacija į žetonus, susijusius su „Rug pull“ finansiniu nusikaltimu, atliktų pervedimų skaičiaus ir Eterio kainos palyginimas.

9 paveikslas

Pervedimų į „Rug pull“ nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2021-11-09 – 2022-06-18



Šaltinis: sudaryta autorės, remiantis Etherscan (2024), yahoo!finance (2024), Solidus Labs (2024)

Toliau apžvelgiamas, tačiau nenagrinėjamas ketvirtasis laikotarpis, tai yra, nuo 2022 metų birželio 19 dienos iki 2023 metų rugsėjo 24 dienos (imtinai), nes šiuo laikotarpiu Eterio kaina buvo nusistovėjusi. Tyrimo metu nustatyta, kad nagrinėjamu laikotarpiu buvo sukurti 35 žetonai, kurie susiję su „Rug pull“ nusikalstama veika, apie kuriuos buvo sukurti pranešimai internetiniame puslapyje Chainabuse (2024), taip pat papildomai yra nagrinėjami 48 žetonai, apžvelgti pirmuoju, antruoju ir trečiuoju nagrinėjamais laikotarpiais, į kuriuos buvo atlikti pervedimai tiriamuoju laikotarpiu (žr. 7 lentelę, 5 priedą).

7 lentelė

Ketvirtuoju tyrimo analizuojamu laikotarpiu 2022-06-19 – 2023-09-24 nagrinėjami žetonai

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data
1	Tradecurve (TCRV)	2023-04-28	19	XXX (XXX)	2023-07-26
2	Wall Street Memes (WSM)	2023-05-30	20	SARATOSHI NAGAMOTO (SARATOSHI)	2023-07-27
3	ShibaMemu (SHMU)	2023-06-28	21	HarryPotterObamaSonic20Inu (ETHEREUM)	2023-07-27
4	JUGS (\$JUGS)	2023-05-02	22	0xCoco (COCO)	2023-07-28
5	Kizuna AI (KIZUNA)	2023-08-29	23	tetris (TETRIS)	2023-07-28
6	EspressoBot (ESPS)	2023-08-31	24	RNS (RNS)	2023-07-29
7	Bitcoin30 (BTC30)	2023-08-13	25	iBOT (IBOT)	2023-07-29
8	watcher (WATCHER)	2023-08-13	26	Pond Coin (PNDC)	2023-08-05
9	Sugartown (SUGARTOWN)	2023-08-14	27	Towelie (TOWELIE)	2023-07-22
10	Unibot X (UNIBOT X)	2023-08-16	28	voQui Token (VOQUI)	2023-06-08
11	Jada AI (JADA AI)	2023-08-18	29	Mojo Jojo (MOJO)	2023-07-17
12	https://symbiosis.finance/ (SYMBIOSIS)	2023-08-28	30	YouGetNothing.eth (NOTHING)	2023-07-11
13	world AI (WORLD AI)	2023-08-11	31	PUMBAA (PUMB)	2023-07-05
14	SHIBBOT (SHIBBOT)	2023-08-16	32	Torochain (TORO)	2023-05-07
15	SHIC (SHIC)	2023-09-04	33	Eggs Pepe (EGGSPEPE)	2023-05-03
16	ハチ公 (HACHIKO)	2023-08-12	34	Matrix (MATRIX)	2022-10-02
17	SOPH AI Token (SOPH)	2023-07-25	35	Pixel Cats (PIXCATS)	2022-07-21
18	Algobot (ALGO)	2023-07-25			

Šaltinis: sudarytas autorės, remiantis Solidus Labs (2024)

Tam kad papildomai įsitikinti, kad šie žetonai yra susiję su neteisėta veikla, jie buvo patikrinti internetiniame puslapyje „Token Sniffer“ (Solidus Labs, 2024). Nustatyta, kad „Token Sniffer“ internetiniame puslapyje žetonų įvertinimas yra nulis ir dešimt iš šimto ir viena iš priežasčių, lėmusių tokius žetonų įvertinimus yra: „Tradecurve“ (TCRV), „voQui Token“ (VOQUI) (nepakeičiamasis žetonas) žetonų negalimas pardavimas, „ShibaMemu“ (SHMU) žetono neužrakintas likvidumas, vienuolikos – „Wall Street Memes“ (WSM), „Sugartown“ (SUGARTOWN), „<https://symbiosis.finance/>“ (SYMBIOSIS), „SHIBBOT“ (SHIBBOT), „SHIC“ (SHIC), „ハチ公“

(HACHIKO), „Mojo Jojo“ (MOJO), „YouGetNothing.eth“ (NOTHING), „PUMBAA“ (PUMB), „Torochain“ (TORO), „Pixel Cats“ (PIXCATS) – žetonų nepakankamas ir neužrakintas likvidumas, bei dvidešimt vieno – „JUGS“ (\$JUGS), „Kizuna AI“ (KIZUNA), „EspressoBot“ (ESPS), „Bitcoin30“ (BTC30), „watcher“ (WATCHER), „Unibot X“ (UNIBOT X), „Jada AI“ (JADA AI), „world AI“ (WORLD AI), „SOPH AI Token“ (SOPH), „Algobot“ (ALGO), „XXX“ (XXX), „SARATOSHI NAGAMOTO“ (SARATOSHI), „HarryPotterObamaSonic20Inu“ (ETHEREUM), „0xCoco“ (COCO), „tetris“ (TETRIS), „RNS“ (RNS), „iBOT“ (IBOT), „Pond Coin“ (PNDC), „Towelie“ (TOWELIE), „Eggs Pepe“ (EGGSPEPE), „Matrix“ (MATRIX) – žetonų negalimas pardavimas, nepakankamas bei neužrakintas likvidumas.

8 lentelė

Žetonų, kurių dabartinis likvidumas mažiau nei 0,01 Eterio, likvidumo analizė

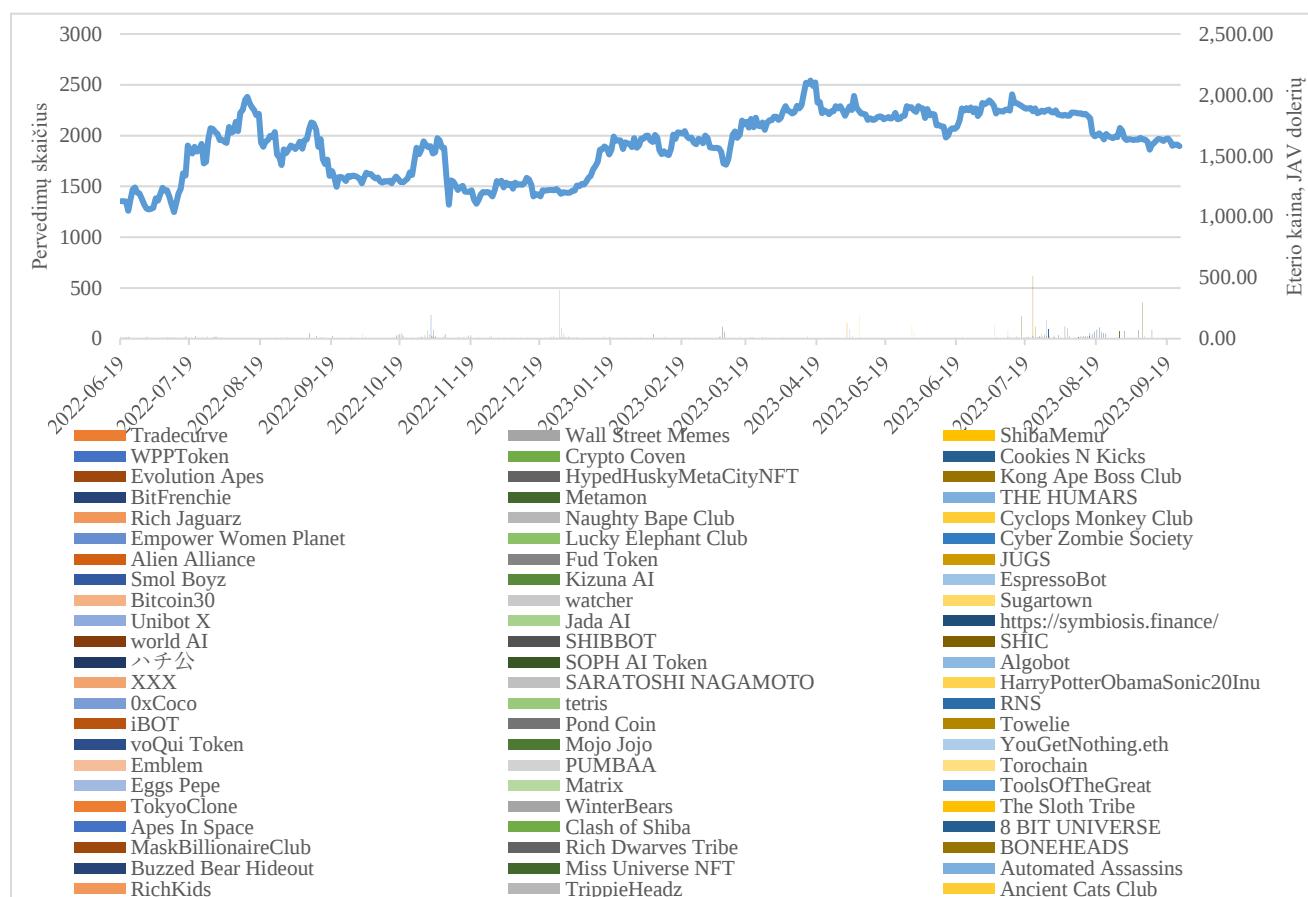
Eilės nr.	Žetono pavadinimas	Pradinis likvidumas	Likvidumas 2024-12-02 duomenimis, JAV dol.	Likvidumo pokytis, kartais
1	JUGS (\$JUGS)	22	80156.56	2200
2	Kizuna AI (KIZUNA)	2	7286.96	200
3	EspressoBot (ESPS)	5	18217.40	500
4	Bitcoin30 (BTC30)	10	36434.80	1000
5	watcher (WATCHER)	5	18217.40	500
6	Sugartown (SUGARTOWN)	10	36434.80	1000
7	Unibot X (UNIBOT X)	10	36434.80	1000
8	Jada AI (JADA AI)	10	36434.80	1000
9	https://symbiosis.finance/ (SYMBIOSIS)	10	36434.80	1000
10	world AI (WORLD AI)	15	54652.20	1500
11	SHIBBOT (SHIBBOT)	10	36434.80	1000
12	SHIC (SHIC)	47.88	174449.82	4788
13	ハチ公 (HACHIKO)	20	72869.60	2000
14	SOPH AI Token (SOPH)	10	36434.80	1000
15	Algobot (ALGO)	10	36434.80	1000
16	XXX (XXX)	10	36434.80	1000
17	SARATOSHI NAGAMOTO (SARATOSHI)	13	47365.24	1300
18	HarryPotterObamaSonic20Inu (ETHEREUM)	5	18217.40	500
19	0xCoco (COCO)	25	91087.00	2500
20	tetris (TETRIS)	20	72869.60	2000
21	RNS (RNS)	15	54652.20	1500
22	iBOT (IBOT)	15	54652.20	1500
23	Pond Coin (PNDC)	10.5	38256.54	1050
24	Towelie (TOWELIE)	1.11	4044.26	111
25	Mojo Jojo (MOJO)	5.01	18253.83	501
26	YouGetNothing.eth (NOTHING)	0.7	2550.44	70
27	PUMBAA (PUMB)	18.02	65655.51	1802
28	Torochain (TORO)	22.28	81176.73	2228
29	Eggs Pepe (EGGSPEPE)	3.5	12752.18	350
30	Matrix (MATRIX)	2.1	7651.31	210
31	Pixel Cats (PIXCATS)	1.01	3679.91	101

Šaltinis: sudarytas autorės, remiantis Solidus Labs (2024)

2024 metų gruodžio antros dienos duomenimis „Tradecurve“ (TCRV) likvidumas siekė 5,02 Eterio (2024 metų gruodžio antros dienos duomenimis – 18290,27 JAV dolerių), kai pradinis likvidumas siekė 55,5 Eterio (2024 metų gruodžio antros dienos duomenimis – 202213,14 JAV dolerių), tai yra, likvidumas per visą žetono gyvavimo laikotarpį sumažėjo 11,06 karto. Kalbant apie „Wall Street Memes“ (WSM) 2024 metų gruodžio antrą dieną likvidumas siekė 0,06 Eterio (2024 metų gruodžio antros dienos duomenimis – 218,61 JAV dolerių), kai pradinis likvidumas – 738,14 Eterio (2024 metų gruodžio antros dienos duomenimis – 2,69 mln. JAV dolerių), tai yra, likvidumas per visą žetono gyvavimo laikotarpį sumažėjo 12302,33 karto. Kitų žetonų pradinis likvidumas ir likvidumo pasikeitimas per visą žetonų gyvavimo laikotarpį pateikiamas 8 lentelėje, nes visų šių žetonų dabartinis likvidumas yra mažesnis nei 0,01 Eterio (2024 metų gruodžio antros dienos duomenimis – 36,43 JAV dolerių).

10 paveikslas

Pervedimų į “Rug pull” nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2022-06-19 – 2023-09-24



Šaltinis: sudaryta autorės, remiantis Etherscan (2024), yahoo!finance (2024), Solidus Labs (2024)

Taigi, pagal pateiktą 10 paveikslą galime matyti, kad Eterio kainai išliekant ganėtinai pastoviai operacijų kiekis į žetonus, susijusius su „Rug pull“ nusikalstama veikla, yra nedidelis. Daugiausiai pervedimų buvo atlikta 2023-07-22 į žetoną „Towelie“ (TOWELIE) – 617.

9 lentelė

Penktuoju tyrimo analizuojamu laikotarpiu 2023-09-25 – 2024-12-02 nagrinėjami žetonai

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data
1	Based Chill Guy (CHILLGUY)	2024-11-22	32	BVM (BVM)	2024-05-23
2	Rexas Finance (RXS)	2024-09-11	33	Espresso Systems (ESP)	2024-04-24
3	Ethereum Games (ETHG)	2024-06-22	34	LayerZero (ZRO)	2024-04-21
4	Pepe Unchained (PEPU)	2024-08-17	35	Renzo Protocol (EZ)	2024-04-23
5	American True Hero (TRUMP)	2024-11-18	36	RedSHIB (REDSHIB)	2024-01-24
6	Trump MAGA (TRUMPMAGA)	2024-10-30	37	Trism AI (TRISM)	2024-04-14
7	47th President of the United States (TRUMP47)	2024-10-22	38	BD20 (BD20)	2024-04-12
8	MOG CAT (MOG)	2024-09-14	39	Espresso (ESP)	2024-04-07
9	Bridge Payments (BRIDGE)	2024-10-27	40	NVIDIA AI (NVIDIA AI)	2024-04-05
10	BOME TRUMP (TRUMP)	2024-09-07	41	AZTEC (AZT)	2024-03-25
11	Neiro Pump (NEIRO)	2024-09-24	42	MetaStreet (MSTR)	2024-03-25
12	BlockDAG (BDAG)	2024-07-07	43	PIKAMOON (PIKA)	2024-03-12
13	Polymarket (POL)	2024-09-05	44	Apeiron (APRS)	2024-03-16
14	Babylon (BABL)	2024-08-25	45	SNAP (NAP)	2024-03-17
15	XELON (XELON)	2024-08-27	46	Fire (FIRE)	2024-02-19
16	BlackMythWukong (WUKONG)	2024-08-20	47	SUBSQUID (SQD)	2024-02-04
17	Morpho (MORPHO)	2024-08-09	48	Fluid Finance (FLUID)	2024-02-03
18	Linea Network (LINEA)	2024-08-02	49	Fuel Network (FUEL)	2024-02-01
19	zkEVM (ZKE)	2024-07-18	50	RAIT (RAIT)	2023-12-07
20	GanNamDog (GNDOG)	2024-07-31	51	Moon App (APP)	2024-10-10
21	Tos Coin (TOS)	2024-06-22	52	BEBE (BEBE)	2023-12-19
22	FreeDurov Token (FREED)	2024-08-24	53	Venom Network (VENOM)	2023-12-11
23	W Token (W)	2024-10-26	54	WRAPPED Protocol (WRAP)	2023-12-13
24	PEIPEI coin (PEIPEI)	2024-09-10	55	Circle Coin (CIRCLE)	2023-11-30
25	LayerZero (ZRO)	2024-06-19	56	BonkBob (BOBONK)	2023-11-30
26	DADDY TATE (DADDY)	2024-06-13	57	wagmicatgirlkanye420etfmoon hero (WCGH)	2023-11-17
27	SupraOracles (SUPRA)	2024-05-19	58	LINEA (L)	2023-10-17
28	Chaos Labs (CHAOS)	2024-05-24	59	Paxos Coin (PAXOS)	2023-10-30
29	Scroll (SCROLL)	2024-05-31	60	PEPEClassic (PEPECLASSIC)	2023-10-10
30	Monad (TBD)	2024-05-30	61	Fish (FISH)	2023-09-25
31	Scroll (SCROLL)	2024-05-18			

Šaltinis: sudarytas autorės, remiantis Solidus Labs (2024)

Galiausiai yra nagrinėjamas 3.1 magistro darbo dalyje minimas penktasis laikotarpis, tai yra, nuo 2023 metų rugsėjo 25 dienos iki 2024 metų gruodžio 2 dienos (imtinai). Tyrimo metu nustatyta, kad nagrinėjamu laikotarpiu buvo sukurti 61 žetonas, kurie susiję su „Rug pull“ nusikalstama veika,

apie kuriuos buvo sukurti pranešimai internetiniame puslapyje Chainabuse (2024), taip pat papildomai yra nagrinėjamas 61 žetonas, kurie buvo apžvelgti pirmuoju – ketvirtuoju nagrinėjamu laikotarpiu, į kuriuos buvo atlikti pervedimai tiriamuoju laikotarpiu (žr. 9 lentelę, 6 priedą).

