

VILNIAUS UNIVERSITETAS
EKONOMIKOS IR VERSLO ADMINISTRAVIMO FAKULTETAS

Finansai ir bankininkystė

Stela Andriuškaitė
MAGISTRO BAIGIAMASIS DARBAS

Nusikalstamų veikų kriptovaliutų rinkoje tyrimas	Research on criminal activity in cryptocurrency market
---	---

Darbo vadovė: Prof. dr. Alfreda Šapkauskienė

Vilnius, 2024

Turinys

LENTELIŲ SĄRAŠAS.....	4
PAVEIKSLŲ SĄRAŠAS.....	6
ĮVADAS.....	7
1. NUSIKALSTAMŲ VEIKŲ KRIPTOVALIUTŲ RINKOJE LITERATŪROS ANALIZĖ	10
1.1. Kripto valiutos samprata ir savybės	10
1.2. Kripto valiutų rinkos reglamentavimo problematika	19
1.3. Nusikalstamos veikos pasireiškiančios kripto valiutų rinkoje	27
2. NUSIKALSTAMŲ VEIKŲ KRIPTOVALIUTŲ RINKOJE TYRIMO METODOLOGIJA	38
2.1. Tyrimo tikslas, uždaviniai ir metodai.....	39
2.2. Tyrimo modelis ir hipotezės.....	40
3. NUSIKALSTAMŲ VEIKŲ KRIPTOVALIUTŲ RINKOJE TYRIMO REZULTATAI	47
3.1. BitcoinAbuse.com identifikuotų charakteristikų rezultatai.....	48
3.1.1. Kripto valiutų piniginių adresų ir nusikalstamų veikų charakteristikų rezultatai	48
3.1.2. Kartai, kiek buvo pateikta pranešimų, charakteristikos rezultatai	55
3.1.3. Pranešimų pateikimo laikotarpių charakteristikos rezultatai.....	61
3.2. Blockchain.com tyrimo metu surinktų charakteristikų rezultatai	63
3.2.1. Operacijų skaičiaus, kripto valiutų piniginių adresuose, charakteristikos rezultatai	63
3.2.2. Lėšų, gautų iš nusikalstamos veikos vykdymo kripto valiutų rinkoje, charakteristikos rezultatai.....	66
3.2.3. Išsiųstų lėšų iš kripto valiutų piniginių ir galutinio balanso charakteristikų rezultatai	68
IŠVADOS IR PASIŪLYMAI.....	71
LITERATŪROS IR ŠALTINIŲ SĄRAŠAS	74

SUMMARY	86
PRIEDAI	88
Priedas Nr. 1. Mokslinėje literatūroje aptartos nusikalstamos veikos.....	88
Priedas Nr. 2. Mokslinėje literatūroje identifikuotos nusikalstamos veikos kriptovaliutų rinkoje.....	90
Priedas Nr. 3. BitcoinAbuse.com duomenys tyrimo laikotarpyje.....	94
Priedas Nr. 4. BlockChain.com duomenys tyrimo laikotarpyje.....	112
Priedas Nr. 5. Statistinių rodiklių „Kriptovaliutų piniginių adresų skaičius“ ir „Kartai, kiek buvo pranešta apie nusikalstamą veiką“ apskaičiavimas	128
Priedas Nr. 6. Hipotezės 3 skaičiavimas	130
Priedas Nr. 7. Statistinių rodiklių „Pirma kartą pateiktas pranešimas“ ir „Paskutinį kartą pateiktas pranešimas“ apskaičiavimas.....	133
Priedas Nr. 8. Hipotezės 4 skaičiavimai.....	135

LENTELIŲ SĄRAŠAS

1 lentelė. Kripto valiutų klasės.....	14
2 lentelė. Kripto valiutų rinkos ir dekretinių pinigų rinkos skirtumai.....	16
3 lentelė. Kripto valiutų rinkos ir padengtųjų pinigų (aukso standarto) rinkos panašumai ir skirtumai.....	18
4 lentelė. Penkios populiariausios kripto valiutos 2022 m. lapkričio 14 dienai pagal kapitalizaciją (CoinMarketCap duomenimis).....	20
5 lentelė. Autorių nuomonės apie kripto valiutų rinką.....	24
6 lentelė. Kripto valiutų rinkai palankios ir nepalankios šalys reguliavimo aspektu (susiskirstytos pagal žemynus).....	25
7 lentelė. Kripto valiutų rinkos veikimo principai, sudarantys sąlygas nusikalstamų veikų vykdymui.....	29
8 lentelė. BitcoinAbuse.com internetiniame tinklapyje tyrimo metu identifikuoti parametrai apie nusikalstamas veikas kripto valiutų rinkoje.....	41
9 lentelė. BlockChain.com internetiniame tinklapyje tyrimo metu identifikuoti duomenų parametrai apie kripto valiutų piniginių adresus.....	43
10 lentelė. Išsikeltos hipotezės.....	45
11 lentelė. Duomenų apie kripto valiutų piniginių adresus iš BitcoinAbuse.com ir Blockchain.com suvestinė.....	47
12 lentelė. Nusikalstamos veikos, identifikuotos tiriamuoju laikotarpiu BitcoinAbuse.com internetiniame tinklapyje.....	49
13 lentelė. Duomenys apie nusikalstamų veikų dažnumą ir jų pasiskirstymą kripto valiutų piniginių adresų atžvilgiu.....	52
14 lentelė. Duomenys apie nusikalstamų veikų dažnumą ir jų pasiskirstymą kripto valiutų piniginių adresų atžvilgiu.....	54
15 lentelė. Susisteminti duomenys apie kartus, kiek buvo pranešta apie tyrimo metu identifikuotas nusikalstamas veikas.....	56
16 lentelė. Kripto valiutų piniginių adresų skaičiaus ir kartų, kiek buvo pranešta apie nusikalstamas veikas statistiniai duomenys.....	60
17 lentelė. Kripto valiutų piniginių adresų TOP1 duomenų parametrai.....	61

18 lentelė. Laiko skirtumo tarp pirmo ir paskutinio pranešimo apie galimai vykdoma nusikalstama veiką, panaudojant kriptovaliutų piniginės adresus, procentinis pasiskirstymas.....	62
19 lentelė. Duomenų, susijusių su lėšomis, gautomis iš nusikalstamos veikos (BTC), apibendrinimas.....	67
20 lentelė. Duomenų, susijusių su išsiųstomis lėšomis iš kriptovaliutų piniginės (BTC) ir 2023 m. kovo 31 d. likutis kriptovaliutų piniginių adresuose (BTC), apibendrinimas.....	69

PAVEIKSLŲ SĄRAŠAS

1 paveikslas. Kriptovaliutų rinkoje vykstančių operacijų vizuali reprezentacija.....	11
2 paveikslas. Centralizuotos ir decentralizuotos sistemų veikimo principas.....	13
3 paveikslas. Bendra kriptovaliutų vertė (mlrd. JAV dol.), gauta panaudojant neteisėtus adresus, 2017-2021 m. duomenys.....	21
4 paveikslas. MiCA reglamente išskirtas kriptoturtas.....	26
5 paveikslas. Nusikalstamų veikų kriptovaliutų rinkoje, aptartų mokslinėje literatūroje, pasiskirstymas.....	31
6 paveikslas. Nusikalstamų veikų kriptovaliutų rinkoje pasiskirstymas pagal požymius.....	32
7 paveikslas. Tyrimo struktūra.....	44
8 paveikslas. Santykinis nusikalstamų veikų paminėtų ir nepaminėtų mokslinėje literatūroje palyginimas.....	48
9 paveikslas. Nusikalstamų veikų kriptovaliutų rinkoje išsidėstymas pagal kriptovaliutų piniginių adresus.....	51
10 paveikslas. Pateiktų pranešimų apie tyrimo metu identifikuotas kriptovaliutų piniginių adresus procentinės dalies išraiška.....	56
11 paveikslas. Kriptovaliutų piniginių adresų skaičiaus, kurie vykdė nusikalstamas veikas ir kartų, kiek buvo pranešta apie nusikalstamą veiką santykis.....	58
12 paveikslas. Kriptovaliutų piniginių adresų skaičiaus ir kartų, kiek buvo pranešta apie nusikalstamas veikas palyginimas.....	58
13 paveikslas. Operacijų skaičiaus kriptovaliutų piniginių adresuose pasikartojimų atvaizdavimas	65
14 paveikslas. Operacijų skaičiaus pagal nusikalstamas veikas kriptovaliutų piniginių adresuose procentinė išraiška.....	65

IVADAS

Darbo temos aktualumas. Inovacijos ir naujosios technologijos neabejotinai sparčiai keičia kasdieninio gyvenimo įpročius. Nepaisant to, jog dažniausia tokio tipo pasikeitimai vyksta technologiniame sektoriuje ir būtent šiam sektoriui turi reikšmingos įtakos, tačiau tokie pasikeitimai dažnai turi įtakos ir, be kita ko, finansiniam sektoriui. Kripto valiutų rinka šiai dienai tampa nebeatsiejama nuo kasdieninio asmenų gyvenimo, nepaisant to, ar tai susiję su bendromis kripto valiutų rinkos naujienomis ar tiesioginiu asmenų įsitraukimu į kripto valiutų rinką. Sparčiai plečiantis kripto valiutų rinkai pastarosios vartotojai (investuotojai) susiduria tiek su pozityvia šios rinkos puse (pavyzdžiui, sėkmingą investavimą), tiek galimai ir su negatyvia (pavyzdžiui, nukentėjimą nuo nusikalstamos veikos kripto valiutų rinkoje). Vis daugiau kripto valiutų rinkos vartotojų renkasi šią rinką tiek kasdieninėms investicijoms, tiek ir atsiskaitymams už prekes ir (ar) paslaugas. Tačiau atkreiptinas dėmesys, kad yra ir tokių kripto valiutų rinkos vartotojų, kurie kripto valiutų rinką mato kaip tinkamą rinką, siekiant vykdyti nusikalstamas veikas ir tokiu būdu įgyti kripto valiutų. Nusikalstamų veikų kripto valiutų rinkoje atsiradimui ir paplitimui turi įtakos pačios kripto valiutų rinkos, kaip tokios, funkcionavimas, nepilnai išvystytas kripto valiutų rinkos reglamentavimas bei taip pat ir bendra kripto valiutų rinkos vartotojų ribota patirtis ir patiklumas. Šios priežastys sudaro tam tikrą terpę į nusikalstamų veikų vykdymą linkusiems asmenims itin lengvai vykdyti nusikalstamas veikas, pasinaudojant kripto valiutų rinka. Tuo tarpu kripto valiutų rinkos vartotojams prarandant ne tik dideles sumas, tačiau ir pasitikėjimą kripto valiutų rinka.

Kripto valiutų rinka mokslinėje literatūroje paskutiniu metu yra vis dažniau analizuojama įvairiais aspektais. Pastebėtina, kad dažniausia kripto valiutų rinka yra nagrinėjama iš:

- teisinės (pvz., Ferreira, A., ir kt., 2021, Blandin, A., ir kt., 2019, Nabilou, H, ir kt., 2019);
- ekonominės (pvz., Fang, F., ir kt., 2022, Lambert, T., ir kt., 2022);
- informacinių technologijų (pvz., Chen, W., ir kt., 2021, Hu, H., ir kt., 2021, Jin, J., ir kt., 2022), perspektyvos.

Atitinkamai, mokslinėje literatūroje yra skiriamas dėmesys ir nusikalstamų veikų kripto valiutų rinkoje tyrimams (pvz., Bartoletti, M., ir kt., 2021, Boshmaf, Y., ir kt., 2020, Leuprecht, C., ir kt., 2022). Visgi, dažniausia tokie moksliniai darbai apsiriboja tik pakankamai siauru, kelių konkrečių nusikalstamų veikų kripto valiutų rinkoje aspektu (pvz., Chen, W., ir kt., 2021, Wronka, C., ir kt., 2022, Cong, L., ir kt., 2021, Faccia, A., ir kt., 2020). Mokslinės literatūros,

kuri nagrinėtų nusikalstamas veikas kriptovaliutų rinkoje platesne perspektyva, analizuojant įvairius su tuo susijusius parametrus, yra pakankamai negausu (pvz., Trozze1, A., ir kt., 2022, Kerr, S. D., ir kt., 2023).

Analizuojamos temos ištyrimo lygis. Mokslinė literatūra, kuri analizuoja nusikalstamas veikas kriptovaliutų rinkoje, nemažai dėmesio skiria tyrimams, susijusiems su nusikalstamų veikų šioje rinkoje identifikavimui. Pavyzdžiui, Trozze, A., ir kt., (2022), atliko tyrimą, kurio metu buvo analizuojamos kriptovaliutų rinkoje pasireiškiančios nusikalstamos veikos bei tyrimo metu nustatė, kad kriptovaliutų piniginių sukčiavimas, *Pump* ir *dump* schema, investavimo schemas (ICO, Ponzi schemas), kenkėjiškų programų kasimas ir kenkėjiškų programų sukčiavimas buvo vienos iš dažniausiai tyrimo metu pasireiškiančių nusikalstamų veikų kriptovaliutų rinkoje. Taip pat autoriai atlieka tyrimus, kurių metu, pasitelkiant tam tikras platformas, yra analizuojama kaip konkrečiai nusikalstamos veikos yra vykdomos prieš šios rinkos vartotojus (investuotojus). Autoriai Morgia, L. M., ir kt., (2021), naudojant stebėjimo ir mašininio mokymosi metodus, trejus metus stebėjo grupes, kurios *Telegram* ir *Discord* socialiniuose tinkluose organizuoja *Pump* ir *dump* schemas bei nustatė iš viso 900 šios nusikalstamos veikos atvejų. Taip pat Dhawan, A., ir kt., (2021), atliko tyrimą, kurio metu, panaudodami duomenų rinkimo ir analizės metodus, dviejuose kriptovaliutų keityklose – Binance ir Yobit, per 6 mėn. laikotarpį identifikavo 355 *Pump* ir *dump* schemas atvejų. Galiausia, autoriai, atlikdami tyrimus, orientuojasi į investuotojų patirtą nuostolį, pastariesiems susidūrus su nusikalstamomis veikomis kriptovaliutų rinkoje. Autoriai Xia, P., ir kt.,(2020b), atliko tyrimą, kurio metu, panaudojant spausdinimo klaidų metodą, buvo siekiama nustatyti nusikalstamas veikas, vykdomas pasitelkiant kriptovaliutų keityklas. Tyrimo metu nustatyta, kad per tyrimo laikotarpį dėl netikrų kriptovaliutų keityklos nusikalstamų veikų investuotojai patyrė mažiausia 520 000 JAV dolerių nuostolių. Taip pat Hong, G., ir kt., (2018), atliko tyrimą, kurio metu, panaudojant CMTracker buvo atpažintos 2 770 interneto svetainių, kuriose buvo vykdoma neteisėta kriptovaliutų gavyba bei nustatyta, kad šią nusikalstamą veiką vykde asmenys 2018 m. per dieną neteisėtai įgydavo bent 59 000 JAV dolerių.

Darbo naujumas. Šio darbo naujumas pasižymi tuo, jog šiame darbe yra atliekama mokslinė analizė, kurios metu, be kita ko, yra identifikuojamos, detalios aprašomos, sugrupuojamos kriptovaliutų rinkoje pasireiškiančios nusikalstamos veikos. Šiai dienai mokslinių darbų, kurie atliktų detalesnę nusikalstamų veikų kriptovaliutų rinkoje ir įtaką šios rinkos vartotojams analizę yra pakankamai nedaug. Taip pat šiame darbe yra atliekamas tyrimas, kurio

metu yra identifikuojamos ir vertinamos ne tik pačios nusikalstamos veikos kriptovaliutų rinkoje, bet ir su šiomis veikomis susiję kiti parametrai. Tuo tarpu šiai dienai esantys moksliniai darbai dažnai pakankamai siauru požiūriu atlieka tyrimus, susijusius su nusikalstamomis veikomis kriptovaliutų rinkoje, bei retai skiria dėmesį realių skaičių analizei.

Darbo problema. Kriptovaliutų rinka yra neatsiejamai susijusi su finansais, t. y., nepaisant to, jog kriptovaliuta yra virtuali valiuta, kuria galima naudotis, panaudojant informacines technologijas, visgi ji turi finansinę išraišką. Kaip ir kiekvienas objektas, turintis finansinę išraišką, taip ir kriptovaliutų rinka, yra neatsiejamai susijusi su nusikalstamomis veikomis, kadangi objektai, turintys finansinę reikšmę, dažnai yra siejami būti įgytais asmenų, kurie yra linę neteisėtai praturtėti. Todėl šiuo atveju galima darbo problemą formuoti klausimu – ar kriptovaliutų rinkoje yra paplitusios nusikalstamos veikos, kurių metu potencialiai į nusikalstamų veikų vykdymą linę asmenys, siekia neteisėtai įgyti kriptovaliutų?

Darbo tikslas. Atlikti nusikalstamų veikų kriptovaliutų rinkoje tyrimą.

Darbo uždaviniai.

1. Atlikti mokslinės literatūros analizę nusikalstamų veikų kriptovaliutų rinkoje aspektu.
2. Sudaryti nusikalstamų veikų kriptovaliutų rinkoje tyrimo metodologiją.
3. Atlikti nusikalstamų veikų kriptovaliutų rinkoje tyrimą, išanalizuojant tyrimo metu nustatytas charakteristikas nusikalstamų veikų kriptovaliutų rinkoje aspektu ir pateikti gautus tyrimo rezultatus.

Darbo metodai. Šiame darbe naudojami duomenų rinkimo, aprašomosios statistikos, Pearson koreliacinės, paprastosios regresijos, Chi-kvadrato, statistinių duomenų analizės, tyrimo rezultatų analizės, apibendrinimo ir vertinimo metodai.

Darbo struktūra. Šį darbą sudaro įvadas, dėstomoji dalis, išvados, literatūros sąrašas, santrauka ir priedai. Dėstomąją dalį sudaro trys skyriai. Pirmasis skyrius – nusikalstamų veikų kriptovaliutų rinkoje literatūros analizė. Šiame skyriuje analizuojama mokslinė literatūra, susijusi su kriptovaliutų samprata, veikimo principu, reglamentavimo problematika ir kriptovaliutų rinka kaip nusikalstamų veikų objektu. Antrasis skyrius yra nusikalstamų veikų kriptovaliutų rinkoje tyrimo metodologija, kuriame aptariama su atliekamu tyrimu susijusi metodologija. Trečiasis skyrius pateikia tyrimo metu gautų rezultatų apibendrinimą.

1. NUSIKALSTAMŲ VEIKŲ KRIPTOVALIUTŲ RINKOJE LITERATŪROS ANALIZĖ

1.1. Kripto valiutos samprata ir savybės

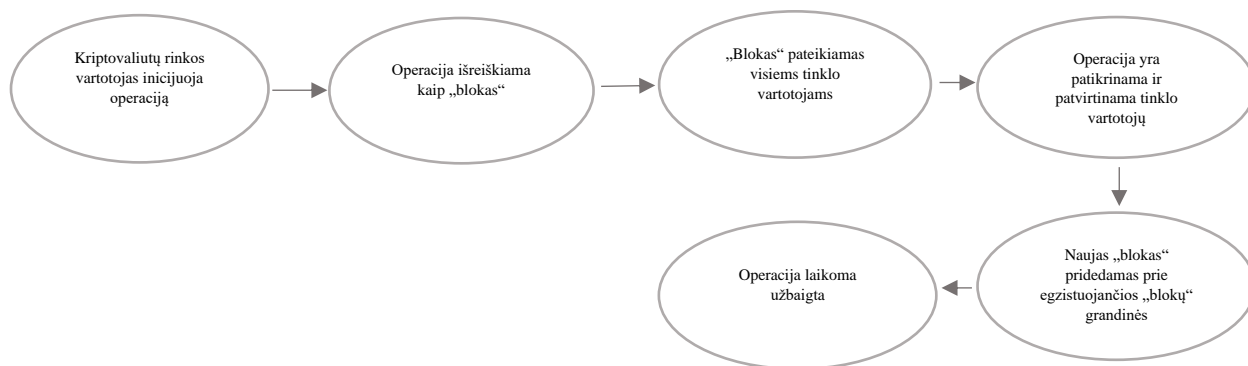
Kripto valiuta yra laikoma skaitmenine mainų priemone (skaitmeninė arba virtuali valiuta), kuri yra sukurta, įsigyjama, laikoma ir ja prekiaujama elektroniniu būdu (Hruska, B. S., ir kt., 2018, Fang, F., ir kt., 2022). 2008 metais asmuo ar asmenų grupė, pasivadinęs (-usi) slapyvardžiu Satoshi Nakamoto, išleido baltąją knygą (angl. *white-paper*), kurioje apibūdino kriptovaliutą, kaip: „Gryna lygiavertė elektroninių grynųjų pinigų versija, kurią galima naudoti perlaidoms iš vienos šalies, kitai šaliai be trečiųjų asmenų įsikišimo“, t. y. be finansų įstaigų. Pagrindinis kriptovaliutų tikslas buvo decentralizuoti elektroninius mokėjimus ir tokiu būdu palengvinti (paspartinti) operacijų įvykdymo procesą (Solat, S., ir kt., 2016, Chaim, P., 2019).

Kriptovaliutų veikimui, kitaip nei dekretiniams pinigams (angl. *fiat money*), yra būdingas tam tikras specifiškumas, kuris yra neatsiejamai susijęs su šiuolaikinėmis technologijomis. Iš esmės be šiuolaikinių technologijų kriptovaliutų rinkai atsirasti ir apskritai funkcionuoti būtų neįmanoma (Rehman ur, H. M., ir kt., 2020). Tokia išvada daroma atsižvelgiant į tai, koku būdu kriptovaliutų rinka funkcionuoja. Pirmiausia, svarbu atkreipti dėmesį, kaip apskritai gali būti įgyjamos kriptovaliutos. Analizuojant mokslinę literatūrą pastebėtina, jog kriptovaliutas galima įgyti dviem skirtingais būdais. Vienas būdas yra kriptovaliutų kasimas (angl. *mining*), kurio metu yra sprendžiami matematiniai algoritmai ir tokiu būdu, išsprendus matematinius algoritmus, yra (iš)gaunamos kriptovaliutos. Kitas būdas yra kriptovaliutų įsigijimas per platformas, kuriose yra prekiaujama kriptovaliutomis (Möser, M., ir kt., 2013, Varlioglu, S., ir kt., 2020). Antra, yra svarbu suprasti, koku būdu galima vykdyti operacijas kriptovaliutų rinkoje. Operacijų veikimo principą kriptovaliutų rinkoje galima apibūdinti sekančiais: kriptovaliuta atlikus finansinę operaciją, ši operacija yra įrašoma į, taip vadinamą, „bloką grandinę“ (angl. *BlockChain*). Bloką grandinės technologija yra laikoma (suvokiama) kaip tam tikra duomenų bazė, kurioje kompiuterių tinklo pagalba yra užfiksuojamos operacijos. Kiekviena bloką grandinė yra užkoduota ir suskirstyta į mažesnes duomenų grupes, kurios yra vadinamos blokais (angl. *Block*) (Möser, M., ir kt., 2013, Wolfgang, K., H, ir kt., 2019, Andonia, M., ir kt., 2019, Kerr, S. D., ir kt., 2023). Šiuose blokuose

yra kaupiama informacija apie tam tikrą operacijų skaičių, nuorodos į ankstesnius grandinės blokus bei pateikiamas atsakymas į išspręstą matematinį algoritmą, kuris yra panaudojamas patvirtinant duomenis, susijusius su konkrečiu bloku. Kiekvienas tinkle esantis technologinis įrenginys saugo blokų grandinės kopiją (Oh, J., ir kt., 2017, Wolfgang, K., H, ir kt., 2019, Andonia, M., ir kt., 2019). Atkreiptinas dėmesys, kad technologinių įrenginių tinklas yra viešas bei visiems prieinamas (Towler, M. B., 2020). Nepaisant to, jog viešumas yra egzistuojantis, visgi atpažinti grandinėje esamus duomenis yra pakankamai sunku. Kiekvienas blokas yra kriptografiškai užkoduotas. Užkodavimas yra atliekamas tokiu principu, kad nebūtų rodoma informacija apie atliktą operaciją. Taigi, šiuo atveju yra tik pateikiami operacijos šalių adresai, kurie yra sukuriami kriptovaliutų rinkos vartotojo pinigineje (angl. *e-wallet*) (Andonia, M., ir kt., 2019, Teichmann, F. M. J., ir kt., 2021, Hoffmann, H. C., 2021). Kiekviena atlikta operacija turi būti patikrinama tinkle esančių vartotojų. Tokiu būdu yra patvirtinamas operacijos galiojimas. Po patikrinimo ir patvirtinimo operacija yra išsaugoma bloke, kuris turi specialų tam blokui kodą (angl. *Hash*) (Wolfgang, K., H, ir kt., 2019, George, P. H., ir kt., 2019, Andonia, M., ir kt., 2019, Xia, P., ir kt., 2021). Šis specialus kodas yra nuoroda į prieš tai buvusį bloką. Taigi, tokiu principu yra sujungiamas kiekvienas blokas ir taip yra sukuriama blokų grandinė (1 paveikslas). Atkreiptinas dėmesys, kad po to, kai blokas yra pridodamas prie grandinės, šio bloko nebegalima ištrinti (Hooper, A., ir kt., 2020).

1 paveikslas

Kriptovaliutų rinkoje vykstančių operacijų vizuali reprezentacija



Šaltinis: Sudaryta autorės, remiantis Möser, M., ir kt., 2013, Oh, J., ir kt., 2017, Wolfgang, K., H, ir kt., 2019, George, P. H., ir kt., 2019, Towler, M. B., 2020, Xia, P., ir kt., 2021, Teichmann, F. M. J., ir kt., 2021, Hoffmann, H. C., 2021.

Trečia, kriptovaliutų rinkai yra būdinga kriptovaliutų piniginė. Kriptovaliutų piniginė yra programinė įranga, kuri saugo viešuosius ir privačius paskyros raktus ir gali sąveikauti su bloku grandine tam, kad būtų galima valdyti paskyrą. Kriptovaliutų piniginės gali būti saugomos technologiniame įrenginyje arba piniginės programinėje įrangoje, kuria galima išsaugoti kompiuteryje arba kriptovaliutų biržoje. Šios piniginės leidžia lengvai perkelti kriptovaliutas iš vienos sąskaitos į kitą (Teichmann, F. M. J., ir kt., 2021, Hoffmann, H. C., 2021). Galiausia, paminėtina tai, jog kriptovaliutų rinkai yra būdinga kriptovaliutų keitykla, kuri suteikia galimybę keisti kriptovaliutas vieną į kitą arba į dekretinius pinigus (De-Vries, P. D., 2016). Taigi, iš aukščiau aptartų kriptovaliutų rinkos veikimo principų matyti, kad kriptovaliutų rinkai yra būdinga tam tikra, specifinė, veikimo sistema, kuri skiriasi nuo visiems įprastos ir kasdieniniame gyvenime naudojamos dekretinių pinigų veikimo sistemos.

Analizuojant kriptovaliutų rinkos veikimo sistemos principus, galima išskirti ir plačiau aptarti pagrindinius kriptovaliutų rinkai būdingus sistemos bruožus:

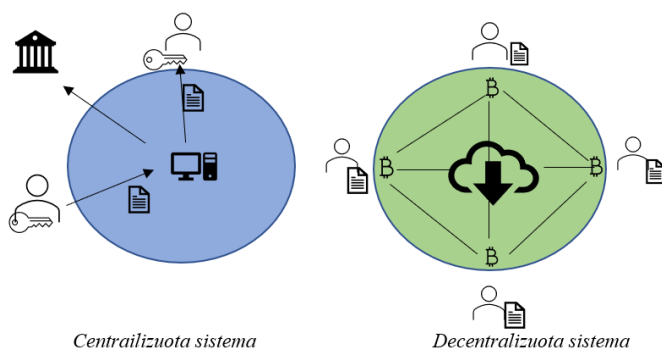
- kriptovaliutų kasyba (Teichmann, F. M. J., ir kt., 2021);
- kriptovaliutų mainai (Mattke, J., ir kt., 2020, Khan, R., ir kt., 2022);
- kriptovaliutų priėmimas (Mattke, J., ir kt., 2020).

Pirmasis kriptovaliutų rinkos sistemos bruožas yra kriptovaliutų kasyba. Kriptovaliutų kasyba yra procesas, kurio metu asmenys, būdami tinklo nariais, generuoja kriptovaliutas, panaudojant savo kompiuterio apdorojimo galią sudėtingam matematiniam algoritmui išspręsti (Teichmann, F. M. J., ir kt., 2021). Matematinio algoritmo užbaigimas sukuria eilutės kodą, kuris registruoja kiekvieną operaciją. Tokiu būdu yra užtikrinama, kad kriptovaliuta nebūtų išleista du kartus ir kad būtų užkirstas kelias operacijos atšaukimui (De-Vries, P. D., 2016, Sotiropoulou, A., ir kt., 2017). Paminėtina ir tai, jog sudėtingo matematinio algoritmo išsprendimas (angl. *Proof of Work*) prisideda ir prie saugumo užtikrinimo. Kaip jau buvo minėta, kriptovaliutų rinka veikia be trečiųjų asmenų įsikišimo. Kriptovaliutų rinkai būnant decentralizuotai yra svarbu užtikrinti pastarosios saugumą. Taigi, sudėtingo matematinio algoritmo išsprendimas, reikalaujantis didelės ir brangios skaičiavimo galios, sukuria tam tikrą pasitikėjimą kasyba, kadangi neteisėtus veiksmus norintys atlikti asmenys greičiausiai nesistengs išspręsti sudėtingo matematinio algoritmo, nes tai jiems bus pakankamai nuostolingas veikimas (Hruska, B. S., ir kt., 2018, Teichmann, F. M. J., ir kt., 2021). Antrasis kriptovaliutų rinkos sistemos veikimo bruožas yra kriptovaliutų mainai. Kriptovaliutų rinka nėra paremta nei auksu, nei kita preke, kuri išreikštų tam tikrą kriptovaliutų

rinkos perkamąją galią. Kriptovaliutų vertė priklauso nuo to, kokią vertę kriptovaliutoms priskirs vartotojai, t. y., veikiama paklausos ir pasiūlos principu (Wolfgang, K., H, ir kt., 2019, Fang, F., ir kt., 2022). Kriptovaliutas pirkti ir parduoti galima kriptovaliutų biržoje (angl. *Cryptocurrency Exchange*). Kriptovaliutų mainai dažniausia būna dviejų rūšių: (a) centralizuoti; (b) decentralizuoti (2 paveikslas). Centralizuotų kriptovaliutų mainų atveju viskas vyksta kriptovaliutų biržoje. Centralizuota kriptovaliutų birža yra skaitmeninių prekių pirkimo ir (ar) pardavimo vieta. Tokiu atveju yra pasikliaujama trečiaja šalimi, kuri prižiūri operaciją bei apsaugo pirkėją ir pardavėją (pavyzdžiui, *Binance, Coinbase*). Tokio tipo operacijos nėra registruojamos blokų grandinėje, todėl yra privaloma pateikti savo asmeninę informaciją autentifikavimo tikslais. Decentralizuotų kriptovaliutų mainų atveju viskas vyksta taip pat kriptovaliutų biržoje. Decentralizuota kriptovaliutų birža yra kiek panaši į centralizuotą, tačiau šiuo atveju nėra trečiosios šalies. Tai yra visiškai decentralizuotos platformos, palaikančios tarpusavio prekybą (angl. *Peer-to-peer*) naudodamos turta, tarpinius žetonus ir sąlyginio deponavimo sistemą (Hruska, B. S., ir kt., 2018, Puthal, D., ir kt., 2018, Xia, P., ir kt., 2021, Khan, R., ir kt., 2022, Kerr, S. D., ir kt., 2023). Paskutinis kriptovaliutų rinkos sistemos bruožas yra kriptovaliutų priėmimas. Šis veikimo sistemos bruožas yra svarbus tuo, jog tam, kad kriptovaliutos galėtų cirkuliuoti rinkoje, atlikdamos atsiskaitymo priemonės funkcijas yra privaloma, kad kriptovaliutos būtų priimamos ne tik vartotojų, bet ir prekybininkų. Tai reiškia, kad prekybininkai turi priimti kriptovaliutą kaip atsiskaitymo priemonę. (Mattke, J., ir kt., 2020). Šiai dienai matyti, kad daugėja prekybininkų, kurie sudaro sąlygas, įsigyjant prekę ir (ar) paslaugą už ją susimokėti (atsiskaityti), be kita ko, kriptovaliutomis (pvz., Microsoft, Tesla).

2 paveikslas

Centralizuotos ir decentralizuotos sistemų veikimo principas



Šaltinis: Sudaryta autorės, remiantis Hruska, B. S., ir kt., 2018, Puthal, D., ir kt., 2018, Xia, P., ir kt., 2021, Khan, R., ir kt., 2022, Kerr, S. D., ir kt., 2023.

Aptarus kriptovaliutų rinkos veikimo principus bei sistemos bruožus yra svarbu atkreipti dėmesį, jog kriptovaliutų rinka yra pakankamai skirtinga. Tai reiškia, kad kriptovaliutų rinkoje egzistuoja skirtingos kriptovaliutos, kurios veikia (funkcionuoja) skirtingu principu. Mokslinėje literatūroje yra išskiriamos septynios skirtingos kriptovaliutų klasės (1 lentelė) (Wolfgang, K., H, ir kt., 2019, Grobysa, K., ir kt., 2021, Lambert, T., ir kt., 2022, Son, J., ir kt., 2022).

1 lentelė

Kriptovaliutų klasės

Pavadinimas	Angliškas pavadinimas	Trumpas aprašymas	Kriptovaliutos pavyzdys
Transakcijos mechanizmas	<i>A transaction mechanism</i>	Kriptovaliutos platforma, skirta būti naudojama pavedimams atlikti.	Bitcoin
Paskirstytas skaičiavimų žetonas	<i>Distributed computation token</i>	Kriptovaliutos platformoje yra sudaroma galimybė paleisti nedideles programas.	Ethereum
Naudingumo žetonas	<i>Utility token</i>	Turtas blokų grandinėje, kuris gali būti programuojamas.	Golem
Vertybinių popierių žetonas	<i>Security token</i>	Tai yra investicijų produktas, kaip, pavyzdžiui, akcijos, obligacijos.	Sia Funds
Pakeičiamas žetonas	<i>Fungible tokens</i>	Tai yra tokie žetonai, kurie gali būti pakeičiami į kitą tokio pačio tipo žetoną.	ERC-20
Nepakeičiamas žetonas	<i>Non-fungible token</i>	Tai yra tokie žetonai, kurie negali būti pakeičiami į kitą tokio pačio tipo žetoną.	Decentraland (LAND)
Pastovios kriptovaliutos	<i>Stablecoins</i>	Kriptovaliutos yra susietos su valiutomis, kurių vertę užtikrina ją išleidusi vyriausybė.	Tether

Šaltinis: Sudaryta autorės, remiantis Wolfgang, K., H, ir kt., 2019, Grobysa, K., ir kt., 2021, Lambert, T., ir kt., 2022, Son, J., ir kt., 2022.