Tam kad papildomai įsitikinti, kad šie žetonai yra susiję su neteisėta veikla, jie buvo patikrinti internetiniame puslapyje „Token Sniffer“ (Solidus Labs, 2024). Nustatyta, kad „Token Sniffer“ internetiniame puslapyje žetonų įvertinimas yra nulis ir dešimt iš šimto ir viena iš priežasčių, lėmusių tokius žetonų įvertinimus yra: „47th President of the United States“ (TRUMP47), „MOG CAT“ (MOG), „BOME TRUMP“ (TRUMP), „Neiro Pump“ (NEIRO) žetonų negalimas pardavimas, „Ethereum Games“ (ETHG), „W Token“ (W), „PEIPEI coin“ (PEIPEI) žetonų neužrakintas likvidumas, „Rexas Finance“ (RXS), „Pepe Unchained“ (PEPU), „BlockDAG“ (BDAG), „Linea Network“ (LINEA), „PIKAMOON“ (PIKA), „PIKAMOON“ (PIKA), „Moon App“ (APP) žetonų negalimas pardavimas bei neužrakintas likvidumas, dvidešimt dviejų – „American True Hero“ (TRUMP), „Polymarket“ (POL), „Morpho“ (MORPHO), „zkEVM“ (ZKE), „Tos Coin“ (TOS), „FreeDurov Token“ (FREED), „LayerZero“ (ZRO), „Chaos Labs“ (CHAOS), „Monad“ (TBD), „Scroll“ (SCROLL), „BVM“ (BVM), „Espresso Systems“ (ESP), „LayerZero“ (ZRO), „Renzo Protocol“ (EZ), „NVIDIA AI“ (NVIDIA AI), „MetaStreet“ (MSTR), „SUBSQUID“ (SQD), „Fluid Finance“ (FLUID), „RAIT“ (RAIT), „LINEA“ (L), „Paxos Coin“ (PAXOS), „PEPEClassic“ (PEPECLASSIC) – žetonų nepakankamas ir neužrakintas likvidumas, bei likusių dvidešimt šešių – žetonų negalimas pardavimas, nepakankamas bei neužrakintas likvidumas.

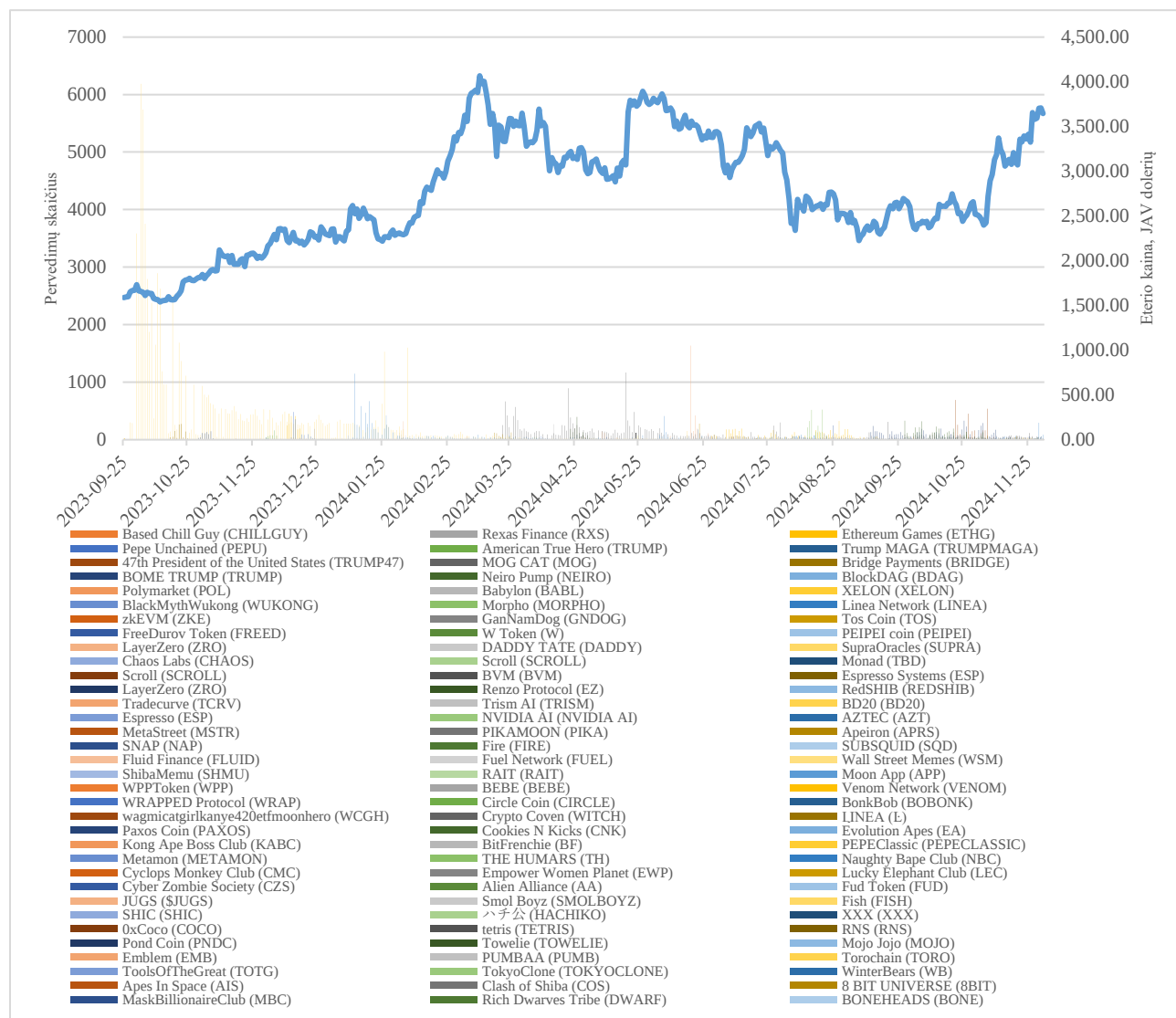
2024 metų gruodžio antros dienos duomenimis „Based Chill Guy“ (CHILLGUY) likvidumas siekė 0,58 Eterio (2024 metų gruodžio antros dienos duomenimis – 2113,22 JAV dolerių), kai pradinis likvidumas siekė 1 Eterį (2024 metų gruodžio antros dienos duomenimis – 3643,48 JAV dolerių), tai yra, likvidumas per visą žetono gyvavimo laikotarpį sumažėjo 1,72 karto. Kalbant apie „FreeDurov Token“ (FREED) 2024 metų gruodžio antrą dieną likvidumas siekė 0,76 Eterio (2024 metų gruodžio antros dienos duomenimis – 2769,04 JAV dolerių), kai pradinis likvidumas – 8 Eterio (2024 metų gruodžio antros dienos duomenimis – 29147,84 JAV dolerių), tai yra, likvidumas per visą žetono gyvavimo laikotarpį sumažėjo 10,53 karto. Kitų žetonų pradinis likvidumas ir likvidumo pasikeitimas per visą žetonų gyvavimo laikotarpį pateikiamas 7-ajame priede, nes visų šių žetonų dabartinis likvidumas yra mažesnis nei 0,01 Eterio (2024 metų gruodžio antros dienos duomenimis – 36,43 JAV dolerių).

Taigi, atlikus antrojo laikotarpio, tai yra, nuo 2023 metų rugsėjo 25 dienos iki 2024 metų gruodžio 2 dienos (imtina), duomenų analizę, nustatyta, kad iš 122 žetonų, susijusių su „Rug pull“

nusikalstama veikla, 24 žetonų kritinių t-reikšmių neįmanoma apskaičiuoti, nes pervedimai buvo atlikti tik vieną dieną.

11 paveikslas

Pervedimų į „Rug pull“ nusikalstama veika susijusius žetonus palyginimas su Eterio kainomis laikotarpiu 2023-09-25 – 2024-12-02



Šaltinis: sudaryta autorės, remiantis Etherscan (2024), yahoo!finance (2024), Solidus Labs (2024)

Taip pat nustatyta, kad 51 žetono apskaičiuotos t-testo reikšmės viršija apskaičiuotas kritines t-reikšmes, tai reiškia, kad yra statistiškai reikšminga koreliacija tarp Eterio kainos augimo ir į 51 žetoną, kurie susiję su finansiniu nusikaltimu „Rug pull“, atliktų pervedimų (žr. 8 priedą). 32 žetonų statistiškai reikšminga koreliacija yra neigiama, tai yra, Eterio kainai didėjant mažėja pervedimų

skaičius, o 19 žetonų statistiškai reikšminga koreliacija yra teigiama, tai yra, kad Eterio kainai mažėjant padaugėjo pervedimų skaičius. Atsižvelgus į tai, kad pervedimų skaičius į žetonus, susijusius su „Rug pull“ nusikaltimu, yra dalinamas per nagrinėjamus laikotarpius, o taip pat atskirai nagrinėjant pervedimus į žetonus galima matyti, kad pervedimų skaičius yra labai didelis, kuomet yra sukuriamas žetonas, papildomai yra apskaičiuota bendroji T.testo reikšmė nagrinėjamu penktuoju laikotarpiu. Nustatyta, kad bendroji T.testo reikšmė – -171,74, o kritinė t-reikšmė – -1,96, tai reiškia, kad bendroji koreliacija neigiamai statistiškai reikšminga. Tai parodo, kad Eterio kainai tik pradėjus augti, padaugėjo pervedimų į žetonus, susijusius su „Rug pull“ nusikalstama veikla ir vėliau jų kiekis palaipsniui mažėjo. Tačiau svarbu atkreipti dėmesį į tai, kad Eterio kaina, paskutiniu nagrinėjamu laikotarpiu, gali būti dar nepasiekus piko, tai reiškia, kad tolimesniais, nenagrinėjamais laikotarpiais, Eterio kaina galėjo kilti ir todėl vertinant bendrąjį pervedimų skaičių į žetonus, susijusius su „Rug pull“ nusikaltimu, gali būti neteisingas. Taip yra todėl, kad Eterio kainai kylant, daugėja kuriamų žetonų, susijusių su nusikalstama veika „Rug pull“, tačiau pranešimai yra sukuriami tik tuomet kai, investuotojas supranta, kad žetonas yra susijęs su sukčiavimu. Taip pat 10-jame paveiksle pateikiama grafinė vizualizacija į žetonus, susijusius su „Rug pull“ finansiniu nusikaltimu, atliktų pervedimų skaičiaus ir Eterio kainos palyginimas.

Taigi, susisteminus visus gautus rezultatus, atsižvelgiant į tai, kad antruoju bei penktuoju laikotarpiais Eterio kaina kilo, o trečiuoju – krito, rezultate buvo gauta, kad 100 žetonų, kurie susiję su finansiniu nusikaltimu „Rug pull“, atliktų pervedimų skaičius, atsižvelgiant į nagrinėjamus laikotarpius, statistiškai reikšmingai neigiamai arba teigiamai koreliuoja, atsižvelgiant į tai ar Eterio kaina kilo ar mažėjo (statistiškai reikšmingai neigiamai koreliuoja 79 žetonų, kurie susiję su finansiniu nusikaltimu „Rug pull“, atliktų pervedimų skaičius su augančia Eterio kaina, o su mažėjančia Eterio kaina, statistiškai reikšmingai teigiamai koreliuoja 21 žetonas, kurie susiję su finansiniu nusikaltimu „Rug pull“, pervedimų skaičius). Todėl rezultate parodoma, kad atlikus tyrimą daugiau nei pusės įvertintų į žetonus, susijusių su „Rug pull“ nusikalstama veika, atliktų pervedimų skaičius mažėjo, lyginant su Eterio kainos žymiu pokyčiu (*10 formulė*).

$$H_0: 100 \geq 43 \quad (10)$$

Daroma išvada, kad H_0 , iškelta, magistro darbo 2.2 dalyje, hipotezė yra patvirtinama (*6 formulė*), ir teigiama, kad Eterio kainos žymus pokytis lemia pervedimų skaičiaus mažėjimą į daugumą žetonų, susijusių su „Rug pull“ finansiniu nusikaltimu. Taip pat, susisteminus visus gautus ir minėtas anksčiau žinias apie „Rug pull“ finansinį nusikaltimą, įvertinus gautus duomenis bei

patvirtinus hipotezę ir jau teorinėje dalyje pastebėjus, jog nuoseklaus apsisaugojimo metodo ar modelio investuotojui į virtualius žetonus nėra, yra pereinama prie tokio modelio sukūrimo.

3.3 Modelis, skirtas investuotojams įsitikinti, kad žetonas nėra susijęs su „Rug pull“ finansiniu nusikaltimu

Remiantis magistrinio darbo teorine ir tyrimo dalimis, buvo pastebėta, jog asmenys pastebėje virtualių valiutų, tokių kaip Eteris, kainų kylimą ar kritimą pradeda investuoti neatsakingai. Šiais atvejais asmenys susiduria su įvairiomis apgaulės formomis susijusiomis su virtualiomis valiutomis ir šie neapdairūs veiksmai, gali lemti didelį nuostolį investuotojams. Išanalizavus mokslinę literatūrą pirmoje magistro darbo dalyje ir pateikus įvairius su skaitmeninėmis valiutomis susijusius nusikaltimus, buvo pastebėta, jog nuo 2021 metų tapo populiariu „Rug pull“ virtualios valiutos Eterio pagrindu kuriamų žetonų sukčiavimo būdas, kuriam iki šių dienų dar nėra sukurtų prevencinių priemonių. Atsižvelgus į tai, kad „Rug pull“ finansiniam nusikaltimui įvykdyti reikia mažai kaštų, o taip pat minimas sukčiavimo atvejis yra sėkmingai įvykdomas, nes nėra sukurtų prevencinių priemonių tokiam nusikaltimui sustabdyti, šis būdas vis dar taikomas praktikoje, o investuotojai vis dar atiduoda savo pinigus netikrų žetonų kūrėjams. Mokslinėje literatūroje pateikiami tam tikri aspektai, kuriuos galima pasitikrinti prieš investuojant į tokius apgaulingus žetonus, tačiau nenurodant kokiais būdais tai turi būti atlikta. Tiriant „Rug pull“ nusikaltimus, o ypač atsekant pavedimus buvo identifikuota kaip pasitikrinti ar žetonas, yra susijęs su „Rug pull“ nusikalstama veika. Tokiu atveju remiantis moksliniais straipsniais, ir pridėjus ištirtą bei pastebėtą informaciją, šioje magistro darbo dalyje sukuriamas modelis, kuris padės asmenims investuojant į žetonus, prieš tai pasitikrinti ir nepapulti į virtualių valiutų nusikaltimų pinkles.

Taigi, sukurtą modelį sudaro 9 žingsniai. 7 pirmieji žingsniai yra pateikiami, remiantis išanalizuotais kriterijais 1.4 magistro darbo dalyje, kurie padeda suprasti, kad žetonas yra susijęs su „Rug pull“ decentralizuotų finansų finansiniu nusikaltimu, kuriuos pateikia Cernera ir kt. (2022), Chainalysis (2022), Huang ir kt. (2023), Jeleskovic (2024), Sharma ir kt. (2024), Stangl ir Neumann (2024), Sun ir kt. (2024), Xia ir kt. (2021) ir taip tyrimo metu įgyta praktika, kaip praktiškai šiuos žingsnius atlikti. Tačiau, kuriant modelį pastebėta jog šių 7 žingsnių negana ir remiantis asmenine bei tyrimo metu įgyta patirtimi, buvo sukurti dar 2 nauji modelio etapai, kurie užtikrins dar didesnę šio modelio efektyvumą. Tęsiant apie teorinę dalimi remiantis kurtus žingsnius – pavyzdžiui, 2-ojo žingsnio atveju, remiantis tyrimui atrinktais duomenimis, galima identifikuoti, kad iš 146 žetonų,

susijusių su „Rug pull“ finansiniu nusikaltimu, į 138 žetonus, žetonų kūrėjas atliko daugiau negu vieną pervedimą. 3-iojo žingsnio atveju, remiantis tyrimui atrinktais duomenimis, nustatyta, kad 10 žetonų, susijusių su „Rug pull“ nusikaltimu, gyvavo tik vieną dieną, o 8 aštuoni žetonai – tik 2 dienas. 5-ojo žingsnio atveju, nustatyta, kad iš 146 žetonų, susijusių su „Rug pull“ finansiniu nusikaltimu, 141 žetonų, tai yra, 96,6 procentai visų analizuojamų žetonų, buvo neužrakintas likvidumas. 6-ojo žingsnio atveju, remiantis internetinio puslapio „Token Sniffer“ duomenimis, identifikuota, kad 83 žetonų likvidumas yra nepakankamas, tai yra, 56,8 procentai visų analizuojamų žetonų, iš kurių, 81 žetono likvidumas nesiekia 300 JAV dolerių. 7-ojo žingsnio atveju buvo nustatyta, kad 58 žetonų, kurie susiję su „Rug pull“ nusikalstama veika, remiantis internetinio puslapio „Token Sniffer“ duomenimis, nebuvo galima parduoti. Galiausiai, 8-ojo žingsnio atveju, nustatyta 5 žetonų kūrėjai sukūrė daugiau negu 2 žetonus susijusius su „Rug pull“ nusikaltimu. 2 žetono kūrėjai sukūrė po 2 žetonus, 1 žetono kūrėjas sukūrė – 3 žetonus, 1 žetono kūrėjas sukūrė – 6 žetonus ir 1 žetono kūrėjas sukūrė – 10 žetonų. Taigi, galima matyti, kad praktinė patirtis, atsižvelgiant į teorinius aspektus, rodo, kad iš tiesų tokie kriterijai, kaip neužrakintas, nepakankamas likvidumas ar negalimas žetonų pardavimas lemia, kad buvo įvykdyta „Rug pull“ nusikalstama veika susijusi su žetonais, todėl yra svarbu ištransliuoti būsimiems ir esamiems investuotojams, kas parodo, kad žetonas gali būti susijęs sukčiavimu, konkrečiai „Rug pull“ atveju.

Toliau pateikiamas modelis, skirtas investuotojams įsitikinti, kad žetonas nėra susijęs su „Rug pull“ finansiniu nusikaltimu (žr. 12 pav.).

12 paveikslas

Apsisaugojimo modelis nuo su „Rug pull“ finansiniu nusikaltimu susijusio žetono



Šaltinis: sudarytas autorės

1 žingsnis. Anoniminių kūrėjų vertinimas. Investuotojas turėtų atsižvelgti į asmenis, atsakingus už naujų virtualių valiutų projektų kūrimą, patikimumą. Reikėtų įsivertinti tokius dalykus kaip - ar kūrėjai ir projekto reklamuotojai yra žinomi virtualių valiutų bendruomenėje bei kokia yra jų reputacija? Tai galima padaryti, naudojantis internetinius šaltinius, tokius kaip „Twitter“, prisijungiant į komunikacijai skirtas programines įrangas, tokias kaip „Discord“ ir kitais prieinamais žiniasklaidos šaltiniais. Taip pat, jeigu žetono kūrėjai, turi sukūrę internetinius puslapius, susijusius su žetonais, verta paanalizuoti informaciją apie žetonus. Jeigu jokios informacijos apie kūrėjus nėra, tai gali būti labai svarbus ženklas, jog vertėtų į tokį žetoną neinvestuoti.

*2 žingsnis. Staiga ir didelio kainų pokyčio (angl. **skyrocketing price movement**) vertinimas.* Didelis kainų pokytis yra dažnas variantas pasitaikantis tik sukūrus naują projektą, tačiau dažniausiai didelis kylimas nurodo, jog tai tiesiog žetono vertės užkėlimas prieš didelį smukimą. Jeigu žetonas susijęs su Eteriu, kainos svyravimą galima patikrinti „Etherscan“ internetiniame puslapyje, pasirinkus norimą žetoną (į paieškos lauką suvedus žetono adresą arba žetono pavadinimą), ir nuėjus į skiltį „Analytics (Etherscan, 2024)“. Atkreiptinas dėmesys, kad kainų augimą gali lemti patys žetono kūrėjai, todėl taip pat svarbu patikrinti ar žetono kūrėjas, siekdamas išpūsti žetono kainą, neatliko didelio kiekio pervedimų tik sukūrus žetoną. Šiuo atveju reikėtų atlikti žetono operacijų analizę. Kaip ir minėta anksčiau, tai galima atlikti internetiniame puslapyje „Etherscan“. Pasirinkus norimą žetoną (į paieškos lauką suvedus žetono adresą arba žetono pavadinimą) reikėtų peržiūrėti žetono pirmąsias operacijas. Identifikavus žetono kūrėjo adresą (pirmoje operacijoje, stulpelyje „In“ yra nurodoma, kad žetonas yra sukurtas „Create: „žetono pavadinimas““, o stulpelyje „From“ yra nurodomas žetono kūrėjo adresas), investuotojas turėtų peržiūrėti kiek į žetoną buvo atlikta žetono kūrėjo pervedimų.

3 žingsnis. Projekto gyvavimo laikotarpio vertinimas. Investuotojams reikėtų pasisaugoti nuo ką tik sukurtų ir nežinomų žetonų, kadangi dažnu atveju sukčiavimai, taip ir „Rug pull“ atveju, įvyksta per pirmąsias projekto gyvavimo dienas. Jeigu projektas gyvuoja ilgiau nei vieną dieną ar net daugiau, tai ženklas, tačiau ne pats patikimiausias, jog žetonas nėra susijęs su nusikalstamos veikos atveju. Žetono gyvavimo laiką galima patikrinti internetiniame puslapyje „Token sniffer“ (Solidus Labs, 2024).

4 žingsnis. Žetono operacijų analizė. Investuotojams reikėtų išanalizuoti operacijų kiekį per pirmąsias projekto dienas, nes žetonai susiję su nusikalstama veikla, pasižymi tokiomis savybėmis kaip trumpalaikis prekybos ciklas, tai reiškia, kad operacijos susijusios su žetonu pagrinde įvyksta per pirmąsias žetono sukūrimo dienas. Šį žingsnį galima atlikti pasinaudojant „Etherscan“ internetiniu puslapiu, jei žetonas buvo sukurtas Eterio pagrindu (Etherscan, 2024). Vienas iš būdų tai atlikti, yra

rankiniu būdu peržiūrint žetono operacijas, kuomet „Etherscan“ internetiniame puslapyje pasirinkus norimą žetoną (į paieškos lauką suvedus žetono adresą arba žetono pavadinimą), galima matyti stulpelyje „Age“ kada ir kokios operacijos buvo sukurtos arba galima išsitraukti visų žetonų operacijų istoriją, paspaudus lauką „Download: CSV export“.

5 žingsnis. Neužrakinto likvidumo patikrinimas. Vienas iš paprasčiausių būdų patikrinti ar žetonas, į kurį planuojama investuoti, nėra susijęs su „Rug pull“ nusikalstama veika, yra likvidumo tikrinimas. Jeigu likvidumas nėra užrakintas, projekto kūrėjui niekas nedraudžia atsitraukti ištraukus visą likvidumą. Likvidumas nuo žetono pasiūlymo yra užrakinamas ir galioja dažniausiai tris ar net penkis metus. Ar žetono likvidumas yra užrakintas, galima patikrinti internetiniame puslapyje „Token sniffer“ (Solidus Labs, 2024). Jei žetonas yra nepakeičiamasis žetonas, ar likvidumas yra užrakintas, galima patikrinti žetono kūrėjo piniginėje – prie operacijų, susijusių su kūrėjo žetonu turi būti nurodyta angliškai „Locked liquidity“, naudojantis internetiniu puslapiu „Etherscan“ (Etherscan, 2024).

6 žingsnis. Pakankamo likvidumo patikrinimas. Taip pat investuotojas turėtų patikrinti likvidumo fondo procentą, jeigu jis yra užrakintas. Vertinama, kad tinkamas likvidumas yra daugiau nei 95 procentai viso likvidumo fondo arba ne mažiau nei 300 JAV dolerių. Ar žetono likvidumas yra pakankamas, galima patikrinti internetiniame puslapyje „Token sniffer“ (Solidus Labs, 2024).

7 žingsnis. Žetonų patikrinimas. Visi saugūs žetonų projektai pereina trečiųjų šalių patikrinimus bei saugos reikalavimų atitikimus - auditus. Jeigu nerandate informacijos iš patikimų ir gerai žinomų trečiųjų šalių tikrintojų tai taip pat, gali būti dar vienas ženklas jog vienetas, į kurį norima investuoti yra nepatikimas. Ar žetonas yra saugus investuoti, tai galima patikrinti internetiniame puslapyje „Token sniffer“, skiltyje „Score“ (Solidus Labs, 2024).

8 žingsnis. Dirbtinio intelekto pasitelkimas. Dirbtinis intelektas šiais laikais yra puiki priemonė ne tik generuoti paveikslėlius ar pasiklausti įprastinių, kasdinių klausimų, tačiau mokančiam juo naudotis, tai yra galimybė atlikti sunkias ir laiko užtrunkančias analizes bei palyginimus. Būtent dirbtinis intelektas šiame modelyje gali greitai ir efektyviai patikrinti informaciją bei pateikti analizę, tokiu formatu kokiu jo paprašysite, apie pasirinktą virtualų žetoną. Šioje vietoje galima pasikliauti pasaulyje populiariausiais ir viešai prieinamais sukurtais dirbtiniais intelektais tokiais kaip „Chat GPT“, „Claude.ai“ ar „Microsoft Copilot“.

9 žingsnis. Išplėstinio „Rug pull“ atvejo analizė. Mokslinės literatūros analizės metu, buvo identifikuotas „Rug pull“ finansinio nusikaltimo metodas apibrėžiamas kaip išplėstinis „Rug pull“, kuomet kūrėjai tuo pačiu piniginės adresu sukuria kelis žetonus, susijusius su „Rug pull“ finansiniu

nusikaltimu (Sharma ir kt., 2024). Todėl 9-ajame žingsnyje siūloma, atlikus visus aukščiau minėtus žingsnius ir identifikavus žetono kūrėją ir žetoną, kurie susiję su „Rug pull“ finansiniu nusikaltimu, peržiūrėti ar žetono kūrėjas nėra sukūręs daugiau žetonų, tam kad nereikėtų atlikti visų modelio žingsnių iš naujo pasirenkant kitą žetoną, kuris susijęs su tuo pačiu žetono kūrėju, į kurį norima investuoti.

IŠVADOS IR PASIŪLYMAI

1. Išnagrinėjus mokslinius šaltinius, pirmiausia buvo išryškinti decentralizuotų ir tradicinių finansų panašumai bei skirtumai. Taip pat nustatyta, kad dėl decentralizuoto veikimo, trūkstamo reguliavimo bei anonimiškumo - decentralizuotų finansų sritis tampa vis patrauklesnė nusikalstamai veiklai. Remiantis anksčiau paminėtu faktu, identifikuota, kad yra svarbu ir aktualu analizuoti finansinius nusikaltimus decentralizuotų finansų ekosistemoje, tam kad žinoti kaip juos atpažinti ir kaip nuo jų apsisaugoti. Atlikus mokslinės literatūros analizę identifikuota, kad „Rug pull“ finansinis nusikaltimas yra svarbus analizės atvejis, nes 2021 metais, „Rug pull“ tapo vienas iš pagrindinių finansinių nusikaltimų schemų, atsižvelgiant į pasisavintų lėšų kiekį bei nusikaltimų dažnumą. Išnagrinėjus mokslinius šaltinius, nustatyta, kad bendro sutarimo, kokie finansinio nusikaltimo „Rug pull“ tipai nėra, todėl remiantis moksline literatūra ir susisteminus ją, buvo sukurta „Rug pull“ finansinio nusikaltimo tipologija. Nustatyta, kad „Rug pull“ gali būti suskirstoma į tris tipus: švelnusis „Rug pull“, sunkusis „Rug pull“ ir pasikartojantis „Rug pull“. Taip pat identifikuota, kad „Rug pull“ gali įvykti trejomis kryptimis: apribojant žetonų pardavimus, pašalinant likvidumą bei išpūtus kainas atliekamas staigus žetono pardavimas.
2. Atlikus išsamią literatūros analizę ir identifikavus, kad net iki dabar dar nėra sukurtų priemonių, kurios identifikuotų „Rug pull“ finansinius nusikaltimus decentralizuotoje finansų rinkoje, taip pat išgryninus, kad 2021 metais, „Rug pull“ tapo vienas iš pagrindinių finansinių nusikaltimų schemų, atsižvelgiant į pasisavintų lėšų kiekį bei nusikaltimų dažnumą, antrojoje magistro darbo dalyje pateikiama metodologija, kurios pagrindu yra atliekama trečiojoje darbo dalyje: Eterio kainų ir finansinių nusikaltimų lyginamoji analizė, Eterio kainų ir pervedimų į žetonus, susijusių su „Rug pull“, palyginimas, modelio, kaip patikrinti, jog žetonas susijęs su „Rug pull“ nusikalstama veikla, kūrimas.
3. Pasirinkus Eterio kainos analizuojamą laikotarpį, tai yra, nuo 2014 metų iki dabar, dėl išaugusio virtualių valiutų populiarumo, įvertinus pateiktus duomenis ir tam, kad būtų lengviau apsibrėžti bei analizuoti pateiktus duomenis, virtualios valiutos Eterio gyvavimą ir vertingumą suskirsčius į penkis etapus, buvo atliktas palyginimas su decentralizuotų finansų finansinių nusikaltimų aktyvumu. Nustatyta, kad virtualių valiutų vertė ir atliekamų finansinių nusikaltimų, susijusių su skaitmeninėmis valiutomis, kiekiai koreliuoja tarpusavyje. Pritaikius

inferencinės statistikos metodą Eterio kainų kitimo ir investuotojų pervedimų į decentralizuotų finansų finansinio nusikaltimo „Rug pull“ virtualius žetonus palyginimui, patvirtinta hipotezė, kad Eterio kainos žymus pokytis lemia pervedimų skaičiaus mažėjimą į daugumą žetonų, susijusių su „Rug pull“ finansiniu nusikaltimu.

4. Identifikavus, kad nuo 2021 metų tapo populiariu „Rug pull“ virtualios valiutos Eterio pagrindu kuriamų žetonų sukčiavimo būdas, ir nustačius, kad iki šių dienų dar nėra sukurtų prevencinių priemonių siekiant apsaugoti nuo „Rug pull“ finansinio nusikaltimo, trečiojoje magistro darbo dalyje buvo sukurtas modelis, skirtas investuotojams įsitikinti, kad žetonas nėra susijęs su „Rug pull“ finansiniu nusikaltimu. Sukurtas modelis susideda iš 9 žingsnių: pirmasis žingsnis – anoniminių kūrėjų vertinimas, antrasis – staigaus ir didelio kainų pokyčio vertinimas, trečiasis – projekto gyvavimo laikotarpio vertinimas, ketvirtasis – žetono operacijų analizė, penktasis – neužrakinto likvidumo patikrinimas, šeštasis – pakankamo likvidumo patikrinimas, septintasis – žetonų patikrinimas, aštuntasis – dirbtinio intelekto pasitelkimas, devintasis – išplėstinio „Rug pull“ atvejo analizė.

Remiantis magistro darbo tyrime gautais rezultatais ir sukurtu modeliu, skirtu investuotojams įsitikinti, kad žetonas nėra susijęs su „Rug pull“ finansiniu nusikaltimu, teikiami pasiūlymai:

1. Atliktos mokslinės literatūros analizės metu pastebėta, jog nuo 2021 metų išpopuliarėjusio „Rug pull“ decentralizuotų finansų finansinio nusikaltimo nėra susisteminto būdo apsaugoti. Tyrimo dalyje įvertinus keliamus nuostolius ir pastebėjus, jog investuotojai yra linkę investuoti į virtualius žetonus yra siūloma investuotojams naudotis sudarytu modeliu iš 9 žingsnių, eiliškumo tvarka, kurių visų laikydamasis investuotojas galės pasitikrinti ir įsitikinti, jog virtualus žetonas į kurį planuojama investuoti nėra eilinis „Rug pull“ decentralizuotų finansų finansinis nusikaltimas.
2. Remiantis įgyta praktika atliekant magistro darbo tyrimo dalį, buvo pastebėta, jog analizuojant virtualius žetonus ir tiriant jų savybes dažnai tenka naudoti ne vieną įrankį, svetainę ar programinę įrangą. Atsižvelgus į sunaudojamus laiko kaštus, atliekant kiekvieną modelio žingsnį, ir siekiant lengviau pasiekti susistemintą informaciją apie decentralizuotus finansus yra siūloma įsigyti trečiųjų šalių, tokių kaip „Chainalysis“, analizės paslaugas. Tai internetinė svetainė, trečiosios šalies, kuri atlieka įvairiapusių auditus susijusius su virtualiomis valiutomis. Tai patogus ir paprastas naudotis, dėl savo nesudėtingos grafinės sąsajos, įrankis virtualių valiutų ar žetonų analizei.

3. Atsižvelgiant į tai, kad investuotojai vis dar investuoja į virtualius žetonus susijusius su „Rug pull“ finansiniu nusikaltimu buvo pastebėta, jog programinė įranga ir sistemos pritaikytos prekiavimui virtualiais žetonais turi nepakankamą apsaugą. Siūloma programinėje įrangoje ir sistemose, kuriose yra prekiaujama tokiais žetonais įdiegti automatizuotą apsaugos sistemą, kuri neleistų paleisti projekto viešai prieš tai jo atsakingai nepatikrinus.
4. Tęsiant šio magistro darbo mintį, siūloma išnagrinėti kitus finansinius nusikaltimus decentralizuotų finansų ekosistemoje ir išnagrinėjus tų nusikaltimų ypatybes bei įvertinus kitų mokslininkų pateikiamus rezultatus, sudaryti modelius apsisaugojimui nuo decentralizuotų finansų finansinių nusikaltimų.