Analizuojant mokslinę literatūrą taip pat pastebėtina, kad kriptovaliutų rinką nuo tradicinių – dekretinių – valiutų rinkos skiria bent jau keturios pagrindinės kriptovaliutų rinkoms būdingos savybės (2 lentelė). Pirmiausia, kitaip nei dekretinių valiutų rinkoje, kriptovaliutų rinkoje vykdomos operacijos yra decentralizuotos (Fleder, M., ir kt., 2015, Brenig, Ch., ir kt., 2015, Puthal, D., ir kt., 2018, Hruska, B. S., ir kt., 2018, Campbell-Verduyn, M., 2018, Nabilou, H., ir kt., 2019, Wronka, C., 2021). Tai reiškia, jog operacijos kriptovaliutų rinkoje yra vykdomos lygiavertiškai (angl. *peer-to-peer*), t. y., be finansinių tarpininkų įsikišimo, o būtent ši savybė yra būdinga dekretinių valiutų rinkai (Puthal, D., ir kt., 2018, Felix, T. H., ir kt., 2019, Aalborg A. H., ir kt.,

2019). Antra, kriptovaliutų operacijos pasižymi anonimiškumu (Brühl, V., 2017, Marella, V., ir kt., 2020, Bartoletti, M., ir kt., 2021, Leuprecht, C., ir kt., 2022). Nepaisant to, kad mokslinėje literatūroje pasitaiko nuomonių, jog anonimiškumas nėra absoliutus, kadangi, operacijai būnant atliekamai blokų grandinėje, operacijos yra įrašomos į viešuosius sąrašus, kurie yra viešai prieinami, bei tai, jog kriptovaliutos neužtikrina tokio anonimiškumo kaip gryniesi pinigai, tačiau anonimiškumas yra laikomas viena iš pagrindinių kriptovaliutų savybių (Reid, F., *et al*, 2011, Marella, V., ir kt., 2020, Bartoletti, M., ir kt., 2018, Fang, F., ir kt., 2022). Tuo tarpu dekretinių valiutų rinkoje anonimiškumas yra negalimas – tiek atliekant operaciją, tiek atidarant sąskaitas ar suteikiant kitokio pobūdžio finansines paslaugas įstatymai numato įpareigojimą nustatyti asmens tapatybę. Trečia, kriptovaliutoms yra būdingas skaidrumas. Skaidrumas pasireiškia tuo, jog visos įvykusios operacijos yra įrašomos į viešai prieinamą blokų grandinę, t. y. operacijos yra registruojamos (Marella, V., ir kt., 2020). Tuo tarpu dekretinių valiutų rinkoje tokio tipo viešumo nėra, t. y. apie operaciją žino tik konkrečioje operacijoje dalyvaujančios šalys. Galiausiai, vertinant kriptovaliutų ir dekretinių pinigų rinkų skirtumus galima pastebėti, kad, be kita ko, kriptovaliuta nuo dekretinių pinigų skiria ir viena vartotojui ypač patraukli savybė, o būtent tai, kaip greitai galima įgyti kriptovaliutas ir jas panaudoti. Kriptovaliutų rinkoje įgyti kriptovaliutas ir jas panaudoti galima sąlyginai greitai, kadangi šioje rinkoje nedalyvauja trečioji šalis – finansų įstaiga, kuri turi tvirtinti operacijas, nustatyti asmenų tapatybes ir atlikti kitus privalomus veiksmus (Campbell-Verduyn, M., 2018 De-Vries, P. D., 2016, Dupuis, D., ir kt., 2021). Taigi, iš aptartų kriptovaliutų rinkos skirtumų nuo tradicinių – dekretinių – valiutų rinkos, matyti, kad kriptovaliutų rinka, kaip nei tradicinių – dekretinių – valiutų rinka, funkcionuoja atskirtai nuo finansų įstaigų, savaip užtikrinant kriptovaliutų rinkos saugumą bei nereikalaujant nustatyti asmens tapatybės, kas turi įtakos operacijų (į)vykdymo spartumui. Atitinkamai iš šios rinkos vartotojų perspektyvos, tokiu būdu kriptovaliutų rinka suteikia galimybę dalyvauti operacijose be tradicinių finansų įstaigų sukeltamų apsunkinimų ir taikomų apribojimų.

2 lentelė

Kripto valiutų rinkos ir dekretinių pinigų rinkos skirtumai

Kripto valiutų rinka	Dekretinių pinigų rinka	Autoriai
Decentralizuota rinka	Centralizuota rinka	Fleder, M., ir kt., 2015, Brenig, Ch., ir kt., 2015, Puthal, D., ir kt., 2018, Hruska, B. S., ir kt., 2018, Campbell-Verduyn, M., 2018, Nabilou, H., ir kt., 2019, Felix, T. H., ir kt., 2019, Aalborg A. H., ir kt., 2019, Wronka, C., 2021).
Būdingas anonimiškumas	Anonimiškumas nėra būdingas, kadangi sandorio šalys turi būti identifikuotos	Brühl, V., 2017, Bartoletti, M., ir kt., 2018, Marella, V., ir kt., 2020, Bartoletti, M., ir kt., 2021, Leuprecht, C., ir kt., 2022, Reid, F., <i>et al</i> , 2011, Marella, V., ir kt., 2020, Fang, F., ir kt., 2022.
Būdingas operacijų skaidrumas	Operacijų skaidrumas nėra būdingas	Marella, V., ir kt., 2020.
Greitesnė operacijos įvykdymo trukmė, kadangi operacijos nėra tvirtinami finansų įstaigos.	Operacija vykdomas ilgesnį laikotarpį, kadangi operacijos tvirtinami finansų įstaigos.	Campbell-Verduyn, M., 2018 De-Vries, P. D., 2016, Dupuis, D., ir kt., 2021.

Šaltinis: Sudaryta autorės, remiantis lentelėje nurodyta mokslinė literatūra.

Išanalizuoti kripto valiutų rinkos skirtumai nuo dekretinių pinigų rinkos bei pačios kripto valiutų rinkos savybės nesunkiai leidžia identifikuoti kripto valiutų rinkos pagrindinius trūkumus. Pirmiausia, kripto valiutų rinka nėra paremta institucijų priežiūra ir (ar) išsamiu teisės aktų reglamentavimu. Šis trūkumas turi įtakos tuo aspektu, jog tokiu būdu kripto valiutų rinka yra laikoma nepastovia ir rizikinga investicija, taip pat laikoma itin pažeidžiama rinka nusikalstamų veikų vykdymo atžvilgiu (Sharma, P. S., ir kt., 2018). Antra, jau anksčiau minėtas anonimiškumas iš dalies yra priskiriamas prie kripto valiutų rinkos trūkumu. Aplinkybė, kad vartotojas yra identifikuojamas ne pagal vardą ir pavardę, o pagal viešojo rakto adresą (32 bitų eilutę su simbolių ir skaičių deriniu), atveria kelią nusikalstamų veikų vykdymui (Reid, F., *et al*, 2011, Marella, V., ir kt., 2020, Bartoletti, M., ir kt., 2021, Fang, F., ir kt., 2022). Galiausiai, kripto valiutų vertė yra

nuolatos ir pakankamai drastiškai kintanti, o tai neabejotinai turi įtakos vartotojų elgesiui kriptovaliutų rinkos atžvilgiu (Marella, V., ir kt., 2020).

Analizuojant kriptovaliutų rinką taip pat yra pravartu palyginti kriptovaliutų rinką su padengtųjų pinigų (aukso standarto) rinka (3 lentelė). Analizuojant šių dviejų rinkų panašumus, pirmiausia, galima pabandyti palyginti kriptovaliutų ir aukso gavybą. Tiek kriptovaliutų, tiek aukso gavyba yra sąlyginai brangi. Aukso gavyboje yra investuojama į darbą ir įrangą, siekiant išgauti auksą. Tuo tarpu kriptovaliutų rinkoje yra investuojama į kompiuterių galią, siekiant išspręsti matematinius algoritmus, tokiu būdu (iš)gaunant kriptovaliutas. Išgavus auksą – aukso gavėjui yra atlyginama. Panašiai veikiama ir kriptovaliutų rinkoje, t. y., kriptovaliutos kasėjui yra atlyginta išsprendus matematinį algoritmą ir tokiu būdu (iš)gavus kriptovaliutą (Wolfgang, K., H, ir kt., 2019). Antra, tiek auksas, tiek tam tikros kriptovaliutos turi tam tikrą vidinę vertę. Didžiąją savo vertę kriptovaliutos ir auksas įgyja todėl, jog tiek tam tikrų kriptovaliutų kiekis, tiek aukso kiekis yra ribotas. Galiausiai, aukso ir kriptovaliutų panašumas yra toks, kad nei kriptovaliutos, nei auksas nėra kontroliuojamos valstybinių institucijų. Taigi, matyti, kad kriptovaliutų rinka ir padengtųjų pinigų (aukso standarto) rinka turi bendrų požymių, kurie leidžia tam tikru aspektu palyginti šias rinkas. Tačiau, nepaisant bendrų požymių egzistavimo, visgi, šie panašumai nepaneigia, kad tarp kriptovaliutų rinkos ir padengtųjų pinigų (aukso standarto) rinkos egzistuoja ir tam tikri skirtumai. Auksas yra plačiai naudojamas dėl savo vertės išsaugojimo, todėl jis yra naudingas siekiant apsidrausti, ypač ekonomiškai nepalankiu metu. Tuo tarpu vienareikšmiškai konstatuoti, kad kriptovaliutos turi tokį bruožą, šiai dienai negalime (Conlon, T., ir kt., 2020, Choi, S., ir kt., 2022). Taip pat auksas gali būti naudojamas įvairiems produktams (pavyzdžiui, papuošalams) ir išlaiko savo prekinę vertę, tuo tarpu kriptovaliutos jokios kitokio tipo naudos neturi, išskyrus savo vaidmenį kriptovaliutų rinkoje (Beer, C., ir kt., 2015, Dyhrberg, H. A., 2016). Taigi, nepaisant to, jog padengtųjų pinigų (aukso standarto) ir kriptovaliutų rinkų skirtumų yra kur kas mažiau nei panašumų, tačiau įvardinti skirtumai gali būti laikomi itin svarbiais, vartotojui priimant sprendimą dėl naudojimosi (investavimo) į kriptovaliutų rinką.

3 lentelė

Kripto valiutų rinkos ir padengtųjų pinigų (aukso standarto) rinkos panašumai ir skirtumai

Kripto valiutų rinka	Padengtųjų pinigų (aukso standarto) rinka
<i>Panašumai</i>	
Tiek kripto valiutų, padengtųjų pinigų (aukso) gavyba yra brangi.	
Asmeniui, išgavusiam kripto valiutas ir padengtus pinigus (auksą) yra atlyginama.	
Kripto valiutos ir padengtieji pinigai (auksas) turi vidinę vertę (ypač dėl to, kad yra ribotas limitas).	
Priskiriami decentralizuotai rinkai.	
<i>Skirtumai</i>	
Nėra vienareikšmiškai nustatyta, ar kripto valiutos išsaugo savo vertę, ekonomiškai nepalankiu metu.	Padengtieji pinigai (auksas) išsaugo savo vertę ekonomiškai nepalankiu metu.
Kripto valiutos neturi jokios kitos panaudojimo paskirties.	Auksas gali būti panaudojamas produktų gamybai.

Šaltinis: Sudaryta autorės, remiantis Beer, C., ir kt., 2015, Dyhrberg, H. A., 2016, Wolfgang, K., H., ir kt., 2019, Conlon, T., ir kt., 2020, Choi, S., ir kt., 2022.

Apibendrintai galima daryti išvadą, kad kripto valiutų rinka šiai dienai vis dar yra laikoma sąlyginai nauja rinka, turinti savo atskirus veikimo sistemos principus ir būdingus sistemos bruožus. Kripto valiutų rinkai būdingos savybės nebejotinai daro šią rinką itin patrauklia vartotojams (investuotojams). Nenuginčijami kripto valiutų rinkos skirtumai nuo dekretinių pinigų ir padengtųjų pinigų (aukso standarto) leidžia daryti išvadą, kad kripto valiutų rinka yra neabejotinai inovatyvi perspektyva ateities mokėjimų sistemai. Visgi, nepaisant kripto valiutų rinkos patrauklių savybių bei inovatyvaus veikimo principo, nereikėtų ignoruoti ir tų aplinkybių, dėl kurių kripto valiutų rinka gali sukelti potencialių rizikų tiek pavieniams vartotojams (investuotojams), tiek visuomeninei gerovei.

1.2. Kriptovaliutų rinkos reglamentavimo problematika

Kriptovaliutų rinka yra besiformuojanti rinka, kuri, manoma, ateityje turės daug naudos finansų sektoriui, įskaitant sąnaudų mažinimą, efektyvumo padidėjimą ir finansinių paslaugų kokybės bei skaidrumo gerinimą (Cumming, J. D., ir kt., 2019). Šiai dienai kriptovaliutų rinka yra ne tik investavimo rinka, tačiau kriptovaliutomis jau galima naudotis kaip mokėjimo priemone atsiskaitant už daugelį prekių ir (ar) paslaugų. Kriptovaliutos, kurios yra vadinamos stabiliomis monetoms (angl. *StableCoin*), yra netgi susietos su dekretinėmis valiutomis, pavyzdžiui, kriptovaliuta Tether yra susieta su JAV doleriu (Oordt van R. C. M, 2022). Daugybė skirtingų kriptovaliutų tipų ir galimų kriptovaliutų panaudojimo būdų gali suteikti daug vertės ekonomikoje ir formuoti skaitmeninės, žetonais pagrįstos, ekonomikos ateitį (Bons, W. H R., ir kt., 2020) (4 lentelė). Tačiau, nepaisant to, jog kriptovaliutų rinka šiai dienai jau yra veikianti bei pritraukianti didelį vartotojų skaičių, tačiau kriptovaliutų rinka iki šios dienos nėra aiškiai reglamentuojama (Kamps, J., ir kt., 2018).

Kriptovaliutų rinka patraukė reguliatorių dėmesį dėl savo sparčiai augančios vertės bei plataus paplitimo tarp vartotojų (4 lentelė) (Oh, J., ir kt., 2017, Bartoletti, M., ir kt., 2021). Šiame kontekste paminėtinas Roppelt, J. C., (2019), tyrimas, kurio metu, be kita ko, panaudojant kiekybinį tyrimo metodą – anketines apklausas, 81 respondento buvo paklausta, ar jie šiuo metu turi, praityje turėjo ar ateityje žada turėti (įsigyti) kriptovaliutų (t. y. įsitraukti į kriptovaliutų rinką). Iš apklaustųjų net 40 respondentų atsakė, kad anketos pildymo metu turėjo kriptovaliutų, 27 nurodė, kad ateityje žada įsigyti kriptovaliutų, o 14 nurodė, kad anksčiau yra turėję, tačiau anketos pildymo metu kriptovaliutų neturi. Taigi, kaip matyti iš atlikto tyrimo rezultatų, susidomėjimas kriptovaliutų rinka iš tiesų yra pakankamai nemažas tiek vertinant vartotojų norą šiai dienai būti įsitraukusiems į kriptovaliutų rinką, tiek vertinant ateities perspektyvas. Šiuo aspektu paminėtinas taip pat ir Adewole, K., ir kt., (2020), tyrimas, kurio metu, panaudojant anketinių apklausų metodą, buvo apklausti 100 įvairių specialybių respondentų iš kurių 58% į klausimą, ar jie nori naudotis kriptovaliutų rinka (neapsiribojant, ar jau naudojasi kriptovaliutų rinka, ar dar tik ketina naudotis) atsakė, jog nori naudotis kriptovaliutų rinka, tiek tyrimo metu, tiek ateityje. Šio tyrimo rezultatai leidžia teigti, kad vartotojai pakankamai palankiai vertina kriptovaliutų rinką.

4 lentelė

Penkios populiariausios kriptovaliutos 2022 m. lapkričio 14 dienai pagal kapitalizaciją (CoinMarketCap duomenimis)

Kriptovaliuta	Kaina, JAV doleriai	Kriptovaliutos kiekis apyvartoje	Parduotas kiekis per 24 val., JAV doleriai
Bitcoin (BTC)	16 321,65	19 207 393	49 188 146 212
Ethereum (ETH)	1 217,32	122 373 866	14 931 262 734
Thether (USDT)	0,9989	66 382 365 892	65 645 818 341
USB Coin (USDC)	1,00	44 073 437 004	3 933 572 411
BNB (BNB)	274,24	159 974 373	1 556 578 697

Šaltinis: Sudaryta autorės, remiantis „CoinMarketCap“.¹

Visgi, vartotojų apsauga, nusikalstamų veikų skaičiaus didėjimas, susirūpinimas dėl kainų ir finansinio stabilumo, taip pat poveikio pinigų politikai ir bendras tradicinių mokėjimų sistemų vientisumas yra pagrindiniai reguliatorių rūpesčiai, kurie taip pat yra aktualūs ir šios rinkos vartotojams (Beer, C., ir kt., 2015, Nabilou, H., ir kt., 2019). Kriptovaliutų rinkos bendrieji privalumai, tokie kaip operacijų greitis ir saugumas, blokų grandinės naudojimo paprastumas, maži mokesčiai, pasaulinis pasiekiamumas ir anonimiškumas pritraukė didelę dalį teisėtų vartotojų. Tačiau dėl tokių pačių priežasčių buvo patrauktas ir tokių asmenų dėmesys, kurie yra linkę, dėl savo neteisėtų veiksmų atlikimo, pasislėpti nuo reguliatorių priežiūros bei neteisėtai gauti finansinės naudos. (Foley, S., ir kt., 2018).

Analizuojant kriptovaliutų rinką reikėtų atkreipti dėmesį, jog ne visos kriptovaliutos, egzistuojančios kriptovaliutų rinkoje, yra tikros (autentiškos). Kriptovaliutų rinkoje egzistuoja ir netikros (neautentiškos) kriptovaliutos (angl. *ScamCoin*). Šiuo aspektu galima išskirti tokias kriptovaliutas, kurios yra sukuriamos apskritai kaip naudos kriptovaliutos ir yra sukčiavimo įrankis (pavyzdžiui, *ViralUP*) arba gali būti sukuriamos netikros kriptovaliutos jau egzistuojančių kriptovaliutų aspektu. Gao, B., ir kt., (2020), atliko tyrimą, kurio metu buvo analizuojama iki 2020 m. kovo mėn. išleistos *Ethereum* kriptovaliutos. Tyrimo metu, panaudojant empirinį metodą, buvo siekiama nustatyti, kiek tyrimo metu kriptovaliutų rinkoje buvo padirbtų *Ethereum* kriptovaliutų. Tyrimo metu buvo nustatyta, kad rinkoje egzistavo net 2 117 netikros (padirbtos) *Ethereum*

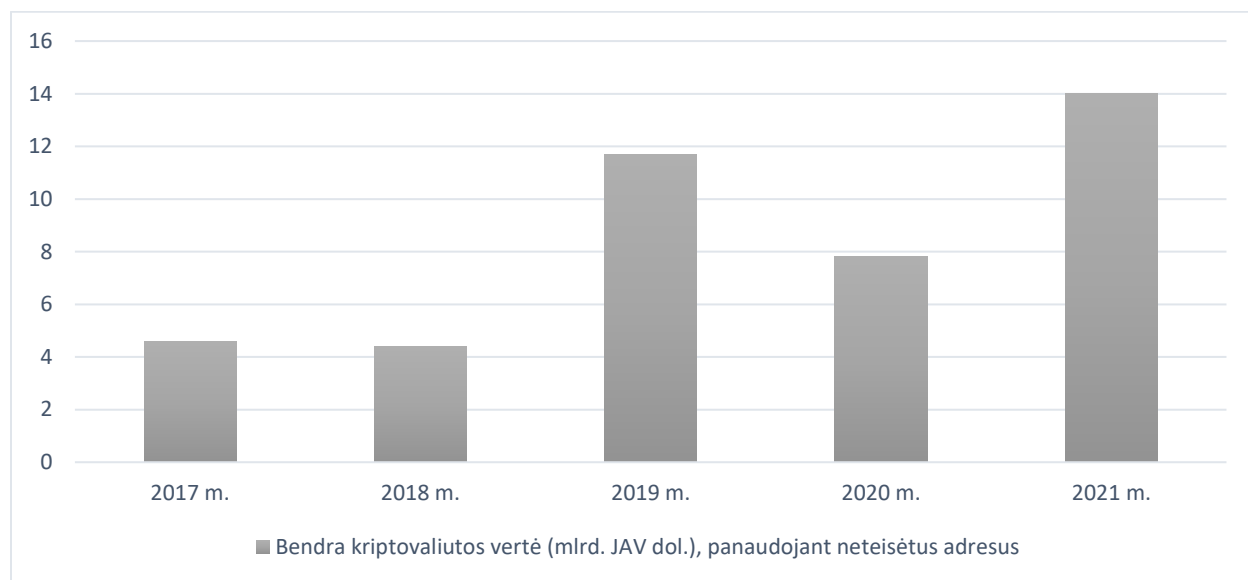
¹ CoinMarketCap. Prieiga internetu: <https://coinmarketcap.com/>, žiūrėta 2022-11-14.

kripto valiutos. Netikros (neautentiškos) kripto valiutos yra viena iš pagrindinių priežasčių, kodėl daugelis šiuo metu egzistuojančių kripto valiutų gali tapti bevertėmis ateityje.

Remiantis 2021 m. duomenimis, per šiuos metus (2021 m.), panaudojant neteisėtus adresus (angl. *illicit addresses*), buvo gauta 14 mlrd. JAV dolerių vertės kripto valiutų, kai tuo tarpu 2020 m. – 7,8 mlrd. JAV dolerių.² Taigi, per 1 metus neteisėtu būdu buvo gauta apie dvigubai daugiau kripto valiutų (3 paveikslas).

3 paveikslas

Bendra kripto valiutų vertė (mlrd. JAV dol.), gauta panaudojant neteisėtus adresus, 2017-2021 m. duomenys



Šaltinis: Sudaryta autorės, remiantis The Chainalysis, 2022.

Kadangi šiai dienai dar nėra aiškaus kripto valiutų rinkos reglamentavimo (požiūrio į kripto valiutas) pasauliniu mastu, kripto valiutų rinka yra sudėtingoje ir neapibrėžtoje reguliavimo aplinkoje, kuri neabejotinai kenkia investicijoms, naujovių plėtrai bei stabdo tvirtos skaitmeninės ekosistemos susiformavimą (Demertzis, M., ir kt., 2018; Luther, W. J., 2019). Reguliavimo priemonės, kurios yra tinkamos šiai dienai reguliuojamai dekretinių pinigų rinkai, nėra tinkamos kripto valiutų rinkai. Todėl akivaizdu, jog siekiant reguliuoti kripto valiutų rinką, yra būtinas

² Remiantis The Chainalysis, 2022 Crypto Crime Report. Prieiga internetu: <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>, žiūrėta 2022-11-21.

atskiras reglamentavimas. Taigi, spartus inovacijų tempas, susijęs su kriptovaliutų rinka, priverčia reguliatorius siekti tinkamai reaguoti bei sumažinti potencialias rizikas, kartu neapribojant technologinės plėtros. Šiai dienai yra neabejotina, jog egzistuoja spraga kriptovaliutų rinkos reglamentavime. Ši spraga turi įtakos, be kita ko, ir ekonominiam neapibrėžtumui (Ferreira, A., ir kt., 2021).

Analizuojant mokslinę literatūrą galima išskirti keturis šaltinius, turinčius įtakos kriptovaliutų rinkos reguliavimo neapibrėžtumui:

- Nefunkcionuojantis reguliavimo dviprasmiškumo šaltinis;
- Netikslus reguliavimo dviprasmiškumo šaltinis;
- Prieštaraujantis reguliavimo dviprasmiškumo šaltinis;
- Pasirinktinais vykdomo reguliavimo dviprasmiškumo šaltinis (Blandin A., ir kt., 2019).

Nefunkcionuojantis reguliavimo dviprasmiškumo šaltinis sietinas su klausimu, ar reguliatorius turi teisę reguliuoti tam tikrą rinką. Taip pat gali būti siejamas su situacijai, kai reguliatorius faktiškai turi teisę reguliuoti tam tikrą rinką, tačiau nėra aišku, kada tai bus pradėta daryti bei kokia apimtimi (Blandin A., ir kt., 2019). Netikslus reguliavimo dviprasmiškumo šaltinis yra toks šaltinis, kai priimtas teisės aktas sukuria akstiną interpretacijoms. Nepaisant to, kad tam tikri netikslumai teisės aktuose yra neišvengiami, tačiau kai kuriais atvejais šie netikslumai gali būti sąmoningi, tokiu būdu siekiant prisitaikyti prie ateities technologinių pokyčių (Blandin A., ir kt., 2019). Prieštaraujantis reguliavimo dviprasmiškumo šaltinis yra toks dviprasmiškumo šaltinis, kai esantis teisės aktas, nepaisant jo aiškumo, gali nebūti vientisas kitų teisės aktų atžvilgiu, sukuriant neaiškumą dėl tokio reguliavimo praktinio taikymo (Blandin A., ir kt., 2019). Pasirinktinais vykdomo reguliavimo dviprasmiškumo šaltinis yra toks dviprasmiškumo šaltinis, kai reguliavimas yra vykdomas atmetinai, savavališkai ar nenuspėjamai (Blandin A., ir kt., 2019, Luther, W. J., 2019). Reguliavimo neapibrėžtumui turi įtakos tai, jog šiuo metu nėra tarptautinio, vientiso susitarimo dėl minimalių reguliavimo reikalavimų kriptovaliutų rinkai ar net elementaraus susitarimo dėl oficialios kriptovaliutų sampratos (Blandin A., ir kt., 2019).

Kriptovaliutų rinkos reguliavimo neapibrėžtumas turi įtakos ekonominėms perspektyvoms, kibernetiniam saugumui bei teisinės sistemos stabilumui. Vertinant įtaką ekonominėms perspektyvoms, paminėtina, jog Europos Centrinis Bankas³, vertindamas skaitmenines valiutas

³ Europos Centrinis Bankas. *Virtual currency schemes*, 2012. Prieiga internetu: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, žiūrėta 2022-11-21.

ekonominio stabilumo požiūriu, nustatė, kad, nepaisant to, jog skaitmeninės valiutos gali turėti įtakos monetariniai politikai ir kainų stabilumui, tačiau jos nesukels pavojaus kainų stabilumui, kadangi pinigų kūrimo lygis ir toliau bus mažas. Taip pat buvo nustatyta, kad skaitmeninės valiutos yra linkusios būti itin nestabilios, tačiau dėl savo veiklos negali pakenkti šalies finansiniam stabilumui. Didžiausia grėsmė buvo siejama su nusikalstamų veikų vykdymu bei centrinių bankų reputacijos pažeidžiamumu. Taigi, nepaisant to, jog visgi didelio masto neigiamos įtakos, pasak Europos Centrinio Banko, kriptovaliutų rinkos reguliavimo neapibrėžtumas neturės, visgi, absoliučiai atmesti prielaidos, kad tam tikra įtaka jaučiama, negalima. Vertinant kitas sritis, kurioms neabejotinai daro įtaka kriptovaliutų rinkos reguliavimo neapibrėžtumas, svarbu atkreipti dėmesį, jog ne tik vietinės priežiūros įstaigos atkreipia dėmesį į nusikalstamų veikų kriptovaliutų rinkoje vykdymų padidėjimą, tačiau ir pats Europos Centrinis Bankas. Nusikalstamų veikų kriptovaliutų rinkoje vykdymo skaičiaus padidėjimas gali turėti įtakos tiek kibernetiniam saugumui, tiek valstybių teisinės ir ekonominės sistemų stabilumui. Šiame kontekste kibernetinis saugumas iš esmės yra neatsiejamas nuo teisinės ir ekonominės sistemų stabilumo, kadangi kriptovaliutų rinkoje kibernetinio pažeidimo atveju yra siekiama vykdyti tam tikro pobūdžio nusikalstamą veiką, kad neteisėtais veiksmais būtų įgyjamos kitam asmeniui priklausančios kriptovaliutos ar prieiga prie kriptovaliutų. Tuo tarpu grynojo (tiesioginio) sistemų stabilumo pažeidimai šiuo atveju siejamas su tuo, jog kriptovaliutų rinka būtų naudojama nusikalstamų veikų vykdymui.

Mokslinėje literatūroje yra išskiriami trys požiūriai, susiję su kriptovaliutų rinkos reglamentavimu – konservatyvus, liberalus ir neutralus.

- Konservatyvus požiūris į kriptovaliutų rinkos reguliavimą yra toks požiūris, kai siekiama apriboti ar apskritai drausti kriptovaliutas. Ši pozicija veikia taip, jog dėl jos skatinimo gali sumažėti inovatyvių projektų (Savona, P., 2022, Chudinovskikh, M. V., ir kt., 2019).
- Liberalusis požiūris į kriptovaliutų rinkos reguliavimą yra toks požiūris, kuris leidžia (pripažįsta) kriptovaliutas. Šis požiūris leidžia taikyti mokesčių lengvatas, tai pat pasireiškia licencijavimo ir finansinių kontrolių mažinimas (Savona, P., 2022, Chudinovskikh, M. V., ir kt., 2019).
- Neutralus požiūris į kriptovaliutų rinką yra toks požiūris, kuris siekia rasti geriausią kompromisą kriptovaliutų rinkos reglamentavime, nustatyti teisinę prigimtį ir požiūrį

į rinkos dalyvių veiklos licencijavimą, apsispręsti dėl sandorių ir pajamų apmokestinimo (Savona, P., 2022, Chudinovskikh, M. V., ir kt., 2019).

Tokio pobūdžio reglamentavimo skirstymas mokslinėje literatūroje gali būti sietinas su tuo, jog analizuojant mokslinę literatūrą kriptovaliutų rinkos nuomonių kontekste, pastebėtina, kad yra autorių, kurie, analizuodami kriptovaliutų rinką išskiria teigiamas ir neigiamas kriptovaliutų rinkos savybės (5 lentelė). Todėl atitinkamai mokslinėje literatūroje yra išskiriamos įvairios pozicijos, susijusios su tuo, kaip turėtų būti reguliuojama kriptovaliutų rinka.

5 lentelė

Autorių nuomonės apie kriptovaliutų rinką

Autorius	Nuomonė
Tredinnick, L., 2019	„<...> Tačiau per pastaruosius penkerius metus Bitcoin vertė daugiausia kilo dėl spekuliacinio motyvo, o ne dėl nusikalstamų veikų.“
Potgieter, P. H., ir kt., 2021	„Problema yra ta, kad tie patys kriptovaliutų rinkai būdingi požymiai, kurie pritraukia vartotojus į šią rinką, daro ją patrauklia į nusikalstamas veikas linkusiems asmenims.“
Butler, S., 2019	„Vis dar nedidelė dalis operacijų, susijusių su kriptovaliutų rinka, yra naudojamos nusikalstamoms veikoms vykdyti. <...> Vertinant kriptovaliutų rinką, nėra didelės grėsmės, kad ši rinka taps plačiai naudojama į nusikalstamą veiką linkusių asmenų.“
Wang, J., ir kt., 2022	„<...> kriptovaliutų rinkoje <...> neišvengiamai atsiranda elektroninių nusikaltimų dėl kriptovaliutų rinkai būdingo anonimiškumo ir decentralizacijos<...>.“
Barnes, P., 2018	„<...> kriptovaliutas (kitaip nei dekretinius pinigus) yra sunku padirbti dėl juose naudojamos kriptografijos ir dėl to, kad jos nėra išleistos oficialios institucijos, taip pat yra užtikrinamas sandorių privatumas.“

Šaltinis: Sudaryta autorės, remiantis Barnes, P., 2018, Tredinnick, L., 2019, Potgieter, P. H., ir kt., 2021, Butler, S., 2019, Wang, J., ir kt., 2022.

Nepaisant to, jog be šalių, kurios apkritai nepripažįsta kriptovaliutų rinkos, egzistuoja šalys, kurios siekia nustatyti tam tikrus reguliavimus kriptovaliutų rinkai. Visgi daugelyje

jurisdikcijų šiai dienai kriptovaliutų rinka vis dar nėra reguliuojama, o siekis reguliuoti yra vis dar pirminėse stadijose (6 lentelė).

6 lentelė

Kriptovaliutų rinkai palankios ir nepalankios šalys reguliavimo aspektu (suskirstytos pagal žemynus)

Palanki šalis	Trumpas apibūdinimas
Švedija	Švedijos Finansų priežiūros tarnyba ir centrinis bankas viešai paskelbė, kad kriptovaliutos yra legalios šalyje, bet tai nėra oficiali mokėjimo. Mokesčių požiūriu tai yra turtas, o ne valiuta.
Kanada	Kanada yra patvirtinusi kriptovaliutos – bitkoino – biržoje prekiaujamus fondus. Kanados mokesčių inspekcija paprastai kriptovaliutą traktuoja kaip prekę.
Japonija	Japonija turi vieną pažangiausių ir išvystytų kriptovaliutų reguliavimo režimų. Japonijoje pelnas, susijęs su kriptovaliutomis, laikomas įvairiomis pajamomis. Kripto pelno mokesčių tarifai skiriasi ir priklauso nuo asmens pajamų.
Nepalanki šalis	Trumpas apibūdinimas
Kinija	Kinijos liaudies bankas uždraudė finansų įstaigoms prekiauti kriptovaliutomis 2013 m., o vėliau išplėtė draudimą, kuris apėmė kriptovaliutų biržas ir ICO.
Marokas	2017 metais buvo priimtas įstatymas, draudžiantis kriptovaliutų naudojimą šalyje.
Bolivija	Bolivijos vyriausybė 2014 m. uždraudė naudotis kriptovaliutomis, manydama, kad kriptovaliutų rinka palengvina nusikalstamų veikų vykdymą.

Šaltinis: Sudaryta autorės, remiantis Cumming, J. D., ir kt., 2019, Kirkpatrick, K., ir kt., 2021, Haq, M. Z., ir kt., 2022, Thomson Reuters, 2022.⁴

Žvelgiant į bendrą Europos Sąjungos lygio reguliavimą matoma, kad 2023 m. balandžio 20 d. Europos Sąjungos Parlamentas patvirtino „Markets in Crypto-Assets“ (MiCA)⁵ reglamento (Reglamentas (ES) 2023/1114) priėmimą, kuris įsigalios 2024 m. MiCA reglamentas taikytinas visiems kriptoturtams, kuriems netaikomi Europos Sąjungos finansinių paslaugų teisės aktai, jų emitentams ir paslaugų teikėjams, suteikiant vieną licencijavimo režimą visose Europos Sąjungos valstybėse narėse. O būtent, MiCA taikytina sekančio kriptoturto atžvilgiu: kriptoturtas, kuris

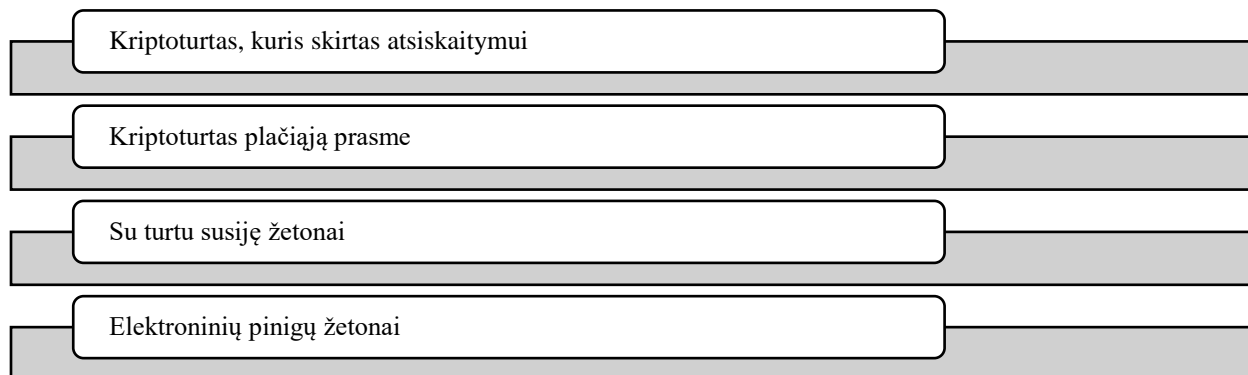
⁴ Remiantis Thomson Reuters, Cryptocurrency regulations by country, 2022. Prieiga internetu: <https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf> Žiūrėta: 2022-11-23.