LITERATŪRA IR ŠALTINIAI

- Abdelrahman, M. (2022). Blockchain Cryptography and Security Issues. *International Journal of Computer Science & Engineering Survey*, 13(5/6), 01–07. Žiūrėta 2024-10-17. Prieiga internetu: <https://doi.org/10.5121/ijcses.2022.13601>
- Acharya, B. ir Holz, T. (2024). *An Explorative Study of Pig Butchering Scams*. Žiūrėta 2024-12-15. Prieiga internetu: <http://arxiv.org/abs/2412.15423>
- Aggarwal, D. (2022). Defining and measuring market sentiments: a review of the literature. *Qualitative Research in Financial Markets*, 14(2), 270–288. Žiūrėta 2024-10-17. Prieiga internetu: <https://doi.org/10.1108/QRFM-03-2018-0033>
- Ahmed, J. (2022). *French Influencer Rug Pulls \$960,000 from Billionaire Dogs NFT Project*. Žiūrėta 2024-12-20. Prieiga internetu: <https://www.cryptoknowmics.com/news/french-influencer-rug-pulls-960000-from-billionaire-dogs-nft-project>
- Albina Hysaj. (2023). Decentralized Finance. *International Journal of Advanced Natural Sciences and Engineering Researches*. Žiūrėta 2024-10-17. Prieiga internetu: <https://doi.org/10.59287/as-ijanser.195>
- Allua, S., Thompson, C. (2009). Inferential Statistics. *Air Medical Journal*, 28(4), 168–171. Žiūrėta 2024-12-01. Prieiga internetu: <https://doi.org/10.1016/j.amj.2009.04.013>
- Anna Fleck. (2022). *The Evolution of the Crypto Economy*. Žiūrėta 2024-10-25. Prieiga internetu: <https://www.statista.com/chart/27561/evolution-of-the-crypto-economy/>
- Aramonte S., Huang W. ir Schrimpf A. (2021). *DeFi risks and the decentralisation illusion*. Žiūrėta 2024-10-17. Prieiga internetu: https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf
- Askar, S., Shamal Abdulkhaleq, I. ir Wahhab Kareem, S. (2021). *Blockchain systems: analysis, applications, & risks*. Žiūrėta 2024-10-10. Prieiga internetu: <https://doi.org/10.5281/zenodo.5221972>
- Auer, R., Haslhofer, B., Kitzler, S., Saggese, P. ir Victor, F. (2024). The technology of decentralized finance (DeFi). *Digital Finance*, 6(1), 55–95. Žiūrėta 2024-10-10. Prieiga internetu: <https://doi.org/10.1007/s42521-023-00088-8>
- Aurangzeb, S., Aleem, M., Iqbal, M. A. ir Islam, M. A. (2017). Ransomware: A Survey and Trends. *Journal of Information Assurance and Security* (T. 12). Žiūrėta 2024-10-17. Prieiga internetu: https://www.researchgate.net/publication/317380115_Ransomware_A_Survey_and_Trends

- Autorité des Marchés Financiers (AMF). (2023). *DECENTRALISED FINANCE (DEFI), TRADING PROTOCOLS AND GOVERNANCE ISSUES*. Žiūrėta 2024-10-10. Prieiga internetu: <https://www.amf-france.org/sites/institutionnel/files/private/2023-06/AMF%20Discussion%20Paper%20on%20Decentralised%20Finance%20VEN.pdf>
- Azar, P. D., Baughman, G., Carapella, F., Gerszten, J., Lubis, A., Perez-Sangimino, J., Rappoport, D. E., Scotti, C., Swem, N., Vardoulakis, A. ir Werman, A. (2022). The Financial Stability Implications of Digital Assets. *Finance and Economics Discussion Series*, 2022–058, 1–31. Žiūrėta 2024-10-17. Prieiga internetu: <https://doi.org/10.17016/feds.2022.058>
- Beinke, M., Beinke, J. H., Anton, E. ir Teuteberg, F. (2024). Breaking the chains of traditional finance: A taxonomy of decentralized finance business models. Žiūrėta 2024-12-01. Prieiga internetu: *Electronic Markets*, 34(1), 29. <https://doi.org/10.1007/s12525-024-00704-4>
- Bekemeier, F. (2023). A primer on the insurability of decentralized finance (DeFi). *Digital Finance*, 5(3–4), 643–687. Žiūrėta 2024-11-15. Prieiga internetu: <https://doi.org/10.1007/s42521-023-00093-x>
- BIS. (2023). *The crypto ecosystem: key elements and risks*. Žiūrėta 2024-11-15. Prieiga internetu: <https://www.bis.org/publ/othp72.pdf>
- Boyle, P. (2022). *Project Shura Rug Pulls for Over \$1.7M*. Žiūrėta 2024-12-20. Prieiga internetu: <https://medium.com/coinmonks/project-shura-rug-pulls-for-over-1-7m-949e3770ee83>
- Botha, J. G., Botha, D. ir Leenen, L. (2023). An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022. *International Conference on Cyber Warfare and Security*, 18(1), 36–48. Žiūrėta 2024-11-15. Prieiga internetu: <https://doi.org/10.34190/iccws.18.1.1087>
- Bourveau, T., Brendel, J. ir Schoenfeld, J. (2024). Decentralized Finance (DeFi) assurance: early evidence. *Review of Accounting Studies*, 29(3), 2209–2253. Žiūrėta 2024-10-17. Prieiga internetu: <https://doi.org/10.1007/s11142-024-09834-8>
- Brini, A. ir Lenz, J. (2024). A comparison of cryptocurrency volatility-benchmarking new and mature asset classes. *Financial Innovation*, 10(1), 122. Žiūrėta 2024-10-17. Prieiga internetu: <https://doi.org/10.1186/s40854-024-00646-y>
- Campbell-Verduyn, M. (2018). *Bitcoin and Beyond*. Žiūrėta 2024-12-01. Prieiga internetu: <https://library.oapen.org/bitstream/handle/20.500.12657/29557/1000376.pdf>
- Cernera, F., Morgia, M. La, Mei, A. ir Sassi, F. (2022). *Token Spammers, Rug Pulls, and SniperBots: An Analysis of the Ecosystem of Tokens in Ethereum and the Binance Smart Chain (BNB) SEE PROFILE Token Spammers, Rug Pulls, and SniperBots: An Analysis of the Ecosystem of Tokens*

- in *Ethereum and the Binance Smart Chain (BNB)*. Žiūrėta 2024-11-15. Prieiga internetu: <https://doi.org/10.48550/arXiv.2206.08202>
- Chainabuse. (2024). *Report malicious crypto activity*. Žiūrėta 2024-12-30. Prieiga internetu: <https://www.chainabuse.com/>
- Chainalysis. (2022). *The 2022 Crypto Crime Report*. Žiūrėta 2024-12-20. Prieiga internetu: <https://www.chainalysis.com/blog/2021-crypto-scam-revenues/>
- Chainalysis. (2023). *The 2023 Crypto Crime Report*. Žiūrėta 2024-12-20. Prieiga internetu: https://static.poder360.com.br/2024/01/Chainalysis-Crypto_Crime_Report_2023.pdf
- Chainalysis. (2024). *The 2024 Crypto Crime Report*. Žiūrėta 2024-12-20. Prieiga internetu: <https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/>
- Cheraghali, H., Molnár, P., Storsveen, M. ir Veliqi, F. (2024). The impact of cryptocurrency-related cyberattacks on return, volatility, and trading volume of cryptocurrencies and traditional financial assets. Žiūrėta 2024-11-17. Prieiga internetu: *International Review of Financial Analysis*, 95, 103439. <https://doi.org/10.1016/j.irfa.2024.103439>
- Chokor, A. ir Alfieri, E. (2021). Long and short-term impacts of regulation in the cryptocurrency market. *The Quarterly Review of Economics and Finance*, 81, 157–173. Žiūrėta 2024-10-25. Prieiga internetu: <https://doi.org/10.1016/j.qref.2021.05.005>
- CoinCu. (2023). *The Dark Side Of Crypto Promotions: Influencers And 50+ Scams Uncovered*. Žiūrėta 2024-12-20. Prieiga internetu: <https://cryptorank.io/news/feed/12646-178798-dark-side-of-crypto-promotion-influencers>
- CoinGecko. (2024). Žiūrėta 2024-12-20. Prieiga internetu: *Global Cryptocurrency Market Cap Charts*. <https://www.coingecko.com/en/global-charts>
- Congressional Research Service. (2024). *Terrorist Financing: Hamas and Cryptocurrency Fundraising*. Žiūrėta 2024-12-20. Prieiga internetu: <https://crsreports.congress.gov/product/pdf/IF/IF12537>
- Consensus. (2019). *The Decade in Blockchain — 2010 to 2020 in Review*. Žiūrėta 2024-11-17. Prieiga internetu: <https://consensus.io/blog/the-decade-in-blockchain-2010-to-2020-in-review>
- Crystal Blockchain's Analytics Team. (2023). *Crypto & DeFi Hacks & Scams Report*. Žiūrėta 2024-12-01. Prieiga internetu: <https://crystalintelligence.com/rohirov/2023/04/HACKS-report-1.pdf>
- Čekanavičius, V. ir Murauskas, G. (2001). *Statistika ir jos taikymai*. Žiūrėta 2024-11-18. Prieiga internetu: https://www.spssanalyze.lt/wp-content/uploads/2014/03/ius__Murauskas_-_Statistika_ir_jos_taikymai.pdf

- De Silva, H., McMurran, G. M. ir Miller, M. N. (2017). Diversification and the Volatility Risk Premium. *Factor Investing* (p. 365–387). Žiūrėta 2024-11-17. Prieiga internetu: Elsevier. <https://doi.org/10.1016/B978-1-78548-201-4.50014-3>
- Dong, S., Abbas, K., Li, M. ir Kamruzzaman, J. (2023). Blockchain technology and application: an overview. Žiūrėta 2024-10-17. Prieiga internetu: *PeerJ Computer Science*, 9, e1705. <https://doi.org/10.7717/peerj-cs.1705>
- Dubey, P. (2022). *NFT Collection Promoted By Jason Derulo, Ne-Yo Rug Pulled For \$3.04 Million*. Žiūrėta 2024-12-20. Prieiga internetu: https://www.ibtimes.com/nft-collection-promoted-jason-derulo-ne-yo-rug-pulled-304-million-3592581?utm_source=chatgpt.com
- Egmont group. (2023). *REPORT ON ABUSE OF VIRTUAL ASSETS FOR TERRORIST FINANCING PURPOSES*. Žiūrėta 2024-12-01. Prieiga internetu: <https://egmontgroup.org/wp-content/uploads/2023/12/2023-July-HoFIU-06-IEWG-Project-Abuse-of-VA-for-TF-Summary-1.pdf>
- Elliptic. (2020). *Financial Crime Typologies in Cryptoassets. The Concise Guide for Compliance Leaders*. Žiūrėta 2024-11-27. Prieiga internetu: [https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20\(All%20Assets\)/Typologies_Concise%20Guide_12-20.pdf](https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf)
- Elst, H. (2019). *Foundations of Descriptive and Inferential Statistics*. Žiūrėta 2024-11-17. Prieiga internetu: <https://doi.org/10.13140/RG.2.1.2112.3044>
- en.ethereumworldnews.com. (2022). *Four Croatians Allegedly Rugged NFT Collectors Of Over \$2.8 Million In A Few Months*. Žiūrėta 2024-12-20. Prieiga internetu: https://cryptonews.net/news/nft/5728369/?utm_source=chatgpt.com
- Etherscan. (2024). *The Ethereum Blockchain Explorer*. Žiūrėta 2024-12-30. Prieiga internetu: <https://etherscan.io/>
- FATF. (2019). *Terrorist Financing Risk Assessment Guidance*. Žiūrėta 2024-12-01. Prieiga internetu: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf>
- Felix Adebayo Bakare, Jide Omojola ir Augustine Chibuzor Iwuh. (2024). Blockchain and decentralized finance (DEFI): Disrupting traditional banking and financial systems. *World Journal of Advanced Research and Reviews*, 23(3), 3075–3089. Žiūrėta 2024-11-18. Prieiga internetu: <https://doi.org/10.30574/wjarr.2024.23.3.2968>

- Financial Intelligence Unit. (2022). *Guidelines on the Characteristics of Suspicious Transactions*. Žiūrėta 2024-11-18. Prieiga internetu: <https://fiu.ee/sites/default/files/documents/2024-05/Guidelines%20on%20the%20Characteristics%20of%20Suspicious%20Transactions.pdf>
- Firdaus, A., Razak, M. F. A., Feizollah, A., Hashem, I. A. T., Hazim, M. ir Anuar, N. B. (2019). The rise of “blockchain”: bibliometric analysis of blockchain study. *Scientometrics*, 120(3), 1289–1331. Žiūrėta 2024-10-17. Prieiga internetu: <https://doi.org/10.1007/s11192-019-03170-4>
- Flagship Team. (2022). *OnlyFans Model Vanessa Sierra, NFT Founder, Accused Of Scam*. Žiūrėta 2024-12-20. Prieiga internetu: https://flagship.fyi/outposts/crypto-news/onlyfans-model-vanessa-sierra-nft-founder-accused-of-scam/?utm_source=chatgpt.com
- Gandal, N., Halaburda, H., Chiu, J., Dunbar, G., Fung, B., Giacomini, R., Hendry, S., Pomorski, L., Molico, M., Stuber, G. ir Wong, R. (2014). *Competition in the Cryptocurrency Market*. Žiūrėta 2024-12-01. Prieiga internetu: <https://www.econstor.eu/handle/10419/103105>
- Garg A., Patel A., Tyagi A., Raj D. ir Chaudhary G. (2023). *BlockChain and Decentralized Apps*. Žiūrėta 2024-10-25. Prieiga internetu: <https://doi.org/10.48550/arXiv.2303.12536>
- Garin, L. ir Gisin, V. (2023). Machine learning in classifying bitcoin addresses. *The Journal of Finance and Data Science*, 9, 100109. Žiūrėta 2024-10-25. Prieiga internetu: <https://doi.org/10.1016/j.jfds.2023.100109>
- Gaurav, R. (2024). 5 “Worst” Rug-Pulls in Crypto. Žiūrėta 2024-12-21. Prieiga internetu: https://www.securities.io/5-worst-rug-pulls-in-crypto/?utm_source=chatgpt.com
- Gudavičiūtė, B. (2021). *SANDORIO ŠALIES KREDITO RIZIKOS VERTINIMAS COVID-19 PANDEMIJOS KONTEKSTE* [Baigiamasis bakalauro darbas, VILNIAUS UNIVERSITETAS, EKONOMIKOS IR VERSLO ADMINISRAVIMO FAKULTETAS]. Žiūrėta 2024-12-01. Prieiga internetu: https://www.lvb.lt/discovery/fulldisplay?docid=alma9912935211608451&context=L&vid=370LABT_NETWORK:ELABA_UNION&lang=lt&search_scope=ELABA&adaptor=Local%20Search%20Engine&tab=ELABA&query=any,contains,beatric4%8D%C4%97%20gudavi%C4%8Di%C5%ABt%C4%97&offset=0
- Hafner, M., de Luze, R., Greber, N., Beccuti, J., Biondi, B., Katten, G., Riccobene, M. ir Arrigoni, A. (2023). DeFi Lending Platform Liquidity Risk: The Example of Folks Finance. *The Journal of The British Blockchain Association*, 6(1), 1–8. Žiūrėta 2024-11-18. Prieiga internetu: [https://doi.org/10.31585/jbba-6-1-\(5\)2023](https://doi.org/10.31585/jbba-6-1-(5)2023)

- Hazim, C., Analyst, R. ir Reddy, R. (2022). *DeFi: The Basics*. Žiūrėta 2024-10-25. Prieiga internetu: <https://www.globalxetfs.com/content/files/DeFi-The-Basics-US-Final.pdf>
- Homeland Security. (2022). *Combating Illicit Activity utilizing financial technologies and cryptocurrencies*. Žiūrėta 2024-10-25. Prieiga internetu: <https://www.dhs.gov/sites/default/files/2022-09/Combating%20Illicit%20Activity%20.pdf>
- Hoseini, A. (2022). *Ransomware and phishing cyberattacks: analyzing the public's perception of these attacks in Sweden*. Žiūrėta 2024-11-18. Prieiga internetu: <https://uu.diva-portal.org/smash/get/diva2:1678538/FULLTEXT01.pdf>
- Huang, J., He, N., Ma, K., Xiao, J. ir Wang, H. (2023). *A Deep Dive into NFT Rug Pulls*. Žiūrėta 2024-12-01. Prieiga internetu: <http://arxiv.org/abs/2305.06108>
- yahoo!finance. (2024). *Ethereum USD (ETH-USD)*. Žiūrėta 2024-12-02. Prieiga internetu: <https://finance.yahoo.com/quote/ETH-USD/history/>
- International Monetary Fund. (2003). *Global Financial Stability Report, September 2003: Market Developments and Issues*. Žiūrėta 2024-10-25. Prieiga internetu: International Monetary Fund. <https://doi.org/10.5089/9781589062368.082>
- Investing.com. (2024). *Ethereum*. Žiūrėta 2024-12-30. Prieiga internetu: <https://www.investing.com/crypto/ethereum/historical-data>
- Islam, S. ir Apu, K. U. (2024). DECENTRALIZED VS. CENTRALIZED DATABASE SOLUTIONS IN BLOCKCHAIN: ADVANTAGES, CHALLENGES, AND USE CASES. *Global mainstream journal of innovation, engineering & emerging technology*, 3(4), 58–68. Žiūrėta 2024-11-03. Prieiga internetu: <https://doi.org/10.62304/jieet.v3i04.195>
- Jeleskovic, V. (2024). *An Empirical Analysis of Scam Tokens on Ethereum Blockchain*. Žiūrėta 2024-11-03. Prieiga internetu: <https://arxiv.org/abs/2402.19399>
- Kar, J. (2022). *Rug Pull Finder Exposes Over 15 NFT Scams That Have Stolen Over 40,000 ETH*. Žiūrėta 2024-12-21. Prieiga internetu: https://www.nftgators.com/rug-pull-finder-exposes-over-15-nft-scams-that-have-stolen-over-40000-eth/?utm_source=chatgpt.com
- Katina, P. F., Keating, C. B., Sisti, J. A. ir Gheorghe, A. V. (2019). Blockchain governance. *International Journal of Critical Infrastructures*, 15(2), 121–135. Žiūrėta 2024-12-01. Prieiga internetu: <https://EconPapers.repec.org/RePEc:ids:ijcist:v:15:y:2019:i:2:p:121-135>
- Kern, S. E. (2013). *Inferential statistics, power estimates, and study design formalities continue to suppress biomedical innovation*. Žiūrėta 2024-12-03. Prieiga internetu: <https://arxiv.org/ftp/arxiv/papers/1411/1411.0919.pdf>

- Khan, R. ir Ali Hakami, T. (2022). Cryptocurrency: usability perspective versus volatility threat. *Journal of Money and Business*, 2(1), 16–28. Žiūrėta 2024-11-25. Prieiga internetu: <https://doi.org/10.1108/jmb-11-2021-0051>
- Kissell, R. (2014). Price Volatility. *The Science of Algorithmic Trading and Portfolio Management* (p. 193–234). Elsevier. Žiūrėta 2024-11-25. Prieiga internetu: <https://doi.org/10.1016/B978-0-12-401689-7.00006-4>
- Kitonyi, N. (2022). *How the Winter Bears NFT Team Rug Pulled the Project*. Žiūrėta 2024-12-03. Prieiga internetu: https://www.nftgators.com/how-the-winter-bears-nft-team-rug-pulled-the-project/?utm_source=chatgpt.com
- Kuznetsov, O., Peliukh, O., Poluyanenko, N., Bohucharskyi, S. ir Kolovanova, I. (2023). *Comparative Analysis of Cryptographic Hash Functions in Blockchain Systems*. Žiūrėta 2024-10-17. Prieiga internetu: <https://ceur-ws.org/Vol-3550/paper7.pdf>
- Lazar, J., Feng, J. H. ir Hochheiser, H. (2017). Experimental research. *Research Methods in Human Computer Interaction* (p. 25–44). Elsevier. Žiūrėta 2024-12-03. Prieiga internetu: <https://doi.org/10.1016/B978-0-12-805390-4.00002-9>
- Lewis, R., Mcpartland, J. ir Ranjan, R. (2017). *Blockchain and Financial Market Innovation*. Žiūrėta 2024-10-26. Prieiga internetu: <https://ideas.repec.org/p/fip/fedhpd/93559.html>
- LiDA. (2020). *Inferencinė statistika socialiniuose moksluose*. Žiūrėta 2024-12-01. Prieiga internetu: http://www.lidata.eu/index.php?file=files/mokymai/inferencine_2011/infer.html&course_file=infer_ivadas.html
- Long, Y., Gong, Y., Huang, W., Cai, J., Xu, N. ir Li, K. (2023). *Cryptography of Blockchain* (p. 340–349). Žiūrėta 2024-10-18. Prieiga internetu: https://doi.org/10.1007/978-3-031-28124-2_32
- Makarov, I. ir Schoar, A. (2022). *Cryptocurrencies and Decentralised Finance (DeFi)*. Žiūrėta 2024-11-05. Prieiga internetu: <https://www.bis.org/publ/work1061.htm>
- Marc Truchet. (2022). *Decentralized Finance (DeFi): opportunities, challenges and policy implications*. Žiūrėta 2024-11-05. Prieiga internetu: <https://www.eurofi.net/publications/>
- Marshall, G. ir Jonker, L. (2011). An introduction to inferential statistics: A review and practical guide. *Radiography* (T. 17, Numeris 1). Žiūrėta 2024-12-01. Prieiga internetu: <https://doi.org/10.1016/j.radi.2009.12.006>
- Massimo Doria, Bassan, F., Rabitti, M., Alibrandi, A. S. ir Malvagna, U. (2024). *Characteristics of smart contracts* (Numeris 863). Žiūrėta 2024-11-05. Prieiga internetu: https://ideas.repec.org/p/bdi/opques/qef_863_24.html

- Mehdi Manaa, Teresa Chimienti, M., Adachi, M., Athanassiou, P., Balteanu, I., Calza, A., Devaney, C., Diaz Fernandez, E., Eser, F., Ganoulis, I., Laot, M., Philipp, G., Poignet, R., Sauer, S., Schneeberger, D., Stracca, L., Tapking, J., Toolin, C., Tyler, C. ir Wacket, H. (2019). *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures ECB Crypto-Assets Task Force*. Žiūrėta 2024-11-27. Prieiga internetu: <https://doi.org/10.2866/162>
- Metelski, D. ir Sobieraj, J. (2022). Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations. Žiūrėta 2024-11-03. Prieiga internetu: *International Journal of Financial Studies*, 10(4), 108. <https://doi.org/10.3390/ijfs10040108>
- Millard, M. (2024). *US charges three UK nationals in connection with 'Evolved Apes' NFT rug pull*. Žiūrėta 2024-12-20. Prieiga internetu: <https://www.dlnews.com/articles/regulation/us-charges-three-in-connection-with-nft-rugpull-scam/>
- Mironeanu, A., Irimia, B., Săndulescu, V. ir Teodoroiu, C. (2021). The impact of Tesla's bitcoin investment and its plans to accept it as payment method on the evolution of bitcoin. *Proceedings of the International Conference on Business Excellence*, 15(1), 58–74. Žiūrėta 2024-12-21. Prieiga internetu: <https://doi.org/10.2478/picbe-2021-0007>
- Moosavi, N., Taherdoost, H., Mohamed, N., Madanchian, M., Farhaoui, Y. ir Khan, I. U. (2024). Blockchain Technology, Structure, and Applications: A Survey. *Procedia Computer Science*, 237, 645–658. Žiūrėta 2024-11-06. Prieiga internetu: <https://doi.org/10.1016/j.procs.2024.05.150>
- Murphy, C. (2024). Žiūrėta 2024-11-27. Prieiga internetu: *Understanding the EU's response to money laundering*.
- NFT degenz. (2022). *Winter Bears is a rug pull if they don't fund their DAO vault, here's why*. Žiūrėta 2024-12-21. Prieiga internetu: https://medium.com/@NFT_degenz/winter-bears-is-a-rug-pull-if-they-dont-fund-their-dao-vault-here-s-why-ee0fde041102
- NFTevening. (2023). *Blockchain Sleuth ZachXBT's Investigation Cited in \$3.1M NFT Rug Pull Lawsuit*. Žiūrėta 2024-12-21. Prieiga internetu: https://nftevening.com/blockchain-sleuth-zachxbts-investigation-cited-in-3-1m-nft-rug-pull-lawsuit/?utm_source=chatgpt.com
- OJOG, S. (2021). The Emerging World of Decentralized Finance. *Informatica Economica*, 25(4/2021), 43–52. Žiūrėta 2024-12-05. Prieiga internetu: <https://doi.org/10.24818/issn14531305/25.4.2021.05>

- Ozili, P. K. (2022). Decentralized finance research and developments around the world. *Journal of Banking and Financial Technology*, 6(2), 117–133. Žiūrėta 2024-11-06. Prieiga internetu: <https://doi.org/10.1007/s42786-022-00044-x>
- Quarmby, B. (2023). *ZachXBT's research cited in Canadian NFT rug pull class-action lawsuit*. Žiūrėta 2024-12-21. Prieiga internetu: <https://cointelegraph.com/news/zachxbt-s-research-cited-in-canadian-nft-rug-pull-class-action-lawsuit>
- Rahmanda, B. (2024). Rug Pull Cryptocurrency Case Analysis in the Perspective of Indonesian Business Law. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS*, 07(04). Žiūrėta 2024-12-06. Prieiga internetu: <https://doi.org/10.47191/ijmra/v7-i04-41>
- Rahmani, M. K. I. (2022). *Blockchain Technology* (p. 16–27). Žiūrėta 2024-10-28. Prieiga internetu: <https://doi.org/10.4018/978-1-7998-8382-1.ch002>
- Raimond James. (2023). *Weathering market volatility*. Žiūrėta 2024-11-02. Prieiga internetu: <https://www.raymondjames.com/-/media/rj/common/resources/investment-strategy/weathering-market-volatility.pdf>
- Reagan Ronald. (2023). *Financial Crime Risk definition and regulatory context*. 16–21. Žiūrėta 2024-11-02. Prieiga internetu: <https://www.managementsolutions.com/sites/default/files/minisite/static/7805cb71-d48b-407e-9c40-9353639337c7/fincrime/pdf/financial-crime-en.pdf>
- Ross, S. M. (2017). Testing Statistical Hypotheses. *Introductory Statistics* (p. 381–432). Elsevier. Žiūrėta 2024-12-01. Prieiga internetu: <https://doi.org/10.1016/B978-0-12-804317-2.00009-6>
- Ruževičius, J. (2016). *MAGISTRANTŪROS STUDIJOS: BAIGIAMOJO DARBO PROJEKTŲ (BDP) IR MAGISTRO DARBO (MD) RAŠYMAS*. Žiūrėta 2024-12-01. Prieiga internetu: https://www.evaf.vu.lt/dokumentai/katedros/Vadybos_katedra/Informacija_stud/BDP_ir_MD_rasymas.pdf
- Sarode, R. P., Poudel, M., Shrestha, S. ir Bhalla, S. (2021). Blockchain for committing peer-to-peer transactions using distributed ledger technologies. *International Journal of Computational Science and Engineering*, 24(3), 215. Žiūrėta 2024-10-18. Prieiga internetu: <https://doi.org/10.1504/IJCSE.2021.115651>
- Savelyev, A. (2016). *CONTRACT LAW 2.0: «SMART» CONTRACTS AS THE BEGINNING OF THE END OF CLASSIC CONTRACT LAW*. Žiūrėta 2024-10-18. Prieiga internetu: <https://wp.hse.ru/data/2016/12/14/1111743800/71LAW2016.pdf>

- Schueffel, P., Groeneweg, N. ir Baldegger, R. (2019). *The Crypto Encyclopedia. Coins, Tokens and Digital Assets from A to Z*. Žiūrėta 2024-10-18. Prieiga internetu: https://www.heg-fr.ch/media/lbdfnyd1/schueffeltgroenewegbaldegger2019_crypto-encyclopedia_eng.pdf
- Schuler, K., Cloots, A. S. ir Schär, F. (2024). On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance. *Journal of Financial Regulation*, 10(2), 213–242. Žiūrėta 2024-11-05. Prieiga internetu: <https://doi.org/10.1093/jfr/fjad014>
- Shaleva, A. ir Korkhov, V. (2021). EFFICIENT GOSSIP-BASED PROTOCOL IN THE NEO BLOCKCHAIN NETWORK. *9th International Conference „Distributed Computing and Grid Technologies in Science and Education“*, 508–513. Žiūrėta 2024-11-02. Prieiga internetu: <https://doi.org/10.54546/MLIT.2021.71.22.002>
- SharkTeam. (2021). *Squid game Rugpull: Fund flow analysis*. Žiūrėta 2024-12-03. Prieiga internetu: https://sharkteam.org/report/analysis/20211112001A_en.pdf
- Sharma, T., Agarwal, R. ir Shukla, S. K. (2024). Understanding Rug Pulls: An In-depth Behavioral Analysis of Fraudulent NFT Creators. *ACM Transactions on the Web*, 18(1), 1–39. Žiūrėta 2024-11-03. Prieiga internetu: <https://doi.org/10.1145/3623376>
- Sila, J., Kocenda, E., Kristoufek, L. ir Kukacka, J. (2024). Good vs. bad volatility in major cryptocurrencies: The dichotomy and drivers of connectedness. *Journal of International Financial Markets, Institutions and Money*, 96, 102062. Žiūrėta 2024-10-29. Prieiga internetu: <https://doi.org/10.1016/j.intfin.2024.102062>
- Simoiu, C., Symantec, C. G., Bonneau, J. ir Goel, S. (2017). „*I was told to buy a software or lose my computer. I ignored it*“: A study of ransomware. Žiūrėta 2024-12-21. Prieiga internetu: <https://5harad.com/papers/ransomware.pdf>
- Solidus Labs. (2024). *TokenSniffer*. Žiūrėta 2024-12-30. Prieiga internetu: <https://tokensniffer.com/>
- Stangl, P. ir Neumann, C. P. (2024). *The Kosmosis Use-Case of Crypto Rug Pull Detection and Prevention*. Žiūrėta 2024-12-21. Prieiga internetu: <http://arxiv.org/abs/2405.19762>
- Sun, D., Ma, W., Nie, L. ir Liu, Y. (2024). *SoK: Comprehensive Analysis of Rug Pull Causes, Datasets, and Detection Tools in DeFi*. Žiūrėta 2024-12-03. Prieiga internetu: <http://arxiv.org/abs/2403.16082>
- Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information*, 14(2), 117. Žiūrėta 2024-11-01. Prieiga internetu: <https://doi.org/10.3390/info14020117>

- The European Union Blockchain Observatory. (2022). *Decentralised Finance (DeFi)*. Žiūrėta 2024-11-01. Prieiga internetu: https://www.standict.eu/sites/default/files/2022-06/DeFi%20Report%20EUBOF%20-%20Final_0.pdf
- The Graph. (2024). *Fast, easy access to blockchain data*. Žiūrėta 2024-11-01. Prieiga internetu: <https://thegraph.com/>
- Tierno, P. (2023). *Introduction to Cryptocurrency*. Žiūrėta 2024-11-01. Prieiga internetu: <https://sgp.fas.org/crs/misc/IF12405.pdf>
- Tmeizeh, M., Rodríguez-Domínguez, C. ir Hurtado-Torres, M. V. (2023). *A Survey of Decentralized Storage and Decentralized Database in Blockchain-Based Proposed Systems: Potentials and Limitations* (p. 204–213). Žiūrėta 2024-10-18. Prieiga internetu: https://doi.org/10.1007/978-3-031-45155-3_21
- Two Hop Ventures. (2017). *Block Spec for Bitcoin*. Žiūrėta 2024-11-25. Prieiga internetu: <https://twohop.ventures/wp-content/uploads/2019/12/BSVSpec-Blocks-V1.0.pdf>
- United States Attorney's Office. (2024). *Three United Kingdom Nationals Charged In Connection With "Evolved Apes" NFT Scam*. Žiūrėta 2024-12-21. Prieiga internetu: <https://www.justice.gov/usao-sdny/pr/three-united-kingdom-nationals-charged-connection-evolved-apes-nft-scam>
- Vaghela, P. S. (2024). *Sample Size Determination for Social Science Research*. Žiūrėta 2024-12-01. Prieiga internetu: <https://doi.org/10.13140/RG.2.2.15657.40800>
- Valiente, M.-C. ir Tschorsch, F. (2021). Blockchain-based technologies. *Internet Policy Review*, 10(2). Žiūrėta 2024-11-23. Prieiga internetu: <https://doi.org/10.14763/2021.2.1552>
- Wieandt, A. ir Heppding, L. (2023). *Centralized and Decentralized Finance: Coexistence or Convergence?* (p. 11–51). Žiūrėta 2024-10-29. Prieiga internetu: https://doi.org/10.1007/978-3-031-23069-1_2
- World economic forum. (2023). *Pathways to the Regulation of Crypto-Assets: A Global Approach*. Žiūrėta 2024-11-18. Prieiga internetu: https://www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf
- Wu, L., Lu, W., Zhao, R. ir Xue, F. (2022). *Smart Contract: Is it Really Smart in Construction?* (p. 751–759). Žiūrėta 2024-10-27. Prieiga internetu: https://doi.org/10.1007/978-981-19-5256-2_59

- Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Luo, X., Zhang, C., Xiao, X. ir 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*, 5(3), 1–26. Žiūrėta 2024-11-03. Prieiga internetu: <https://doi.org/10.1145/3491051>
- Zenonas, N. (2008). *PAVYZDINIS METODOLOGINIS MOKOMASIS STUDIJŲ PAKETAS*. https://data.ktu.edu/wp-content/uploads/2023/06/Lyginamieji_tyrimai_su_tosmana_fs_qca.pdf
- Zhang, X., Chen, Z. ir Wang, S. (2024). A study of the impact of cryptocurrency price volatility on the stock and gold markets. *Finance Research Letters*, 69, 106114. Žiūrėta 2024-12-01. Prieiga internetu: <https://doi.org/10.1016/j.frl.2024.106114>
- Zheng, P., Jiang, Z., Wu, J. ir Zheng, Z. (2023). Blockchain-Based Decentralized Application: A Survey. *IEEE Open Journal of the Computer Society*, 4, 121–133. Žiūrėta 2024-10-27. Prieiga internetu: <https://doi.org/10.1109/OJCS.2023.3251854>
- Zhou, Y., Sun, J., Ma BNRist, F., Chen BNRist, Y., Yan BNRist, Z. ir Jiang BNRist, Y. (2024). Stop Pulling my Rug: Exposing Rug Pull Risks in Crypto Token to Investors. *Proceedings of ACM Conference (ICSE'24)* (T. 1). Žiūrėta 2024-11-23. Prieiga internetu: <https://conf.researchr.org/details/icse-2024/icse-2024-software-engineering-in-practice/11/Stop-Pulling-my-Rug-Exposing-Rug-Pull-Risks-in-Crypto-Token-to-Investors>
- Zmudzinski, A. (2023). *Mutant Ape Planet scammer also probably pulled rug on Crazy Camels and Fashion Ape NFTs*. Žiūrėta 2024-12-21. Prieiga internetu: <https://crypto.news/mutant-ape-planet-scammer-also-probably-pulled-rug-on-crazy-camels-and-fashion-ape-nfts/>

FINANSINIŲ NUSIKALTIMŲ DECENTRALIZUOTOJE FINANSŲ EKOSISTEMOJE VERTINIMAS

BEATRIČĖ PANAVIDIENĖ

Baigiamojo magistro darbas

Finansų ir bankininkystės programa

Vilniaus universitetas, Ekonomikos bei verslo administravimo fakultetas

Darbo vadovė – prof. dr. Alfreda Šapkauskienė

Vilnius, 2025

SANTRAUKA

Darbą sudaro: 79 puslapiai, 12 paveikslų, 9 lentelės, 124 literatūros šaltiniai ir 8 priedai.