⁵ Prieiga internetu: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>, žiūrėta 2022-11-24.

skirtas atsiskaitymui; kriptoturtas plačiąją prasme; su turtu susiję žetonai ir elektroniniai pinigų žetonai (Bočánek, M., 2021, Ferreira, A., ir kt., 2021) (4 paveikslas).

4 paveikslas

MiCA reglamente išskirtas kriptoturtas



Šaltinis: Sudaryta autorės, remiantis MiCA reglamentu.

Vertinant paminėtą kriptoturtą per kriptovaliutas ir žetonus paminėtina, kad kriptoturtui, kuris yra skirtas atsiskaitymui, priskiriami tokie žetonai kaip *Ankr*, *Filecoin*, *Arweave*. Kriptoturtas plačiąją prasme laikytini *Bitcoin*, *Ethereum* ir kitos kriptovaliutos. Su turtu susiję žetonai ir elektroninių pinigų žetonai yra tokie žetonai, kurie yra susieti su keliomis valiutomis.

Analizuojant MiCA identifikuotina, kad pastarosios tikslas yra užtikrinti teisinį tikrumą ir užtikrinti atitinkamą vartotojų ir investuotojų apsaugos lygį, finansinį stabilumą ir rinkos vientisumą, nesudarant kliūčių naujų technologijų taikymui. Paminėtina ir tai, kad MiCA reglamente yra numatyti reikalavimai kriptovaliutų leidėjams, tokie kaip veiklos leidimai, minimalus įstatinis kapitalas, bei kriptoturto baltosios knygos (angl. *white-paper*) parengimas. Kriptoturto, kuris neturi vieno leidėjo, keitykloms taip pat bus taikomas reikalavimas skelbti baltąją knygą apie galimas valiutos rizikas. Tai reiškia, kad šioms keitykloms bus keliamas reikalavimas ir atsakomybė už tinkamą (teisingą) pateiktos baltosios knygos turinį (Bočánek, M., 2021, Ferreira, A., ir kt., 2021). Vertinant MiCA reglamento naudą akivaizdu, kad reglamentu nustatomas reguliavimas įves tam tikrą aiškumą į rinką bei prisidės prie vartotojų (investuotojų) apsaugos stiprinimo. Tačiau matoma ir tam tikrų iššūkių, tokių kaip kad verslui reikės daugiau išteklių, siekiant įgyvendinti keliamus reikalavimus bei, tikėtina, kad bus tam tikrų iššūkių

žetonams, susietiems su JAV doleriu, kadangi reguliavimas galimai apribos JAV verslų veiklą Europos Sąjungoje.

Apibendrinant, galima daryti išvadą, kad kriptovaliutų rinkų vystymasis ir plėtra neabejotinai turi įtakos ekonominiams, kibernetiniams ir teisiniams aspektams. Kadangi kriptovaliutų rinka šiai dienai yra funkcionuojanti, t. y., galima kriptovaliutas pirkti-parduoti, atsiskaityti jomis už prekes ir (ar) paslaugas, yra labai svarbu užtikrinti kriptovaliutų rinkos reglamentavimą. Tokiu būdu būtų užkardomas kelias nusikalstamų veikų vykdymui kriptovaliutų rinkoje, o tai turėtų įtakos vartotojų (investuotojų) teisių apsaugai, bendresniam rinkos stabilumui ir tvariai kriptovaliutų rinkos plėtrai.

1.3. Nusikalstamos veikos pasireiškiančios kriptovaliutų rinkoje

Technologinių inovacijų plėtra neabejotinai lenkia ekonominės politikos vystymąsi. Felson, M., ir kt., (1998), teigia, kad nusikalstamos veikos šaltinis yra „išsišaknijusi“ galimybė. Tai reiškia, jog, be kita ko, galimybių (vykdyti nusikalstamas veikas) egzistavimas yra viena iš priežasčių nusikalstamoms veikoms būti vykdomoms. Pritaikant šią mokslinėje literatūroje išreikštą poziciją kriptovaliutų rinkai, galima daryti išvadą, kad kriptovaliutų rinka gali būti priskiriama tokioms rinkoms, kurios suteikia galimybę nusikalstamų veikų vykdymui dėl kriptovaliutų rinkai būdingų veikimų principų ir skiriamųjų savybių (De-Vries, P. D., 2016). Tokiu būdu šios rinkos vartotojas (investuotojas) tampa lengviau pažeidžiamas potencialių finansinių nuostolių aspektu.

Kaip minėta šio darbo 1.1. poskyryje, kriptovaliutų rinka, lyginant su kitomis rinkomis, turi tik kriptovaliutų rinkai būdingų savybių, dėl kurių šiai dienai kriptovaliutų rinka yra laikoma daugeliui priimtiniu investiciniu sprendimu bei atsiskaitymo priemone (Corbet, S., ir kt., 2022). Tačiau dėl tų pačių savo savybių ir bendro veikimo principo, kriptovaliutų rinka yra laikoma patrauklia rinka asmenims, kurie siekia vykdyti nusikalstamas veikas (De-Vries, P. D., 2016). Šiame kontekste yra svarbu sukonkretinti anksčiau aptartas kriptovaliutų rinkos savybes, kurios pritraukia nusikalstamą veiką vykdančius asmenis į šią rinką (7 lentelė). Pirma, paminėtinas kriptovaliutų rinkos decentralizuotumas. Tai reiškia, jog operacijos kriptovaliutų rinkoje yra vykdomi lygiavertiškai (angl. *peer-to-peer*), t. y., be finansinių tarpininkų įsikišimo (Felix, T. H., ir kt., 2019, Aalborg A. H., ir kt., 2019, Wronka, C., 2021). Dėl šios priežasties kriptovaliutų

operacijoms nėra taikomi „Pažink savo klientą“ (angl. *Know Your Customer*) ir pinigų plovimo ir teroristų finansavimo prevencijos įstatyme numatyti reikalavimai (Campbell-Verduyn, M., 2018). Šiame kontekste paminėtinas Teichmann, F. M. J., ir kt., (2020), atliktas tyrimas, kurio metu, panaudojant interviu ir apklausos metodus, buvo kalbinti 18 atitikties pareigūnų (angl. *compliance officer*). Šiame tyrime buvo iškeltas klausimas, ar yra pastebima tendencija tarp reguliuojamų (finansų įstaigų) ir nereguliuojamų (kripto valiutų) rinkų nusikalstamų veikų vykdymo aspektu, t. y., kokiose rinkose dažniau pasireiškia nusikalstamos veikos. Atsakydami į šį klausimą tyrimo dalyviai nurodė, jog yra matoma tendencija, lyginant rinkų patrauklumą, kuri parodo, kad vis dažniau nusikalstamas veikas vykdyti linkę asmenys renkasi nereguliuojamas rinkas arba silpnai reguliuojamas rinkas. Pagrindine priežastimi buvo įvardinta situacija, jog nereguliuojamoje arba silpnai reguliuojamoje rinkoje yra tiesiog paprasčiau vykdyti nusikalstamas veikas, o galimybė, jog asmuo bus patrauktas baudžiamojon atsakomybėn drastiškai nukrenta, lyginant su stipriai reguliuojamomis rinkomis. Antra, kripto valiutų operacijos pasižymi anonimiškumu (Brühl, V., 2017, Marella, V., ir kt., 2020, Bartoletti, M., ir kt., 2018, Leuprecht, C., ir kt., 2022). Kaip jau minėta, nors mokslinėje literatūroje yra nurodoma, kad anonimiškumas nėra absoliutus, kadangi operacijai būnant atliekamai blokų grandinėje, operacijos yra įrašomos į viešuosius sąrašus, kurie yra viešai prieinami, bei tai, jog kripto valiutų rinka neužtikrina tokio anonimiškumo kaip gryniesi pinigai, tačiau anonimiškumas yra laikomas viena iš kripto valiutų rinkos savybių (Reid, F., ir kt., 2011, Weber, M., ir kt., 2019). Ši savybė reiškia, jog atlikus operaciją kripto valiutų rinkoje, operacijos šalių asmenybės nebus nustatytos, priešingai nei vykdant operacijas per finansų įstaigas. Taigi, kadangi kripto valiutų atveju yra maža asmens tapatybės nustatymo galimybė, atitinkamai yra sumažėjusi patraukimo baudžiamojon atsakomybėn rizika asmeniui už jo įvykdytas nusikalstamas veikas kripto valiutų rinkoje (Badawi, E., ir kt., 2020, Dupuis, D., ir kt., 2021). Šiame kontekste paminėtinas Möser, M., ir kt., (2013), atliktas tyrimas, panaudojant atvirkštinės inžinerijos metodą. Tyrimo metu buvo analizuojami trys paslaugų tiekėjai – *Bitcoin Fog*, *BitLaundry* ir *Blockchain.info* – kurie teikia anonimizavimo kripto valiutų rinkoje paslaugas. Tai reiškia, jog pasinaudojant šių paslaugų teikėjų teikiamomis paslaugomis, kripto valiutų rinkoje galima anonimizuoti duomenis apie atliktą operaciją. Tokiu būdu yra padaroma taip kad būtų neįmanoma atsekti asmens, kuris įvykdė atitinkamą operaciją. Tyrimo rezultatai parodė, kad pasinaudojant *Bitcoin Fog* ir *Blockchain.info* paslaugomis anonimizavimas buvo atliktas sėkmingai. Tai reiškia, kad atliktos operacijos nebeturėjo jokios atsekamumo sąsajos. Galiausiai,

kripto valiutų rinkos savybė, kuri prisideda prie to, jog kripto valiutų rinkoje yra sąlyginai paprasta vykdyti nusikalstamas veikas, yra operacijų įvykdymo greitis (Dupuis, D., ir kt., 2021, Campbell-Verduyn, M., 2018). Tai reiškia, kad, kaip jau minėta, kadangi kripto valiutų rinka yra decentralizuota, todėl nėra pareigos laukti atitinkamą laiką, siekiant, jog operacija būtų įvykdyta (Dupuis, D., ir kt., 2021). Spartesnis operacijų vykdymas leidžia lengviau paslėpti neteisėtų veiksmų atlikimą ir padaryti taip, jog šie veiksmai būtų arba apskritai nebeatsekami arba jų atsekamumas būtų apsunkintas. Šiame kontekste paminėtinas Teichmann, F. M. J., ir kt., (2020), atliktas tyrimas, panaudojant apklausų ir interviu metodus, kurio metu dalyvavo 18 atitikties pareigūnų. Šio tyrimo metu buvo užduotas klausimas, jeigu yra galimybė rinktis, kurioje rinkoje asmenys labiau linkę vykdyti operacijas – įprastoje finansų rinkoje per finansų įstaigas ar kripto valiutų rinkoje. Tyrimo metu buvo išreikšta pozicija, kad vienas iš kripto valiutų rinkos privalumų yra tai, jog siekiant atlikti operaciją nereikia atlikti pavedimo per finansų įstaigą, užtenka tik pasinaudoti šifruota sistema, kuri leidžia atsiskaityti greitai be trečiųjų šalių įsikišimo. Toliau plėtojant šią poziciją buvo nurodyta, kad tokiu būdu nebelieka prasmės asmeniui, siekiančiam vykdyti neteisėtus veiksmus, bandyti atlikti operaciją per finansų įstaigas ir susidurti su realia galimybe būti demaskuotam arba bent jau susidurti su apsunkinimais, siekiant atlikti operaciją. Kadangi kripto valiutų rinka suteikia galimybę be finansų įstaigų įsikišimo itin sklandžiai atlikti operaciją. Taigi, paminėti kripto valiutų rinkos veikimo principai sudaro sąlygas į nusikalstamą veiką linkusiems asmenims paprasčiau vykdytini nusikalstamas veikas, išvengiant baudžiamosios atsakomybės, lyginant su operacijomis, kurie būtų vykdomi per finansų įstaigas arba akcijų rinkose.

7 lentelė

Kripto valiutų rinkos veikimo principai, sudarantys sąlygas nusikalstamų veikų vykdymui

Kripto valiutų rinkos veikimo principai	Autoriai
Decentralizuotumas	Fleder, M., ir kt., 2015, Brenig, Ch., ir kt., 2015, Puthal, D., ir kt., 2018, Campbell-Verduyn, M., 2018, Felix, T. H., ir kt., 2019, Aalborg A. H., ir kt., 2019, Wronka, C., 2021.
Anonimiškumas	Reid, F., ir kt., 2011, Weber, M., ir kt., 2019, Brühl, V., 2017, Marella, V., ir kt., 2020, Bartoletti, M., ir kt., 2018, Leuprecht, C., ir kt., 2022.
Operacijų vykdymo spartumas	Campbell-Verduyn, M., 2018 De-Vries, P. D., 2016, Dupuis, D., ir kt., 2021.

Šaltinis: Sudaryta autorės, remiantis lentelėje nurodyta mokslinė literatūra.

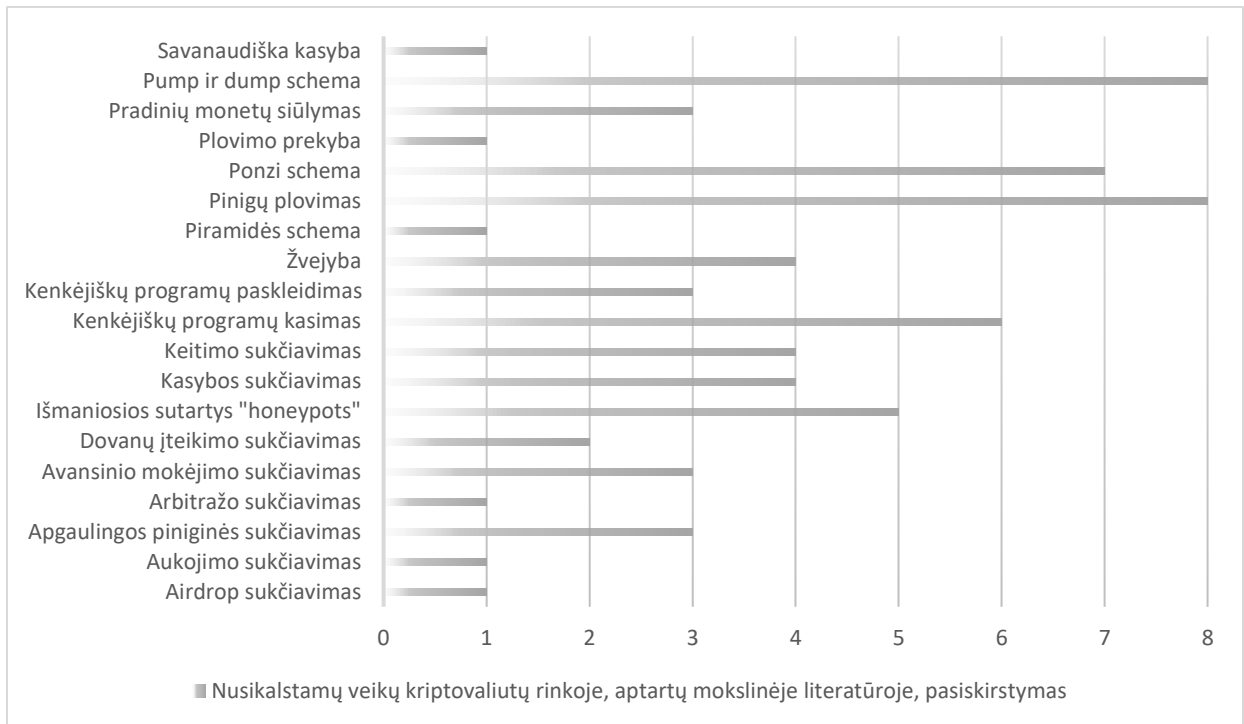
Vertinant nusikalstamas veikas kriptovaliutų rinkoje, Trozze, A., ir kt., (2022) atliko tyrimą, kurio metu, be kita ko, panaudojant apklausos metodą, buvo apklausti 27 finansų sektoriaus, teisinio sektoriaus bei akademinio sektoriaus atstovai. Apklausos metu buvo pateiktos penkios literatūros analizėje dažniausiai identifikuotos nusikalstamos veikos (kriptovaliutų piniginių sukčiavimas, *Pump* ir *dump* schema, investavimo schemas (ICO, Ponzi schemas), kenkėjiškų programų kasimas ir kenkėjiškų programų sukčiavimas), siekiant išsiaiškinti, kurios iš jų apklaustųjų manymu, laikytinos pačiomis kenksmingiausiomis, pelningiausiomis, lengviausiai įgyvendinamomis ir lengviausiai įveikiamomis. Pati kenksmingiausia iš paminėtų nusikalstamų veikų kriptovaliutų rinkoje buvo pripažinta investicinis sukčiavimas, tuo tarpu mažiausia kenksminga buvo pripažinta *Pump* ir *dump* schema. Pelningiausia – *Pump* ir *dump* schema, tuo tarpu mažiausia pelninga – kenkėjiškų programų kasimas. Lengviausia įgyvendinama nusikalstama veika – *Pump* ir *dump* schema, sunkiausia – kriptovaliutų piniginių sukčiavimas. Galiausia, lengviausia įveikiama – *Pump* ir *dump* schema, sunkiausia – investicinis sukčiavimas. Taigi, nepaisant to, kad *Pump* ir *dump* schema laikytina mažiausia kenksminga ir pakankamai lengvai įveikiama, visgi tai yra pelningiausia ir lengviausia įgyvendinama nusikalstamos veikos schema, siekiant neteisėtai įgyti kriptovaliutas. Taip pat paminėtinas ir Vasek, M., ir kt., (2018), tyrimas, kurio metu, pritaikant duomenų rinkimo ir analizės tyrimo metodus, buvo atrinktos ir nustatytos 192 potencialios nusikalstamos veikos (sukčiavimo atvejai) atitinkamose kriptovaliutų tinklapiuose – *Bitcointalk.org*, <http://www.badbitcoin.org/thebadlist/index.htm> ir *Cryptohyips.com*. Tyrimo metu buvo nustatytos 4 nusikalstamos veikos, susijusios su sukčiavimu kriptovaliutų rinkoje: Ponzi schema, kasybos sukčiavimas, sukčiavimo piniginės ir nesąžiningi mainai. Taip pat nustatyta, kad laikotarpiu nuo 2011 m. iki 2014 m. buvo mažiausiai 13 000 nukentėjusių asmenų iš kurių buvo neteisėtai įgyta apie 11 mln. JAV dolerių. Šis tyrimas, be kita ko, leidžia daryti išvadą, kad kriptovaliutų rinkos formavimosi pradžioje sukčiavimo atvejai buvo dažni kriptovaliutų rinkoje ir įgyjamos sumos buvo pakankamai didelės, tačiau sukčiavimo schemas pakankamai ribotos.

Siekiant nustatyti kriptovaliutų rinkoje pasireiškiančias nusikalstamas veikas mokslinės literatūros apimtyje, šiame darbe buvo išanalizuoti 52 atsitiktiniu būdu pasirinkti straipsniai, kuriuose buvo aptariamos (tiriamos) nusikalstamos veikos kriptovaliutų rinkoje. Mokslinės literatūros paieška buvo vykdoma per Google Scholar, Emerald, SSNR ir SPRING paieškos sistemas, vedant raktinius žodžius [*crypto*] *crime*, *illicit*, *fraud*, *scam*. Išanalizavus mokslinę

literatūrą nusikalstamų veikų kriptovaliutų rinkoje aspektu pastebėta, kad iš viso buvo nustatyta 19 skirtingų nusikalstamų veikų, kurios pasireiškia kriptovaliutų rinkoje (5 paveikslas; Priedas Nr. 1; Priedas Nr. 2).

5 paveikslas

Nusikalstamų veikų kriptovaliutų rinkoje, aptartų mokslinėje literatūroje, pasiskirstymas



Šaltinis: Sudaryta autorės pagal išanalizuotą literatūrą (žr. Priedas Nr. 1).

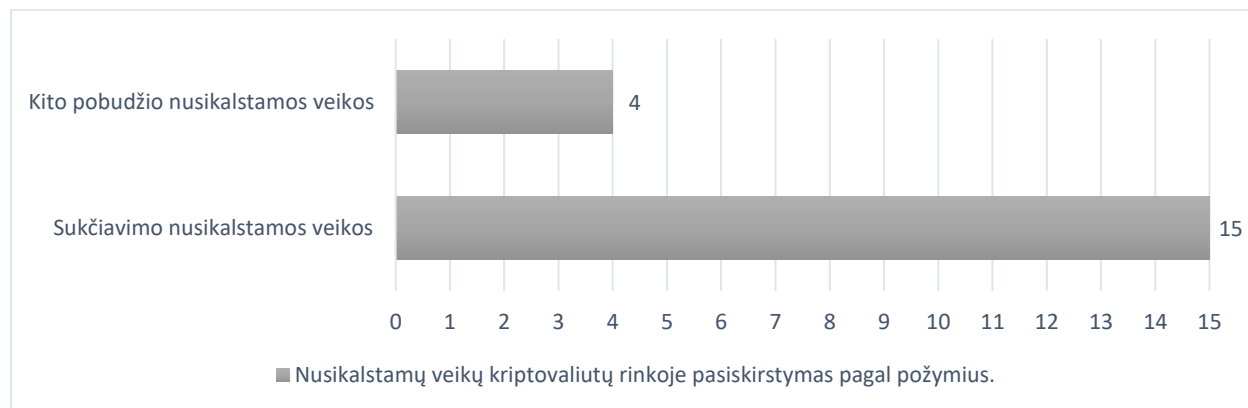
Iš išanalizuotos mokslinės literatūros matyti, kad mokslinėje literatūroje aptariamas nusikalstamas veikas kriptovaliutų rinkoje dažnai apibūdina bendra sąvoka – sukčiavimas, pavyzdžiui, aukojimo sukčiavimas, arbitražo sukčiavimas, avansinio mokėjimo sukčiavimas, kasybos sukčiavimas ir panašūs kitokio pobūdžio sukčiavimo atvejai. Todėl galima pastebėti, kad net iš 19 skirtingų kriptovaliutų rinkoje pasireiškiančių nusikalstamų veikų, 15 nusikalstamų veikų galėtų būti priskiriamos bendrai prie sukčiavimo, tuo tarpu likusios – 4⁶ – nusikalstamos veikos

⁶ Kenkėjiškų programų kasimas, kenkėjiškų programų paskleidimas, pinigų plovimas, savanaudiška kasyba.

galėtų būti atirbojamos nuo sukčiavimo ir inkriminuojamos atitinkamai pagal kitus nusikalstamų veikų požymius⁷ (6 paveikslas).

6 paveikslas

Nusikalstamų veikų kriptovaliutų rinkoje pasiskirstymas pagal požymius



Šaltinis: Sudaryta autorės pagal išanalizuotą mokslinę literatūrą (žr. Priedas Nr. 1).

Analizuojant mokslinę literatūrą pastabėtina, kad nusikalstamas veikas, vykdomas kriptovaliutų rinkoje, galima susiskirstyti į dvi kategorijas. Pirmoji kategorija yra tokios nusikalstamos veikos, kurios yra neatsiejamai susijusios su kriptovaliutų rinka. Šiai kategorijai priskiriamos nusikalstamos veikos yra tokio tipo, kurių būtų neįmanoma įvykdyti, jei neegzistuoūtų kriptovaliutų rinka. Iš mokslinės literatūros analizės rezultatų, šiai kategorijai galime priskirti kriptovaliutų gavybos (angl. *cryptojacking*), kriptovaliutų piniginės (angl. *cryptocurrency wallet*) ir kriptovaliutų keityklos paslaugų (angl. *crypto exchange service*) nusikalstamas veikas. Kriptovaliutų gavybos nusikalstamos veikos aspektu, paminėtinas Hong, G., ir kt., (2018), tyrimas, kurio metu buvo pasiūlytas CMTracker, elgesiu pagrįstas detektorius, skirtas automatiškai sekti kriptovaliutų gavybos scenarijus ir su jais susijusius duomenis. Tyrimo metu, panaudojant CMTracker buvo atpažintos 2 770 interneto svetainių, kuriose buvo vykdoma neteisėta kriptovaliutų gavyba bei nustatyta, kad šią nusikalstamą veiką vykde asmenys 2018 m. per dieną neteisėtai įgydavo bent 59 000 JAV dolerių. Panaudojant Hong, G., ir kt., (2018) pasiūlytą CMTracker įrankį, Varlioglu, S., ir kt., (2020), atliko tyrimą, kurio metu, analizuojant Hong, G.,

⁷ Nustatytų nusikalstamų veikų kvalifikavimas ir atitinkamai nekvalifikavimas prie sukčiavimo nusikalstamų veikų buvo atliktas vertinant tik pirminius nusikalstamų veikų požymius pagal Priedą Nr. 2.

ir kt., (2018), tyrime atpažintas 2 770 interneto svetaines, kuriose buvo vykdoma neteisėta kriptovaliutų gavyba, buvo siekiama, nustatyti, ar *Coinhive* (įdiegiama kenkėjiška programa, skirta neteisėtai kriptovaliutų gavybai naudoti) eliminavimas iš rinkos, pakeitė rinką ir kokius rezultatus, analizuojant 2 770 interneto svetainių, kuriuose Hong, G., ir kt., (2018), tyrimo metu buvo vykdoma neteisėta kriptovaliutų gavyba, parodytą. Paminėtina, jog *Coinhive* yra įdiegiama kenkėjiška programa, kuri egzistavo tuo metu, kai Hong, G., ir kt., (2018) atliko tyrimą, tačiau buvo panaikinta iš rinkos 2019 m., kai Varlioglu, S., ir kt., (2020) atliko šį tyrimą. Taigi, tyrimo rezultatai parodė, kad 99% nustatytų interneto tinklapių (kuriuos nustatė Hong, G., ir kt., (2018), tyrimo metu) nebetęsė nusikalstamos veikos ir tik 1% nustatytų internetinių tinklapių vykdė neteisėtą kriptovaliutų gavybą. Taigi, *Coinhive* buvo itin populiarus kenkėjiška programa, skirta neteisėtai kriptovaliutų gavybai, o šios programos eliminavimas iš rinkos turėjo stiprią įtaką kriptovaliutų gavybos nusikalstamos veikos sumažėjimui. Galiausiai paminėtinas Xia, P., ir kt., (2020b), tyrimas, kurio metu, panaudojant spausdinimo klaidų metodą, buvo siekiama nustatyti nusikalstamas veikas, vykdomas pasitelkiant kriptovaliutų keityklas. Tyrimo metu buvo identifikuota daugiau nei 1 595 duomenys, kuriuos pasitelkiant buvo vykdomas sukčiavimas ir daugiau nei 300 netikrų programėlių (angl. *apps*), kurių pagalba buvo vykdomos nusikalstamos veikos kriptovaliutų rinkoje. Tyrimo metu taip pat nustatyta, kad dėl netikrų kriptovaliutų keityklos nusikalstamų veikų investuotojai patyrė mažiausia 520 000 JAV dolerių finansinių nuostolių. Antrajai kategorijai yra priskiriamos tokios nusikalstamos veikos, kurios egzistavo ir buvo vykdomos dar iki susiformuojant kriptovaliutų rinkai, tačiau atsiradus šiai rinkai, tokios nusikalstamos veikos buvo pradėtos vykdyti pasinaudojant kriptovaliutų rinka. Šiai kategorijai galime priskirti tokias nusikalstamas veikas kaip kad, pavyzdžiui, Ponzi schema, *Pump* ir *dump* schema, Piramidės schema, žvejyba (angl. *Phishing*), pinigų plovimas. Iš 5 paveiksle pateiktų duomenų matyti, jog analizuotoje mokslinėje literatūroje daugiausia buvo kalbama apie *Pump* ir *dump* schemą, Ponzi schemą ir pinigų plovimą kaip nusikalstamas veikas kriptovaliutų rinkoje, todėl toliau bus plačiau aptariamos šios nusikalstamos veikos kriptovaliutų rinkoje.

Pirmoji nusikalstama veika kriptovaliutų rinkoje, kuri dažniausia buvo aptariama pasirinktuose mokslinės literatūros straipsniuose, yra pumpavimo ir išmetimo schema (angl. *Pump and dump*). Šios nusikalstamos veikos vykdymo metu, nusikalstamą veiką vykdančias asmenys per tam tikrą laikotarpį dirbtinai didina prekės kainą, skleisdami dezinformaciją (siurbdami), prieš parduodami tą prekę už padidintą kainą (išmesdami). Kadangi kaina yra padidinama fiktyviai,

todėl dažniausia kaina ilgainiui nukrenta, o pirkėjai, įsigiję prekę, patiria nuostolius. Taigi, galima teigti, kad šiai nusikalstamai veikai yra būdingi trys etapai: (a) kaupimo (prekės, valiutos ir pan.); (b) siurbimo (fiktyvus kainos, vertės didinimas); (c) išmetimo (parduodama prekė, valiuta už fiktyviai didesnę kainą). *Pump* ir *dump* schema yra jau seniai žinoma, šiai dienai *Pump* ir *dump* schemos vyksta internetinėje erdvėje, o kriptovaliutų rinkai sparčiai išpopuliarėjus, *Pump* ir *dump* schemos persikėlė ir į šią rinką. Taigi, ši nusikalstama veika gali būti priskiriama prie tokių nusikalstamų veikų kriptovaliutų rinkoje, kuri egzistavo ir buvo vykdoma dar iki kriptovaliutų rinkos susiformavimo, o pastarajai atsiradus – persikėlė ir į kriptovaliutų rinką. (Temple, S., 2000, Kamps, J. ir kt., 2018, Morgia, L. M., ir kt., 2021). *Pump* ir *dump* schema kriptovaliutų rinkos kontekstu gali būti apibūdinama kaip nusikalstama veika, kurios vykdymo metu nusikalstama veiką vykdytys asmenys sukaupia mažos vertės kriptovaliutų kiekius ir siekia juos dirbtinai branginti (auginti jų vertę), skleisdami dezinformaciją. Kai kriptovaliutų vertė fiktyviai (pa)didėja, nusikalstama veiką vykdytys asmenys parduoda visą turimą kriptovaliutų kiekį, kad uždirbtų pelną (Mansourifar, H., ir kt., 2020). Kadangi kriptovaliutų rinka nėra visapusiškai reguliuojama, kriptovaliutų kainomis yra itin lengva manipuliuoti. Tai yra viena pagrindinių priežasčių, kodėl *Pump* ir *dump* schema yra paplitusi kriptovaliutų rinkoje (Kamps, J., ir kt., 2018). Kaip matyti iš mokslinės literatūros analizės, *Pump* ir *dump* nusikalstama veika kriptovaliutų rinkos atžvilgiu yra atliekama panaudojant šiais laikais itin populiarius socialinius tinklus (Nizzoli, L., ir kt., 2020, Morgia, L. M., ir kt., 2021). Nizzoli, L., ir kt., (2020), atliko tyrimą, kurio metu, panaudojant modeliavimo technikos metodą, socialiniuose tinkluose *Twitter*, *Telegram* ir *Discord* per tris mėnesius buvo identifikuotos 50 mln. žinučių iš daugiau nei 7 mln. vartotojų. Vertinant identifikuotas žinutes pastebėta, kad *Discord* socialiniame tinkle buvo tik 1 *Pump* ir *dump* schemos kanalas, tačiau *Telegram* socialiniame tinkle net 296 kanalai. Be to, tyrimo metu nustatyta, kad net 56% socialinio tinklo *Twitter* pranešimų buvo parašyti robotų (angl. *bots*) arba iš netikrų paskyrų, kurios buvo susijusios su *Pump* ir *dump* schemos platinimu, perkeliant vartotojus į *Discord* arba *Telegram* socialinius tinklus, kuriuose jau buvo įgyvendinamos *Pump* ir *dump* schemos. Panaudojant tuos pačius socialinius tinklus – *Telegram* ir *Discord*, Morgia, L. M., ir kt., (2021), naudojant stebėjimo ir mašininio mokymosi metodus, trejus metus stebėjo grupes, kurios *Telegram* ir *Discord* socialiniuose tinkluose organizuoja *Pump* ir *dump* schemas. Šio tyrimo metu buvo nustatyti 900 *Pump* ir *dump* schemos atvejai *Telegram* ir *Discord* socialiniuose tinkluose. Galiausia, Dhawan, A., ir kt., (2021), atliko tyrimą, kurio metu, panaudodami duomenų rinkimo ir

analizės metodus, dviejuose kriptovaliutų keityklose – *Binance* ir *Yobit*, per 6 mėn. (nuo 2017 m. gruodžio mėn. iki 2018 m. birželio mėn.) laikotarpį identifikavo 355 *Pump* ir *dump* schemos atvejų, kurie neteisėtai padėjo įgyti 6 mln. JAV dolerių nusikalstamą veiką vykdančiams asmenims.

Antra nusikalstama veika kriptovaliutų rinkoje, kuri dažniausia buvo aptariama pasirinktuose straipsniuose, yra Ponzi schema. Sąvokos „Ponzi schema“ kilmė siekia 1919 m. ir reiškia Charlesą Ponzi, kuris iš tūkstančių žmonių išviliojo maždaug 10 mln. JAV dolerių. Ponzi schema veikia tokiu principu, jog Ponzi schemos siūlomoms investicijoms grąžos yra kur kas didesnės grąžos nei yra nusistovėjusios rinkoje. Tokiu būdu, t. y., siūlant didesnę nei rinkoje nusistovėjusi grąža, yra sukeliama investuotojų susidomėjimas. Tačiau, kadangi iš pradžių didelė grąža kelia įtarimų potencialiems investuotojams, tik nedidelė dalis investuotojų būna linkę išbandyti investuoti. Tačiau laikui bėgant vis daugiau investuotojų prisijungia prie šios schemos. Kol prie schemos jungiasi nauji investuotojai, senesnieji (pirmesnieji) investuotojai gauna žadėtą grąžą. Ši schema egzistuoja tol, kol yra įmanoma rasti naujų investuotojų, taip padengiant senesniųjų (pirmesniųjų) investuotojų išmokamą grąžą. Nustojus į schemą jungtis naujiems investuotojams, schema sugriūna, kadangi nebelieka galimybės mokėti grąžos investuotojams (Bartoletti, M., ir kt., 2018; Reddy, E., ir kt., 2018; Vasek, M. ir kt., 2015). Analizuojant mokslinę literatūrą pastebėtina, jog buvo atliekami tyrimai, siekiant nustatyti, ar kriptovaliutų rinkoje Ponzi schema iš tiesų yra itin dažnas reiškinys. Chen, W., ir kt., (2018), tyrimo metu, panaudojant duomenų gavybos ir mašininio mokymosi metodus, tirdami išmaniąsias sutartis *Ethereum* platformoje, sukūrė regresijos medžio modelį, kuris leido aptikti Ponzi schemas. Tyrimo metu buvo nustatyta, kad kriptovaliutos *Ethereum* rinkoje vienu metu yra daugiau nei 400 veikiančių Ponzi schemų. Vasek, M., ir kt., (2019), tyrimo metu, panaudodami stebėjimo metodą, tyrė internetines svetaines, siekdami įvertinti kriptovaliutų sukčiavimo skaičių 2011–2016 m. Tyrimo metu, tirdami trijuose skirtingose kriptovaliutos – bitkoino – *bitcointalk.org* subformuose esančius pranešimus, laikotarpyje nuo 2011 m. birželio mėn. iki 2016 m. lapkričio mėn., nustatė, jog buvo vykdomas 42 sukčiavimo schemos. Iš viso buvo 13 000 asmenų, nukentėjusių nuo nusikalstamų veikų iš kurių neteisėtai buvo įgyta 11 mln. JAV dolerių. Nizzoli, L., ir kt., (2020), atliko tyrimą, kurio metu, panaudojant modeliavimo technikos metodą, socialiniuose tinkluose *Twitter*, *Telegram* ir *Discord* per tris mėnesius buvo identifikuotos 50 mln. žinučių iš daugiau nei 7 mln. vartotojų. Vertinant

identifikuotas žinutes pastebėta, kad *Discord* socialiniame tinkle buvo tik vienas Ponzi schemos kanalo atvejais, tačiau *Telegram* socialiniame tinkle net 432 kanalo atvejais.