Decentralizuotuose finansuose, padaugėjo ir sukčiavimo, apgavystės bei nusikaltimų apraiškų dėl savo ypatingų decentralizuotų finansų savybių, tokių kaip - pseudonimiškumas ir tarpininkų nebuvimas. Šiame magistro darbe pasirinkta išnagrinėti šiuos nusikaltimus, jiems būdingus bruožus, dažnumą, išsirinkti populiariausią bei didžiausią žalą nešantį nusikaltimą, jį ištirti bei pateikti būdus kaip nuo to apsisaugoti. Darbe detaliai išnagrinėtas ir pasirinktas 2021 metais išpopuliarėjęs „Rug pull“ decentralizuotų finansų finansinis nusikaltimas, kurio metu investuotojai gali prarasti visas savo investuotas lėšas. Darbo tikslas – išnagrinėjus finansinių nusikaltimų decentralizuotų finansų ekosistemoje teorinius aspektus, atlikti finansinių nusikaltimų decentralizuotoje finansų ekosistemoje vertinimą. Darbe taikyti metodai: mokslinės literatūros šaltinių nagrinėjimas bei informacijos susistemimas, komparatyvinės analizės, inferencinės statistikos, T.testo, Pearsono koreliacijos metodai. Darbo išvados atsako į išsikeltus magistro darbo metu uždavinius: išryškintas finansinių nusikaltimų decentralizuotuose finansuose ir „Rug pull“ finansinio nusikaltimo nagrinėjimo aktualumas, bei pateikta „Rug pull“ finansinio nusikaltimo tipologija, parengta metodologija decentralizuotų finansų finansinių nusikaltimų ir virtualių valiutų palyginimui, „Rug pull“ finansinio nusikaltimo vertinimui ir atpažinimui, bei modelio, skirtam apsisaugojimui nuo „Rug pull“ decentralizuotų finansų finansinio nusikaltimo, kūrimui, palygintas finansinių nusikaltimų aktyvumas su Eterio verte pasirinktais laikotarpiais, ištirta kaip pasirinktais laikotarpiais Eterio kainų kitimas koreliuoja su investuotojų pervedimais į finansinio nusikaltimo „Rug pull“ žetonus, galiausiai sukurtas modelis apsisaugojimui nuo „Rug pull“ finansinio nusikaltimo. Taip pat buvo suformuluoti pasiūlymai: siūloma investuotojams naudotis magistro darbe sudarytu modeliu, kuris leidžia patikrinti

ar žetonas yra susijęs su decentralizuotų finansų finansiniu nusikaltimu „Rug pull“, siekiant lengviau pasiekti susistemintą informaciją apie decentralizuotus finansus yra siūloma įsigyti trečiųjų šalių analizės paslaugas, taip pat siūloma programinėje įrangoje ir sistemose, kuriose yra prekiaujama žetonais įdiegti automatizuotą apsaugos sistemą, galiausiai siūloma išnagrinėti kitus finansinius nusikaltimus decentralizuotų finansų ekosistemoje ir išnagrinėjus tų nusikaltimų ypatybes bei įvertinus kitų mokslininkų pateikiamus rezultatus, sudaryti modelius apsisaugojimui nuo decentralizuotų finansų finansinių nusikaltimų.

ASSESING FINANCIAL CRIMES IN DECENTRALIZED FINANCIAL EKOSYSTEM

BEATRICĖ PANAIVIENĖ

Master thesis

Finance and Banking program

Vilnius University, Faculty of Economics and Business Administration

Supervisor – prof. dr. Alfreda Šapkauskienė

Vilnius, 2025

SUMMARY

The work consists of: 79 pages, 12 figures, 9 tables, 124 literature sources and 8 appendices.

In decentralized finance, the manifestations of fraud, fraud and crime have also increased due to the special characteristics of decentralized finance, such as pseudonymity and the absence of intermediaries. In this master's thesis, it was chosen to examine these crimes, their characteristic features, frequency, choose the most popular and the most damaging crime, investigate it and present ways to protect yourself from it. The paper examines in detail and selects the "Rug pull" decentralized finance financial crime that became popular in 2021, during which investors can lose all their invested funds. The aim of the work - after examining the theoretical aspects of financial crimes in the decentralized financial ecosystem, perform an assessment of financial crimes in the decentralized financial ecosystem. Methods used in the work: examination of scientific literature sources and information systematization, comparative analysis, inferential statistics, T.test, Pearson's correlation methods. The conclusions of the work respond to the tasks set during the master's work: highlighted the relevance of investigating financial crimes in decentralized finance and "Rug pull" financial crime, presented a typology of "Rug pull" financial crime, developed a methodology for comparing decentralized finance financial crimes and virtual currencies, evaluating and recognizing "Rug pull" financial crime, and a model for to protect against "Rug pull" decentralized finance financial crime, development, financial crime activity compared to Ether value in selected time periods, investigated how Ether price variation in selected time periods correlates with investor transfers to Rug pull financial crime tokens, finally developed a model to protect against Rug pull financial crime. Proposals were also formulated: it is suggested that investors use the model created in the master's thesis, which allows checking whether the token is related to the financial crime of decentralized finance "Rug pull", in order to facilitate access to structured information about decentralized finance,

it is proposed to purchase third-party analysis services, and it is also proposed to implement an automated security system in the software and systems where tokens are traded, it is finally proposed to examine other financial crimes in the decentralized finance ecosystem and after examining the characteristics of those crimes and after evaluating the results presented by other scientists, create models for protection against financial crimes of decentralized finance.

PRIEDAI

1 Priedas. Atsižvelgus į atrinktus pranešimus, atrinkti 146 žetonai, kurie susiję su „Rug pull“
(Šaltinis: sudaryta autoriaus, remiantis Chainabuse (2024); Solidus Labs (2024).

Eilės nr.	Žetono pavadinimas
1	Based Chill Guy (CHILLGUY)
2	Rexas Finance (RXS)
3	Ethereum Games (ETHG)
4	Pepe Unchained (PEPU)
5	American True Hero (TRUMP)
6	Trump MAGA (TRUMPMAGA)
7	47th President of the United States (TRUMP47)
8	MOG CAT (MOG)
9	Bridge Payments (BRIDGE)
10	BOME TRUMP (TRUMP)
11	Neiro Pump (NEIRO)
12	BlockDAG (BDAG)
13	Polymarket (POL)
14	Babylon (BABL)
15	XELON (XELON)
16	BlackMythWukong (WUKONG)
17	Morpho (MORPHO)
18	Linea Network (LINEA)
19	zkEVM (ZKE)
20	GanNamDog (GNDOG)
21	Tos Coin (TOS)
22	FreeDurov Token (FREED)
23	W Token (W)
24	PEIPEI coin (PEIPEI)
25	LayerZero (ZRO)
26	DADDY TATE (DADDY)
27	SupraOracles (SUPRA)
28	Chaos Labs (CHAOS)
29	Scroll (SCROLL)
30	Monad (TBD)
31	Scroll (SCROLL)
32	BVM (BVM)
33	Espresso Systems (ESP)
34	LayerZero (ZRO)
35	Renzo Protocol (EZ)

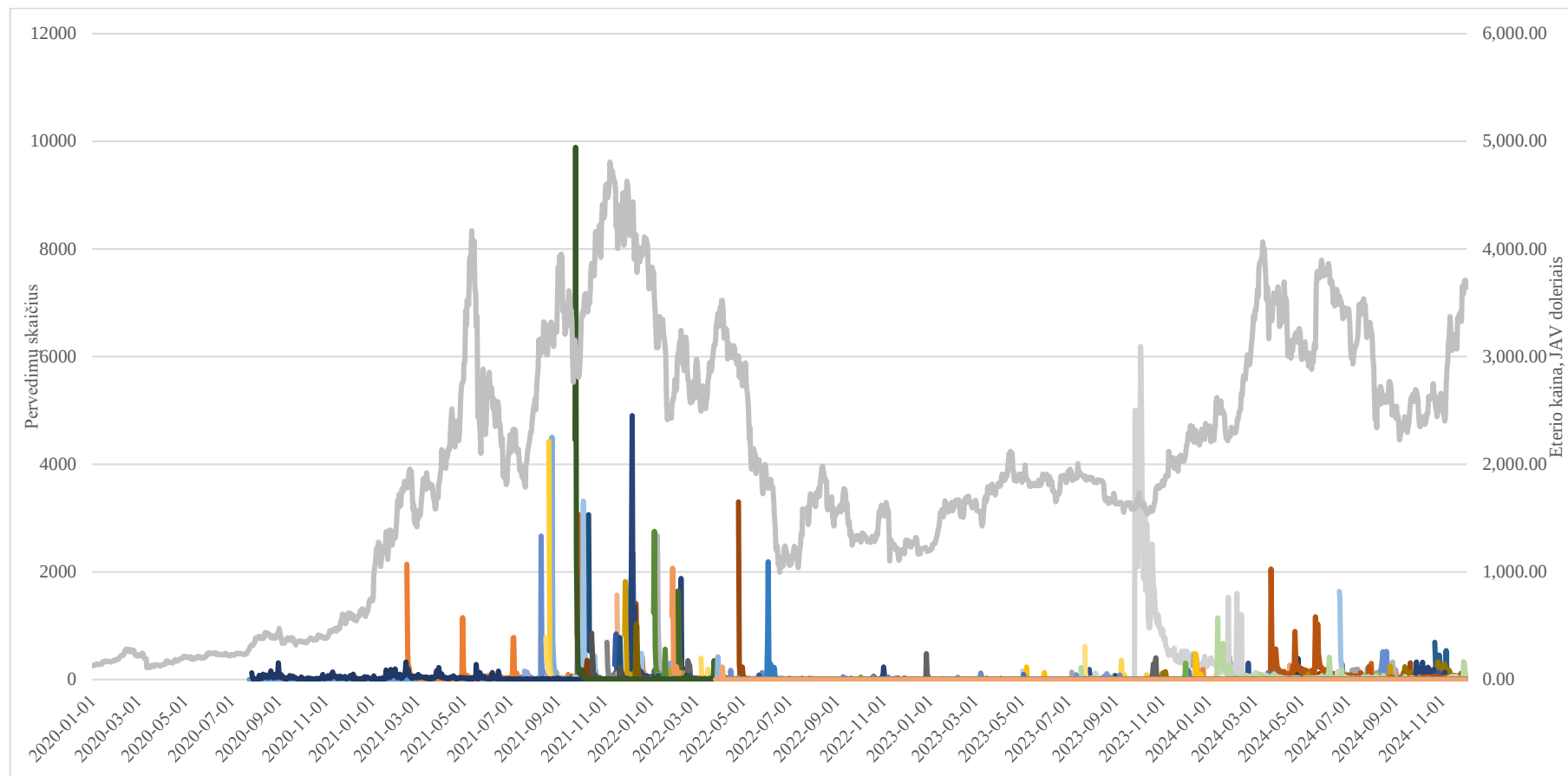
Eilės nr.	Žetono pavadinimas
74	Naughty Bape Club (NBC)
75	Cyclops Monkey Club (CMC)
76	Empower Women Planet (EWP)
77	Lucky Elephant Club (LEC)
78	Cyber Zombie Society (CZS)
79	Alien Alliance (AA)
80	Fud Token (FUD)
81	JUGS (\$JUGS)
82	Smol Boyz (SMOLBOYZ)
83	Fish (FISH)
84	Kizuna AI (KIZUNA)
85	EspressoBot (ESPS)
86	Bitcoin30 (BTC30)
87	watcher (WATCHER)
88	Sugartown (SUGARTOWN)
89	Unibot X (UNIBOT X)
90	Jada AI (JADA AI)
91	https://symbiosis.finance/ (SYMBIOSIS)
92	world AI (WORLD AI)
93	SHIBBOT (SHIBBOT)
94	SHIC (SHIC)
95	ハチ公 (HACHIKO)
96	SOPH AI Token (SOPH)
97	Algobot (ALGO)
98	XXX (XXX)
99	SARATOSHI NAGAMOTO (SARATOSHI)
100	HarryPotterObamaSonic20Inu (ETHEREUM)
101	0xCoco (COCO)
102	tetris (TETRIS)
103	RNS (RNS)
104	iBOT (IBOT)
105	Pond Coin (PNDC)
106	Towelie (TOWELIE)
107	voQui Token (VOQUI)
108	Mojo Jojo (MOJO)

1 Priedo pabaiga

Eilės nr.	Žetono pavadinimas
36	RedSHIB (REDSHIB)
37	Tradecurve (TCRV)
38	Trism AI (TRISM)
39	BD20 (BD20)
40	Espresso (ESP)
41	NVIDIA AI (NVIDIA AI)
42	AZTEC (AZT)
43	MetaStreet (MSTR)
44	PIKAMOON (PIKA)
45	Apeiron (APRS)
46	SNAP (NAP)
47	Fire (FIRE)
48	SUBSQUID (SQD)
49	Fluid Finance (FLUID)
50	Fuel Network (FUEL)
51	Wall Street Memes (WSM)
52	ShibaMemu (SHMU)
53	RAIT (RAIT)
54	Moon App (APP)
55	WPPToken (WPP)
56	BEBE (BEBE)
57	Venom Network (VENOM)
58	WRAPPED Protocol (WRAP)
59	Circle Coin (CIRCLE)
60	BonkBob (BOBONK)
61	wagmicatgirlkanye420etfmoonhero (WCGH)
62	Crypto Coven (WITCH)
63	LINEA (L)
64	Paxos Coin (PAXOS)
65	Cookies N Kicks (CNK)
66	Evolution Apes (EA)
67	HypedHuskyMetaCityNFT (HHMC)
68	Kong Ape Boss Club (KABC)
69	BitFrenchie (BF)
70	PEPEClassic (PEPECLASSIC)
71	Metamon (METAMON)
72	THE HUMARS (TH)
73	Rich Jaguarz (RJ)

Eilės nr.	Žetono pavadinimas
109	YouGetNothing.eth (NOTHING)
110	Emblem (EMB)
111	PUMBAA (PUMB)
112	Torochain (TORO)
113	Eggs Pepe (EGGSPEPE)
114	Matrix (MATRIX)
115	ToolsOfTheGreat (TOTG)
116	TokyoClone (TOKYOCLONE)
117	WinterBears (WB)
118	The Sloth Tribe (SLOTHS)
119	Apes In Space (AIS)
120	Clash of Shiba (COS)
121	8 BIT UNIVERSE (8BIT)
122	MaskBillionaireClub (MBC)
123	Rich Dwarves Tribe (DWARF)
124	BONEHEADS (BONE)
125	Buzzed Bear Hideout (BEAR)
126	Miss Universe NFT (MU)
127	Automated Assassins (AA)
128	RichKids (RKS)
129	TrippieHeadz (TRIPP)
130	Ancient Cats Club (CAT)
131	Crazy Camels (CAMEL)
132	Project Shura (SHURA)
133	DAO Turtles (DTS)
134	Bored Ape Tattoo Shop (BATS)
135	Acid Apes Candy Syndicate (AACS)
136	Trippy Ape Yacht Club (TAYC)
137	High Club (HC)
138	Pixel Cats (PIXCATS)
139	Ethermonkeys (EB)
140	Etherbananas (EB)
141	ZombieMonkeys (ZM)
142	Billionaire Dogs Club (BDC)
143	FinNexus (FNX)
144	EvolvedApes (EVA)
145	ThePlayBox (PLAYBOX)
146	HighRise Land (HIGHRISE)

2 Priedas. Visų į žetonus, kurie susiję viena iš nusikalstamos veiklos kategorijų „Rug pull“, atliktų pervedimų ir virtualios valiutos Eterio kainos palyginimas (Šaltinis: sudaryta autoriaus, remiantis Chainabuse (2024), Etherscan (2024), Solidus Labs (2024)).



2 Priedo pabaiga

Based Chill Guy	Rexas Finance	Ethereum Games	Pepe Unchained
American True Hero	Trump MAGA	47th President of the United States	MOG CAT
Bridge Payments	BOME TRUMP	Neiro Pump	BlockDAG
Polymarket	Babylon	XELON	BlackMythWukong
Morpho	Linea Network	zkEVM	GanNamDog
Tos Coin	FreeDurov Token	W Token	PEIPEI coin
LayerZero	DADDY TATE	SupraOracles	Chaos Labs
Scroll	Monad	Scroll	BVM
Espresso Systems	LayerZero	Renzo Protocol	RedSHIB
Tradecurve	Trism AI	BD20	Espresso
NVIDIA AI	AZTEC	MetaStreet	PIKAMOON
Apeiron	SNAP	Fire	SUBSQUID
Fluid Finance	Fuel Network	Wall Street Memes	ShibaMemu
RAIT	Moon App	WPPToken	BEBE
Venom Network	WRAPPED Protocol	Circle Coin	BonkBob
wagmicatgirlkanye420etfmoonhero	Crypto Coven	LINEA	Paxos Coin
Cookies N Kicks	Evolution Apes	HypedHuskyMetaCityNFT	Kong Ape Boss Club
BitFrenchie	PEPEClassic	Metamon	THE HUMARS
Rich Jaguarz	Naughty Bape Club	Cyclops Monkey Club	Empower Women Planet
Lucky Elephant Club	Cyber Zombie Society	Alien Alliance	Fud Token
JUGS	Smol Boyz	Fish	Kizuna AI
EspressoBot	Bitcoin30	watcher	Sugartown
Unibot X	Jada AI	https://sybiosis.finance/	world AI
SHIBBOT	SHIC	ハチ公	SOPH AI Token
Algotbot	XXX	SARATOSHI NAGAMOTO	HarryPotterObamaSonic20Inu
0xCoco	tetris	RNS	iBOT
Pond Coin	Towelie	voQui Token	Mojo Jojo
YouGetNothing.eth	Emblem	PUMBAA	ToroChain
Eggs Pepe	Matrix	ToolsOfTheGreat	TokyoClone
WinterBears	The Sloth Tribe	Apes In Space	Clash of Shiba
8 BIT UNIVERSE	MaskBillionaireClub	Rich Dwarves Tribe	BONEHEADS
Buzzed Bear Hideout	Miss Universe NFT	Automated Assassins	RichKids
TrippieHeadz	Ancient Cats Club	Crazy Camels	Project Shura
DAO Turtles	Bored Ape Tattoo Shop	Acid Apes Candy Syndicate	Trippy Ape Yacht Club
High Club	Pixel Cats	Ethermonkeys	Etherbananas
ZombieMonkeys	Billionaire Dogs Club	FinNexus	EvolvedApes
ThePlayBox	HighRise Land	Eteris (ETH)	

3 Priedas. Antruoju tyrimo analizuojamu laikotarpiu nagrinėjami visi žetonai (Šaltinis: sudaryta autoriaus, remiantis Chainabuse (2024), Etherscan (2024), Solidus Labs (2024)).

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Pervedimų skaičius
1	WPPToken (WPP)	2020-07-24	448
2	Crypto Coven (WITCH)	2021-11-04	7220
3	Cookies N Kicks (CNK)	2022-02-08	2861
4	Evolution Apes (EA)	2022-01-31	5763
5	HypedHuskyMetaCityNFT (HHMC)	2022-01-25	264
6	Kong Ape Boss Club (KABC)	2022-12-21	416
7	BitFrenchie (BF)	2022-12-13	2043
8	Metamon (METAMON)	2022-04-14	686
9	THE HUMARS (TH)	2021-12-20	585
10	Rich Jaguarz (RJ)	2022-01-25	121
11	Naughty Bape Club (NBC)	2021-12-20	769
12	Cyclops Monkey Club (CMC)	2021-12-06	6734
13	Empower Women Planet (EWP)	2022-01-26	1169
14	Lucky Elephant Club (LEC)	2021-11-18	526
15	Cyber Zombie Society (CZS)	2021-11-20	689
16	Alien Alliance (AA)	2021-12-05	1115
17	Fud Token (FUD)	2021-11-17	2256
18	Smol Boyz (SMOLBOYZ)	2022-03-07	880
19	Emblem (EMB)	2021-02-15	938
20	ToolsOfTheGreat (TOTG)	2022-05-21	190
21	TokyoClone (TOKYOCLONE)	2022-04-25	1290
22	WinterBears (WB)	2021-09-18	4606
23	The Sloth Tribe (SLOTHS)	2021-11-16	1050
24	Apes In Space (AIS)	2021-12-03	9644
25	Clash of Shiba (COS)	2022-03-22	134
26	8 BIT UNIVERSE (8BIT)	2021-08-21	791
27	MaskBillionaireClub (MBC)	2022-02-28	2753
28	Rich Dwarves Tribe (DWARF)	2022-02-09	6121
29	BONEHEADS (BONE)	2021-08-20	544
30	Buzzed Bear Hideout (BEAR)	2021-07-15	729
31	Miss Universe NFT (MU)	2021-12-12	1685
32	Automated Assassins (AA)	2022-06-01	3844
33	RichKids (RKS)	2021-09-26	574
34	TrippieHeadz (TRIPP)	2021-11-04	468
35	Ancient Cats Club (CAT)	2021-11-27	4553
36	Crazy Camels (CAMEL)	2021-11-14	2919
37	Project Shura (SHURA)	2022-01-04	6320
38	DAO Turtles (DTS)	2021-10-03	688
39	Bored Ape Tattoo Shop (BATS)	2021-11-18	179
40	Trippy Ape Yacht Club (TAYC)	2021-08-16	139
41	High Club (HC)	2021-07-19	34
42	Ethermonkeys (EB)	2021-10-11	2013
43	Etherbananas (EB)	2021-10-05	226
44	ZombieMonkeys (ZM)	2021-10-15	579
45	Billionaire Dogs Club (BDC)	2021-12-11	2079
46	FinNexus (FNX)	2020-07-27	66
47	EvolvedApes (EVA)	2021-07-23	1010
48	ThePlayBox (PLAYBOX)	2022-03-28	716
49	HighRise Land (HIGHRISE)	2022-03-26	258

4 Priedas. Trečiuoju tyrimo analizuojamu laikotarpiu nagrinėjami visi žetonai (Šaltinis: sudaryta autoriaus, remiantis Chainabuse (2024), Etherscan (2024), Solidus Labs (2024)).

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Pervedimų skaičius
1	Tradecurve (TCRV)	2023-04-28	2
2	Wall Street Memes (WSM)	2023-05-30	57
3	ShibaMemu (SHMU)	2023-06-28	3
4	WPPToken (WPP)	2020-07-24	483
5	Crypto Coven (WITCH)	2021-11-04	2683
6	Cookies N Kicks (CNK)	2022-02-08	136
7	Evolution Apes (EA)	2022-01-31	226
8	HypedHuskyMetaCityNFT (HHMC)	2022-01-25	13
9	Kong Ape Boss Club (KABC)	2022-12-21	25
10	BitFrenchie (BF)	2022-12-13	75
11	Metamon (METAMON)	2022-04-14	84
12	THE HUMARS (TH)	2021-12-20	6
13	Rich Jaguarz (RJ)	2022-01-25	1
14	Naughty Bape Club (NBC)	2021-12-20	36
15	Cyclops Monkey Club (CMC)	2021-12-06	245
16	Empower Women Planet (EWP)	2022-01-26	71
17	Lucky Elephant Club (LEC)	2021-11-18	35
18	Cyber Zombie Society (CZS)	2021-11-20	29
19	Alien Alliance (AA)	2021-12-05	16
20	Fud Token (FUD)	2021-11-17	37
21	JUGS (\$JUGS)	2023-05-02	160
22	Smol Boyz (SMOLBOYZ)	2022-03-07	134
23	Kizuna AI (KIZUNA)	2023-08-29	72
24	EspressoBot (ESPS)	2023-08-31	72
25	Bitcoin30 (BTC30)	2023-08-13	10
26	watcher (WATCHER)	2023-08-13	21
27	Sugartown (SUGARTOWN)	2023-08-14	15
28	Unibot X (UNIBOT X)	2023-08-16	23
29	Jada AI (JADA AI)	2023-08-18	8
30	https://symbiosis.finance/ (SYMBIOSIS)	2023-08-28	17
31	world AI (WORLD AI)	2023-08-11	15
32	SHIBBOT (SHIBBOT)	2023-08-16	16
33	SHIC (SHIC)	2023-09-04	490
34	ハチ公 (HACHIKO)	2023-08-12	641
35	SOPH AI Token (SOPH)	2023-07-25	25
36	Algobot (ALGO)	2023-07-25	21
37	XXX (XXX)	2023-07-26	68
38	SARATOSHI NAGAMOTO (SARATOSHI)	2023-07-27	33
39	HarryPotterObamaSonic20Inu (ETHEREUM)	2023-07-27	49
40	0xCoco (COCO)	2023-07-28	240
41	tetris (TETRIS)	2023-07-28	27
42	RNS (RNS)	2023-07-29	93
43	iBOT (IBOT)	2023-07-29	26
44	Pond Coin (PNDC)	2023-08-05	268

4 Priedo pabaiga

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Pervedimų skaičius
45	Towelie (TOWELIE)	2023-07-22	822
46	voQui Token (VOQUI)	2023-06-08	416
47	Mojo Jojo (MOJO)	2023-07-17	233
48	YouGetNothing.eth (NOTHING)	2023-07-11	89
49	Emblem (EMB)	2021-02-15	824
50	PUMBAA (PUMB)	2023-07-05	160
51	Torochain (TORO)	2023-05-07	481
52	Eggs Pepe (EGGSPEPE)	2023-05-03	121
53	Matrix (MATRIX)	2022-10-02	55
54	ToolsOfTheGreat (TOTG)	2022-05-21	38
55	TokyoClone (TOKYOCLONE)	2022-04-25	354
56	WinterBears (WB)	2021-09-18	2320
57	The Sloth Tribe (SLOTHS)	2021-11-16	20
58	Apes In Space (AIS)	2021-12-03	1210
59	Clash of Shiba (COS)	2022-03-22	39
60	8 BIT UNIVERSE (8BIT)	2021-08-21	466
61	MaskBillionaireClub (MBC)	2022-02-28	176
62	Rich Dwarves Tribe (DWARF)	2022-02-09	159
63	BONEHEADS (BONE)	2021-08-20	393
64	Buzzed Bear Hideout (BEAR)	2021-07-15	1177
65	Miss Universe NFT (MU)	2021-12-12	31
66	Automated Assassins (AA)	2022-06-01	291
67	RichKids (RKS)	2021-09-26	256
68	TrippieHeadz (TRIPP)	2021-11-04	57
69	Ancient Cats Club (CAT)	2021-11-27	72
70	Crazy Camels (CAMEL)	2021-11-14	181
71	Project Shura (SHURA)	2022-01-04	253
72	DAO Turtles (DTS)	2021-10-03	261
73	Bored Ape Tattoo Shop (BATS)	2021-11-18	8
74	Trippy Ape Yacht Club (TAYC)	2021-08-16	72
75	High Club (HC)	2021-07-19	19
76	Pixel Cats (PIXCATS)	2022-07-21	29
77	Ethermonkeys (EB)	2021-10-11	206
78	Etherbananas (EB)	2021-10-05	65
79	ZombieMonkeys (ZM)	2021-10-15	82
80	Billionaire Dogs Club (BDC)	2021-12-11	80
81	FinNexus (FNX)	2020-07-27	234
82	EvolvedApes (EVA)	2021-07-23	338
83	ThePlayBox (PLAYBOX)	2022-03-28	12

5 Priedas. Ketvirtuoju tyrimo analizuojamu laikotarpiu nagrinėjami visi žetonai (Šaltinis: sudaryta autoriaus, remiantis Chainabuse (2024), Etherscan (2024), Solidus Labs (2024)).

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Pervedimų skaičius
1	Tradecurve (TCRV)	2023-04-28	2
2	Wall Street Memes (WSM)	2023-05-30	57
3	ShibaMemu (SHMU)	2023-06-28	3
4	WPPToken (WPP)	2020-07-24	483
5	Crypto Coven (WITCH)	2021-11-04	2683
6	Cookies N Kicks (CNK)	2022-02-08	136
7	Evolution Apes (EA)	2022-01-31	226
8	HypedHuskyMetaCityNFT (HHMC)	2022-01-25	13
9	Kong Ape Boss Club (KABC)	2022-12-21	25
10	BitFrenchie (BF)	2022-12-13	75
11	Metamon (METAMON)	2022-04-14	84
12	THE HUMARS (TH)	2021-12-20	6
13	Rich Jaguarz (RJ)	2022-01-25	1
14	Naughty Bape Club (NBC)	2021-12-20	36
15	Cyclops Monkey Club (CMC)	2021-12-06	245
16	Empower Women Planet (EWP)	2022-01-26	71
17	Lucky Elephant Club (LEC)	2021-11-18	35
18	Cyber Zombie Society (CZS)	2021-11-20	29
19	Alien Alliance (AA)	2021-12-05	16
20	Fud Token (FUD)	2021-11-17	37
21	JUGS (\$JUGS)	2023-05-02	160
22	Smol Boyz (SMOLBOYZ)	2022-03-07	134
23	Kizuna AI (KIZUNA)	2023-08-29	72
24	EspressoBot (ESPS)	2023-08-31	72
25	Bitcoin30 (BTC30)	2023-08-13	10
26	watcher (WATCHER)	2023-08-13	21
27	Sugartown (SUGARTOWN)	2023-08-14	15
28	Unibot X (UNIBOT X)	2023-08-16	23
29	Jada AI (JADA AI)	2023-08-18	8
30	https://symbiosis.finance/ (SYMBIOSIS)	2023-08-28	17
31	world AI (WORLD AI)	2023-08-11	15
32	SHIBBOT (SHIBBOT)	2023-08-16	16
33	SHIC (SHIC)	2023-09-04	490
34	ハチ公 (HACHIKO)	2023-08-12	641
35	SOPH AI Token (SOPH)	2023-07-25	25
36	Algobot (ALGO)	2023-07-25	21
37	XXX (XXX)	2023-07-26	68
38	SARATOSHI NAGAMOTO (SARATOSHI)	2023-07-27	33
39	HarryPotterObamaSonic20Inu (ETHEREUM)	2023-07-27	49
40	0xCoco (COCO)	2023-07-28	240
41	tetris (TETRIS)	2023-07-28	27
42	RNS (RNS)	2023-07-29	93
43	iBOT (IBOT)	2023-07-29	26
44	Pond Coin (PNDC)	2023-08-05	268
45	Towelie (TOWELIE)	2023-07-22	822
46	voQui Token (VOQUI)	2023-06-08	416
47	Mojo Jojo (MOJO)	2023-07-17	233
48	YouGetNothing.eth (NOTHING)	2023-07-11	89
49	Emblem (EMB)	2021-02-15	824
50	PUMBAA (PUMB)	2023-07-05	160
51	Torochain (TORO)	2023-05-07	481
52	Eggs Pepe (EGGSPEPE)	2023-05-03	121

5 Priedo pabaiga

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Pervedimų skaičius
53	Matrix (MATRIX)	2022-10-02	55
54	ToolsOfTheGreat (TOTG)	2022-05-21	38
55	TokyoClone (TOKYOCLONE)	2022-04-25	354
56	WinterBears (WB)	2021-09-18	2320
57	The Sloth Tribe (SLOTHS)	2021-11-16	20
58	Apes In Space (AIS)	2021-12-03	1210
59	Clash of Shiba (COS)	2022-03-22	39
60	8 BIT UNIVERSE (8BIT)	2021-08-21	466
61	MaskBillionaireClub (MBC)	2022-02-28	176
62	Rich Dwarves Tribe (DWARF)	2022-02-09	159
63	BONEHEADS (BONE)	2021-08-20	393
64	Buzzed Bear Hideout (BEAR)	2021-07-15	1177
65	Miss Universe NFT (MU)	2021-12-12	31
66	Automated Assassins (AA)	2022-06-01	291
67	RichKids (RKS)	2021-09-26	256
68	TrippieHeadz (TRIPP)	2021-11-04	57
69	Ancient Cats Club (CAT)	2021-11-27	72
70	Crazy Camels (CAMEL)	2021-11-14	181
71	Project Shura (SHURA)	2022-01-04	253
72	DAO Turtles (DTS)	2021-10-03	261
73	Bored Ape Tattoo Shop (BATS)	2021-11-18	8
74	Trippy Ape Yacht Club (TAYC)	2021-08-16	72
75	High Club (HC)	2021-07-19	19
76	Pixel Cats (PIXCATS)	2022-07-21	29
77	Ethermonkeys (EB)	2021-10-11	206
78	Etherbananas (EB)	2021-10-05	65
79	ZombieMonkeys (ZM)	2021-10-15	82
80	Billionaire Dogs Club (BDC)	2021-12-11	80
81	FinNexus (FNX)	2020-07-27	234
82	EvolvedApes (EVA)	2021-07-23	338
83	ThePlayBox (PLAYBOX)	2022-03-28	12

6 Priedas. Penktuoju tyrimo analizuojamu laikotarpiu nagrinėjami visi žetonai (Šaltinis: sudaryta autoriaus, remiantis Chainabuse (2024), Etherscan (2024), Solidus Labs (2024)).