Galiausia, paskutinė nusikalstama veika kriptovaliutų rinkoje, kuri dažniausia buvo aptariama pasirinktoje mokslinėje literatūroje, yra pinigų plovimas (angl. *money laundering*). Šios nusikalstamos veikos vykdymo metu, nusikalstamą veiką vykdantys asmenys neteisėtai gautus pinigus perkelia per kriptovaliutų pinigines prieš išgrynindami lėšas kriptovaliutų biržoje, tokiu būdu panaikinant (arba iš esmės apsunkinant) galimybę atsekti iš kur buvo įgytos lėšos (Brenig, Ch., ir kt., 2015). Kriptovaliutų rinka yra palanki rinka pinigų plovimui vykdyti. Pinigų plovimo nusikalstama veika apima tris stadijas – įkėlimas, sluoksniavimas, integravimas. Kriptovaliutų rinka, dėl kriptovaliutoms būdingų savybių, sudaro sąlygas paslėpti nusikalstamos veikos žingsnius, todėl yra apsunkinamos sąlygos atsekti įgytus pinigus iki nusikalstamos veikos, iš kurios pinigai buvo įgyti. Be to, neteisėtai įgytas lėšas galima įvesti į kriptovaliutų rinką tiesiog įsigyjant kriptovaliutas, o kaip jau buvo aptarta, norint įsigyti kriptovaliutas nėra taikomi jokie reguliaciniai reikalavimai. Tokiu būdu neteisėtai įgyti pinigai yra įkeliami į finansų sistemą. Toliau, pasinaudojant kriptovaliutų rinka, neteisėtai įgytas lėšas galima pervesti iš vienos kriptovaliutų piniginės į kitą bei keisti vieną kriptovaliutą į kitą. Taip pat nusikalstamą veiką vykdantys asmenys gali pasinaudoti nereguliuojama kriptovaliutų birža bei atlikti valiutų keitimus (Teichmann, F. M. J., ir kt., 2020, Weber, M., ir kt., 2019). Panaudojant šiuos kriptovaliutų rinkos siūlomus būdus yra itin lengva įvesti į finansų rinką pinigus, įgytus iš nusikalstamos veikos ir galiausia juos padaryti tokius, jog atrodytų, kad jie atsirado iš teisėtų veiksmų. Mokslinėje literatūroje pastebima, kad kriptovaliutų rinkos panaudojimas pinigų plovimui yra dar apibūdinamas kaip kibernetinis plovimas (angl. *cyber-laundering*) arba bitkoino plovimas (angl. *Bitcoin-laundering*). Tokio tipo pinigų plovimas yra daug greitesnis ir pigesnis, palyginus su senuoju pinigų plovimo metodu. Inovatyvūs mokėjimo būdai, leidžia neteisėtais būdais įgytoms lėšoms judėti žymiai greičiau, didesniais atstumais ir apsunkina teisėsaugos darbą (Wronka, C., 2022). Mokslinėje literatūroje taip pat pastebimas svarbus aspektas, būdingas pinigų plovimui, pasinaudojant kriptovaliutų rinka, o būtent – du pagrindiniai kriptovaliutų plovimo komponentai – maišymas ir mainai (Möser, M., ir kt., 2013). Maišymas yra toks veiksmas, kuriuo siekiama atskirti kriptovaliutas nuo nusikalstamo šaltinio. Tuo tarpu mainų veiksmas yra toks veiksmas, kuriuo siekiama anonimiškai konvertuoti kriptovaliutas į išleistus pinigus. Taigi, šie komponentai sukuria sąlygas itin sklandžiam ir sėkmingam pinigų plovimui kriptovaliutų rinkoje. Fanusie, J.

Y., ir kt., (2018), 2013-2016 m. atlikto tyrimo metu, panaudodami *Elliptic* analizės įrankį, kuris naudoja blokų grandinės duomenis su patentuotu bitkoinų adresų rinkiniu, susietu su 102 žinomais neteisėtais subjektais. Autoriai išsiaiškino, kad „Tamsiojo interneto“ (angl. *darknet*) prekyvietės, tokios kaip *Silk Road* ar *AlphaBay*, buvo beveik visų nelegalių bitkoinų, išplautų naudojant konvertavimo paslaugas (keityklas, bankomatus, internetinių žaidimų svetaines), nustatytas šiame tyrime, šaltinis. Tyrime taip pat nustatyta, kad Europoje teikiamos konvertavimo paslaugos gavo didžiausią nelegalių bitkoinų dalį, lyginant su kitais regionais. Teichmann, F. M. J., (2021), atliko tyrimą, kurio metu, buvo išanalizuotos 153 apklausų anketos, siekiant, be kita ko, išsiaiškinti, ar apklaustieji (atitikties pareigūnai) mano, kad pinigų plovėjai persikelia į nereguliuojamus sektorius, siekiant apeiti pinigų plovimo prevencijos teisės aktų reguliavimus. Tyrimo rezultatai parodė, kad 74,5% respondentų sutiko, kad pinigų plovėjai persikelia į nereguliuojamus sektorius dėl finansų sektoriuje taikomų atitikties priemonių.

Apibendrintai galima daryti išvadą, kad kriptovaliutų rinka, dėl būdingų veikimo principų, savybių bei reguliavimo nebuvimo, yra akivaizdžiai itin pažeidžiama nusikalstamų veikų vykdymo aspektu. Nusikalstamą veiką vykdančiams asmenims yra sudaromos galimybės, pasinaudojant kriptovaliutų rinka, ne tik vykdyti nusikalstamas veikas, tačiau ir nebūti identifikuotiems. Taip pat svarbus momentas šiuo aspektu, kodėl, visgi, yra asmenų, kurie patenka į nusikalstamą veiką vykdančių asmenų schemas. Šiuo aspektu galima būtų paminėti, jog didelę įtaką turi asmens godumas, t. y. manymas, kad bus galima lengvai uždirbti dideles sumas pinigų, nepagalvojant apie tai, jog lengvos praturtėjimo galimybės yra neatsiejamoms su nusikalstamą veiką vykdančių asmenų neteisėtais ketinimais (Vasek, M., ir kt., 2015, Bartoletti, M., ir kt., 2021). Taip pat didelę įtaką turi finansinis budrumas (finansinio budrumo nebuvimas), t. y. veikti racionaliai, įvertinti visas egzistuojančias aplinkybes prieš pradėdant investuoti. Galiausiai yra svarbi patirtis ir (arba) patirties stoka (Vakilinia, I., 2022), kuri leidžia investuotojams lengviau atskirti potencialias nusikalstamas veikas nuo realių investicinių galimybių.

2. NUSIKALSTAMŲ VEIKŲ KRIPTOVALIUTŲ RINKOJE TYRIMO METODOLOGIJA

Ankstesniame darbo skyriuje buvo apžvelgiama ir analizuojama mokslinė literatūra, susijusi su nusikalstamomis veikomis kriptovaliutų rinkoje. Nagrinėjant mokslinę literatūrą buvo analizuojami nusikalstamų veikų kriptovaliutų rinkoje teoriniai aspektai, reguliacinė įtaka kriptovaliutų rinkai, identifikuojamos nusikalstamos veikos, pasireiškiančios kriptovaliutų rinkoje, taip pat analizuojami nusikalstamų veikų pasireiškimo kriptovaliutų rinkoje atvejai ir jų įtaka šios rinkos vartotojams.

Išanalizavus mokslinę literatūrą galima teigti, kad didžioji mokslinės literatūros dalis skiria dėmesį siauresnio pobūdžio tyrimams, susijusiems su nusikalstamomis veikomis kriptovaliutų rinkoje. Tai reiškia, kad nemaža dalis mokslinės literatūros daugiau dėmesio skiria vienai arba dviem nusikalstamoms veikoms kriptovaliutų tyrime ir jų išanalizavimui (pvz., Nizzoli, L., ir kt., 2020, Morgia, L. M., ir kt., 2021, Dhawan, A., ir kt., 2021, Chen, W., ir kt., 2018, Fanusie, J. Y., ir kt., 2018). Taip pat didelį dėmesį sutelkia būtent į pačios nusikalstamos veikos kriptovaliutų rinkoje nustatytą ir investuotojų patirtą nuostolį (pvz., Nizzoli, L., ir kt., 2020, Vasek, M., ir kt., 2019, Dhawan, A., ir kt., 2021). Tačiau, galima teigti, kad ne vien šie keli identifikuoti parametrai yra svarbūs, analizuojant nusikalstamas veikas kriptovaliutų rinkoje. Visgi, yra svarbu atkreipti dėmesį ir į kriptovaliutų piniginių adresų aktyvumą, rinkos vartotojų dėmesio pritraukimą, kriptovaliutų judėjimą kriptovaliutų piniginėse ir kitus parametrus. Taigi, siekiant nustatyti kriptovaliutų rinkoje pasireiškiančias nusikalstamas veikas bei išanalizuoti su tokio pobūdžio nusikalstamomis veikomis susijusius kitus neatsiejamus parametrus, yra svarbu atlikti tyrimą, pirmiausia, identifikuojant kriptovaliutų piniginių adresus, kuriuos panaudojant yra vykdomos nusikalstamos veikos kriptovaliutų rinkoje. Identifikavus tokio pobūdžio kriptovaliutų piniginių adresus būtų galima identifikuoti ne tik potencialias nusikalstamas veikas, tačiau ir kitus svarbius, su kriptovaliutų piniginių adresais ir investuotojais, o kartu ir su nusikalstamomis veikomis kriptovaliutų rinkoje, susijusius parametrus.

2.1. Tyrimo tikslas, uždaviniai ir metodai

Darbo tikslas. Atlikti nusikalstamų veikų kriptovaliutų rinkoje tyrimą.

Darbo uždaviniai.

1. Atlikti mokslinės literatūros analizę nusikalstamų veikų kriptovaliutų rinkoje aspektu.
2. Sudaryti nusikalstamų veikų kriptovaliutų rinkoje tyrimo metodologiją.
3. Atlikti nusikalstamų veikų kriptovaliutų rinkoje tyrimą, išanalizuojant tyrimo metu nustatytas charakteristikas nusikalstamų veikų kriptovaliutų rinkoje aspektu ir pateikti gautus tyrimo rezultatus.

Tyrimo metodai. Tyrimo metu buvo panaudoti duomenų rinkimo, aprašomosios statistikos, Pearson koreliacinės, paprastosios regresijos, Chi-kvadrato, statistinių duomenų analizės, tyrimo rezultatų analizės, apibendrinimo ir vertinimo metodai.

Panaudojant duomenų rinkimo metodą tyrimo metu iš dviejų internetinių tinklapių – BitcoinAbuse.com ir BlockChain.com – rankiniu būdu buvo renkami tyrimui reikšmingi duomenys. Taikant aprašomosios statistikos metodą buvo atliktas duomenų klasifikavimas ir grupavimas, apibendrintų statistinių rodiklių (minimumas, maksimumas, mediana, 1-asis bei 3-iasis kvartiliai (Q1 ir Q3), vidurkis, moda) vertinimas (Čekanavičius, V., ir kt., 2002). Taikant statistinius tyrimo būdus – Pearson koreliacija ir paprastąją regresiją – buvo siekiama nustatyti, ar egzistuoja tam tikras ryšys tarp tyrimo metu surinktų duomenų bei patikrinti ryšio stiprumą ir statistinį reikšmingumą (Bartosevičienė, V., 2010). O būtent – Pearson koreliacijos metodu buvo siekiama nustatyti, ar egzistuoja statistiškai reikšmingas ryšys tarp kintamųjų „Kiek kartų buvo pateiktas pranešimas“ ir „Dienų skaičius tarp pirmo ir paskutinio pranešimo“ bei „Kriptovaliutų piniginių adresų skaičius“ ir „Kartais, kiek buvo pranešta apie nusikalstamą veiką“. Tokiu būdu buvo siekiama nustatyti, ar egzistuoja ryšys tarp pateikiamų pranešimų skaičiaus ir dienų skaičiaus nuo pirmojo ir paskutinio pranešimo ir ar yra ryšys tarp to, jog padidėjus kriptovaliutų piniginių skaičiui gali padidėti pranešimų skaičius tarp kriptovaliutų piniginių adresų, kuriuos panaudojant vykdomos nusikalstamos veikos. Taip pat buvo naudojamas Chi-kvadrato metodas, siekiant išanalizuoti, ar didelė dalis su kriptovaliutomis susijusių pranešimų apie nusikalstamas veikas kriptovaliutų rinkoje yra susiję su nedidele dalimi kriptovaliutų adresais. Galiausia, buvo atliktas gautų rezultatų apibendrinimas ir vertinimas bei atitinkamai daromos išvados.

Tyrimo metodai buvo pasirinkti atsižvelgiant į tai, jog literatūros analizės metu buvo nustatyta, kad autoriai, analizuodami nusikalstamas veikas kriptovaliutų rinkoje dažnai pasitelkdavo būtent tokio tipo tyrimo metodus. Pavyzdžiui, Chen, W. L., ir kt., 2018, naudojo koreliacijos ir regresijos metodus siekiant nustatyti ryšį tarp Ethereum blokų grandinėje vykdomų Ponzi schemas; Dhawan, A., ir kt., 2021, tyrimo metu naudojo regresijos metodą, siekiant iširti *Pump* ir *dump* nusikalstamos veikos ryšį su kriptovaliutų rinka; Foley, S., ir kt., 2018, tyrimo metu naudojo regresijos metodą analizuojant ryšį tarp nelegalių veiklų finansavimo, panaudojant kriptovaliutas; Kerr, D. S., ir kt., 2023, tyrimo metu naudojo koreliacijos ir regresijos metodus, siekiant išanalizuoti sukčiavimo atvejų ryšį kriptovaliutų rinkoje; Teichmann, F. M. J., ir kt., 2020, tyrimo metu, panaudojant koreliacijos ir regresijos metodus, tyrė pinigų plovimo nusikalstamą veiką kriptovaliutų rinkoje ir jų ryšius su kriptovaliutų rinka; Vasek, M., 2019, tyrimo metu naudojo koreliacijos ir regresijos metodus, siekiant analizuoti Ponzi schemą kriptovaliutų rinkoje, identifikuojant ryšį tarp galimai nusikalstamą veiką vykdančių asmenų ir jų galimai vykdomų nusikalstamų veikų. Roppelt, J. C., 2019, naudojo aprašomosios statistikos metodą, siekiant aprašyti ir paaiškinti savanaudišką kasybą kriptovaliutų rinkoje; Vakilinia, I., 2022, naudojo aprašomąją statistiką siekiant apibūdinti dovanų įteikimo sukčiavimą kriptovaliutų rinkoje. Taigi, iš mokslinės literatūros analizės matyti, kad minėti metodai yra naudojami, siekiant analizuoti nusikalstamas veikas kriptovaliutų rinkoje bei jų įtaką rinkos vartotojams.

Duomenų analizės metodai. Rankiniu būdu surinkti duomenys analizuoti naudojantis *Microsoft Excel* programa.

2.2. Tyrimo modelis ir hipotezės

Tyrimo organizavimas. Tyrimui reikšmingi duomenys buvo renkami iš dviejų skirtingų internetinių svetainių – BitcoinAbuse.com ir Blockchain.com laikotarpyje nuo 2023 m. kovo 1 d. iki 2023 m. kovo 31 d.

BitcoinAbuse.com yra vieša platforma, kurioje kriptovaliutų rinkos vartotojai gali pateikti pranešimus apie kriptovaliutų piniginių adresus, kurie siejami su nusikalstamų veikų vykdymu kriptovaliutų rinkoje. BitcoinAbuse.com pateikiami duomenys, susiję su kriptovaliutų piniginių adresais, pateiktų pranešimų skaičiumi, nusikalstama veika, laikotarpiais, kada buvo pirmą kartą pateiktas pranešimas ir kada buvo pateiktas paskutinį kartą pranešimas (8 lentelė).

8 lentelė

BitcoinAbuse.com internetiniame tinklapyje tyrimo metu identifikuoti parametrai apie nusikalstamas veikas kriptovaliutų rinkoje

Parametras
Kriptovaliutų piniginės adresas
Kartai, kiek buvo pateikti pranešimai, kad panaudojant kriptovaliutų piniginės adresą yra galimai vykdoma nusikalstama veika
Nusikalstama veika
Data, kada pirmą kartą pateiktas pranešimas apie kriptovaliutų piniginės adresą
Data, kada paskutinį kartą pateiktas pranešimas apie kriptovaliutų piniginės adresą

Šaltinis: Sudaryta autorės, remiantis BitcoinAbuse.com internetinio tinklapio duomenimis.

Duomenys iš BitcoinAbuse.com internetinio tinklapio yra duomenys, kuriuos kriptovaliutų rinkos vartotojai pateikia apie identifikuotus kriptovaliutų piniginių adresus, kurie galimai susiję su nusikalstamų veikų vykdymu kriptovaliutų rinkoje ir ši informacija savarankiškai atrinkta iš asmenų, pateikusių pranešimus BitcoinAbuse.com imties, kuri nebūtinai reprezentuoja visus įmanomus nuo nusikalstamų veikų kriptovaliutų rinkoje nukentėjusius asmenis. Tai reiškia, jog, tikėtina, kad asmenys, pateikę pranešimus, yra tokie, kurie dažniau naudojami internetinėmis platformomis, skirtomis dalintis informacija. Visgi, BitcoinAbuse.com pateikiama informacija yra laikoma vertingu informacijos šaltiniu, leidžiančiu suprasti nusikalstamų veikų kriptovaliutų rinkoje koncentraciją ir charakteristikas. Nepaisant to, kad galima reikšti teiginius dėl tyrimo metu surinktos informacijos patikimumo, kadangi ne visi galimai nuo nusikalstamos veikos kriptovaliutų rinkoje nukentėję asmenys pateikia pranešimus BitcoinAbuse.com internetiniame tinklapyje, visgi tyrimo metu nebuvo nustatyta jokių objektyvių duomenų, kurie leistų konstatuoti, kad imtis, kurioje yra surinkti duomenys, gali būti nepilnos apimties arba netikslūs. Taip pat tai neturėtų turėti didelės įtakos kriptovaliutų piniginių adresų, susijusių su nusikalstamomis veikomis kriptovaliutų rinkoje, informacijos patikimumui, kuri yra surinkta tyrimo metu. Šiuo aspektu reikėtų atkreipti dėmesį, kad yra daugiau internetinių tinklapių, kurie kaupia pranešimus apie galimas nusikalstamas veikas kriptovaliutų rinkoje, kaip kad, pavyzdžiui, *Bitcoin Who's Who*, *CryptoScamDB*, *ScamAlert* ir *Bitcoin.org*. Tačiau šiuose internetiniuose tinklapiuose pateikiama informacija yra ribota, todėl tyrimui šie internetiniai tinklapiai nebuvo tinkami.

Be to BitcoinAbuse.com internetinis tinklapis yra naudojamas tyrimuose kaip patikimas šaltinis, siekiant nustatyti nusikalstamas veikas kriptovaliutų rinkoje įvairiais aspektais. Kaip

pavyzdys paminėtini Azani ir kt., (2020), kurie tyrimo metu naudojo iš BitcoinAbuse.com surinktus duomenis, siekiant patikrinti interneto svetainėje pateiktus pranešimus apie kriptovaliutų piniginių adresų sąsajas su Hamas organizacija. Taip pat paminėtina ir Xia, ir kt., (2020), kurie, panaudojant, be kita ko, BitcoinAbuse.com internetinio tinklapio duomenis analizavo su COVID-19 susijusių sukčiavimų atvejus kriptovaliutų rinkoje.

BitcoinAbuse.com internetinėje svetainėje nuo nusikalstamos veikos nukentėję asmenys gali pateikti pranešimą apie kriptovaliutų pinigines adresą, kuris yra susijęs su atitinkamos nusikalstamos veikos vykdymu. Pildant pranešimą apie kriptovaliutų piniginių adresus, kurie susiję su nusikalstamų veikų kriptovaliutų rinkoje vykdymu, asmuo pranešime turi nurodyti, kokia konkreiti nusikalstama veika yra vykdoma pasitelkiant kriptovaliutų pinigines adresą; kiek lėšų asmuo neteko (USD); kriptovaliutos pinigines adresą; plačiau aprašyti susiklosčiusią situaciją.

Tyrimo metu iš BitcoinAbuse.com buvo identifikuotos šios nusikalstamos veikos kriptovaliutų rinkoje, kurios nebuvo aptariamoms mokslinėje literatūroje. Toliau prie pateikiamų nusikalstamų veikų kriptovaliutų rinkoje pateikiamas nusikalstamos veikos kriptovaliutų rinkoje aprašymas, suformuotas pagal BitcoinAbuse.com pranešimuose pateikiamus apibūdinimus apie vykdomas nusikalstamas veikas kriptovaliutų rinkoje, panaudojant atitinkamų kriptovaliutų piniginių adresus:

- a. Teroristų finansavimo nusikalstama veika – tai yra tokia nusikalstama veika kriptovaliutų rinkoje, kurios metu yra įgyjamos kriptovaliutos, vėliau panaudojant jas remti teroristines organizacijas ir (ar) vykdyti teroristinius veiksmus.
- b. Seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika – tai yra tokia nusikalstama veika kriptovaliutų rinkoje, kurios metu yra įgyjami aukos asmeninio turinio vaizdo įrašai ir (ar) nuotraukos arba yra apsimetama, kad tokia medžiaga yra įgyta, bei reikalaujama į kriptovaliutų pinigines adresą pervesti atitinkamą kiekį kriptovaliutų, kitu atveju tokia įgyta medžiaga bus paviėšinta internete.
- c. Meilės sukčiavimo nusikalstama veika – tai yra tokia nusikalstama veika, kurios metu asmuo ir kitas asmuo – auka – sukuria tam tikrus artimus santykius, kurių metu yra palenkiamas aukos valia bei siekiama iš aukos įgyti kriptovaliutų, neturint ketinimo tęsti artimų santykių su auka.
- d. Kriptovaliutos investavimo sukčiavimas – tai yra tokia nusikalstama veika, kurios metu asmuo pritraukia kitą asmenį (auką) neva investuoti į kriptovaliutų rinką

pastarojo pagalba, tačiau auka patenka į neteisėtas schemas, kurių metu praranda kriptovaliutas arba asmuo įgyja kriptovaliutų iš aukos, neva tai ketindamas padėti jas investuoti, tačiau neturėdamas tikslo iš tiesų jas investuoti.

Tyrimui reikšmingi duomenys buvo renkami rankiniu būdu kiekvieną dieną, visą anksčiau nurodytą tyrimo laikotarpį. Iš viso tyrimo laikotarpio metu buvo identifikuoti 1 174 kriptovaliutų piniginių adresai apie kuriuos buvo pateikti pranešimai BitcoinAbuse.com internetiniame tinklapyje. Iš identifikuotų 1 174 kriptovaliutų piniginių buvo atrinkti nepasikartojantys kriptovaliutų piniginių adresai ir iš viso buvo nustatyti 162 nepasikartojantys kriptovaliutų piniginių adresai. Identifikavus nepasikartojančius kriptovaliutų piniginių adresus buvo surinktos kriptovaliutų piniginių adresams būdingos charakteristikos tyrimo rezultatų apibendrinimui (Priedas Nr. 3).

Tyrimo metu identifikuoti kriptovaliutų piniginių adresai buvo tikrinami BlockChain.com internetinėje svetainėje. Šioje interneto svetainėje yra renkama informacija, susijusi su kriptovaliutų piniginių adresų atliktomis operacijomis. Taigi, tyrimo metu buvo atrinktos visos BlockChain.com pateikiamos charakteristikos kiekvienam identifikuotam kriptovaliutų piniginių adresui (Priedas Nr. 4; 9 lentelė).

9 lentelė

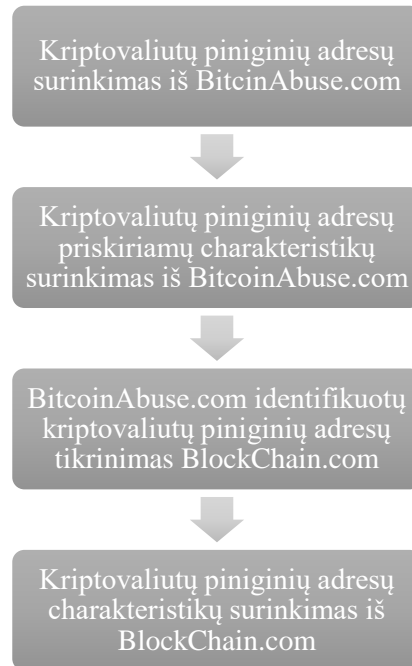
BlockChain.com internetiniame tinklapyje tyrimo metu identifikuoti duomenų parametrai apie kriptovaliutų piniginių adresus

Parametras
Kriptovaliutų piniginių adresai
Operacijų skaičius, atliktas kriptovaliutų piniginėje
Lėšos, gautos iš nusikalstamos veikos (BTC (USD))
Išsiųstos lėšos iš kriptovaliutų piniginės (BTC (USD))
2023 m. kovo 31 dienos balansas kriptovaliutų piniginėje (BTC (USD))

Šaltinis: Sudaryta autorės, remiantis BlockChain.com.

7 paveikslas

Tyrimo struktūra



Šaltinis: Sudaryta autorės.

Atrinkti duomenys iš BitcoinAbuse.com ir BlockChain.com buvo susisteminti ir paruošti tyrimo rezultatų apibendrinimui.

Išsikeltos hipotezės. Prieš atliekant tyrimą buvo išsikeltos ir tyrimo rezultatų apibendrinimo metu tikrinamos hipotezės. Hipotezės išsikeltos ir pasirinktos atsižvelgiant į mokslinės literatūros analizės metu pastebėtus tam tikrus pasikartojančius teiginius. Siekiant šiuos teiginius patikrinti, buvo išsikeltos minimos hipotezės ir tikrinama, kaip mokslinės literatūros analizės metu pastebėti teiginiai atsispindi tyrimo metu surinktų duomenų visete (10 lentelė).

10 lentelė

Išsikeltos hipotezės

Nr.	Hipotezė	Autoriai
1 hipotezė	<p>H0: Vertinant nusikalstamų veikų apimtį kriptovaliutų rinkoje labiau tikėtina, kad mokslinėje literatūroje minimų nusikalstamų veikų apimtis yra lygi faktinei nusikalstamų veikų apimčiai kriptovaliutų rinkoje.</p> <p>H1: Vertinant nusikalstamų veikų apimtį kriptovaliutų rinkoje labiau tikėtina, kad mokslinėje literatūroje minimų nusikalstamų veikų apimtis skiriasi nuo faktinės nusikalstamų veikų apimties kriptovaliutų rinkoje.</p>	Trozze1, A., ir kt., (2022).
2 hipotezė	<p>H0: Vertinant tyrimo metu identifikuotų kriptovaliutų piniginių adresus labiau tikėtina, kad jie nėra siejami su nusikalstamomis veikomis kriptovaliutų rinkoje, kurias vykdančiam apgaulės būdu (suklaidinant) neteisėtai įgyti kriptovaliutų.</p> <p>H1: Vertinant tyrimo metu identifikuotų kriptovaliutų piniginių adresus labiau tikėtina, kad jie yra siejami su nusikalstamomis veikomis kriptovaliutų rinkoje, kurias vykdančiam apgaulės būdu (suklaidinant) neteisėtai įgyti kriptovaliutų.</p>	Trozze1, A., ir kt., (2022), Kerr, S. D., ir kt., (2023).
3 hipotezė	<p>H0: Vertinant tyrimo metu identifikuotą nusikalstamą veiką, labiau tikėtina, kad didelė dalis su kriptovaliutomis susijusių elektroninių nusikaltimų yra siejama su nedidele dalimi kriptovaliutų piniginių adresų.</p> <p>H1: Vertinant tyrimo metu identifikuotą nusikalstamą veiką, labiau tikėtina, kad didelė dalis su kriptovaliutomis susijusių elektroninių nusikaltimų nėra siejama su nedidele dalimi kriptovaliutų piniginių adresų.</p>	Christin, N., (2013), Fleder, M., ir kt., (2015).
4 hipotezė	<p>H0: Vertinant tyrimo metu identifikuotus kriptovaliutų piniginių adresus, labiau tikėtina, kad tyrimo pabaigos dienai kriptovaliutų piniginių adresai, daugiausia neteisėtai įgijusių kriptovaliutų iš galimai nusikalstamos veikos, bus tokie, kurie vykdė dažniausia kriptovaliutų piniginių adresuose identifikuotą nusikalstamą veiką.</p> <p>H1: Vertinant tyrimo metu identifikuotus kriptovaliutų piniginių adresus, labiau tikėtina, kad tyrimo pabaigos dienai kriptovaliutų piniginių adresai, daugiausia neteisėtai įgijusių kriptovaliutų iš galimai nusikalstamos veikos, bus tokie, kurie nevykdė dažniausia kriptovaliutų piniginių adresuose identifikuotų nusikalstamų veikų.</p>	Christin, N., (2013), Fleder, M., ir kt., (2015).

Šaltinis: Sudaryta autorės.

1 hipotezė – Hipotezė tikrinama pasitelkiant statistinių duomenų analizę, kurios metu analizuojami tyrimo metu gauti rezultatai bei tyrimo metu identifikuotų nusikalstamų veikų skaičius ir šio skaičiaus atitiktis su mokslinės literatūros analizės metu nustatytais nusikalstamomis veikomis.

2 hipotezė – Hipotezė tikrinama pasitelkiant statistinių duomenų analizę, kurios metu analizuojami ir tyrimo metu gauti rezultatai apie sukčiavimo nusikalstamos veikos pasireiškimo dažnumą kriptovaliutų rinkoje.

3 hipotezė – Hipotezė tikrinama išskaičiuojant TOP1 kriptovaliutų piniginių adresų skaičių, atliekamas Chi-kvadrato skaičiavimas, Pearson koreliacija ir paprasta regresija.

4 hipotezė – Hipotezė tikrinama pasitelkiant statistinių duomenų analizę, kurios metu yra analizuojama ir vertinami gauti tyrimo rezultatai bei tyrimo metu nustatytų kriptovaliutų piniginių adresų skaičius, siejant su nustatytais nusikalstamomis veikomis.

3. NUSIKALSTAMŲ VEIKŲ KRIPTOVALIUTŲ RINKOJE TYRIMO REZULTATAI

Tyrimo metu iš dviejų internetinių tinklapių – BitcoinAbuse.com ir BlockChain.com – rankiniu būdu buvo surinkti duomenys laikotarpyje nuo 2023 m. kovo 1 d. iki 2023 m. kovo 31 d. Surinkti duomenys yra susiję su kriptovaliutų piniginių adresais, kuriuos panaudojant buvo vykdomos nusikalstamos veikos kriptovaliutų rinkoje, siekiant neteisėtai iš rinkos investuotojų įgyti kriptovaliutas. Bendra duomenų apie kriptovaliutų piniginių adresus, kurie buvo surinkti iš BitcoinAbuse.com ir BlockChain.com internetinių tinklapių, suvestinės statistika yra pavaizduota 11 lentelėje. Šioje lentelėje pateikti statistiniai duomenys atskleidžia nusikalstamų veikų kriptovaliutų rinkoje požymius, identifikuotus tyrimo laikotarpyje. Analizuojant ir vertinant lentelėje pateiktus duomenis galima daryti apibendrintą išvadą, kad pakankamai didelė dalis kriptovaliutų piniginių adresų sutelkia pakankamai mažai kartų, kiek buvo pateiktas pranešimas, dienų skaičius, nusikalstamų veikų rūšių, operacijų skaičius, lėšų skaičius bei galutinio balanso skaičiaus vertes. Tuo tarpu maža kriptovaliutų piniginių adresų dalis sukaupia dideles paminėtų kintamųjų (charakteristikos) vertes.

11 lentelė

Duomenų apie kriptovaliutų piniginių adresus iš BitcoinAbuse.com ir BlockChain.com suvestinė

Charakteristika	Mažiausia vertė	Pirma kvartilė	Mediana	Vidurkis	Trečia kvartilė	Didžiausia vertė
Kartai, kiek buvo pateiktas pranešimas	1	3	6	45.68	19	2531
Skaičius nusikalstamų veikų, priskirtinų vienam kriptovaliutų piniginės adresui	1	1	1	1.31	1	2
Dienų skaičius nuo pirmo pranešimo apie kriptovaliutos piniginę ir paskutinio pranešimo	0	0	6	48.57	28	955
Operacijų skaičius, atliktas kriptovaliutų piniginėje (iš viso)	0	0	2	6079.29	12	805058
Lėšos, gautos iš galimai nusikalstamos veikos (iš viso) (BTC)	0	0	0.0074	243518.5	0.1927	38885199.3
Išsiųstos kriptovaliutos iš adreso (BTC)	0	0	0.003	244864.11	0.179	75982.33
Paskutinės tyrimo dienos BTC balansas kriptovaliutų piniginėje	0	0	0	364.53	0	57822.56

Šaltinis: Sudaryta autorės pagal BitcoinAbuse.com ir Blockchain.com duomenis.

3.1. BitcoinAbuse.com identifikuotų charakteristikų rezultatai

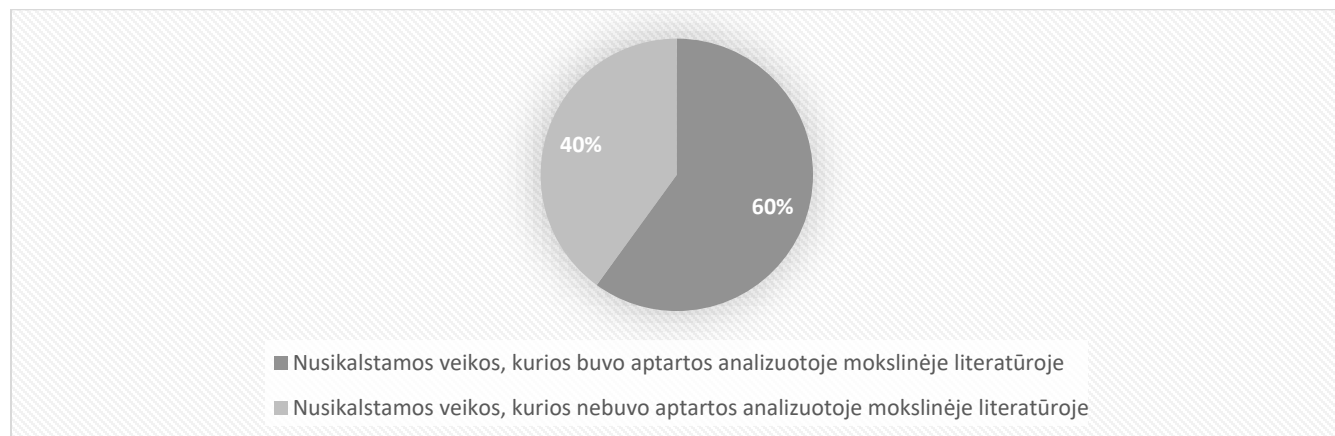
Analizuojant tyrimo metu surinktų duomenų visetą iš internetinio tinklapio BitcoinAbuse.com (Priedas Nr. 3) galima daryti išvadą, kad iš BitcoinAbuse.com internetinio tinklapio tyrimo metu buvo identifikuotos 5 charakteristikos, kurios naudotinos tyrimo rezultatų pateikimui (8 lentelė).

3.1.1. Kriptovaliutų piniginių adresų ir nusikalstamų veikų charakteristikų rezultatai

Tyrimo metu, atrinkus nepasikartojančius kriptovaliutų piniginių adresus, nustatyta, kad per tiriamąjį laikotarpį internetinėje svetainėje BitcoinAbuse.com buvo pateikti pranešimai iš viso apie 162 nepasikartojančius kriptovaliutų piniginių adresus, kurie buvo panaudojami nusikalstamų veikų kriptovaliutų rinkoje vykdyme. Iš nustatytų skirtingų 162 kriptovaliutų piniginių adresų buvo identifikuota 10 skirtingų nusikalstamų veikų kriptovaliutų rinkoje. Tyrimo metu surinkti duomenys leidžia konstatuoti, kad iš tyrimo metu identifikuotų 10 nusikalstamų veikų kriptovaliutų rinkoje, kurios buvo siejamos su nustatytais kriptovaliutų piniginių adresais, 4 nusikalstamos veikos kriptovaliutų rinkoje nebuvo identifikuotos mokslinės literatūros analizės metu (12 lentelė). Tai sudaro 40% tyrimo metu identifikuotų nusikalstamų veikų kriptovaliutų rinkoje (8 paveikslas).

8 paveikslas

Santykinis nusikalstamų veikų kriptovaliutų rinkoje analizuotų ir neanalizuotų mokslinėje literatūroje palyginimas



Šaltinis: Sudaryta autorės pagal BitcoinAbuse.com duomenis.

12 lentelė

Nusikalstamos veikos, identifikuotos tiriamuoju laikotarpiu BitcoinAbuse.com internetiniame tinklapyje

Tyrimo metu nustatytos nusikalstamos veikos pavadinimas	Angliška reikšmė	Numeris lentelėje pagal Priedus Nr. 1 ir Nr. 2
Kenkėjiškų programų paskleidimo nusikalstama veika	<i>Malware scam</i>	Nr. 10
Teroristų finansavimo nusikalstama veika	<i>Terrorist financing</i>	-
Žvejybos nusikalstama veika	<i>Phishing</i>	Nr. 12
Seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika	<i>Sextortion</i>	-
Avansinio mokėjimo sukčiavimo nusikalstama veika	<i>Advance-fee scam</i>	Nr. 5
Meilės sukčiavimo nusikalstama veika		-
Dovanų įteikimo sukčiavimo nusikalstama veika	<i>Giveaway scam</i>	Nr. 6
Apgaulingos piniginės nusikalstama veika	<i>Scam wallet</i>	Nr. 3
Kripto valiutos investavimo sukčiavimas	<i>Crypto investment scam</i>	-
Aukojimo sukčiavimo nusikalstama veika	<i>Donation scam</i>	Nr. 2

Šaltinis: Sudaryta autorės pagal BitcoinAbuse.com duomenis.

Ši išvada reiškia, kad kriptovaliutų rinkoje yra vykdomos, be kita ko, ir tokios nusikalstamos veikos investuotojų atžvilgiu, kurios mokslinėje literatūroje yra arba apskritai neaptariamoms, arba aptariamoms itin nedidele apimtimi. Vadinasi, šiuo atveju turime pagrįstą pagrindą atmesti 1 hipotezės H0 ir priimti H1, kuri leidžia daryti išvadą, kad kriptovaliutų rinkoje galimai vykdomos nusikalstamos veikos investuotojų atžvilgiu nėra visa apimtimi panašios (tokios pačios), kokios yra aptariamoms mokslinėje literatūroje. Tai reiškia, kad kriptovaliutų rinkoje veikiantiems investuotojams yra rizika susidurti su tokiomis nusikalstamomis veikomis apie kurias investuotojai gali apskritai nežinoti. Tai reikštų, kad investuotojams atsiranda rizika, veikiant kriptovaliutų rinkoje, susidurti su tokiomis nusikalstamomis veikomis apie kurias jie neturėtų pakankamai žinių, o tai lemtų aplinkybę, kad investuotojams atsiranda rizika nesugebėti nustatyti atvejų, kaip prieš juos gali būti naudojamos nusikalstamos veikos, siekiant įgyti kriptovaliutas ir atitinkamai padidėja rizika netekti turimų investicijų.

Šiuo aspektu vertėtų paminėti, kad taip kaip nusikalstama veika kriptovaliutų rinkoje, kuri yra siejama su atitinkamu kriptovaliutų piniginės adresu, yra įvardinama teikiant pranešimą BitcoinAbuse.com internetiniame tinklapyje, iš esmės nusprendžia pranešimą teikiantis asmuo, t. y. kriptovaliutų rinkos vartotojas (investuotojas). Todėl tokiu atveju išlieka galimybė, kad kai kuriais atvejais kvalifikuojant nusikalstamą veiką kriptovaliutų rinkoje gali būti tam tikrų (nežymių) kvalifikavimo klaidų. Tačiau tyrimo metu nebuvo surinkta jokių objektyvių duomenų, kurie leistų konstatuoti, kad BitcoinAbuse.com internetiniame tinklapyje pranešimus teikiantys asmenys iš esmės netinkamai kvalifikuodavo nusikalstamas veikas kriptovaliutų rinkoje ir kriptovaliutų piniginių adresams priskirdavo netinkamas nusikalstamas veikas. Pažymėtina ir tai, kad kriptovaliutų piniginių adresai, kurie sulaukdavo daugiau nei vieno pranešimo BitcoinAbuse.com internetinėje svetainėje iš esmės turėdavo tokius pačius nusikalstamų veikų kriptovaliutų rinkoje kvalifikavimus iš visų pranešimus pateikusių asmenų.

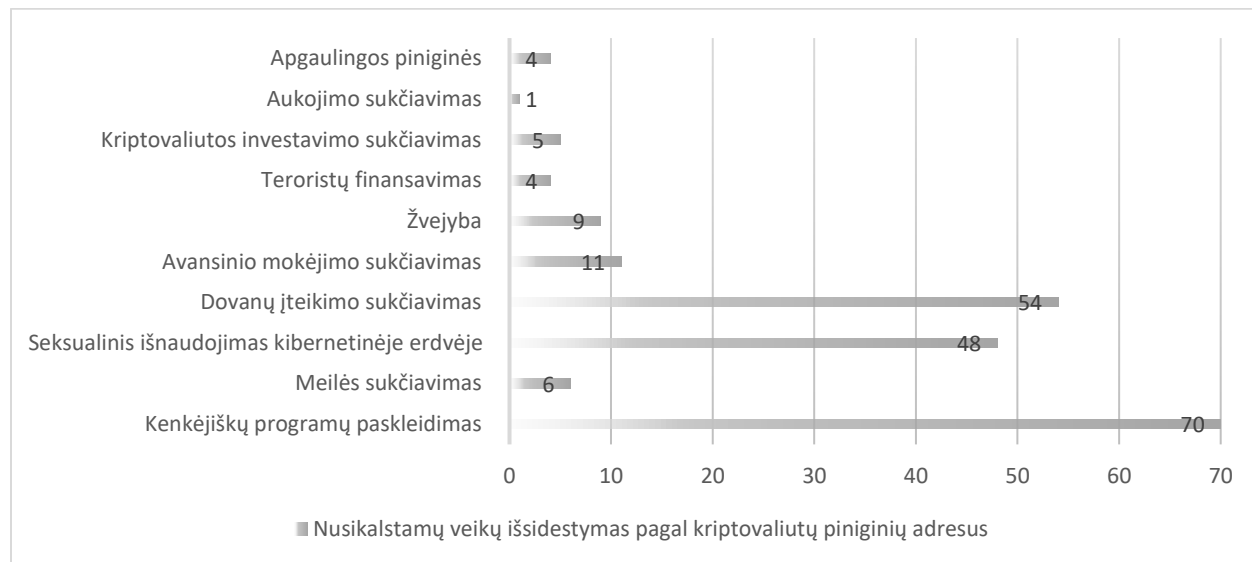
Analizuojant tyrimo metu identifikuotas nusikalstamas veikas kriptovaliutų rinkoje, kurios buvo siejamos su tyrimo metu nustatytais kriptovaliutų piniginių adresais, taip pat atkreiptinas dėmesys, kad tam tikri kriptovaliutų piniginių adresai buvo siejami su daugiau nei viena nusikalstama veika. Tai reiškia, kad tyrimo metu buvo identifikuoti kriptovaliutų piniginių adresai, kurie buvo tuo pačiu metu siejami su bent dvejomis skirtingomis nusikalstamų veikų kriptovaliutų rinkoje vykdymu (11 lentelė). Išanalizavus ir apibendrinus tyrimo metu surinktus duomenis konstatuotina, kad 51 kriptovaliutų piniginių adresas yra siejamas su daugiau nei vienos nusikalstamos veikos kriptovaliutų rinkoje vykdymu tuo pačiu metu. Tai reiškia, kad 31.48% visų tyrimo metu identifikuotų kriptovaliutų piniginių adresų siejama su daugiau nei vienos nusikalstamos veikos kriptovaliutų rinkoje vykdymu tuo pačiu metu. Vertinant šiuos rezultatus iš investuotojo perspektyvos, galima daryti išvadą, kad esant tokiai situacijai, investuotojams padidėja rizika patirti nuostolius veikiant kriptovaliutų rinkoje.

Analizuojant tyrimo metu nustatytą nusikalstamų veikų kriptovaliutų rinkoje paplitimą identifikuotose kriptovaliutų piniginių adresuose matoma, kad iš tyrimo metu surinktų duomenų nustatyti 70 skirtingi kriptovaliutų piniginių adresai, kuriuos panaudojant buvo vykdoma kenkėjiškų programų paskleidimo nusikalstama veika, tokiu būdu siekiant neteisėtai įgyti kriptovaliutas (9 paveikslas, 13 lentelė). Kita nusikalstama veika kriptovaliutų rinkoje, kuri buvo siejama su dideliu kriptovaliutų piniginių adresų skaičiumi yra dovanų įteikimo sukčiavimu nusikalstama veika. Ši nusikalstama veika buvo identifikuota 54 skirtingose kriptovaliutų

piniginių adresuose. Galiausia, matyti, kad seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika taip pat pasižymi pakankamai nemažu paplitimu kriptovaliutų piniginių adresuose, kadangi net 48 kriptovaliutų piniginių adresai yra siejami su šia nusikalstama veika. Paminėtos trys nusikalstamos veikos kriptovaliutų rinkoje, kurias vykdant buvo siekiama neteisėtai įgyti kriptovaliutų, išsiskiria savo skaičiumi ir bendrai sudaro net 81.13% nusikalstamų veikų visuose tyrimo metu nustatytuose kriptovaliutų piniginių adresuose ir kiekviena atskirai viršijo 20%. Analizuojant likusias tyrimo metu identifikuotas nusikalstamas veikas kriptovaliutų rinkoje, kurios buvo vykdomos panaudojant kriptovaliutų piniginių adresus, matoma, kad šios nusikalstamos veikos buvo vykdomos pasitelkiant kur kas mažesnę kriptovaliutų piniginių adresų skaičių. O būtent – apskaičiavus likusių nustatytų nusikalstamų veikų kriptovaliutų rinkoje procentinę dalį matyti, kad likusios nusikalstamos veikos kriptovaliutų rinkoje iš viso buvo siejamos su 18.87% kriptovaliutų piniginių adresų ir kiekviena atskirai neviršijo 6%.

9 paveikslas

Nusikalstamų veikų kriptovaliutų rinkoje išsidėstymas pagal kriptovaliutų piniginių adresus



Šaltinis. Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

13 lentelė

Duomenys apie nusikalstamų veikų dažnumą ir jų pasiskirstymą kriptovaliutų piniginių adresų atžvilgiu

Nusikalstama veika	Kriptovaliutų piniginių adresų skaičius	Procentinė kriptovaliutų piniginių adresų skaičiaus dalis
Kenkėjiškų programų paskleidimo nusikalstama veika	70	33.02%
Dovanų įteikimo sukčiavimo nusikalstama veika	54	25.47%
Seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika	48	22.64%
Avansinio mokėjimo sukčiavimo nusikalstama veika	11	5.19%
Žvejybos nusikalstama veika	9	4.25%
Meilės sukčiavimo nusikalstama veika	6	2.83%
Kriptovaliutų investavimo sukčiavimo nusikalstama veika	5	2.36%
Apgaulingos piniginės nusikalstama veika	4	1.89%
Teroristų finansavimo nusikalstama veika	4	1.61%
Aukojimo sukčiavimo nusikalstama veika	1	0.47%
Iš viso:	212	100%

Šaltinis: Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

Taigi, turimi duomenys leidžia daryti išvadą, kad iš viso buvo nustatyta 212 nusikalstamų veikų, kurios siejamos su tyrimo metu identifikuotais kriptovaliutų piniginių adresais. Kaip buvo minėta, identifikuotų nusikalstamų veikų kriptovaliutų rinkoje skaičius šiuo atveju yra didesnis už tyrimo metu surinktų kriptovaliutų piniginių adresų bendrą skaičių todėl, kad kai kurie kriptovaliutų piniginių adresai vienu metu buvo siejami su daugiau nei vienos nusikalstamos veikos kriptovaliutų rinkoje vykdymu. Anksčiau aptartos trys nusikalstamos veikos kriptovaliutų rinkoje, kurios išsiskyrė savo paplitimu kriptovaliutų piniginių adresuose ir bendrai sudaro net 81,13% nusikalstamų veikų visuose tyrimo metu nustatytuose kriptovaliutų piniginių adresuose, iš viso buvo aptiktos 172 kriptovaliutų piniginių adresuose. Vertinant šiuos tyrimo metu gautus apibendrintus skaičius apie identifikuotų nusikalstamų veikų pobūdį galima, teigti, kad nusikalstamos veikos, kurios sudaro net 81,13% paplitimą visose tyrimo metu nustatytuose kriptovaliutų piniginių adresuose, laikytinos tokiomis nusikalstamomis veikomis, kurias

investuotojams yra pakankamai lengva identifikuoti ir atitinkamai pateikti pranešimus BitcoinAbuse.com internetiniame tinklapyje. Taip pat analizuojant šių nusikalstamų veikų pobūdį galima pastebėti, kad šios nusikalstamos veikos, lyginant su kitomis tyrimo metu identifikuotomis nusikalstamomis veikomis, yra pakankamai nesunkiai įvykdomos, turint tam tikras, nusikalstamai veikai įvykdyti, būdingas žinias. Todėl šios veikos dažniau gali būti pasirenkamos vykdyti prieš investuotojus, siekiant neteisėtai įgyti kriptovaliutas. Tuo tarpu vertinant likusias nusikalstamas veikas galima teigti, kad tai gali būti ne tik tokios nusikalstamos veikos, kurios yra sunkiau įgyvendinamos bei galimai reikalauja didesnių, be kita ko, laiko resursų, tačiau ir patiems rinkos investuotojams gali būti sunkiau šias veikas identifikuoti arba tai užtrunka ilgesnį laiko tarpą, ir atitinkamai apie jas pranešti.

Tyrimo metu nustatytas nusikalstamas veikas kriptovaliutų rinkoje taip pat galime palyginti su mokslinės literatūros analizės metu nustatytomis nusikalstamomis veikomis kriptovaliutų rinkoje (Priedas Nr. 1, 2) ir atlikti tam tikrą nustatytų nusikalstamų veikų grupavimą (14 lentelė). Kaip buvo aptariama pirmoje šio darbo dalyje, išanalizavus mokslinę literatūrą, nusikalstamas veikas kriptovaliutų rinkoje sugrupavome į tokias nusikalstamas veikas, kurias vykdant yra apgaunamas kriptovaliutų rinkos vartotojas (sukčiavimas), tokiu būdu siekiant neteisėtai įgyti kriptovaliutų, ir likusias nusikalstamas veikas, t. y. tokias, kurios nėra susijusios su kriptovaliutų rinkos vartotojo apgavimu, siekiant neteisėtai įgyti kriptovaliutų, tačiau susiję su kitokių pobūdžių veiksmų atlikimu, kurio metu neteisėtai įgyjamos kriptovaliutos. Iš literatūros analizės metu identifikuotų 19 nusikalstamų veikų kriptovaliutų rinkoje, net 15 iš jų buvo siejamos su tokiomis nusikalstamomis veikomis kriptovaliutų rinkoje, kurias vykdant yra siekiama apgaulės būdu nepagrįstai įgyti kriptovaliutų iš kriptovaliutų rinkos investuotojų (6 paveikslas). Vertinant tyrimo metu surinktų duomenų visetą šiame kontekste galima daryti išvadą, kad 118 kriptovaliutų piniginių adresų (t. y. 55,66%) vykdė tokias nusikalstamas veikas kriptovaliutų rinkoje, kurios yra vykdomos darant (tiesioginį) spaudimą kriptovaliutų rinkos vartotojui, siekiant neteisėtai įgyti kriptovaliutas. Tuo tarpu 94 kriptovaliutų piniginių adresų (t. y. 44,34%) vykdė tokias nusikalstamas veikas kriptovaliutų rinkoje, kurios yra vykdomos panaudojant apgaulę, t. y., siekiant suklaidinti kriptovaliutų rinkos vartotoją ir tokiu būdu neteisėtai įgyti kriptovaliutų. Šiuo aspektu pažymėtina taip pat viena tyrimo metu nustatyta aplinkybė, kad į paminėtas 55,66% nusikalstamas veikas, kurias vykdant yra daromas tam tikras (tiesioginis) spaudimas kriptovaliutų rinkos vartotojui, iš viso patenka tik 2 tyrimo nustatytos nusikalstamos veikos kriptovaliutų

rinkoje. Taigi, nepaisant to, jog literatūros analizės metu identifikuotos nusikalstamos veikos kriptovaliutų rinkoje net 78,95% buvo siejamos su tokiomis nusikalstamomis veikomis, kurių vykdymo metu yra siekiama apgauti kriptovaliutų rinkos vartotoją ir tokiu būdu neteisėtai įgyti kriptovaliutų, visgi tyrimo rezultatai parodo, kad nusikalstamas veikas vykdantys asmenys kriptovaliutų rinkoje dažniau renkasi tokias nusikalstamas veikas, kurias vykdant yra daromas tam tikras spaudimas kriptovaliutų rinkos investuotojui, siekiant neteisėtai įgyti kriptovaliutų. Šie gauti rezultatai gali būti paaiškinami tuo, jog panaudojant tokias nusikalstamas veikas yra paprasčiau bei laiko prasme greičiau neteisėtai įgyti kriptovaliutas iš investuotojų.

14 lentelė

Duomenys apie nusikalstamų veikų dažnumą ir jų pasiskirstymą kriptovaliutų piniginių adresų atžvilgiu

Nusikalstama veika	Kriptovaliutų piniginių adresų skaičius	Procentinė kriptovaliutų piniginių adresų skaičiaus išraiška
<i>Nusikalstama veika vykdoma darant (tiesioginį) spaudimą kriptovaliutų rinkos vartotojui</i>		
Kenkėjiškų programų paskleidimo nusikalstama veika	70	33.02%
Seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika	48	22.64%
Iš viso:		55.66%
<i>Nusikalstamas veikas, kurių metu siekiama apgauti (suklaidinti) kriptovaliutų rinkos vartotoją</i>		
Avansinio mokėjimo sukčiavimo nusikalstama veika	11	5.19%
Žvejybos nusikalstama veika	9	4.25%
Meilės sukčiavimo nusikalstama veika	6	2.83%
Dovanų įteikimo sukčiavimo nusikalstama veika	54	25.47%
Kriptovaliutų investavimo sukčiavimo nusikalstama veika	5	2.36%
Apgaulingos piniginės nusikalstama veika	4	1.89%
Aukojimo sukčiavimo nusikalstama veika	1	0.47%
Teroristų finansavimo nusikalstama veika	4	1.89%
Iš viso:		44.34%

Šaltinis: Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

Esant šių duomenų visetui galime 2 hipotezės H0 atmesti ir priimti H1 bei daryti išvadą, kad iš tyrimo metu surinktų duomenų didžioji dalis kriptovaliutų piniginių adresų sietini su nusikalstamų veikų vykdymu, kurias vykdant yra siekiama įgyti kriptovaliutų ne apgaulės būdu, tačiau darant tam tikrą neigiamą poveikį kriptovaliutų rinkos investuotojui. Iš investuotojo perspektyvos tai reiškia, kad naudojantis kriptovaliutų rinka didesnė rizika prarasti investicijas

kyla ne iš apgaulingų veiksmų prieš investuotoją, tačiau kai nusikalstamos veikos vykdytojai renkasi tiesioginį spaudimą prieš investuotoją. Tokios nusikalstamos veikos laikomos lengviau identifikuojamos, todėl investuotojas gali iš karto suprasti, kad prieš jį yra vykdoma nusikalstama veika, kitaip nei sukčiavimo atveju, kurio metu investuotojas gali pagrįstai tikėtis tam tikrą laikotarpį gražos iš investicijų ir ne iš karto suprasti, kad prieš jį buvo vykdoma nusikalstama veika. Tačiau tai yra taip pat tokios nusikalstamos veikos, kurių metu yra tiesiogiai reikalaujama iš investuotojo kriptovaliutų be galimybės investuotojui apskritai įvertinti situaciją ir dažniausiai sukuriamą tokią situaciją, kai investuotojas negali rinktis ir turi, siekdamas išvengti atitinkamų neigiamų pasekmių, turi perduoti kriptovaliutas. Todėl šios nusikalstamos veikos laikytinos kur kas pavojingesnėmis investuotojui investicijų atžvilgiu.

3.1.2. Kartų, kiek buvo pateikta pranešimų, charakteristikos rezultatai

Analizuojant duomenis, susijusius su kiek kartų buvo pateikti pranešimai apie atitinkamos nusikalstamos veikos kriptovaliutų rinkoje įvykdymą, panaudojant atitinkamą kriptovaliutų pinigines adresą, paminėtina, kad pranešimų skaičius šiuo atveju skaičiuojamas nuo pirmojo pranešimo pateikimo iki paskutinio pranešimo, pateikto 2023 m. kovo 31 d. (t. y., iki tyrimo pabaigos). Analizuojant šių duomenų visetą matyti, kad pateiktų pranešimų vidurkis yra 45 pranešimai, tuo tarpu mediana – 6. Daugiausia pranešimų, kiek buvo pateikta apie vieną kriptovaliutų pinigines adresą, yra iš viso 2 531 pranešimai (11 lentelė).

Detaliau analizuojant turimus duomenis galima daryti išvadą, kad kriptovaliutų piniginių adresai, kurie siejami su trijų nusikalstamų veikų vykdymu kriptovaliutų rinkoje, sulaukė daugiau nei 1 000 pranešimų. O būtent, iš turimų duomenų analizės rezultatų matyti, kad daugiausia buvo pranešta apie tokius kriptovaliutų piniginių adresus, kurie buvo siejami su dovanų įteikimo sukčiavimu (4 174 kartai), teroristų finansavimo (1 872 kartai) ir kenkėjiškų programų paskleidimo (1 250 kartai) nusikalstamomis veikomis. Bendrai siejant šias tris nusikalstamas veikas kriptovaliutų rinkoje su kriptovaliutų piniginių adresais matyti, kad iš viso pateiktų pranešimų skaičius sudaro net 83,47% visų pranešimų. Likusios nusikalstamos veikos kriptovaliutų rinkoje, kurios buvo siejamos su tyrimo metu identifikuotais kriptovaliutų piniginių adresais, surinko mažiau nei 1 000 pranešimų ir bendrai sudaro 16,53% visų pranešimų (15 lentelė; 10 paveikslas).

15 lentelė

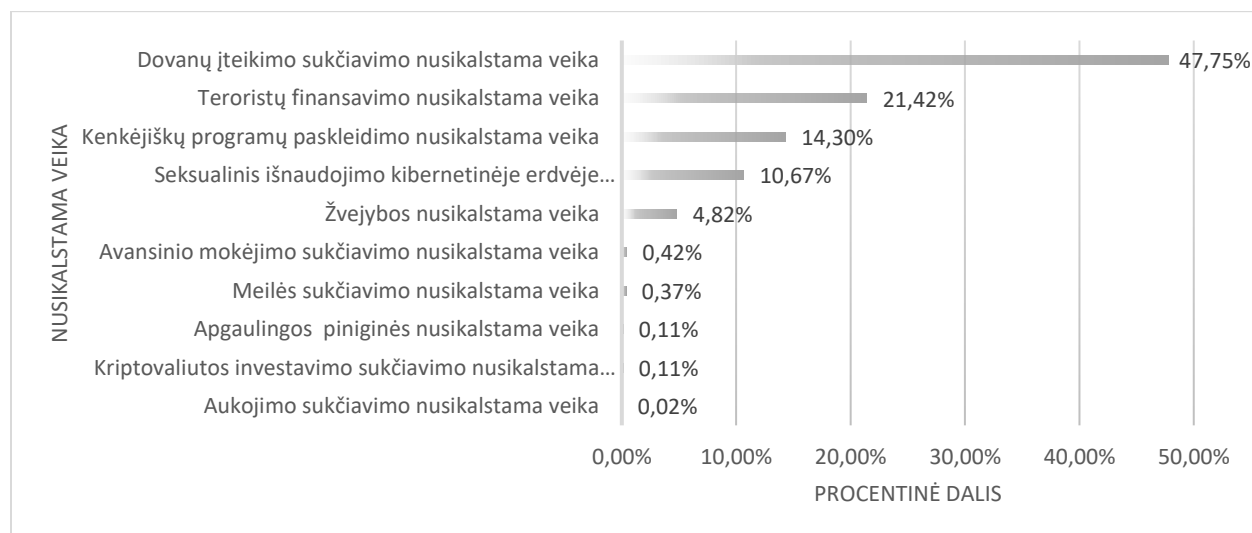
Susisteminti duomenys apie kartus, kiek buvo pranešta apie tyrimo metu identifikuotas nusikalstamas veikas

Nusikalstama veika	Kartai, kiek buvo pranešta apie nusikalstamą veiką
Dovanų įteikimo sukčiavimo nusikalstama veika	4174
Teroristų finansavimo nusikalstama veika	1872
Kenkėjiškų programų paskleidimo nusikalstama veika	1250
Seksualinis išnaudojimo kibernetinėje erdvėje nusikalstama veika	933
Žvejybos nusikalstama veika	421
Avansinio mokėjimo sukčiavimo nusikalstama veika	37
Meilės sukčiavimo nusikalstama veika	32
Kriptovaliutos investavimo sukčiavimo nusikalstama veika	10
Apgaulingos piniginės nusikalstama veika	10
Aukojimo sukčiavimo nusikalstama veika	2

Šaltinis. Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

10 paveikslas

Pateiktų pranešimų apie tyrimo metu identifikuotas kriptovaliutų piniginių adresus procentinės dalies išraiška

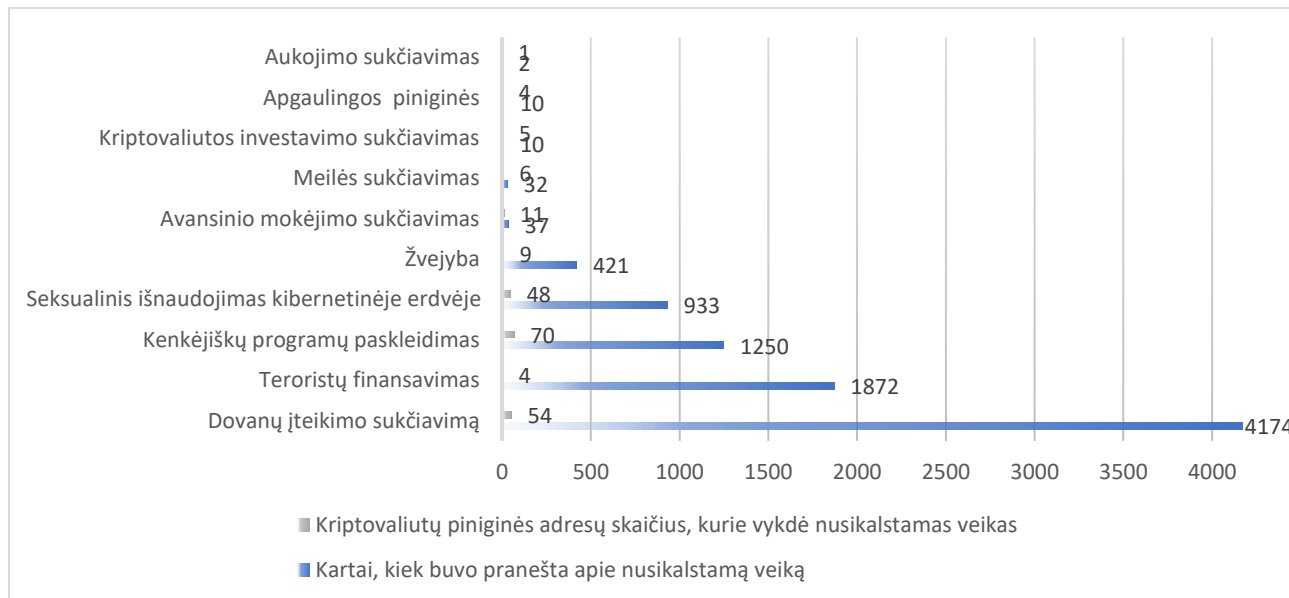


Šaltinis: Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

Taigi, apibendrinant išanalizuotus duomenis, susijusius su kriptovaliutų piniginės adresu skaičiumi, kurios buvo siejamos su nusikalstamų veikų vykdymu, ir kartus, kiek buvo pranešta apie nusikalstamas veikas, duomenis, galima daryti išvadą, kad dovanų įteikimo sukčiavimo nusikalstama veika laikytina nusikalstama veika apie kurią buvo pateikiama daugiausia pranešimų (4 174 kartai), tačiau tai nebuvo ta nusikalstama veika kriptovaliutų rinkoje, kuri buvo dažniausia siejama su kriptovaliutų piniginės adresais (54 kriptovaliutų piniginių adresai). Vertinant kenkėjiškų programų paskleidimo nusikalstamą veiką matyti, kad ši nusikalstama veika sulaukė 1 250 pranešimų ir tai buvo tokia nusikalstama veika, kuri buvo siejama su didžiausiu kiekiu kriptovaliutų piniginių adresų, t. y. 70 kriptovaliutų piniginių adresų. Vertinant nusikalstamas veikas kriptovaliutų rinkoje, kurios sulaukė mažiausiai pranešimų, matyti, kad apgaulingos piniginės nusikalstama veika buvo siejama su 4 skirtingais kriptovaliutų piniginių adresais ir sulaukė 10 pranešimų, tuo tarpu statistiškai paskutinėje vietoje tiek pagal kriptovaliutų piniginių skaičių, tiek pagal pateiktų pranešimų skaičių yra aukojimo sukčiavimo nusikalstama veika, kuri sulaukė 2 pranešimų ir buvo siejama tik su 1 kriptovaliutų piniginių adresu. Vertinant šių duomenų visetą didžiausias skirtumas tarp pranešimų ir kriptovaliutų piniginių adresų skaičiaus pastebėtinai vertinant teroristų finansavimo nusikalstamą veiką. Teroristų finansavimo nusikalstama veika buvo siejama su 4 kriptovaliutų piniginių adresais, tačiau apie šią nusikalstamą veiką buvo pranešta 1 872 kartus. Skirtumas taip pat pastebėtinai ir analizuojant žvejybos nusikalstamą veiką, kadangi su šia nusikalstama veika buvo siejamos 9 kriptovaliutų piniginės adresai, tačiau dėl šios nusikalstamos veikos buvo pateikti 421 pranešimai. Toks stiprus atotrūkis, susijęs su šiomis dvejomis nusikalstamomis veikomis kriptovaliutų rinkoje tarp jų analizuojamų charakteristikų, gali būti siejamas su ta aplinkybe, kad tai yra tokios nusikalstamos veikos kriptovaliutų rinkoje, kurias vykdyti yra kur kas sudėtingiau, todėl tik nedidelė dalis kriptovaliutų piniginių adresų yra siejama su tokiomis nusikalstamomis veikomis. Tai reiškia, kad, siekiant vykdyti šias nusikalstamas veikas kriptovaliutų rinkoje, yra privalu turėti didesnius techninių žinių įgūdžius, šių nusikalstamų veikų vykdymas kriptovaliutų rinkoje pasižymi kompleksiskumu (kuris matytinas ir iš šių nusikalstamų veikų kriptovaliutų rinkoje apibrėžimų), taip pat būdinga sąveika su trečiaisiais asmenimis (pvz., analizuojant teroristų finansavimo nusikalstamą veiką kriptovaliutų rinkoje).