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Pervedimų skaičius
1	Based Chill Guy (CHILLGUY)	2024-11-22	5
2	Rexas Finance (RXS)	2024-09-11	953
3	Ethereum Games (ETHG)	2024-06-22	6484
4	Pepe Unchained (PEPU)	2024-08-17	709
5	American True Hero (TRUMP)	2024-11-18	5
6	Trump MAGA (TRUMPMAGA)	2024-10-30	6
7	47th President of the United States (TRUMP47)	2024-10-22	3358
8	MOG CAT (MOG)	2024-09-14	3495
9	Bridge Payments (BRIDGE)	2024-10-27	341
10	BOME TRUMP (TRUMP)	2024-09-07	6483
11	Neiro Pump (NEIRO)	2024-09-24	4018
12	BlockDAG (BDAG)	2024-07-07	560
13	Polymarket (POL)	2024-09-05	14
14	Babylon (BABL)	2024-08-25	270
15	XELON (XELON)	2024-08-27	334
16	BlackMythWukong (WUKONG)	2024-08-20	181
17	Morpho (MORPHO)	2024-08-09	2258
18	Linea Network (LINEA)	2024-08-02	640
19	zkEVM (ZKE)	2024-07-18	65
20	GanNamDog (GNDOG)	2024-07-31	301
21	Tos Coin (TOS)	2024-06-22	350
22	FreeDurov Token (FREED)	2024-08-24	262
23	W Token (W)	2024-10-26	162
24	PEIPEI coin (PEIPEI)	2024-09-10	73
25	LayerZero (ZRO)	2024-06-19	2844
26	DADDY TATE (DADDY)	2024-06-13	2
27	SupraOracles (SUPRA)	2024-05-19	212
28	Chaos Labs (CHAOS)	2024-05-24	32
29	Scroll (SCROLL)	2024-05-31	62
30	Monad (TBD)	2024-05-30	41
31	Scroll (SCROLL)	2024-05-18	135
32	BVM (BVM)	2024-05-23	111
33	Espresso Systems (ESP)	2024-04-24	254
34	LayerZero (ZRO)	2024-04-21	527
35	Renzo Protocol (EZ)	2024-04-23	1538
36	RedSHIB (REDSHIB)	2024-01-24	468
37	Tradecurve (TCRV)	2023-04-28	1620
38	Trism AI (TRISM)	2024-04-14	273
39	BD20 (BD20)	2024-04-12	8
40	Espresso (ESP)	2024-04-07	211
41	NVIDIA AI (NVIDIA AI)	2024-04-05	157
42	AZTEC (AZT)	2024-03-25	346
43	MetaStreet (MSTR)	2024-03-25	32
44	PIKAMOON (PIKA)	2024-03-12	22431
45	Apeiron (APRS)	2024-03-16	835
46	SNAP (NAP)	2024-03-17	63
47	Fire (FIRE)	2024-02-19	137
48	SUBSQUID (SQD)	2024-02-04	207
49	Fluid Finance (FLUID)	2024-02-03	335
50	Fuel Network (FUEL)	2024-02-01	470
51	Wall Street Memes (WSM)	2023-05-30	87465
52	ShibaMemu (SHMU)	2023-06-28	612

6 Priedo tęsinys

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Pervedimų skaičius
53	RAIT (RAIT)	2023-12-07	22
54	Moon App (APP)	2024-10-10	12314
55	WPPToken (WPP)	2020-07-24	581
56	BEBE (BEBE)	2023-12-19	205
57	Venom Network (VENOM)	2023-12-11	2015
58	WRAPPED Protocol (WRAP)	2023-12-13	1484
59	Circle Coin (CIRCLE)	2023-11-30	538
60	BonkBob (BOBONK)	2023-11-30	104
61	wagmicatgirlkanye420etfmoohero (WCGH)	2023-11-17	36
62	Crypto Coven (WITCH)	2021-11-04	622
63	LINEA (L)	2023-10-17	1077
64	Paxos Coin (PAXOS)	2023-10-30	744
65	Cookies N Kicks (CNK)	2022-02-08	26
66	Evolution Apes (EA)	2022-01-31	70
67	Kong Ape Boss Club (KABC)	2022-12-21	4
68	BitFrenchie (BF)	2022-12-13	38
69	PEPEClassic (PEPECLASSIC)	2023-10-10	20
70	Metamon (METAMON)	2022-04-14	7
71	THE HUMARS (TH)	2021-12-20	2
72	Naughty Bape Club (NBC)	2021-12-20	3
73	Cyclops Monkey Club (CMC)	2021-12-06	94
74	Empower Women Planet (EWP)	2022-01-26	21
75	Lucky Elephant Club (LEC)	2021-11-18	13
76	Cyber Zombie Society (CZS)	2021-11-20	6
77	Alien Alliance (AA)	2021-12-05	2
78	Fud Token (FUD)	2021-11-17	14
79	JUGS (\$JUGS)	2023-05-02	4
80	Smol Boyz (SMOLBOYZ)	2022-03-07	5
81	Fish (FISH)	2023-09-25	26
82	SHIC (SHIC)	2023-09-04	10
83	ハチ公 (HACHIKO)	2023-08-12	14
84	XXX (XXX)	2023-07-26	1
85	0xCoco (COCO)	2023-07-28	3
86	tetris (TETRIS)	2023-07-28	1
87	RNS (RNS)	2023-07-29	2
88	Pond Coin (PNDC)	2023-08-05	1
89	Towelie (TOWELIE)	2023-07-22	15
90	Mojo Jojo (MOJO)	2023-07-17	2
91	Emblem (EMB)	2021-02-15	51
92	PUMBAA (PUMB)	2023-07-05	1
93	Torochain (TORO)	2023-05-07	9
94	ToolsOfTheGreat (TOTG)	2022-05-21	3
95	TokyoClone (TOKYOCLONE)	2022-04-25	33
96	WinterBears (WB)	2021-09-18	283
97	Apes In Space (AIS)	2021-12-03	180
98	Clash of Shiba (COS)	2022-03-22	4
99	8 BIT UNIVERSE (8BIT)	2021-08-21	113
100	MaskBillionaireClub (MBC)	2022-02-28	46
101	Rich Dwarves Tribe (DWARF)	2022-02-09	49
102	BONEHEADS (BONE)	2021-08-20	55
103	Buzzed Bear Hideout (BEAR)	2021-07-15	365
104	Miss Universe NFT (MU)	2021-12-12	15
105	Automated Assassins (AA)	2022-06-01	19

6 Priedo pabaiga

Eilės nr.	Žetono pavadinimas	Žetono sukūrimo data	Pervedimų skaičius
106	RichKids (RKS)	2021-09-26	74
107	TrippieHeadz (TRIPP)	2021-11-04	18
108	Ancient Cats Club (CAT)	2021-11-27	24
109	Crazy Camels (CAMEL)	2021-11-14	21
110	Project Shura (SHURA)	2022-01-04	37
111	DAO Turtles (DTS)	2021-10-03	48
112	Bored Ape Tattoo Shop (BATS)	2021-11-18	2
113	Acid Apes Candy Syndicate (AACS)	2021-09-24	1
114	Trippy Ape Yacht Club (TAYC)	2021-08-16	14
115	Ethermonkeys (EB)	2021-10-11	60
116	Etherbananas (EB)	2021-10-05	9
117	ZombieMonkeys (ZM)	2021-10-15	25
118	Billionaire Dogs Club (BDC)	2021-12-11	12
119	FinNexus (FNX)	2020-07-27	66
120	EvolvedApes (EVA)	2021-07-23	82
121	ThePlayBox (PLAYBOX)	2022-03-28	1
122	HighRise Land (HIGHRISE)	2022-03-26	1

7 Priedas. Žetonų, kurių dabartinis likvidumas mažiau nei 0,01 Eterio, pradinis likvidumas ir likvidumo pokytis kartais (Šaltinis: sudaryta autoriaus, remiantis Solidus Labs (2024)).

Eilės nr.	Žetono pavadinimas	Pradinis likvidumas	Likvidumas 2024-12-02 duomenimis, JAV dol.	Likvidumo pokytis, kartais
1	American True Hero (TRUMP)	1	3,643.48	100
2	Trump MAGA (TRUMPMAGA)	1	3,643.48	100
3	Bridge Payments (BRIDGE)	12.4	45,179.15	1240
4	Polymarket (POL)	10	36,434.80	1000
5	Babylon (BABL)	69.42	252,930.38	6942
6	XELON (XELON)	5	18,217.40	500
7	BlackMythWukong (WUKONG)	33.5	122,056.58	3350
8	Morpho (MORPHO)	50	182,174.00	5000
9	zkEVM (ZKE)	6	21,860.88	600
10	GanNamDog (GNDOG)	66.59	242,619.33	6659
11	Tos Coin (TOS)	8	29,147.84	800
12	LayerZero (ZRO)	15	54,652.20	1500
13	DADDY TATE (DADDY)	5	18,217.40	500
14	SupraOracles (SUPRA)	6.61	24,083.40	661
15	Chaos Labs (CHAOS)	9.97	36,325.50	997
16	Scroll (SCROLL)	2.5	9,108.70	250
17	Monad (TBD)	10.63	38,730.19	1063
18	Scroll (SCROLL)	10	36,434.80	1000
19	BVM (BVM)	7.5	27,326.10	750
20	Espresso Systems (ESP)	8	29,147.84	800
21	LayerZero (ZRO)	30.99	112,911.45	3099
22	Renzo Protocol (EZ)	8	29,147.84	800
23	RedSHIB (REDSHIB)	52.84	192,521.48	5284
24	Trism AI (TRISM)	15	54,652.20	1500
25	BD20 (BD20)	10	36,434.80	1000
26	Espresso (ESP)	3.7	13,480.88	370
27	NVIDIA AI (NVIDIA AI)	3	10,930.44	300
28	AZTEC (AZT)	8.8	32,062.62	880
29	MetaStreet (MSTR)	4	14,573.92	400
30	Apeiron (APRS)	35.49	129,307.11	3549
31	SNAP (NAP)	10	36,434.80	1000
32	Fire (FIRE)	74.99	273,224.57	7499
33	SUBSQUID (SQD)	14.5	52,830.46	1450
34	Fluid Finance (FLUID)	8	29,147.84	800
35	Fuel Network (FUEL)	30	109,304.40	3000
36	RAIT (RAIT)	10	36,434.80	1000
37	BEBE (BEBE)	44.93	163,701.56	4493
38	Venom Network (VENOM)	7.06	25,722.97	706
39	WRAPPED Protocol (WRAP)	3.63	13,225.83	363
40	Circle Coin (CIRCLE)	3.67	13,371.57	367
41	BonkBob (BOBONK)	6	21,860.88	600
42	wagmicatgirlkanye420etfmoonhero (WCGH)	3	10,930.44	300
43	LINEA (L)	99.1	361,068.87	9910
44	Paxos Coin (PAXOS)	98	357,061.04	9800
45	PEPEClassic (PEPECLASSIC)	29.9	108,940.05	2990
46	Fish (FISH)	3.1	11,294.79	310

8 Priedas. Analizuojamu laikotarpiu apskaičiuota T.testo reikšmė ir kritinė t-reikšmė (Šaltinis: sudaryta autorės).

Eilės nr.	Žetono pavadinimas	T.testo reikšmė	Kritinė t-reikšmė
1	Based Chill Guy (CHILLGUY)	-0.78	-2.57
2	Rexas Finance (RXS)	3.50	1.96
3	Ethereum Games (ETHG)	3.82	1.96
4	Pepe Unchained (PEPU)	-5.32	-1.96
5	American True Hero (TRUMP)	0.73	2.57
6	Trump MAGA (TRUMPMAGA)	-0.01	-2.45
7	47th President of the United States (TRUMP47)	-32.83	-1.96
8	MOG CAT (MOG)	-15.14	-1.96
9	Bridge Payments (BRIDGE)	1.71	1.97
10	BOME TRUMP (TRUMP)	-35.12	-1.96
11	Neiro Pump (NEIRO)	-32.95	-1.96
12	BlockDAG (BDAG)	0.46	1.96
13	Polymarket (POL)	-0.41	-2.14
14	Babylon (BABL)	-0.27	-1.97
15	XELON (XELON)	10.35	1.97
16	BlackMythWukong (WUKONG)	-6.10	-1.97
17	Morpho (MORPHO)	-8.15	-1.96
18	Linea Network (LINEA)	-5.13	-1.96
19	zkEVM (ZKE)	4.46	2.00
20	GanNamDog (GNDOG)	23.36	1.97
21	Tos Coin (TOS)	2.10	1.97
22	FreeDurov Token (FREED)	8.41	1.97
23	W Token (W)	-0.61	-1.97
24	PEIPEI coin (PEIPEI)	29.91	1.99
25	LayerZero (ZRO)	14.72	1.96
26	DADDY TATE (DADDY)	nejmanoma apskaičiuoti	
27	SupraOracles (SUPRA)	4.15	1.97
28	Chaos Labs (CHAOS)	3.65	2.04
29	Scroll (SCROLL)	1.58	2.00
30	Monad (TBD)	2.91	2.02
31	Scroll (SCROLL)	1.94	1.98
32	BVM (BVM)	nejmanoma apskaičiuoti	
33	Espresso Systems (ESP)	-0.41	-1.97
34	LayerZero (ZRO)	2.07	1.96
35	Renzo Protocol (EZ)	-4.83	-1.96
36	RedSHIB (REDSHIB)	-6.46	-1.97
37	Tradecurve (TCRV)	2.44	1.96
38	Trism AI (TRISM)	0.02	1.97
39	BD20 (BD20)	nejmanoma apskaičiuoti	
40	Espresso (ESP)	10.15	1.97
41	NVIDIA AI (NVIDIA AI)	1.94	1.98
42	AZTEC (AZT)	-1.52	-1.97
43	MetaStreet (MSTR)	3.61	2.04
44	PIKAMOON (PIKA)	45.70	1.96
45	Apeiron (APRS)	7.44	1.96
46	SNAP (NAP)	-3.49	-2.00
47	Fire (FIRE)	-2.71	-1.98
48	SUBSQUID (SQD)	-3.54	-1.97
49	Fluid Finance (FLUID)	-7.43	-1.97
50	Fuel Network (FUEL)	-15.23	-1.97
51	Wall Street Memes (WSM)	-144.92	-1.96
52	ShibaMemu (SHMU)	-7.93	-1.96

8 Priedo tęsinys

Eilės nr.	Žetono pavadinimas	T.testo reikšmė	Kritinė t-reikšmė
53	RAIT (RAIT)	-2.07	-2.07
54	Moon App (APP)	-11.92	-1.96
55	WPPToken (WPP)	-1.57	-1.96
56	BEBE (BEBE)	-4.58	-1.97
57	Venom Network (VENOM)	-14.67	-1.96
58	WRAPPED Protocol (WRAP)	-8.51	-1.96
59	Circle Coin (CIRCLE)	-7.47	-1.96
60	BonkBob (BOBONK)	-8.19	-1.98
61	wagmicatgirlkanye420etfmoonhero (WCGH)	-2.47	-2.03
62	Crypto Coven (WITCH)	-2.48	-1.96
63	LINEA (L)	-13.47	-1.96
64	Paxos Coin (PAXOS)	-11.48	-1.96
65	Cookies N Kicks (CNK)	-1.59	-2.06
66	Evolution Apes (EA)	1.96	1.99
67	Kong Ape Boss Club (KABC)	nejmanoma apskaičiuoti	
68	BitFrenchie (BF)	0.69	2.02
69	PEPEClassic (PEPECLASSIC)	-2.99	-2.09
70	Metamon (METAMON)	-1.74	-2.36
71	THE HUMARS (TH)	nejmanoma apskaičiuoti	
72	Naughty Bape Club (NBC)	nejmanoma apskaičiuoti	
73	Cyclops Monkey Club (CMC)	0.43	1.99
74	Empower Women Planet (EWP)	1.18	2.08
75	Lucky Elephant Club (LEC)	nejmanoma apskaičiuoti	
76	Cyber Zombie Society (CZS)	nejmanoma apskaičiuoti	
77	Alien Alliance (AA)	nejmanoma apskaičiuoti	
78	Fud Token (FUD)	0.17	2.14
79	JUGS (\$JUGS)	nejmanoma apskaičiuoti	
80	Smol Boyz (SMOLBOYZ)	-27.16	-2.57
81	Fish (FISH)	nejmanoma apskaičiuoti	
82	SHIC (SHIC)	-0.77	-2.23
83	ハチ公 (HACHIKO)	-1.12	-2.14
84	XXX (XXX)	nejmanoma apskaičiuoti	
85	0xCoco (COCO)	nejmanoma apskaičiuoti	
86	tetris (TETRIS)	nejmanoma apskaičiuoti	
87	RNS (RNS)	nejmanoma apskaičiuoti	
88	Pond Coin (PNDC)	nejmanoma apskaičiuoti	
89	Towelie (TOWELIE)	-0.29	-2.13
90	Mojo Jojo (MOJO)	nejmanoma apskaičiuoti	
91	Emblem (EMB)	-1.39	-2.01
92	PUMBAA (PUMB)	nejmanoma apskaičiuoti	
93	Torochain (TORO)	-0.19	-2.26
94	ToolsOfTheGreat (TOTG)	nejmanoma apskaičiuoti	
95	TokyoClone (TOKYOCLONE)	-0.11	-2.03
96	WinterBears (WB)	0.28	1.97
97	Apes In Space (AIS)	-0.03	-1.97
98	Clash of Shiba (COS)	nejmanoma apskaičiuoti	
99	8 BIT UNIVERSE (8BIT)	-1.51	-1.98
100	MaskBillionaireClub (MBC)	-0.93	-2.01
101	Rich Dwarves Tribe (DWARF)	-2.02	-2.01
102	BONEHEADS (BONE)	-0.01	-2.00
103	Buzzed Bear Hideout (BEAR)	-3.77	-1.97
104	Miss Universe NFT (MU)	-3.03	-2.13
105	Automated Assassins (AA)	1.23	2.09
106	RichKids (RKS)	1.78	1.99

8 Priedo pabaiga

Eilės nr.	Žetono pavadinimas	T.testo reikšmė	Kritinė t-reikšmė
107	TrippieHeadz (TRIPP)	-1.76	-2.10
108	Ancient Cats Club (CAT)	2.28	2.06
109	Crazy Camels (CAMEL)	0.90	2.08
110	Project Shura (SHURA)	0.69	2.03
111	DAO Turtles (DTS)	-0.62	-2.01
112	Bored Ape Tattoo Shop (BATS)	nejmanoma apskaičiuoti	
113	Acid Apes Candy Syndicate (AACS)	nejmanoma apskaičiuoti	
114	Trippy Ape Yacht Club (TAYC)	-0.53	-2.14
115	Ethermonkeys (EB)	-1.58	-2.00
116	Etherbananas (EB)	-0.59	-2.26
117	ZombieMonkeys (ZM)	-1.54	-2.06
118	Billionaire Dogs Club (BDC)	1.29	2.18
119	FinNexus (FNX)	-1.57	-2.00
120	EvolvedApes (EVA)	-0.95	-1.99
121	ThePlayBox (PLAYBOX)	nejmanoma apskaičiuoti	
122	HighRise Land (HIGHRISE)	nejmanoma apskaičiuoti	