11 paveikslas

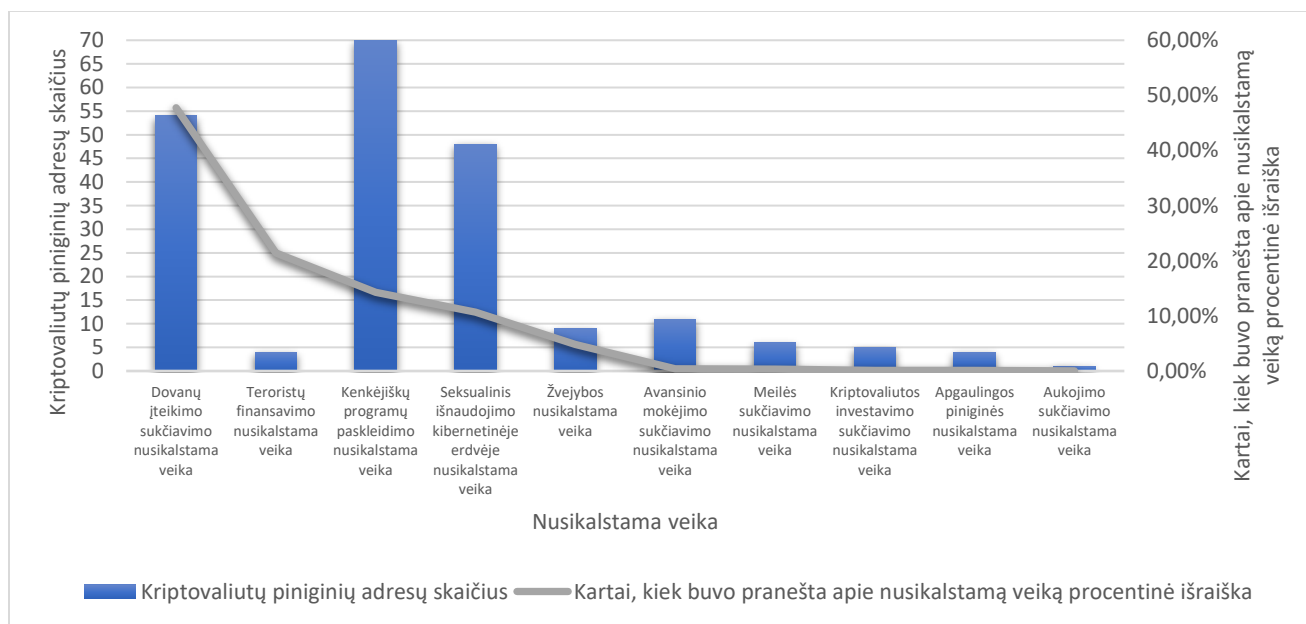
Kriptovaliutų piniginės adresų skaičiaus, kurie vykdė nusikalstamas veikas ir kartų, kiek buvo pranešta apie nusikalstamą veiką, santykis



Šaltinis. Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

12 paveikslas

Kriptovaliutų piniginių adresų skaičiaus ir kartų, kiek buvo pranešta apie nusikalstamas veikas palyginimas



Šaltinis. Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

Siekiant nustatyti, ar tyrimo metu identifikuotos kriptovaliutų piniginių adresų charakteristikos „Kriptovaliutų piniginių adresų skaičius“ ir „Kartai, kiek buvo pranešta apie nusikalstamą veiką“ tarpusavyje koreliuoja, yra atliekamas koreliacijos koeficiento tikrinimas. Koreliacijos koeficientas tarp „Kriptovaliutų piniginių adresų skaičiaus“ ir „Kartų, kiek buvo pranešta apie nusikalstamą veiką“ yra 0,600776042, tai rodo vidutinį teigiamą ryši tarp šių kintamųjų. Tai reiškia, kad didėjant „Kriptovaliutų piniginių adresų skaičiaus“ kintamajam, atitinkamai didėja ir „Kartai, kiek buvo pranešta apie nusikalstamą veiką“. Patikrinus „Kriptovaliutų piniginių adresų skaičius“ ir „Kartai, kiek buvo pranešta apie nusikalstamą veiką“ charakteristikas, atliekant regresijos analizę, buvo nustatyta, kad šiuo atveju nėra statistiškai reikšmingų duomenų. O būtent – ANOVA (analizės kovariacijos) lentelė rodo, kad F statistikos reikšmė yra 4,518226795, o tai reiškia, kad reikšmė yra arti kritinės reikšmės, tačiau jos nepasiekia. Taigi, šiuo atveju nėra statistiškai reikšmingo ryšio tarp kintamųjų regresijos modelyje. Taip pat p-reikšmė yra aukštesnė už 0,05, o tai rodo, kad regresijos koeficientai nėra statistiškai reikšmingi. Taigi, „Kriptovaliutų piniginių adresų skaičiaus“ ir „Kartų, kiek buvo pranešta apie nusikalstamą veiką“ yra vidutinio stiprumo teigiamas ryšys, bet šis ryšys nėra labai stiprus, o regresijos modelio rezultatai vertintini, kaip ribinio statistinio reikšmingumo (Priedas Nr. 5).

Analizuojant šiuos duomenis atitinkamai buvo atlikta tolimesnė duomenų analizė. Vertinant „Kartai, kiek buvo pranešta apie nusikalstamą veiką“ charakteristiką matyti, kad vidutinė pranešimų apie nusikalstamą veiką skaičius yra 46,58. Mažiausias užregistruotas pranešimų skaičius buvo 2, o didžiausias – 4 174. Mediana – vidurinė reikšmė, yra 6. Moda – dažniausiai pasitaikanti reikšmė, yra 10. Vertinant „Kriptovaliutų piniginių adresų skaičius“ charakteristiką pagal suskirstytas nusikalstamas veikas kriptovaliutų rinkoje – vidutinis nusikalstamų veikų skaičius kriptovaliutų piniginių adresuose yra 21 nusikalstama veika. Mažiausias užregistruotas nusikalstamos veikos skaičius, siejamas su kriptovaliutų piniginių adresu, buvo 1 nusikalstama veika, o didžiausias – 70 nusikalstamų veikų. Mediana šiuo atveju buvo 11, tuo tarpu moda – 4 (16 lentelė).

16 lentelė

Kriptovaliutų piniginių adresų skaičiaus pagal nustatytas nusikalstamas veikas kriptovaliutų rinkoje ir kartu, kiek buvo pranešta apie nusikalstamas veikas, statistiniai duomenys

Pavadinimas	Rezultatas	Interpretacija
<i>Kriptovaliutų piniginių adresų skaičius:</i>		
Vidurkis	21.2	Tai reiškia, kad vidutinis kriptovaliutų piniginių skaičius yra 21(.2).
Mediana	11	Dalis duomenų turi reikšmę 11 arba mažesnę.
Moda	4	Tai rodo dažniausiai pasitaikančią reikšmę.
Minimumas	1	Šie duomenys rodo didžiausią ir mažiausią identifikuotų nusikalstamų veikų skaičių kriptovaliutų piniginių adresuose.
Maksimumas	70	
<i>Kartai, kiek buvo pranešta apie nusikalstamą veiką:</i>		
Vidurkis	45.68	Tai reiškia, kad vidutinis pranešimų skaičius yra 874(.1) pranešimas.
Mediana	6	Tai rodo vidutinį pranešimų skaičių, esantį tarp pirmojo ir paskutinio pranešimų.
Moda	10	Tai rodo didžiausią pasitaikančią pranešimų reikšmę.
Minimumas	2	Šie duomenys rodo didžiausią ir mažiausią pranešimų skaičių tarp pirmojo ir paskutinio pranešimų.
Maksimumas	4174	

Šaltinis: Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

Analizuojant nusikalstamų veikų kriptovaliutų rinkoje koncentraciją kriptovaliutų piniginių adresuose bei siekiant išanalizuoti, ar didelė dalis su kriptovaliutomis susijusių pranešimų apie nusikalstamas veikas kriptovaliutų rinkoje yra susiję su nedidele dalimi kriptovaliutų adresais, atliekame sekančius skaičiavimus. Kaip jau nustatyta, tyrimo metu surinktų kriptovaliutų piniginių adresų skaičius yra 162. Nustačius šį skaičių toliau apskaičiuojame TOP1 kriptovaliutų piniginių adresų skaičių. Bendras pranešimų skaičius yra 7 400, TOP1 pranešimų skaičius – 3 573. Atlikus skaičiavimus, matome, kad TOP1 adresų dominuoja pranešimų skaičiaus atžvilgiu, nes jie sudaro 0.482837838, t. y. beveik siekia 0,5 viso pranešimų skaičiaus. Apskaičiavus Chi-kvadratą (Priedas Nr. 6) gauname rezultata, jog Chi-kvadrato reikšmė yra 369,33, tai rodo, kad nėra statistiškai reikšmingo skirtumo tarp TOP1 kriptovaliutų piniginių adresų skaičiaus pateiktų pranešimų ir bendro pranešimų skaičiaus ($\chi^2 = 369,33$, $df = 9$, $p > 0,05$) (17 lentelė).

17 lentelė

Kripto valiutų piniginių adresų TOP1 duomenų parametrai

Parametras	Reikšmė
Bendras pranešimų skaičius	7400
Top 1 adresų pranešimų skaičius	3573
1% nuo bendro pranešimų skaičiaus	87,41
Ar TOP 1 adresų pranešimų skaičius > 0,5?	Taip
Adresu kurie priskiriami 1%	8

Šaltinis: Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

Galime daryti išvadą, kad TOP1 kripto valiutų piniginių adresai neturi didesnio pranešimų skaičių nei likusieji kripto valiutų piniginių adresai. Tai rodo, kad didelė dalis su kripto valiutomis susijusių nusikalstamų veikų nėra siejama su nedidele dalimi kripto valiutų piniginių adresais, kurie yra laikomi TOP1. Taigi, atmetame 3 hipotezės H0 ir priimame H1, darant išvadą, kad nėra pakankamai statistinių įrodymų, jog didelė dalis su kripto valiutų piniginių adresais susijusių elektroninių nusikaltimų būtų siejama su nedidele dalimi kripto valiutų adresų.

3.1.3. Pranešimų pateikimo laikotarpių charakteristikos rezultatai

Analizuojant tyrimo metu surinktus duomenis apie tai, kada buvo pirmą kartą pateiktas pranešimas apie vykdomą nusikalstamą veiką kripto valiutų rinkoje, panaudojant kripto valiutų pinigines adresą, ir paskutinį kartą pateiktas pranešimas apie vykdomą nusikalstamą veiką kripto valiutų rinkoje, panaudojant kripto valiutų pinigines adresą, galime daryti išvadą, kad vidutinis dienų skaičius tarp tokių pranešimų yra 48 dienos. Trumpiausias dienos tarpas tarp pateiktų pranešimų tinklapyje yra 0 dienų, tai reiškia, kad pranešimas buvo pateiktas pirmą ir paskutinį kartą per tiriamąjį laikotarpį tą pačią dieną. Ilgiausias dienos tarpas tarp pirmojo pranešimo apie vykdomą nusikalstamą veiką kripto valiutų rinkoje ir paskutinio pranešimo apie vykdomą nusikalstamą veiką kripto valiutų rinkoje yra 955 dienos. Vadinasi, yra bent vienas atvejis, kai laikotarpis tarp pirmo pateikto pranešimo ir paskutinio pateikto pranešimo yra 955 dienos, o tai yra apie 2,5 metų. Tolimesnė duomenų analizė leidžia daryti išvadą, kad dažniausia

tarp pirmo ir paskutinio pranešimo apie kriptovaliutos piniginės adresą, kurį panaudojant vykdoma nusikalstama veika, skiria viena savaitė, o būtent – net 53,7% tiriamuoju laikotarpių surinktų duomenų nurodo, kad tarp pirmo ir paskutinio pranešimo juos skyrė tik viena savaitė. Visi likę laikotarpiai pasiskirsto tarp 0% ir 11%. Iš investuotojo perspektyvos šie duomenys leidžia teigti, kad kriptovaliutų rinkos investuotojai pakankamai greitai reaguoja į nusikalstamas veikas kriptovaliutų rinkoje. Šie veiksmai leidžia kitiems investuotojams mažinti riziką nukentėti nuo nusikalstamų veikų šioje rinkoje (18 lentelė).

18 lentelė

Laiko skirtumo tarp pirmo ir paskutinio pranešimo apie vykdoma nusikalstamą veiką, panaudojant kriptovaliutų piniginės adresus, procentinis pasiskirstymas

Laiko skirtumas tarp pirmo ir paskutinio pranešimo apie vykdoma nusikalstamą veiką panaudojant kriptovaliutų piniginės adresus	Procentinis pasiskirstymas
Viena savaitė	53,7%
Dvi savaitės	11,11%
Trys savaitės	4,3%
Ketrios savaitės	8,6%
Penkios savaitės	9,25%
Šešios savaitės	1,2%
Trylika savaitių	1,9%
Dvidešimt dvi savaitės	0,6%
Trisdešimt viena savaitė	0,6%
Trisdešimt dvi savaitės	1,2%
Keturiasdešimt penkios savaitės	0,6%
Keturiasdešimt šešios savaitės	0,6%
Keturiasdešimt aštuonios savaitės	0,6%
Daugiau nei vieneri metai	1,2%
Daugiau nei dveji metai	3,7%

Šaltinis: Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

Siekiant nustatyti, ar tarp tyrimo metu identifikuotų „Kiek kartų buvo pateiktas pranešimas“ ir „Dienų skaičius tarp pirmo ir paskutinio pranešimo“ egzistuoja tam tikras priklausomumas buvo atlikta koreliacijos koeficiento analizė. Koreliacijos koeficientas šiuo atveju yra 0,352568. Gautas rezultatas rodo, kad tarp „Kiek kartų buvo pateiktas pranešimas“ ir „Dienų skaičius tarp pirmo ir paskutinio pranešimo“ yra tam tikras teigiamas ryšys, tačiau šis ryšys yra

silpnas. Tai reiškia, kad, nors yra pastebimas tam tikras ryšys tarp šių dviejų kintamųjų, visgi šie kintamieji yra ganėtinai nepriklausomi vienas nuo kito ir koreliacija nėra labai stipri. Atlikus regresijos analizę pastebėta, kad šiuo atveju yra statistiškai reikšmingų duomenų. Koreliacijos koeficientas (R) tarp „Kiek buvo pateikta pranešimų“ ir „Dienų skaičius tarp pirmo ir paskutinio pranešimo“ yra 0,352567961, o R-kvadratas rodo, kad 12,43% priklausomybės tarp šių kintamųjų paaiškinama regresijos modeliu. ANOVA lentelė rodo, kad regresijos modelis yra statistiškai reikšmingas ($F = 22,71184$, $p < 0,05$). Tai reiškia, kad yra ryšys tarp „Kiek buvo pateikta pranešimų“ ir „Dienų skaičius tarp pirmo ir paskutinio pranešimo“, kuris yra statistiškai reikšmingas. Regresijos koeficientas tarp šių kintamųjų yra 0,57780793, tai reiškia, kad tuo atveju, kai dienų skaičius tarp pirmo ir paskutinio pranešimo padidėja vienu kartu, tai pranešimų skaičius padidėja 0,58 karto. Tačiau paminėtina, kad R-kvadratas visgi parodo tai, kad didelė dalis kintamumo yra paaiškinama nežinomaisiais (trečiaisiais) faktoriais, o ne tik tiriamaisiais kintamaisiais.

3.2. BlockChain.com tyrimo metu surinktų charakteristikų rezultatai

Iš tyrimo metu surinktų BlockChain.com duomenų (Priedas Nr. 4) matyti, kad BlockChain.com internetiniame tinklapyje buvo identifikuotos 5 (penkios) charakteristikos tyrimo rezultatų analizei (9 lentelė). Pažymėtina, kad charakteristika „Kripto valiutų piniginių adresai“ buvo nagrinėjamas šio skyriaus pradžioje, todėl pakartotinai nebeaptariama.

3.2.1. Operacijų skaičiaus, kripto valiutų piniginių adresuose, charakteristikos rezultatai

Analizuojant tyrimo metu surinktų duomenų visetą (Priedas Nr. 4) matyti, kad 2 kripto valiutų piniginių adresai neturėjo duomenų apie operacijų istoriją, o 64 kripto valiutų piniginių adresai apskritai neturėjo jokios operacijų istorijos, t. y. bendra piniginės vertė iki tyrimo pabaigos išliko 0 kripto valiutų. Vadinasi, 1,2% identifikuotų kripto valiutų piniginių adresų neturėjo apskritai jokių duomenų apie operacijų istoriją, tuo tarpu 39% nuo identifikuotų kripto valiutų piniginių adresų iki tyrimo pabaigos turėjo iš viso 0 kripto valiutų operacijų vertės.

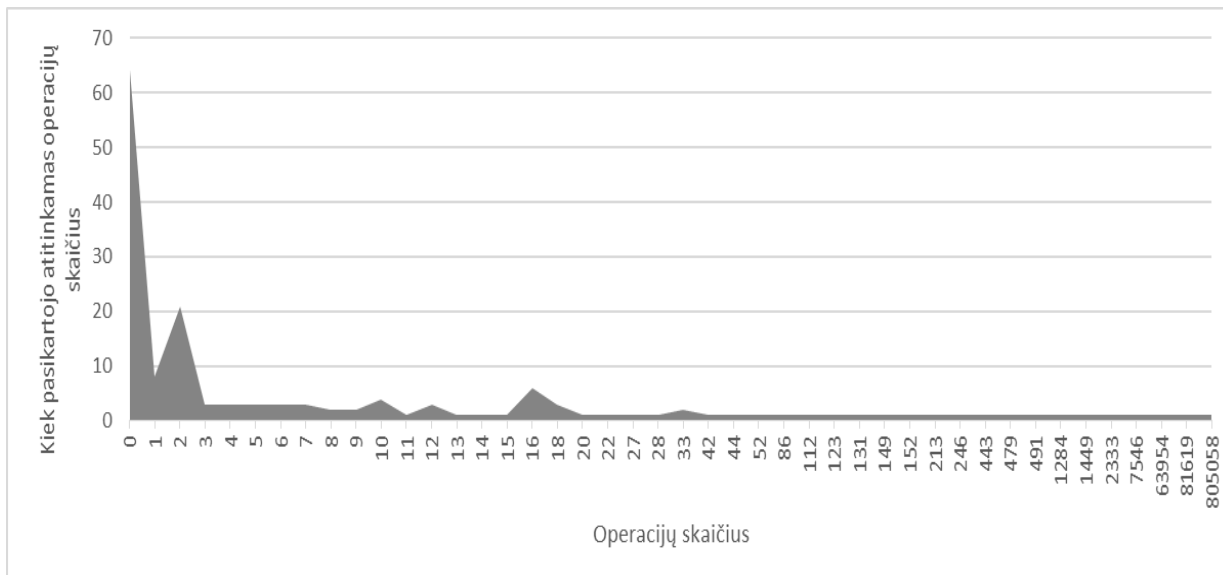
Analizuojant tyrimo metu surinktų duomenų visetą matyti, kad iš viso operacijų kripto valiutų piniginių adresuose skaičius yra 966 607 tyrimo pabaigos dienai. Operacijų skaičiaus

kripto valiutų piniginių adresuose didžiausia vertė yra 805 058 operacijos. Vadinas, net 83% visų operacijų skaičiaus yra susitelkę į vieną kripto valiutų piniginių adresą. Tyrimo duomenų analizė atskleidžia, kad daugiausia operacijų atlikta kripto valiutų piniginių adrese, kuris tuo pačiu metu vykdė teroristų finansavimo ir žvejybos nusikalstamas veikas. Tuo tarpu operacijų vidurkis kripto valiutų piniginių adresuose yra 6 079 operacijos, o mediana yra lygi 2. Taip pat duomenų visetas parodo, kad 25% kripto valiutų piniginių adresų turėtojai atliko 0 operacijų, o 75% kripto valiutų piniginių turėtojų atliko 12 operacijų ar daugiau (11 lentelė).

Analizuojant turimus duomenis, siejant juos su konkrečiomis nusikalstamomis veikomis kripto valiutų rinkoje, matyti, kad, kaip minėta, daugiausia lėšų buvo gauta į kripto valiutų piniginių adresus, kurie buvo naudojami vykdant nusikalstamą veiką, susijusią su teroristų finansavimu. Kaip anksčiau buvo nustatyta, su teroristų finansavimo nusikalstama veika buvo siejami 4 kripto valiutų piniginių adresais, iš šių adresų buvo atliktos iš viso 869 014 operacijos. Panašiu operacijų skaičiumi pasižymi taip pat ir kripto valiutų piniginių adresas, kuris siejamas su žvejybos nusikalstama veika – iš viso buvo atliktos 805 430 operacijos. Paminėtina ir tai, kad kaip ir teroristų finansavimo nusikalstama veika, žvejybos nusikalstama veika siejama su pakankamai nedideliu kripto valiutų piniginių adresų skaičiumi. Iš viso tik 9 kripto valiutų piniginių adresai siejami su šia nusikalstama veika. Tai reiškia, kad tyrimo metu identifikuotų didžiausių operacijų skaičius priskiriamas tik 6.14% tyrimo metu identifikuotiems kripto valiutų piniginių adresams. Likusios nusikalstamos veikos kripto valiutų rinkoje yra stipriai atitrūkusios operacijų skaičiumi nuo pastarųjų dviejų nusikalstamų veikų kripto valiutų rinkoje. Tyrimo rezultatai leidžia daryti išvadą, kad kripto valiutų piniginių adresai, kurie vykdė seksualinio išnaudojimo kibernetinėje erdvėje nusikalstamą veiką, iš viso su šiais kripto valiutų piniginių adresais buvo atliktos 83 998 operacijos, avansinio mokėjimo sukčiavimą – 10 583 operacijos, meilės sukčiavimą – 1 447 operacijos. Su kitomis nusikalstamomis veikomis siejamuose kripto valiutų piniginių adresuose nebuvo įvykdyta daugiau nei 1 000 operacijų. Paminėtina ir tai, kad iš tyrimo metu surinktų duomenų matyti, jog su aukojimo sukčiavimu sietina kripto valiutų piniginių nesulaukė nei vienos operacijos (13 lentelė, 14 paveikslas).

13 paveikslas

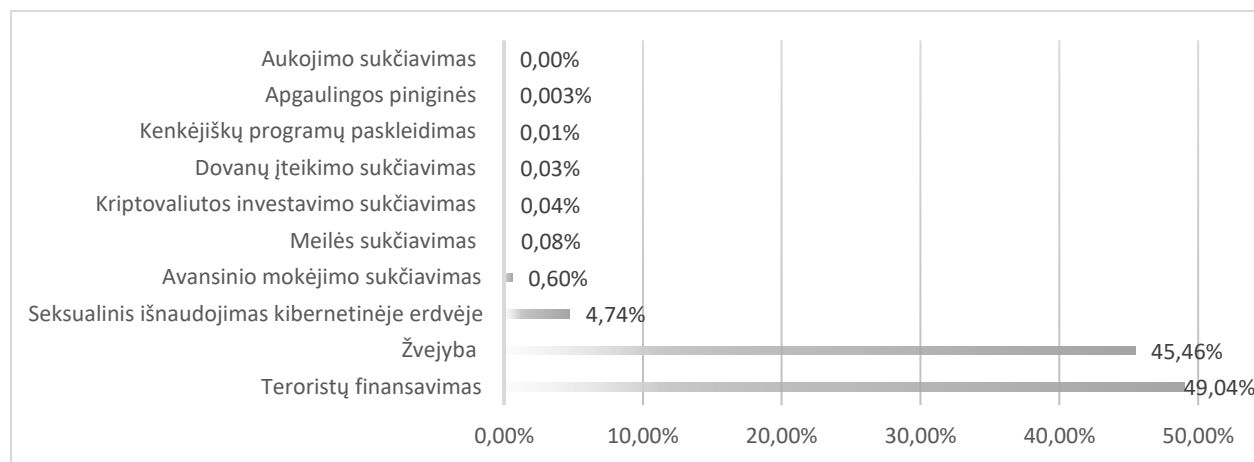
Operacijų skaičiaus kriptovaliutų piniginių adresuose pasikartojimų atvaizdavimas



Šaltinis: Sudaryta autorės, remiantis Blockchain.com duomenimis.

14 paveikslas

Operacijų skaičiaus pagal nusikalstamas veikas kriptovaliutų piniginių adresuose procentinė išraiška



Šaltinis: Sudaryta autorės, remiantis Blockchain.com duomenimis.

Aplinkybę, kodėl su teroristų finansavimo ir žvejybos nusikalstamomis veikomis kriptovaliutų rinkoje siejamos kriptovaliutų piniginės pasižymi didžiausiu operacijų skaičiumi gali būti paaiškinama tuo, jog šie kriptovaliutų piniginių adresai iš tyrimo metu surinktų duomenų buvo siejami su daugiau nei viena nusikalstama veika kriptovaliutų rinkoje. Tai atitinkamai gali būti siejama su didesniu investuotojų, nukentėjusių nuo šių nusikalstamų veikų, skaičiumi ir tokiu būdu didesniu operacijų skaičiumi, kurių metu buvo neteisėtai įgyjamos kriptovaliutos. Iš investuotojo perspektyvos tai parodo, kad, nepaisant to, jog teroristų finansavimo ir žvejybos nusikalstamoms veikoms būdingas pakankamai nedidelis kriptovaliutų piniginių adresų skaičius, visgi būtent šiose veikose susitelkia didžiausias operacijų skaičius. Tai reiškia, kad siekiant valdyti savo investavimo rizikas kriptovaliutų rinkoje svarbu atkreipti dėmesį ne tik į tokias nusikalstamas veikas, kurios yra plačiai paplitusios, panaudojant kriptovaliutų piniginių adresus, bet ir įsivertinti kriptovaliutų piniginių adresų operacijų skaičių, kuris gali indikuoti apie nusikalstamų veikų vykdymą.

3.2.2. Lėšų, gautų iš nusikalstamos veikos vykdymo kriptovaliutų rinkoje, charakteristikos rezultatai

Analizuojant surinktus duomenis apie lėšas, kurios buvo gautos į kriptovaliutų piniginių adresus, matyti, kad bendras vidurkis yra 243 518,5 kriptovaliutos, tuo tarpu mediana – 0,0074. Didžiausia kriptovaliutų suma, kuri buvo gauta už nusikalstamos veikos vykdymą kriptovaliutų rinkoje, į kriptovaliutų pinigines adresą yra 38 885 199,3 kriptovaliutos. Taip pat turimi duomenys atspindi, kad 25% vertės yra lygi arba mažesnė nei 1 kriptovaliuta. Tai reiškia, kad 25% transakcijų yra atlikta su mažesne nei ši suma, o 75% vertės yra lyg arba mažesnė nei 0,1927 kriptovaliuta (11 lentelė). Kaip matyti iš turimų duomenų viseto, daugiausia lėšų buvo gauta būtent į tuos kriptovaliutų piniginių adresus, kurie vykdė teroristų finansavimą ir žvejybos nusikalstamas veikas. Šių nusikalstamų veikų gautos lėšos į kriptovaliutų piniginių adresus sudaro net 99.99% iš visų tyrimo metu nustatytų kriptovaliutų sumos. Tai reiškia, kad net 99.99% iš visų tyrimo metu nustatytų kriptovaliutų sumos yra susitelkę 13 kriptovaliutų piniginių adresuose, kurie yra siejami su teroristų finansavimo ir žvejybos nusikalstamų veikų kriptovaliutų rinkoje vykdymu (19 lentelė).

19 lentelė

Duomenų, susijusių su lėšomis, gautomis iš nusikalstamos veikos (BTC), apibendrinimas

Nusikalstama veika	Lėšos, gautos iš nusikalstamos veikos (BTC)	Procentinė išraiška
Žvejybos nusikalstama veika	38885201.8	49.94%
Teroristų finansavimo nusikalstama veika	38960828	50.05%
Kenkėjiškų programų paskleidimo nusikalstama veika	2054.86	0.00263951%
Seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika	2016.228	0.00258988%
Avansinio mokėjimo sukčiavimo nusikalstama veika	27.70824	0.00003559%
Dovanų įteikimo sukčiavimo nusikalstama veika	26.75075	0.00003436%
Kripto valiutų investavimo sukčiavimo nusikalstama veika	22.95068	0.00002948%
Meilės sukčiavimo nusikalstama veika	21.28985	0.00002735%
Apgaulingos pinginės nusikalstama veika	0.49009498	0.00000063%

Šaltinis: Sudaryta autorės, remiantis BlockChain.com duomenimis.

Tyrimo metu gauti duomenys leidžia atmesti 4 hipotezės H0 ir priimti H1. Pirmiausia, kaip matyti iš tyrimo duomenų viseto, kenkėjiškų programų paskleidimo nusikalstama veika, kuri buvo vykdoma iš 70 kripto valiutų piniginių adresų bendrai įgijo tik 0,002634244% visų kripto valiutų nuo bendros sumos. Dovanų įteikimo sukčiavimo nusikalstama veika, kuri buvo vykdoma panaudojant 54 kripto valiutų piniginių adresų, bendrai įgijo tik 0,00003436% visų kripto valiutų nuo bendros sumos. Galiausiai, seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika buvo vykdoma panaudojant 48 kripto valiutų piniginių adresus bendrai įgijo tik 0,00258988% visų kripto valiutų nuo bendros sumos. Taigi, trys nusikalstamos veikos, kurios buvo vykdomos iš viso 81.13% kripto valiutų piniginių adresų iš viso įgijo bendrai tik 0,005258484% visų kripto valiutų nuo bendros sumos. Tuo tarpu žvejybos nusikalstama veika, kuri buvo vykdoma panaudojant 9 kripto valiutų piniginių adresus iš viso įgijo 49,95 % visų kripto valiutų nuo bendros sumos. Teroristų finansavimo nusikalstama veika, kuri buvo vykdoma panaudojant 4 kripto valiutų

piniginių adresus, iš viso įgijo 50,05 % visų kriptovaliutų nuo bendros sumos (Priedas Nr. 8). Taigi, didelė dalis kriptovaliutų piniginių adresų tyrimo pabaigos dienai, daugiausia neteisėtai įgijusių kriptovaliutų iš nusikalstamos veikos, nėra tokie kriptovaliutų piniginių adresai, kurie vykdė dažniausia kriptovaliutų piniginių adresuose identifikuotas nusikalstamas veikas. Iš investuotojo perspektyvos tai parodo, kad visgi ne kriptovaliutų piniginių adresų paplitimo mastas yra esminis elementas, kuris leidžia įgyti didelį kiekį kriptovaliutų neteisėtu būdu. Tai reiškia, jog jeigu prieš investuotoją būtų įvykdyta nusikalstama veika, kuri statistiškai yra mažiau paplitusi tarp kriptovaliutų piniginių adresų, investuotojo nuostolis būtų didesnis nei tuo atveju, jeigu prieš jį būtų įvykdoma nusikalstama veika, kuri statistiškai pasireiškia dažniau.

3.2.3. Išsiųstų lėšų iš kriptovaliutų piniginių ir galutinio balanso charakteristikų rezultatai

Analizuojant ir vertinant kriptovaliutas, kurios buvo išsiųstos iš kriptovaliutų piniginių adresų matyti, kad vidurkis yra 244 864,11 kriptovaliutos, tuo tarpu mediana – 0,003. Didžiausia kriptovaliutų suma, kuri buvo išsiųsta iš kriptovaliutų piniginių adresu, yra 75 982,33 kriptovaliutos. Taip pat turimi duomenys atspindi, kad 25% vertės yra lygi arba mažesnė nei 1 kriptovaliuta, o taip pat 75% vertės yra lyg arba mažesnė nei 0,179 kriptovaliuta. Kaip matyti iš turimų duomenų viseto, daugiausia kriptovaliutų buvo gauta būtent į tuos kriptovaliutų piniginių adresus, kurie vykdė teroristų finansavimą ir žvejybos nusikalstamas veikas. Šių nusikalstamų veikų gautos lėšos į kriptovaliutų piniginių adresus sudaro net 99,1% iš visų tyrimo metu nustatytų kriptovaliutų sumos. Tai reiškia, kad net 99,1 % iš visų tyrimo metu nustatytų kriptovaliutų sumos yra susitelkę 13 kriptovaliutų piniginių adresuose, kurie yra siejami su teroristų finansavimo ir žvejybos nusikalstamų veikų vykdymu. Taigi, kaip ir iš kriptovaliutų, gautų iš nusikalstamos veikos vykdymo duomenų, taip ir iš kriptovaliutų, kurios buvo išsiųstos iš kriptovaliutų piniginių adresų, duomenų analizės galima daryti išvadą, kad teroristų finansavimo ir žvejybos nusikalstamos veikos sutelkė tiek didžiausią operacijų skaičių, tiek didžiausią gautų kriptovaliutų skaičių.

20 lentelė

Duomenų, susijusių su išsiųstomis lėšomis iš kriptovaliutų piniginės (BTC) ir 2023 m. kovo 31 d. likutis kriptovaliutų piniginių adresuose (BTC), apibendrinimas

Nusikalstama veika	Išsiųstos lėšos iš kriptovaliutų piniginės (BTC)	Procentinė išraiška nuo bendros sumos	2023 m. kovo 31 d. likutis kriptovaliutų piniginių adresuose (BTC)	Procentinė išraiška nuo bendros sumos
Teroristų finansavimo nusikalstama veika	38931227.6	50.05%	57822.89	49.92%
Žvejybos nusikalstama veika	38855247.3	49.95%	57957.68	50.04%
Kenkėjiškų programų paskleidimo nusikalstama veika	2049.198	0.0026342446680246%	22.67865	0.01957988111308%
Seksualinis išnaudojimo kibernetinėje erdvėje nusikalstama veika	2047.107	0.0026315566868725%	1.707518	0.00147420589138%
Avansinio mokėjimo sukčiavimo nusikalstama veika	104.7932	0.0001347116912788%	0.193833	0.00016734801656%
Dovanų įteikimo sukčiavimo nusikalstama veika	24.45661	0.0000314389797816%	0.012834	0.00001108038592%
Meilės sukčiavimo nusikalstama veika	20.96937	0.0000269561316741%	0.278301	0.00024027446491%
Apgaulingos piniginės nusikalstama veika	0.498454	0.0000006407627724%	0	0
Kriptovaliutos investavimo sukčiavimo nusikalstama veika	2.108202	0.0000027100943284%	20.84947846	0.01800064419692%

Šaltinis: Sudaryta autorės, remiantis BlockChain.com duomenimis.

Analizuojant paskutinės tyrimo dienos kriptovaliutų piniginių adresų kriptovaliutų balansą matyti, kad vidurkis yra 364,53 kriptovaliutos, tuo tarpu didžiausia vertė yra 57 822,56 kriptovaliutos. Šiuo atveju didžiausia vertė priskirtina teroristų finansavimo nusikalstamai veikai. Taip pat mažiausia kriptovaliutų vertė, nustatyta kriptovaliutų piniginės adresuose yra 0 kriptovaliutos. Pirmą kvartilę yra 0 kriptovaliutos, o tai rodo, kad 25% balansų yra mažesni arba

lygūs šiai kriptovaliutų kiekiui kriptovaliutų piniginių adresuose. Trečioji kvartilė yra 0 kriptovaliutos ir tai rodo, kad 75% balansų yra mažesni arba lygūs šiai kriptovaliutų sumai kriptovaliutų piniginių adresuose. Vidurinė reikšmė tarp visų identifikuotų kriptovaliutų yra 0,016608 kriptovaliutos (11 lentelė).

Analizuojant 2023 m. kovo 31 d. likutį kriptovaliutų piniginių adresuose matyti, kad teroristų finansavimo ir žvejybos nusikalstamos veikos apylygiai pasiskirsto ties išsiųstų lėšų iš kriptovaliutų piniginių adresų, beveik po 50%. Tačiau kriptovaliutų piniginėse yra šiek tiek mažiau lėšų iš teroristų finansavimo nusikalstamos veikos nei iš žvejybos nusikalstamos veikos. Kenkėjiškų programų paskleidimo nusikalstama veika ir seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika sudaro tik mažą dalį iš visų nusikalstamų veikų sumos. Kriptovaliutų piniginių adresai, kurie siejami su šiomis nusikalstamomis veikomis, sukaupia itin mažą gautų ir išsiųstų kriptovaliutų dalį, t. y. procentinė išraiška yra tik kelios tūkstantųjų procento dalis. Avansinio mokėjimo sukčiavimo nusikalstama veika, dovanų įteikimo sukčiavimo nusikalstama veika ir meilės sukčiavimo nusikalstama veika taip pat sudaro labai mažą dalį iš bendros nusikalstamų veikų sumos. Kriptovaliutų piniginių adresai, kurie siejami su šiomis nusikalstamomis veikomis, savyje turi labai mažą gautų ir išsiųstų lėšų dalį, kuri sudaro tik kelias šimtąsias procento dalis. Galiausia, mažiausia lėšų dalimi pasižymi kriptovaliutų piniginės, kurios yra siejamos su apgaulingos piniginės nusikalstama veika, kadangi procentinė išraiška šiuo atveju yra tik kelios milijono procento dalis. Iš investuotojo perspektyvos šie duomenys reiškia, kad siekiant valdyti savo investavimo rizikas kriptovaliutų rinkoje svarbu atkreipti dėmesį ir į kriptovaliutų judėjimą kriptovaliutų piniginių adresuose, kadangi itin didelis kriptovaliutų judėjimas gali padėti identifikuoti nusikalstamų veikų vykdymą pasitelkiant kriptovaliutų piniginių adresus. Ypač tokias nusikalstamas veikas, kurias vykdant iš investuotojo gali būti bandoma neteisėtai įgyti didelį kiekį kriptovaliutų.

IŠVADOS IR PASIŪLYMAI

1. Kripto valiutų rinka, būdama unikali bei turėdama atskirą veikimo sistemą ir principus, yra itin populiari vartotojų (investuotojų) tarpe. Būtent kripto valiutų rinkai būdinga veikimo sistema ir principai leidžia matyti šią rinką kaip itin inovatyvią ateities mokėjimų sistemą.
2. Kripto valiutų rinkos reguliavimo stoka yra vienas iš kertinių aspektų, kodėl kripto valiutų rinka yra itin pažeidžiama nusikalstamų veikų vykdymo aspektu. Bendras susitarimas, kaip traktuoti kripto valiutų rinką, šiai dienai dar nėra pasiektas. Kiekviena šalis kripto valiutų rinką reguliuoja savo nuožiūra – nuo itin griežto kripto valiutų rinkos uždraudimo iki visiško reguliavimo nebūvimo. Visgi, aiškus šios rinkos reguliavimas ne tik sudarytų prielaidą mažėti nusikalstamų veikų kripto valiutų rinkoje vykdymui, tačiau prisidėtų prie sklandaus skaitmeninės, žetonais pagrįstos, ekonomikos ateities formavimo ir ekonomikos rinkos stabilumo.
3. Kripto valiutų rinka, dėl šiai rinkai būdingos veikimo sistemos ir principų bei vieningo reguliavimo nebuvimo, yra itin pažeidžiama nusikalstamų veikų vykdymo aspektu. Nusikalstamą veiką vykdantys asmenys pasinaudoja ne tik pačia kripto valiutų rinka, bet ir aplinkybę, kad šiai dienai šios rinkos investuotojams vis dar trūksta žinių, patirties bei bendro budrumo, siekiant atskirti nusikalstamą veiką nuo realios investicinės galimybės, tam, jog vykdytų nusikalstamas veikas.
4. Atlikus tyrimą nustatyta, kad kripto valiutų rinkoje vykdomos nusikalstamos veikos skiriasi nuo tų, kurios yra aptariamose mokslinėje literatūroje. Tai reiškia, kad kripto valiutų rinkoje yra vykdomos ne tik tos nusikalstamos veikos, kurias autoriai mini mokslinėje literatūroje, bet ir kitokio pobūdžio nusikalstamos veikos. Atitinkamai investuotojo atžvilgiu tai reiškia, kad investuotojas veikdamas šioje rinkoje gali neturėti pakankamai žinių apie visas nusikalstamas veikas, kurios gali būti įvykdomos jo atžvilgiu kripto valiutų rinkoje.
5. Atlikus tyrimą nustatyta, kad kripto valiutų rinkoje vykdomos nusikalstamos veikos skirstomos į tokias, kurios vykdomos panaudojant apgaulę prieš investuotoją ir tokias, kurios yra vykdomos darant tiesioginį spaudimą investuotojui. Nusikalstamą veiką vykdantys asmenys dažniau renkasi vykdyti tokias nusikalstamas veikas prieš investuotoją, kurios yra susijusios ne su apgaulės panaudojimu, tačiau su tiesioginio spaudimo panaudojimu. Atitinkamai investuotojui tokios nusikalstamos veikos yra kur kas pavojingesnės investicijų atžvilgiu.

6. Atlikus tyrimą nustatyta, kad negalima vienareikšmiškai daryti išvados, jog didelė dalis su kriptovaliutų susijusių elektroninių nusikaltimų yra siejama su nedidele dalimi kriptovaliutų piniginių adresais. Išanalizavus tyrimo duomenis nebuvo gauta pakankamai statistinių įrodymų, jog didelė dalis su kriptovaliutų piniginių adresais susijusių elektroninių nusikaltimų būtų siejama su nedidele dalimi kriptovaliutų adresų.
7. Atlikus tyrimą nustatyta, kad didelė dalis kriptovaliutų piniginių adresų tyrimo pabaigos dienai daugiausia neteisėtai įgijusių kriptovaliutų iš nusikalstamos veikos buvo tokie kriptovaliutų piniginių adresai, kurie nebuvo siejami su dažniausiai kriptovaliutų piniginių adresuose identifikuotomis nusikalstamomis veikomis. Tai reiškia, kad tos nusikalstamos veikos kriptovaliutų rinkoje, kurios buvo vykdomos didesniame kriptovaliutų piniginių adresų skaičiuje pagal išanalizuotus tyrimo duomenis, tyrimo pabaigos duomenimis buvo įgijusios itin mažą kiekį kriptovaliutų (mažiau nei 1%). Tuo tarpu tos nusikalstamos veikos, kurios, buvo vykdomos mažesniame kriptovaliutų piniginių adresų skaičiuje pagal išanalizuotus tyrimo duomenis, buvo tos nusikalstamos veikos, kurios kriptovaliutų piniginių adresams leido neteisėtai įgyti dideles sumas kriptovaliutų.

Pasiūlymai:

Kriptovaliutų rinkai kylančios rizikos iš reglamentavimo stokos valdymas: šiai dienai esant neapibrėžtam kriptovaliutų rinkos reguliavimui ši rinka yra sudėtingoje ir neapibrėžtoje aplinkoje, kuri neabejotinai kenkia investicijoms, naujovių plėtrai bei stabdo tvirtos skaitmeninės ekosistemos susiformavimą. Siekiant, kad kriptovaliutų rinka galėtų sistemingai vystytis ir netapti tik tokia rinka, kuri pritraukia nusikalstamas veikas vykdančius asmenis, tokiu būdu, be kita ko, stabdant šios rinkos efektyvų vystymąsi, yra būtina didinti dėmesį šios rinkos reguliavimui.

Investuotojui kylančio rizikos valdymas: investuotojams svarbu įsivertinti turimą patirtį ir žinias apie kriptovaliutų rinką. Tai reiškia, jog prieš pradėdant naudotis šią rinka reikėtų nesiekti gauti didžiausios įmanomos grąžos per trumpiausią laiką, tačiau šią rinka naudotis tam tikrais etapais, iki kol vartotojui (investuotojui) susiformuos tam tikra patirtis, kuri leis identifikuoti ne tik akivaizdžias potencialias nusikalstamas veikas kriptovaliutų rinkoje, tačiau ir kiek sunkiau suprantamas schemas, tokiu būdu siekiant išvengti potencialių nuostolių. Taip pat investuotojams, naudojantiems kriptovaliutų rinką, yra svarbu išlaikyti racionalumą ir budrumą bei prieš atliekant bet kokio tipo veiksmą įsivertinti, ar veiksmo atlikimas nebus akstinas nusikalstamą veiką vykdančiams asmenims neteisėtai įgyti vartotojo (investuotojo) kriptovaliutų.

Tyrimo apribojimai. Pagrindiniai šio tyrimo apribojimai laikytini tokie, jog, pirma, tyrimo duomenys buvo renkami rankiniu būdu. Toks duomenų rinkimo metodas gali turėti tam tikrų apribojimų, kadangi pasitelkiant informacinių technologijų žinias būtų galima surinkti platesnius duomenis bei paanalizuoti ir kitokio pobūdžio charakteristikas. Antra, analizuojami duomenys yra gauti iš atsitiktinai atrinktos nusikalstamų veikų kriptovaliutų rinkoje potencialių nukentėjusiųjų imties, kurie pateikia pranešimus apie pastebėtas nusikalstamas veikas kriptovaliutų rinkoje. Tai reiškia, jog šiuo atveju remiamasi kriptovaliutų rinkos vartotojų teikiama informacija, tačiau panaudojus informacinių technologijų žinias galima būtų praplėsti surenkamos informacijos ratą.

Tolesnės tyrimo kryptys. Būsiami tyrimai galėtų analizuoti tolimesnius neteisėtus veiksmus, panaudojant kriptovaliutų piniginių adresus, bei nusikalstamų veikų ratą, kuriose šie piniginių adresai yra panaudojami. Taip pat būtų galima analizuoti kitokio pobūdžio charakteristikas, kurios leistų plačiau pažvelgti į nusikalstamų veikų kriptovaliutų rinkoje paplitimą bei rizikas, kylančias investuotojui (pvz. jurisdikcijos).

LITERATŪROS IR ŠALTINIŲ SĄRAŠAS

- Aalborg, H. A., Molnar, P., de Vries, J. E., (2019). *What can explain the price, volatility and trading volume of Bitcoin?* Finance Research Letters, Volume 29, P. 255-265. doi.org/10.1016/j.frl.2018.08.010
- Adewole, K., Saxena, N., Bhadauria, S., (2020). *Application of Cryptocurrencies using Blockchain for E-Commerce Online Payment.* Blockchain for Cybersecurity and Privacy, P. 1-46. dx.doi.org/10.1201/9780429324932-16
- Anderson, R., Barton, C., Rainer, B., Clayton, R., Ga, C., Grasso, T., Levi, M., Moore, T., Vasek, M., (2019). *Measuring the Changing Cost of Cybercrime.* The 18th Annual Workshop on the Economics of Information Security. doi.org/10.17863/CAM.41598
- Andonia, M., Robua, V., Flynn, D., Abramb, S., Geachc, D., Jenkinsd, D., McCallumd, P., Peacockd, A. (2019). *Blockchain technology in the energy sector: A systematic review of challenges and opportunities.* Renewable and Sustainable Energy Reviews, Volume 100, P. 143-174. <https://doi.org/10.1016/j.rser.2018.10.014>
- Badawi, E., Jourdan, V. G., (2020). *Cryptocurrencies Emerging Threats and Defensive Mechanisms: A Systematic Literature Review.* IEEE Access, Volume 8, P. 200021 – 200037, 2169-3536. [10.1109/ACCESS.2020.3034816](https://doi.org/10.1109/ACCESS.2020.3034816)
- Bartoletti, M., Pes, B., Serusi, S., (2018). *Data mining for detecting Bitcoin Ponzi schemes.* Crypto Valley Conference on Blockchain Technology (CVCBT), P. 75-84. [10.1109/CVCBT.2018.00014](https://doi.org/10.1109/CVCBT.2018.00014)
- Bartoletti, M., Lande, S., Loddò, A., Pompianu, L., Serusi, S., (2021). *Cryptocurrency Scams: Analysis and Perspectives.* IEEE Access, Volume 9, P. 148353 - 148373. [10.1109/ACCESS.2021.3123894](https://doi.org/10.1109/ACCESS.2021.3123894).
- Bartosevičienė, V. (2010). *Ekonominės statistikos pagrindai.* Kaunas: Technologija, ISBN 9789955258414.
- Beer, Ch., Weber, B., (2015). *Bitcoin – The Promise and Limits of Private Innovation in Monetary and Payment Systems.* Monetary Policy and the Economy, Q4/2014, P. 53-66. ssrn.com/abstract=2556800

- Barnes, P., (2018). *Crypto Currency and its Susceptibility to Speculative Bubbles Manipulation Scams and Fraud*. Journal of Advanced Studies in Finance, ASERS Publishing, Volume 9(2), P. 60-77. [doi.org/10.14505/jasf.v9.2\(18\).03](https://doi.org/10.14505/jasf.v9.2(18).03)
- Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Grant, A. J., Zhang, B., Cloud, K., (2019). *Global Cryptoasset Regulatory Landscape Study*. University of Cambridge Faculty of Law Research Paper No. 23/2019. dx.doi.org/10.2139/ssrn.3379219
- Bočánek, M., (2021). *First Draft of Crypto-Asset Regulation (MiCA) with the European Union and Potential Implementation*. Financial Law Review, (22(2), 37–53. <https://czasopisma.bg.ug.edu.pl/index.php/flr/article/view/6163>
- Bons, W. H. R., Versendaal, J., Zavolokina, L., Shi, L. W., (2020). *Potential and limits of Blockchain technology for networked businesses*. Electronic Markets, 30, P. 189–194. doi.org/10.1007/s12525-020-00421-8
- Boshmaf, Y., Elvitigala, C., Jawaheri, A.H., Wijesekera, P., Sabah, A. M., (2020). *Investigating MMM Ponzi Scheme on Bitcoin*. ASIA CCS '20: The 15th ACM Asia Conference on Computer and Communications Security. doi.org/10.48550/arXiv.1910.12244
- Brenig, Ch., Accorsi, R., Müller, G., (2015). *Economic Analysis of Cryptocurrency Backed Money Laundering*. ECIS 2015 Completed Research Papers. Paper 20, ISBN 978-3-00-050284-2. [10.18151/7217279](https://doi.org/10.18151/7217279)
- Brühl, V., (2017). *Virtual Currencies, Distributed Ledgers and the Future of Financial Services*. Intereconomics Volume 52, Number 6, P. 370–378. doi.org/10.1007/s10272-017-0706-3
- Butler, S., (2019). *Criminal use of cryptocurrencies: a great new threat or is cash still king?* Journal of Cyber Policy, 4(3), P. 326-345. doi.org/10.1080/23738871.2019.1680720
- Campbell-Verduyn, M., (2018). *Bitcoin, crypto-coins, and global anti-money laundering governance*. Crime Law Social Change, Volume 69, P. 283–305. doi.org/10.1007/s10611-017-9756-5
- Caprolu, M., Raponi, S., Oligeri, G., Pietro, D. R., (2021). *Cryptomining makes noise: Detecting cryptojacking via Machine Learning*. Computer Communications, Volume 171, P. 126-139. doi.org/10.1016/j.comcom.2021.02.016
- Chaim, P., Laurini, M. P., (2019). *Is bitcoin a bubble?* Physica A: Statistical Mechanics and Its Applications, Volume 517, P. 222-232. doi.org/10.1016/j.physa.2018.11.031

- Chen, W. L., Zheng, Z. B., Cui, J. H., Ngai, E., Zheng, P., (2018). *Detecting Ponzi schemes on Ethereum: Towards healthier blockchain technology*. Conference: the 2018 World Wide Web Conference. [10.1145/3178876.3186046](https://doi.org/10.1145/3178876.3186046)
- Chen, W., Zheng, Z., Ngai, E., Zheng, P., Zhou, Y., (2019). *Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum*. IEEE Access, Volume 7, P. 37575 - 37586. [10.1109/ACCESS.2019.2905769](https://doi.org/10.1109/ACCESS.2019.2905769)
- Chen, W., Guo, X., Chen, Z., Zheng, Z., & Lu, Y., (2020). *Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem*. Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence Special Track on AI in FinTech, Article No. 621, P. 4506–4512. [10.24963/ijcai.2020/614](https://doi.org/10.24963/ijcai.2020/614)
- Chen, W., Li, X., Sui, Y., He, N., Wang, H., Wu, L., Luo, X., (2021). *SADPonzi: Detecting and Characterizing Ponzi Schemes in Ethereum Smart Contracts*. Proceedings of the ACM on Measurement and Analysis of Computing Systems, Volume 5, Article No. 26, P. 1–30. doi.org/10.1145/3460093
- Chen, L., Peng, J., Liu, Y., Li, J., Xie, F., Zheng, Z (2021). *Phishing Scams Detection in Ethereum Transaction Network*. ACM Transactions on Internet Technology, Volume 21, Issue 1, Article No. 10, P 1–16. <https://doi.org/10.1145/3398071>
- Chudinovskikh, V. M., Sevryugin, V., (2019). *Cryptocurrency regulation in the BriCs Countries and the eurasian economic union*. BRICS Law Journal 6(1), P. 63-81. doi.org/10.21684/2412-2343-2019-6-1-63-81
- Christin, N., (2013). *Traveling the silk road: A measurement analysis of a large anonymous online marketplace*. P. 213-224 in Proceedings of the 22nd international conference on World Wide Web. Association for Computing Machinery. [10.1145/2488388.2488408](https://doi.org/10.1145/2488388.2488408)
- Clouston, P. M., Haslhofer, B., Dupont, B. (2018). *Ransomware payments in the Bitcoin ecosystem*. Journal of Cybersecurity, P. 1-11. [doi:10.1093/cybsec/tyz00](https://doi.org/10.1093/cybsec/tyz00)
- Cohen, J., Cohen, P., West, S. G., Aiken, L. S. (2003). *Applied Multiple Regression/ Correlation Analysis for the Behavioral Sciences*. Mahwah: Lawrence Erlbaum Associates, Inc.
- Cong, L., Li, X., Tang, K., Yang, Y., (2021). *Crypto Wash Trading*. Papers 2108.10984. dx.doi.org/10.2139/ssrn.3530220

- Corbet, S., Hou, Y., Yang Hu, Larkin, C., Lucey, B., Oxley, L., (2022). *Cryptocurrency liquidity and volatility interrelationships during the COVID-19 pandemic*. Finance Research Letters Volume 45, 102137. doi.org/10.1016/j.frl.2021.102137
- Cumming, J. D., Johan, S., Pant, A., (2019). *Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty*. Journal of Risk and Financial Management 12(3):126, P. 1-14. doi.org/10.3390/jrfm12030126
- Čekanavičius, V., Murauskas, G. (2002). *Statistika ir jos taikymai II knyga*. Leidykla TEV, Vilnius, P. 268, ISBN 9955-491-16-7
- De-Vries, P. D., (2016). *An analysis of cryptocurrency, bitcoin, and the future*. International Journal of Business Management and Commerce, Volume 1, No. 12, P. 1-9. <http://ijbmcnet.com/images/Vol1No2/1.pdf>
- Demertzis, M., Wolff, G., (2018). *The economic potential and risks of crypto assets: is a regulatory framework needed?* Policy Contribution, Volume 14, P. 1–14. https://www.bruegel.org/sites/default/files/wp_attachments/PC-14_2018.pdf
- Dhawan, A., Putnins, T. J., (2021). *A New Wolf in Town? Pump-and-Dump Manipulation in Cryptocurrency Markets*. Review of Finance, P.1-41. doi.org/10.1093/rof/rfac051
- Dyhrberg, H. A., (2016). *Bitcoin, gold and the dollar – A GARCH volatility analysis*. Finance Research Letters, Volume 16, P. 85-92. doi.org/10.1016/j.frl.2015.10.008
- Dupuis, D., Smith, D., Gleason, K., (2021). *Old frauds with a new sauce: digital assets and space transition*. Journal of Financial Crime, Volume 30, No. 1, P. 205-220. doi.org/10.1108/JFC-11-2021-0242
- Durieux, T., Ferreira, F. J., Abreu, R., Cruz, P. (2020). *Empirical Review of Automated Analysis Tools on 47,587 Ethereum Smart Contracts*. ICSE '20: Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, P. 530-541. doi.org/10.1145/3377811.3380364
- Eigelshoven, F., Ullrich, A., Parry, D., (2021). *Cryptocurrency Market Manipulation: A Systematic Literature Review*. ICIS 2021, International Conference on Information Systems. <https://aisel.aisnet.org/icis2021/fintech/fintech/1>
- Faccia, A., Moçteanu, N. R., Cavaliere, L. P. L., Mataruna-Dos-Santos, L. J., (2020). *Electronic Money Laundering, The Dark Side of Fintech: An Overview of the Most Recent Cases*. In

- Proceedings of the 2020 12th International Conference on Information Management and Engineering, P. 29-34. doi.org/10.1145/3430279.3430284
- Fang, F., Ventre, C., Basios, M., Kanthan, L., Martinez-Rego, D., Wu, F., Li, L., (2022). *Cryptocurrency trading: a comprehensive survey*. Financial Innovation, Volume 8, Article number 13. [10.1186/s40854-021-00321-6](https://doi.org/10.1186/s40854-021-00321-6)
- Fanusie, Y. J., Robinson, T., (2018). *Bitcoin laundering: An analysis of illicit flows into digital currency services*. Center Sanctions Illicit Finance Elliptic, London, U.K., Tech. Rep., 2018, P. 1-15. cdn2.hubspot.net
- Felix, T.H., von Eije, H., (2019). *Underpricing in the cryptocurrency world: evidence from initial coin offerings*. Managerial Finance, Volume 45, No. 4, P. 563-578. <https://doi.org/10.1108/MF-06-2018-0281>
- Felson, M., Clarke, R. V., (1998). *Opportunity Makes the Thief: Practical Theory for Crime Prevention*. Police Research Series Paper No. 98, Research, Development and Statistics Directorate, London, P. 1-35. https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf
- Ferreira, A., Sandner, P., (2021). *EU search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*. Computer Law & Security Review, Volume 43, 105632. doi.org/10.1016/j.clsr.2021.105632
- Foley, S., Karlsen, J. R., Putniņš, T. J., (2018). *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?* The Review of Financial Studies, Volume 32, Issue 5, P. 1798–1853. doi.org/10.1093/rfs/hhz015
- Fratrič, P., Sileno, G., Klous, S., Engers van., T., (2022). *Manipulation of the Bitcoin market: an agent-based study*. Financial Innovation, Volume 8, Article No. 60. doi.org/10.1186/s40854-022-00364-3
- Fleder, M., Kester, S. M, Pillai, S., (2015). *Bitcoin transaction graph analysis*. Cryptography and Security. <https://doi.org/10.48550/arXiv.1502.01657>
- Gao, B., Wang, H., Xia, P., Wu, S., Zhou, Y., Luo, X., Tyson, G., (2020). *Tracking Counterfeit Cryptocurrency End-to-end*. Proceedings of the ACM on Measurement and Analysis of Computing Systems, Volume 4, Article No. 50, P. 1–28. [10.1145/3410220.3456282](https://doi.org/10.1145/3410220.3456282)

- George, R. P., Peterson, B. L., Yaros, O., Beam, D. L., Dibbell, J. M., Moore, R. C., (2019). *Blockchain for business*. Journal of Investment Compliance, Volume 20, No. 1, P. 17-21. doi.org/10.1108/JOIC-01-2019-0001
- Grobysa, K., Junttila J., Kolarid, W. J., Sapkota, N., (2021). *On the stability of stablecoins*. Journal of Empirical Finance, Volume 64, P. 207-223. doi.org/10.1016/j.jempfin.2021.09.002
- Haq, M. Z., Farzana, K.F., Md, M., (2022). *Could banning virtual assets be a breach of the doctrine of legitimate expectation?* Journal of Money Laundering Control, Volume 25, No. 4, P. 719-729. doi.org/10.1108/JMLC-07-2021-0077
- Hooper, A., Holtbrügge, D., (2020). *Blockchain technology in international business: changing the agenda for global governance*. Review of International Business and Strategy, Volume 30, No. 2, P. 183-200. doi.org/10.1108/RIBS-06-2019-0078
- Hoffmann, C. H., (2021). *Making more research count: a blockchain enabled one-stop shop for immutable behavioral research*. Foresight, Volume 23, No. 6, P. 628-639. doi.org/10.1108/FS-03-2021-0062
- Hong, G., Yang, Z., Yang, S., Zhang, L., Nan, Y., Zhang, Z., Yang, M., Zhang, Y., Qian, Z., Duan, H., (2018). *How You Get Shot in the Back: A Systematical Study about Cryptojacking in the Real World*. CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, P. 1701–1713. doi.org/10.1145/3243734.3243840
- Hu, H., Xu, Y. (2021). *SCSGuard: Deep Scam Detection for Ethereum Smart Contracts*. IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops New York, NY, USA, 2022, pp. 1-6. doi.org/10.48550/arXiv.2105.10426
- Huang, J., Han, S., You, W., Shi, W., Liang, B. Wu, J., Wu, Y., (2021). *Hunting Vulnerable Smart Contracts via Graph Embedding Based Bytecode Matching*. IEEE Transactions on Information Forensics and Security, Volume 16, P. 2144 – 2156. [10.1109/TIFS.2021.3050051](https://doi.org/10.1109/TIFS.2021.3050051)
- Hruska, B. S., Wagener, T., (2018). *The virtual currency regulatory framework in global context*. Capital Markets Law Journal, Volume 13, Issue 4, P. 487–517. doi.org/10.1093/cmlj/kmy028
- Ivanov, N., Lou, J., Chen, T., Li, J., Yan, Q., (2021). *Targeting the Weakest Link: Social Engineering Attacks in Ethereum Smart Contracts*. ASIA CCS '21: Proceedings of the

- 2021 ACM Asia Conference on Computer and Communications Security, P. 787-801.
doi.org/10.1145/3433210.3453085
- Jiaying, J., (2020). *Regulating Blockchain? A Retrospective Assessment of China's Blockchain Policies and Regulations*. Tsinghua China L. Rev., 12. <https://ssrn.com/abstract=3654439>
- Jin, J., Zhou, J., Jin, C., Yu, S., Zheng, Z., Xuan, Q., (2022). *Dual-channel Early Warning Framework for Ethereum Ponzi Schemes*. Communications in Computer and Information Science, Volume 1640. doi.org/10.1007/978-981-19-7532-5_17
- Kamps, J., Kleinberg, B., (2018). *To the moon: defining and detecting cryptocurrency pump-and-dumps*. Crime Science, Volume 7, Article No. 18. doi.org/10.1186/s40163-018-0093-5
- Kerr, D. S., Loveland, K. A., Smith, K. T., Smith, L. M., (2023). *Cryptocurrency Risks, Fraud Cases, and Financial Performance*. *Cryptocurrencies and Risk Management*, 11(3):51. <https://doi.org/10.3390/risks11030051>
- Kirkpatrick, K., Stephens, A., Gerber, J., Nettesheim, M., Bellm, S., (2021). *Understanding regulatory trends: digital assets & anti-money laundering*. Journal of Investment Compliance, Volume 22, No. 4, P. 345-353. doi.org/10.1108/JOIC-07-2021-0033
- Khan, R., Hakami, T. A., (2022). *Cryptocurrency: usability perspective versus volatility threat*. Journal of Money and Business, Volume 2, No. 1, P. 16-28. doi.org/10.1108/JMB-11-2021-0051
- Lambert, T., Liebau, D., Roosenboom, P., (2022). *Security token offerings*. Small Business Economics, Volume 59, P. 99–325. doi.org/10.1007/s11187-021-00539-9
- Leuprecht, C., Jenkins, C., Hamilton, R., (2022). *Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency*. Journal of Financial Crime, Volume ahead-of-print No. ahead-of-print. doi.org/10.1108/JFC-07-2022-0161
- Li, T., Shin, D., Wang, B., (2018). *Cryptocurrency Pump-and-Dump Schemes*. dx.doi.org/10.2139/ssrn.3267041
- Luther, W. J., (2019). *Regulatory Ambiguity in the Market for Bitcoin*. The Review of Austrian Economics, Volume 35, P. 1-14. dx.doi.org/10.2139/ssrn.3352894
- Marella, V., Upreti, B., Merikivi, J., Tuunainen, V. K., (2020). *Understanding the creation of trust in cryptocurrencies: the case of Bitcoin*. Electron Markets, Volume 30, P. 259–271. doi.org/10.1007/s12525-019-00392-5

- Mansourifar, H., Chen, L., Shi, W., (2020). *Hybrid Cryptocurrency Pump and Dump Detection*. Artificial Intelligence. doi.org/10.48550/arXiv.2003.06551
- Mattke, J., Maier, Ch., Reis, L., (2020). *Is Cryptocurrency Money?: Three Empirical Studies Analyzing Medium of Exchange, Store of Value and Unit of Account*. SIGMIS-CPR'20: Proceedings of the 2020 on Computers and People Research Conference, P. 26–35. [10.1145/3378539.3393859](https://doi.org/10.1145/3378539.3393859)
- Möser, M., Böhme, R., Breuker, D., (2013). *An inquiry into money laundering tools in the Bitcoin ecosystem*. 2013 APWG eCrime Researchers Summit, IEEE. [10.1109/eCRS.2013.6805780](https://doi.org/10.1109/eCRS.2013.6805780)
- Moore, T., Christin, N., Szurd, J., (2018). *Revisiting the Risks of Bitcoin Currency Exchange Closure*. ACM Trans. Internet Technol, Volume 18, Issue 4, Article 50, P. 1-18. doi.org/10.1145/3155808
- Morgia, L. M., Mei, A., Sassi, F., Stefa, J., (2021). *The Doge of Wall Street: Analysis and Detection of Pump and Dump Cryptocurrency Manipulations*. ACM Transactions on Internet Technology. doi.org/10.1145/3561300
- Morgia, L. M., Mei, A., Sassi, F., Stefa, J., (2021). *Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations*. 29th International Conference on Computer Communications and Networks (ICCCN). [10.1109/ICCCN49398.2020.9209660](https://doi.org/10.1109/ICCCN49398.2020.9209660)
- Murko, A., Vrhovec, R. L. S., (2019). *Bitcoin adoption: Scams and anonymity may not matter but trust into Bitcoin security does*. CECC 2019: Proceedings of the Third Central European Cybersecurity Conference, Article No. 15, P. 1–6. doi.org/10.1145/3360664.3360679
- Nabilou, H., Prum, A., (2019). *Central Banks and Regulation of Cryptocurrencies*. Review of Banking and Financial Law (Forthcoming), University of Luxembourg Law Working Paper No. 2019-014. <https://ssrn.com/abstract=3421417>
- Nakamoto, S., (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. <https://bitcoin.org/bitcoin.pdf>
- Naseem, F., Aris, A., Babun, L., Tekiner, E., Uluagac, A. S., (2021). *MINOS: A Lightweight Real-Time Cryptojacking Detection System*. 28th Annual Network and Distributed System Security Symposium (NDSS). doi.org/10.14722/ndss.2021.24444

- Nizzoli, L., Tardelli, S., Avvenuti, M., Cresci, S., Tesconi, M., Ferrara, E., (2020). *Charting the landscape of online cryptocurrency manipulation*. IEEE Access, Volume 8. [10.1109/ACCESS.2020.3003370](https://doi.org/10.1109/ACCESS.2020.3003370)
- Oh, J., Shong, I., (2017). *A case study on business model innovations using Blockchain: focusing on financial institutions*. Asia Pacific Journal of Innovation and Entrepreneurship, Volume 11, No. 3, P. 335-344. doi.org/10.1108/APJIE-12-2017-038
- Oordt van R. C. M., (2022). *The Emerging Autonomy-Stability Choice for Stablecoins*. Tinbergen Institute Discussion Paper 2022-015/IV. doi.org/10.2139/ssrn.4041945
- Phan, L., Li, S., Mentzer, K., (2019). *Blockchain technology and the current discussion on fraud*. International Association for Computer Information Systems, Paper 28. http://www.iaicis.org/iis/2019/4_iis_2019_8-20.pdf
- Phillips, R., Wilder, H., (2020). *Tracing cryptocurrency scams: Clustering replicated advance-fee and Phishing Websites*. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). [10.1109/ICBC48266.2020.9169433](https://doi.org/10.1109/ICBC48266.2020.9169433)
- Potgieter, P.H., Howell, B.E., (2021). *Regulating cryptocurrencies: mapping economic objectives and technological feasibilities*. TPRC49: The 49th Research Conference on Communication, Information and Internet Policy. [10.2139/ssrn.3927658](https://doi.org/10.2139/ssrn.3927658)
- Puthal, D., Malik, N., Mohanty, P., S., Kougiianos E., Yang, C., (2018). *The Blockchain as a Decentralized Security Framework*. IEEE Consumer Electronics Magazine, Volume 7, No. 2, P. 18-21. [10.1109/MCE.2017.2776459](https://doi.org/10.1109/MCE.2017.2776459).
- Reddy, E., Minaar, A., (2018). *Cryptocurrency: a tool and target for cybercrime*. Acta Criminologica: Southern African Journal of Criminology, Volume 31, No. 3 P. 71-92. researchgate.net/publication/338572871_cryptocurrency_a_tool_and_target_for_cybercrime
- Reid, F., Harrigan M., (2011). *An Analysis of Anonymity in the Bitcoin System*. In: Altshuler, Y., Elovici, Y., Cremers, A., Aharony, N., Pentland, A. (eds) Security and Privacy in Social Networks. Springer, New York, NY. doi.org/10.1007/978-1-4614-4139-7_10
- Rehman ur, M. H., Salah, K., Damiani, E., Svetinovic, D., (2020). *Trust in blockchain cryptocurrency ecosystem*. IEEE Transactions on Engineering Management, Volume 67, Issue 4, P. 1196-1212. doi.org/10.1109/TEM.2019.2948861

- Roppelt, J.C., (2019). *Security risks surrounding cryptocurrency usage: a study on the security risks of cryptocurrencies and how security perception affects usage*. EEMCS: Electrical Engineering, Mathematics and Computer Science. <https://essay.utwente.nl/79471/>
- Savona, P., (2022). *Prospects for Reforming the Money and Financial System*. Open Economies Review, Volume 33, P. 187–195. doi.org/10.1007/s11079-021-09628-4
- Scheau, C. M., Crăcunescu, L.S., Brici, I., Achim, V. M., (2020). *A Cryptocurrency Spectrum Short Analysis*. J. Risk Financial Management., Volume 13, Issue 8, P. 184. doi.org/10.3390/jrfm13080184
- Semenihin, A., Kondrashin, A., (2017). *Leading role of state as a regulator of crypto currency*. Proceedings of the 2nd International Conference on Social, Economic and Academic Leadership (ICSEAL 2018). Advances in Social Science, Education and Humanities Research. doi.org/10.2991/icseal-18.2018.47
- Semenihin, A., Kondrashin, A., (2018). *Leading role of state as a regulator of crypto currency*. Proceedings of the 2nd International Conference on Social, Economic and Academic Leadership (ICSEAL 2018), Volume 217, P. 329-334. doi.org/10.2991/icseal-18.2018.47
- Sharma, P. S., Sharma, A., (2018). *Using Crypto Currency and Associated Advantages and Disadvantages*. International Journal of Economics & Finance Research & Applications Volume 2, Issue 2, P. 17-22. [researchgate.net/publication/337973690_using_crypto_currency_and_associated_advantages_and_disadvantages](https://www.researchgate.net/publication/337973690_using_crypto_currency_and_associated_advantages_and_disadvantages)
- Shi, L., Li, Y, Liu, J., Shan, B., Chen, H., (2019). *Dynamic Distributed Honeypot Based on Blockchain*. IEEE Access, Volume 7, P. 72234-72246. [10.1109/ACCESS.2019.2920239](https://doi.org/10.1109/ACCESS.2019.2920239)
- Son, J., Bilgin, M.H., Ryu, D., (2022). *Consumer choices under new payment methods*. Finance Innovations, Volume 8, Article No. 82, P. 1-22. doi.org/10.1186/s40854-022-00387-w
- Sotiropoulou, A., Guegan, D., (2017). *Bitcoin and the challenges for financial regulation*. Capital Markets Law Journal, Volume 12, No. 4, P. 466-479. doi.org/10.1093/cmlj/kmx037
- Solat, S., Potop-Butucaru, M., (2016). *ZeroBlock: Preventing Selfish Mining in Bitcoin*. ArXiv abs/1605.02435. [researchgate.net/publication/302569271](https://www.researchgate.net/publication/302569271)
- Teichmann, F. M. J., Falker, M. C., (2020). *Money laundering via cryptocurrencies – potential solutions from Liechtenstein*. Journal of Money Laundering Control, Volume 24 No. 1, P. 91-101. doi.org/10.1108/JMLC-04-2020-0041

- Teichmann, F. M. J., Falker, M. C., (2021). *Cryptocurrencies and financial crime: solutions from Liechtenstein*. Journal of Money Laundering Control, Volume 24, No. 4, P. 775-788. doi.org/10.1108/JMLC-05-2020-0060
- Temple, S. (2000). *Cybertrading: Financial markets and the internet*. Australian Law Librarian, 8(4)2000 Volume 8, P. 337-345. austlii.edu.au/au/journals/AULawLib/2000/60.pdf
- Tekiner, E., Acar, A., Uluagac S., Kirda, E., Selcuk A., (2021). *SoK: Cryptojacking Malware*. IEEE European Symposium on Security and Privacy (EuroS&P), Vienna, Austria, 2021, P. 120-139. [10.1109/EuroSP51992.2021.00019](https://doi.org/10.1109/EuroSP51992.2021.00019)
- Towler, M. B., (2020). *Blockchains and institutional competition in innovation systems*. Journal of Entrepreneurship and Public Policy, Volume 9, No. 2, P. 185-193. doi.org/10.1108/JEPP-03-2019-0015
- Tredinnick, L., (2019). *Cryptocurrencies and the blockchain*. Business Information Review, Volume 36, Issue 1, P. 39–44. doi.org/10.1177/0266382119836314
- Trozze, A., Kamps, J., Akartuna, A. E., Hetzel, J. F., Kleinberg, B., Davies, T., Johnos, D. S., (2022). *Cryptocurrencies and future financial crime*. Crime science, Volume 11, Article No. 1. [10.1186/s40163-021-00163-8](https://doi.org/10.1186/s40163-021-00163-8)
- Varlioglu, S., Gonen, B., Ozer, M., Bastug, M., (2020). *Is Cryptojacking Dead After Coinhive Shutdown?* 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 2020, pp. 385-389. [10.1109/ICICT50521.2020.00068](https://doi.org/10.1109/ICICT50521.2020.00068)
- Vakilinia, I., (2022). *Cryptocurrency Giveaway Scam with YouTube Live Stream*. 2022 IEEE 13th 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, NY, USA, 2022, P. 0195-0200. [10.1109/UEMCON54665.2022.9965686](https://doi.org/10.1109/UEMCON54665.2022.9965686)
- Vasek, M., Moore, T., (2015). *There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams*. In: Böhme, R., Okamoto, T. (eds) Financial Cryptography and Data Security. FC 2015. Lecture Notes in Computer Science, Volume 8975. Springer, Berlin, Heidelberg. doi.org/10.1007/978-3-662-47854-7_4
- Vasek, M., Moore, T., (2019). *Analyzing the Bitcoin Ponzi Scheme Ecosystem*. Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, Volume 10958. Springer, Berlin, Heidelberg. doi.org/10.1007/978-3-662-58820-8_8

- Wang, J., Chen, P., Xu, X., Wu, J., Shen, M., Xuan, Q., Yang, X., (2022). *TSGN: Transaction Subgraph Networks Assisting Phishing Detection in Ethereum*. Part of the Communications in Computer and Information Science book series, Volume 1490. doi.org/10.48550/arXiv.2208.1293
- Weber, M., Domeniconi G., Chen, J., Weidele, I. K. D., Bellei, C., Robinson, T., Leiserson, E. C., (2019). *Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics*. Tutorial in the Anomaly Detection in Finance Workshop at the 25th SIGKDD Conference on Knowledge Discovery and Data Mining. doi.org/10.48550/arXiv.1908.02591
- Wolfgang, K., H., Campbell R. H., Raphael C. G., (2019). *Editorial: Understanding Cryptocurrencies*. Journal of Financial Econometrics, Volume 18, Issue 2, P. 181–208. doi.org/10.1093/jjfinec/nbz033
- Wronka, C., (2021). *Financial crime in the decentralized finance ecosystem: new challenges for compliance*. Journal of Financial Crime, Vol. 30 No. 1, pp. 97-113 doi.org/10.1108/JFC-09-2021-0218
- Wronka, C., (2022). “*Cyber-laundering*”: *the change of money laundering in the digital age*. Journal of Money Laundering Control, Volume 25, No. 2, P. 330-334. doi.org/10.1108/JMLC-04-2021-0035
- Xia, P., Wang, H., Luo, X., Wu, L., Zhou, Y., Bai, G., Xu, G., Huang, G., Liu, X. (2020a). *Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams*. 2020 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA, USA, 2020, pp. 1-14. [10.1109/eCrime51433.2020.9493255](https://doi.org/10.1109/eCrime51433.2020.9493255)
- Xia, P., Wang, H., Zhanga, B., Ji, R., Bingyu Gao, B., Wu, L., Luo, X., Xu, G., (2020b). *Characterizing cryptocurrency exchange scams*. Computers and Security, Volume 98, P. 1-17. doi.org/10.1016/j.cose.2020.101993
- Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Lou, X., Zhang, C., Xiao, X., Xu., G., (2021). *Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange*. Cryptography and Security . Proc. ACM Meas. Anal. Comput. Syst. 5, 3, Article 39 (December 2021), 26 pages. doi.org/10.48550/arXiv.2109.00229

RESEARCH ON CRIMINAL ACTIVITY IN CRYPTOCURRENCY MARKET

Stela ANDRIUŠKAITĖ

Master thesis

Finance and Banking master study program

Vilnius University, Faculty of Economics and Business Administration

Supervisor – prof. A. Šapkauskienė, PhD

Vilnius, 2024

SUMMARY

85 pages, 20 tables, 14 pictures, 120 references.

The aim of the thesis. To conduct research of criminal activity in the cryptocurrency market.

The objectives of the thesis:

1. Conducting a comprehensive literature review on criminal acts prevalent in the cryptocurrency market.
2. Formulating a research methodology tailored to the study of criminal activity in the cryptocurrency market.
3. Undertaking research on criminal activity within the cryptocurrency market, scrutinizing characteristics established during the investigation of criminal acts, and presenting the resultant research findings.

The methods deployed by the thesis. Data collection, descriptive statistics, Pearson correlation, simple regression, Chi-square, statistical data analysis, analysis of research results, methods of analysis, summarization and evaluation of research results.

The Master's thesis consists of four parts: literature review, research methodology, analysis of research results, and conclusions and proposals.

The literature review part is subdivided into three subsections: the concept and characteristics of cryptocurrencies, regulatory issues in the cryptocurrency market, and criminal activities in the cryptocurrency market. The subsection on the concept and characteristics of cryptocurrencies delves into the analysis of cryptocurrency definitions, operating principles, and a comparative

examination of cryptocurrency and traditional fiat and gold-standard-based markets. The regulatory issues subsection explores contemporary challenges associated with cryptocurrency market regulation, encompassing both theoretical and practical aspects. Lastly, the criminal activities occurring in the cryptocurrency market subsection identifies and discusses criminal behavior in the cryptocurrency market, drawing support from pertinent scientific literature.

To conduct research on the occurrence of criminal activity in the cryptocurrency market, the methods of data collection, descriptive statistics, Pearson correlation, simple regression, Chi-square, statistical data analysis, analysis of research results, methods of analysis, summarization and evaluation were used. The research was conducted from 1st March 2023 to 31st March 2023 utilizing manually collected data from BitcoinAbuse.com and Blockchain.com websites. Such data is related to addresses of cryptocurrency wallets, which were used to commit criminal activity in the cryptocurrency market, as well as other related characteristics. The research findings reveal that criminal acts within the cryptocurrency market extend beyond those identified in existing scientific literature. Furthermore, a significant number of cryptocurrency wallet addresses are linked to criminal acts aimed at acquiring cryptocurrencies, not through fraudulent means, but with an adverse impact on users in the cryptocurrency market. Additionally, a considerable portion of crypto-related crimes is not concentrated within a small number of cryptocurrency wallet addresses.

The results of this Master's thesis are not intended for publication.

PRIEDAI

Priedas Nr. 1. Mokslinėje literatūroje aptartos nusikalstamos veikos

Sudaryta autorės, remiantis išnagrinėta mokslinė literatūra.

Nr.	Mokslinės literatūros skaičius	Nusikalstama veika, aprašyta straipsniuose	Autoriai
1	1	<i>Air drop</i> sukčiavimas	Gao, B., ir kt., 2020.
2	1	Aukojimo sukčiavimas	Xia, P., ir kt., 2020a.
3	3	Apgaulingos piniginės sukčiavimas	Vasek, 2017; Vasek ir kt., 2015, Murko, A., ir kt., 2019.
4	1	Arbitražo sukčiavimas	Gao, B., ir kt., 2020.
5	3	Avansinio mokėjimo sukčiavimas	Phillips, R., ir kt., 2020, Xia, P., ir kt., 2021, Bartoletti, M., ir kt., 2021.
6	2	Dovanų įteikimo sukčiavimas	Xia, P., ir kt., 2020a, Vakilinia, I., 2022.
7	5	Išmaniųjų sutarčių „honeypots“	Shi, L., ir kt., 2019, Ivanov, N., ir kt., 2021, Hu, H., ir kt. 2021, Huang, J., ir kt. 2021, Durieux, T., ir kt. 2020.
8	4	Kasybos sukčiavimas	Vasek, M., ir kt., 2015, Solat, S., ir kt., 2016, Badawi, E., ir kt., 2020, Anderson, R., ir kt. 2019.
9	4	Keitimo sukčiavimas	Vasek, M., ir kt., 2015, Semenišin, A., ir kt., 2017, Moore, T., ir kt., 2018, Murko, A., ir kt., 2019, Xia, P., ir kt., 2020.
10	6	Kenkėjiškų programų kasimo	Hong, G., ir kt., 2018, Anderson, R., ir kt., 2019, Varlioglu, S., ir kt., 2020, Caprolu, M., ir kt., 2021, Naseem, F., ir kt., 2021, Tekiner, E., ir kt., 2021.
11	3	Kenkėjiškų programų sukčiavimas	Clouston, P. M., ir kt., 2018, Xia, P., ir kt., 2020b, Bartoletti, M., ir kt., 2021.
12	4	Žvejyba	Chen, W., ir kt., 2020, Chen, L., ir kt., 2021, Scheau, C., M., <i>at el.</i> , 2021, Wang, J., ir kt., 2022.
13	1	Piramidės schema	Jiaying, J., 2020.
14	8	Pinigų plovimo	Möser, M., ir kt., 2013, Brenig, Ch., ir kt., 2015, Weber, M., ir kt., 2019, Faccia, A., ir kt., 2020, Teichmann F. M. J., ir kt., 2021, Bartoletti, M., ir kt., 2021,

			Wronka, C., 2022, Haq, M., Z., ir kt., 2022.
15	7	Ponzi schema	Vasek, M. ir kt., 2015, Bartoletti, M., ir kt., 2018, Bartoletti, M., ir kt., 2021, Chen, W., ir kt., 2018, Reddy, E., ir kt., 2018, Murko, A., ir kt., 2019, Boshmaf, Y., ir kt., 2020.
16	1	Plovimo prekyba	Cong, W. L., ir kt., 2021.
17	3	Pradinių monetų siūlymas	Barnes, P., 2018, Felix, T. H., ir kt., 2019, Bartoletti, M., ir kt., 2021.
18	8	<i>Pump</i> ir dump schema	Kamps, J., 2018, Mansourifar, H., ir kt., 2020, Morgia, L., M., ir kt., 2021, Nizzoli, L., 2020, Eigelshoven, F., ir kt., 2021, Fratrič, P., ir kt., 2022.
19	1	Savanaudiška kasyba	Phan, L., ir kt., 2019.

Priedas Nr. 2. Mokslinėje literatūroje identifikuotos nusikalstamos veikos kriptovaliutų rinkoje

Sudaryta autorės, remiantis išnagrinėta moksline literatūra.

Nr.	Nusikalstamos veikos kriptovaliutų rinkoje pavadinimas	Anglų atitikmuo	Aprašymas
1	<i>Air drop</i> sukčiavimas	<i>Air drop scam</i>	„Airdrop“ yra kriptovaliutos žetono platinimas, dažniausiai nemokamas, daugeliu vartotojų pinigines adresų. „Airdrop“ pirmiausia įgyvendinama kaip būdas sulaukti dėmesio iš naujų vartotojų. Nusikalstama veika pasireiškia tuo, kad, nusikalstamą veiką vykdančias asmenys pažada, kad išsiuntus tam tikrą kriptovaliutos kiekį (padirbto) žetono adresu, nukentėjusysis gaus (imituojamus) oficialius žetonus pagal fiksuotą valiutos kursą. Tačiau nukentėję asmenys nieko negauna (Gao, B., ir kt., 2020).
2	Aukojimo sukčiavimas	<i>Donation scams</i>	Šios nusikalstamos veikos metu, nusikaltėliai apsimeta, jog yra iš tam tikrų labdarinių organizacijų, prašydami paaukoti kriptovaliutas (Xia, P., ir kt., 2020a).
3	Apgaulingos piniginės	<i>Scam wallet</i>	Apgaulingos piniginės yra apgaulingos paslaugos, kurios prisidengia kriptovaliutų pinigėmis, kad būtų galima siurbti dalį arba visą joms pervestą valiutą (Vasek, M., ir kt., 2015, Murko, A., ir kt., 2019).
4	Arbitražo sukčiavimas	<i>Arbitrage scams</i>	Šios nusikalstamos veikos metu, nusikalstamą veiką vykdančias asmenys platformoje pateikia nuorodą, kurią paspaudę vartotojai neva gali siųsti kriptovaliutas ir neva gauti žetonus, tačiau gauna netikrus (beverčius) žetonus, o nusikalstamą veiką įvykdęs asmuo pasipelno iš asmenų pervestų kriptovaliutų (Gao, B., ir kt., 2020).
5	Avansinio mokėjimo sukčiavimas	<i>Advance-fee scam</i>	Šios nusikalstamos veikos metu nusikalstamą veiką vykdančias asmenys nurodo aukai pervesti avansinį mokėjimą kriptovaliutomis už tam tikrą prekę, tačiau vėliau šiuos pinigus

			pasiima sau ir neduoda aukai sutartos prekės (Phillips, R., ir kt., 2020, Xia, P., ir kt., 2021, Bartoletti, M., ir kt., 2021).
6	Dovanų įteikimo sukčiavimas	<i>Giveaway scams</i>	Šios nusikalstamos veikos metu, nusikalstamą veiką vykdantys asmenys pažada aukoms tam tikrą atlygį už atsiųstas kriptovaliutas (Xia, P., ir kt., 2020a, Vakilinia, I., 2022).
7	Išmaniosios sutartys „honeypots“	<i>Smart contracts honeypots</i>	„Honeypots“ yra išmaniosios sutartys, kurios, atrodo turinčios dizaino problemų, leidžiančių savavališkam vartotojui išleisti kriptovaliutą iš sutarties, jei vartotojas iš anksto į sutartį siunčia tam tikrą kriptovaliutos kiekį. Vietoje to yra įšaldomos vartotojo lėšos ir padaroma taip, jog prie jų gali prieiti tik nusikalstamą veiką vykdantis asmuo (Shi, L., ir kt., 2019, Ivanov, N., ir kt., 2021, Hu, H., ir kt. 2021, Huang, J., ir kt. 2021, Durieeux, T., ir kt. 2020).
8	Kasybos sukčiavimai	<i>Mining scam</i>	Tai yra tokio tipo nusikalstama veika, kai asmenys investuoja pinigus į kriptovaliutų kasybą, siekiant gauti didelę gražą, tačiau jokios gražos negauna, o investuoti pinigai atitenką nusikalstamą veiką vykdančiam asmeniui (Vasek, M., ir kt., 2015, Badawi, E., ir kt., 2020, Anderson, R., ir kt. 2019).
9	Keitimo sukčiavimai	<i>Exchange scam</i>	Ši nusikalstama veika pasireiškia tuo, jog yra sukuriamos apgaulingos keitimo paslaugos, kurios pritraukia vartotojus palankiais valiutų kursais. Kai vartotojai įsigyja kriptovaliutą, nusikalstamą veiką vykdantys asmenys neteisėtai įgyja vartotojų pinigus be jokių sugrąžinimų (Vasek, M., ir kt., 2015, Semenišin, A., ir kt., 2017, Moore, T., ir kt., 2018, Murko, A., ir kt., 2019, Xia, P., ir kt., 2020b).
10	Kenkėjiškų programų kasimas	<i>Mining malware / cryptojacking</i>	Šios nusikalstamos veikos vykdymo metu yra sukuriamos kenkėjiškos programos, kurios paveikia vartotojų kompiuterius ir suteikia galimybę nusikalstamą veiką vykdančiam asmeniui iškasti kriptovaliutas (Hong, G., ir kt., 2018, Anderson, R., ir kt., 2019, Varlioglu,

			S., ir kt., 2020, Caprolu, M., ir kt., 2021, Naseem, F., ir kt., 2021, Tekiner, E., ir kt., 2021).
11	Kenkėjiškų programų paskleidimas	<i>Malware scams</i>	Šios nusikalstamos veikos metu nusikalstamą veiką vykdančio asmens paskleidžia kenkėjišką programą, kuri pažeidžia asmens telefoną, kompiuterį, kol asmuo nesumoka nustatytos sumos kriptovaliutomis (Xia, P., ir kt., 2020a, Bartoletti, M., ir kt., 2021).
12	<i>Žvejyba</i>	<i>Phishing</i>	Šios nusikalstamos veikos metu kriptovaliutų atžvilgiu yra sukuriama netikras internetinis tinklapis, kuriame raginama vartotojus pateikti savo asmeninę informaciją kuri toliau gali būti naudojama tęsti nusikalstamas veikas vartotojų vardu (Chen, W., ir kt., 2020, Chen, L., ir kt., 2021, Scheau, C., M., <i>at el.</i> , 2021, Wang, J., ir kt., 2022).
13	Piramidės schema	<i>Pyramid schemes</i>	Ši nusikalstama veika yra apgaulinga pinigų uždirbimo sistema, pagrįsta vis didesnio „investuotojų“ skaičiaus įdarbinimu. Kriptovaliutų atveju tai yra kriptovaliutų investavimo schema (Jiaying, J., 2020).
14	Pinigų plovimas	<i>Money laundering</i>	Šios nusikalstamos veikos vykdymo metu, nusikalstamą veiką vykdančias asmenys neteisėtai gautus pinigus perkelia per kriptovaliutų pinigines prieš išgrynindami lėšas kriptovaliutų biržoje, tokiu būdu panaikinant sąlygas atsekti iš kur buvo įgytos lėšos (Möser, M., ir kt., 2013, Brenig, C., ir kt., 2015, Weber, M., ir kt., 2019, Faccia, A., ir kt., 2020, Teichmann F. M. J., ir kt., 2021, Bartoletti, M., ir kt., 2021, Wronka, C., 2022 Haq, M., Z., ir kt., 2022).
15	Ponzi schema	<i>Ponzi scheme</i>	Ponzi schema kriptovaliutų rinkoje yra atitinkamo tradiciniai Charlio Ponzio sukčiavimo technikai. Šios nusikalstamos veikos metu už investicijas yra žadama didelė palūkanų norma. Investicijų grąža investuotojams yra išmokama iš naujai į schemą įsitraukusių investuotojų. Ši schema tęsiasi iki

			tol, kol bus nebeįmanoma surasti naujų investuotojų (Vasek, M. ir kt., 2015, Bartoletti, M., ir kt., 2018, Bartoletti, M., ir kt., 2021, Chen, W., ir kt., 2018, Reddy, E., ir kt., 2018, Murko, A., ir kt., 2019, Boshmaf, Y., 2020).
16	Plovimo prekyba	<i>Wash trading</i>	Ši nusikalstama veika apibūdinama kaip tuo pačiu metu vykstantys tų pačių akcijų (arba, šiuo atveju, kriptovaliutų) pirkimo ir pardavimo sandoriai, sudarant rinkos aktyvumo iliuziją (Cong, W. L., ir kt. 2021).
17	Pradinių monetų siūlymo sukčiavimas	<i>Initial Coin Offering (ICO) scams</i>	Nusikalstama veika, susijusi su pradinių monetų siūlymo sukčiavimu, yra tokia nusikalstama veika, kurios vykdymo metu yra parduodamos netikros kriptovaliutos, kurios nesukurs jokios gražos investuotojui (Barnes, P., 2018, Felix, T. H., ir kt., 2019, Bartoletti, M., ir kt., 2021).
18	<i>Pump ir dump</i> schema	<i>Pump and dump scheme</i>	Šios nusikalstamos veikos metu, nusikalstamą veiką vykstantys asmenys sukaupia mažos vertės valiutos kiekius ir siekia juos dirbtinai branginti, skleidami dezinformaciją. Kai kriptovaliutos vertė fiktyviai didėja, jie parduoda viską, kad uždirbtų pelną (Kamps, J., 2018, Mansourifar, H., ir kt., 2020 Morgia, L., M., ir kt., 2021, Nizzoli, L., 2020, Eigelshoven, F., ir kt., 2021, Morgia, L., M., 2021, Fratrič, P., ir kt., 2022).
19	Savanaudiška kasyba	<i>Selfish mining</i>	Savanaudiška kasyba yra tokio tipo nusikalstama veika, kai kasėjai tikslingai slepia rastus blokus, tam kad galėtų kasti ant jau rastų blokų ir tokiu būdu kiti kasėjai eikvoja savo skaičiavimo galią bandydami iškasti jau rastą bloką (Phan, L., ir kt., 2019).

Priedas Nr. 3. BitcoinAbuse.com duomenys tyrimo laikotarpyje

Sudaryta autorės, remiantis BitcoinAbuse.com duomenimis.

Nr.	Kripto pinigines adresas	Kiek kartų buvo pateiktas pranešimas	Nusikalstama veika (lietuviškai (<i>angliškai</i>))	Paskutinį kartą pateiktas pranešimas	Pirmą kartą pateiktas pranešimas
1.	bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h	400	Žvejyba, teroristų finansavimas (<i>Phishing, terrorist finansing</i>)	2023-03-01	2021-11-21
2.	1FbN9mgTzppSUGRgBs1o7N8FpPQVfoRrKd	330	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-01	2021-09-01
3.	1P8Bb873JUZSS7Jp4EDx8Uw aQakGAWhq9S	11	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-01	2023-02-15
4.	bc1qmx76pwe64u2mxy4fdjw8rtxj3ehvdnafgraul2	3	Kripto valiutos investavimo sukčiavimas (<i>Crypto investment scam</i>)	2023-03-01	2023-02-23
5.	bc1qgg5kjckagkr2yk7usl5fajlu9032gryxxmjfys	6	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-01	2023-01-26

6.	bc1q0tj9nn8vjz996vw5ywd0m wc240n8zefuejax52	25	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-01	2022-01-18
7.	bc1qaad67kkffvnuqe0q3vsldcn cc5e5zpg2vjhe9m	3	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-01	2022-04-15
8.	34tiPzriGj3kbYsW28XgE8nH wk18XDBX7E	3	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-01	2023-02-28
9.	DANbgsdXKLWuzP7d7113BY VyGupuzD4CCi	3	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-01	2023-02-28
10.	3FPD9TtnGdqHnc3RVqSSY16 fjL5XtHFokL	3	Žvejyba (<i>Phishing</i>)	2023-03-01	2023-02-28
11.	1Q22EJNqor9f1KUoToahDBg 1XBL5QGp998	6	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-01	2023-02-28
12.	1252NnPXaxc3tkTCGDmfvbX NcU4mfPCCyo	3	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-01	2023-03-01
13.	bc1q98jf2h6nn0cchfapktfltkjmq le0q7pp0ceh2e	3	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje	2023-03-01	2023-03-01

			erdvėje (<i>Malware scams, sextortion</i>)		
14.	bc1qu9dnf40nzm9a6ucedullm2 egat35n55zs8jec9	41	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-01	2022-04-23
15.	bc1qft68zdrgrqamaq4chf15h4qz ptc02zkd2jrcjs	2	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-01	2023-03-01
16.	3KQRDQiKBzK9p6CVkGWf GFLeX8NDun6gAH	11	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-01	2023-02-20
17.	1MKjuerdKXjWKwMwRZnj5 PcX16YikxvSv8	2	Kripto valiutos investavimo sukčiavimas (<i>Crypto investment scam</i>)	2023-03-01	2023-02-28
18.	12nEVuGNtRFMVjeVmLtD4n t2sHX68S47yH	176	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-01	2022-12-04
19.	1LPEXXSN1t4buFWGK7AbJi A57hCKAcJaAT	11	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-02-18
20.	bc1q87nhmmdza2xyfx25vufpf7 gmp80nga28zv49hj	5	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-02	2023-02-27
21.	bc1qw6k0gshwz2u639y2wvua5 gfthse6ztkj9nztvdv	12	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-02	2023-02-24

22.	1MTz9A2NH6DXxjYyEmhVc 2sBhtJnjgenPK	1	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-03-02
23.	146MDjQY2TCQXF9YQx4je V3j5JKQx283cA	3	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-03-02
24.	1P4DZNDv9CjhyrMKDN3pt9 TSBiVt5UDYRW	1	Žvejyba, Kripto valiutos investavimo sukčiavimas (<i>Phishing, Crypto investment scam</i>)	2023-03-02	2023-03-02
25.	bc1qqmun3g4cq4vxr2zvv4sd54 3nxcemdjk89pkv6l	1	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-02	2023-03-02
26.	1NGTAxhLipEp2JfvVh2q1uQ8 UpKhyxQ1zJ	1	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-02	2023-03-02
27.	14kZFbztXBYHaVskcGUgYU 2UTxVJU97N81	1	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-02	2023-03-02
28.	bc1qtw9jqxszv55v4s5m5pja0sh rk50ft8wadzllww	19	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-02-05

29.	bc1qrygp87s80gkvyaxhks9r2pzh54xa5aa2xptwl	2	Kenkėjiškų programų paskleidimas, (<i>Malware scams</i>)	2023-03-02	2023-03-02
30.	1DEoL2Rs2U83skQWc3ffzRWHdoSbp1pHWy	6	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-02-28
31.	19NodFVNkEnx9gnWaRXcm7m7XcRnBxUFrv	3	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-02	2023-02-20
32.	bc1qwv8lt083rqvunnr3nn22jlhx7us5phw4lx5yzm	7	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-02-13
33.	bc1qmmtyguygfh3kxqy68yd2nms0uzq4dhvexlps7u	3	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-02	2023-03-01
34.	1A9A9LAoMRUu9xBMYWgutcKVVwiciuWkw6Z	53	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2022-02-25
35.	1J9YpD5861cN4NC2gUKpBvWYp42v3DfVPU	6	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-02-03
36.	bc1qgmaey0tql50fq2ap60smjul3tn652u4wegu33x	2	Aukojimo sukčiavimas (<i>Donation scam</i>)	2023-03-02	2023-03-01

37.	bc1qqmfqf5vk7rv09fgxh7n372s0f985s8sug7r99v	9	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-02	2023-02-05
38.	18wJeJiu4MxDT2Ts8XJS665vsstiSv6CNK	17	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-02	2022-04-05
39.	1GEqAtWBpe4vaLsbizbaPXXmRzkwH7Swf	13	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-02	2023-02-19
40.	bc1qmelshl4npl9hsmzau6ffw5r6qurlam9naydn5j	2	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-02	2023-03-01
41.	bc1qddyea4408jcz2aelvjgegj9ltxw5ym3z20mmau	10	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-01-21
42.	35nAb8UizXBLVnv5Cb3u8VgKzf62nYug1f	3	Meilės sukčiavimas (<i>Romance scam</i>)	2023-03-02	2023-03-01
43.	bc1qncny3ytl32dxldgcfyr4sqt3zyq3z0vxcrs7	5	Meilės sukčiavimas (<i>Romance scam</i>)	2023-03-02	2022-07-21
44.	bc1qex8e73ymss2rzs0rnax4v5y4dzfz8ly8vlaph	8	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-02-27
45.	1JrrsiUghATTytNJVRz5UwSfsERczoQ3x4	5	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-02	2023-02-28
46.	14u9zyQuEhDS437pspa5V6oFcgecajEywv	4	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-02	2022-08-03

47.	bc1q5q57dsrnf4nm00w0c0yq92 gfmf42g6n9ykccwg	33	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-02	2023-01-29
48.	bc1q5x15tz6ecw6v8un8exvt4ds 9ca389lr32g4fxv	5	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-02-19
49.	1EALokrANLmtk4p97A4pAF wkgjw42bEQ4J	7	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-02	2023-02-28
50.	bc1q44q8fjrp3m0l0rqt073q3a9 m79cexk5my6me8	3	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-02	2023-03-02
51.	1E25R2mHg4J6oYMs3BvswT 39HRbV1HuvsN	3	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-02	2023-03-02
52.	3Pdd4L75gaH8u68wEBctiepU Pjf2MU97pH	3	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-02	2023-03-02
53.	1JNfuUu61dBoN3eH23MZsry WanWky9MT78	3	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-02	2023-03-01
54.	1JPRCLsmvC8oAttCjGwthNT AogpaA5yHqk	3	Žvejyba (<i>Phishing</i>)	2023-03-02	2023-03-01
55.	1LGgfryxMwUUCEHkRuey86 fCa66g1aUogr	5	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-02	2020-07-20
56.	bc1qz0hwyvdrq5xvfwcm9m5eg 7kjtvsux4r058v6g	27	Kenkėjiškų programų paskleidimas (<i>Malware scam</i>)	2023-03-02	2023-01-29
57.	bc1qm5lk7pk866xq8phmv27k9 fkys0h2nv725egvwx	6	Kenkėjiškų programų paskleidimas (<i>Malware scam</i>)	2023-03-02	2023-02-27

58.	bc1q2dgh9v48t2r3sust2m7g6f8xynd74wd6pu3pct	2	Žvejyba (<i>Phishing</i>)	2023-03-02	2023-03-01
59.	bc1qhfdvn656wzegrxdwp9dkwthu40gz3lqxvvr2nd	6	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-02-05
60.	1H3vScyEmRXfTG7bFtHzy3dwKTWwKcxLPj	4	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-02-25
61.	bc1qzgrrt60p0zz6k8gqj93udejudhzwrnx2hhgxrv	11	Kenkėjiškų programų paskleidimas (<i>Malware scam</i>)	2023-03-03	2023-02-26
62.	12qusMrNaac75kHFWMKPQuuSn7L44xozvV	2	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-03	2023-03-03
63.	1PNWafqoNQhTR2jCpcSPL6P5XrCxCoqB3	65	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-03-01
64.	183uCvqjaBnCqGkZ4uRJ7Sj9yQDwRgmytp	2	Kenkėjiškų programų paskleidimas (<i>Malware scam</i>)	2023-03-03	2023-03-03
65.	bc1qsmrpfvsl677t9qh9yfvla3zzzeuxrsmmlyyd	3	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-03	2023-03-03
66.	TEAWsY2JCSjAxix5Bsemt6DiM8HCP65iJP	2	Žvejyba (<i>Phishing</i>)	2023-03-03	2023-03-03

67.	bc1qd6hcw002yjne29c3lf0kjeg xl9unyh0hn4a77u	3	Apgaulingos piniginė (<i>Scam wallet</i>)	2023-03-03	2023-03-03
68.	1L3xeyqmrAGHFAxkZEGH9gf reHaMB2md3t	2	Meilės sukčiavimas (<i>Romance scam</i>)	2023-03-03	2023-03-03
69.	bc1qjgkqcsnk449dwj0mayp4kc 87lewtczxnlycz5	2	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-03	2023-03-03
70.	bc1q49yed4s2lmd5axkijnlak0k 00srstg0xcrx9gs	1	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-03	2023-03-03
71.	bc1q4rmqwdul3g2kdtlr5td99e6 c2ep83udf595azv	4	Meilės sukčiavimas (<i>Romance scam</i>)	2023-03-03	2023-03-03
72.	1JqqCaSoAYwAL52LNtwjsG6 LcwAHexEyXP	3	Apgaulingos piniginė (<i>Scam wallet</i>)	2023-03-03	2023-03-03
73.	155h175vaFRMcDZ9XpkHdR m7t95PG5NNvs	2	Apgaulingos piniginė (<i>Scam wallet</i>)	2023-03-03	2023-03-03
74.	bc1q9k4xlnzqknqxsuzpqttslg20 fdr7g43d79g46l	12	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-03	2023-02-28
75.	bc1q6tru0m2v3uy889ngky4q6c vrm8r028g99yn0pe	417	Teroristų finansavimas (<i>Terrorist financing</i>)	2023-03-03	2021-07-28
76.	bc1qy32vvr6xjd90px78ec227ln 358wpwhxfe0zt9d	1	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-03	2023-03-03
77.	bc1qnpn5fuf7sdmlvvg8xqmqka 85w6hcfnc14gx9sd	4	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-03	2023-03-03
78.	bc1qvghr24v9ujlye8df4kprsm9 7exas4a0yganu3m	5	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-03-03

79.	bc1q77722q3alsdccum7vw07e5 l8dxgpsdnpuczetz	3	Kripto valiutos investavimo sukčiavimas (<i>Crypto investment scam</i>)	2023-03-03	2023-03-03
80.	bc1qv563ugqsy3gnvadxhy07u8 46akzcyv6kk3wlke	3	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-03	2023-03-02
81.	bc1qdhazy5ma8d9n3z4tqqkc6d fax7uwfz56t6yany	3	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-03	2023-03-02
82.	bc1qzgrrt60p0zz6k8ggj93udeju dhzwrmx2hhgxrv	11	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-02-26
83.	bc1quttcc59z92wv5k0qx5avtd9 3zhkzkwpentfay7	9	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-02-11
84.	1H3vScyEmRXfTG7bFtHzy3d wKTWwKcxLP	4	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-02-25
85.	1MRUpyvGTeJ1pyhmWFLvsp jc1AHwKRbrxR	16	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-02-21
86.	1L15W6b9vkkxV81xW5HDtm MBycrdiettHEL	1042	Teroristų finansavimas (<i>Terrorist financing</i>)	2023-03-03	2022-07-28

87.	bc1qknxyy28eksdxsup8e4vyfds a8t47umep5jpezek	4	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-03-03
88.	bc1qk2ldv9tw6psv7sjjh0exjwjtj 4d9r5ym8ea8rmt	13	Kripto valiutos investavimo sukčiavimas, teroristų finansavimas (<i>Crypto investment scam, terrorist financing</i>)	2023-03-03	2023-02-24
89.	15LZSP9wiNvxHJTJYDDnQ5 E5VUUj3KUR78	3	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-03-03
90.	3KLqBYexJHsqcxGNRwDbAv X5V6d3tsYzqX	4	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-03-03
91.	bc1q73lm30rgv6h9wy42y88t0r 8prjh9l9pzpvm9c	22	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-02-26
92.	1DF32oFXRecv5SdoviDChBH fQtxM6k3gAj	4	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje	2023-03-03	2023-03-03

			erdvėje (<i>Malware scams, sextortion</i>)		
93.	18gcvrjDju719nQNXhJxRAaw25Vj6M6i4W	5	Žvejyba (<i>Phishing</i>)	2023-03-03	2023-02-19
94.	bc1qglp4zkaj6r9qzvsvx5t6gnsvcz6v6yzgjk46v5	4	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-02-16
95.	17M2VxWxNFXDJTmmzbaSmhnugtGYwsVkGG	20	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2021-01-25
96.	bc1qsavrtsnj4f4an3lj3gy8nrfs7zyh63alkp3vw	5	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-03	2023-03-01
97.	1LbUexNYyMckM8f4mP8XLMbpAsRe3N9XoM	2	Apgaulingos piniginė (<i>Scam wallet</i>)	2023-03-03	2023-03-03
98.	bc1qr9me5t7excnrx6u4ctav7vtqghwhxr6ndufeys	3	Žvejyba (<i>Phishing</i>)	2023-03-03	2023-03-02
99.	1FtUsNNy7kSHTxozts2ubsUojL8FBRLPYi	17	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-05	2023-02-23
100.	16NVQ7DjNYgGbGU7HtSMLsvnmGsqLnXGWV	17	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-05	2023-02-19
101.	14kf3JpjQLBHFeGGcUpKLWRLq8YbTPhKT4	23	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-05	2023-02-19

102.	14dv87kYBem3Foi7CzQ6nTZ 5BMpK8bGtTv	23	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-05	2023-02-19
103.	bc1qk6gludgv5h6keydqcrapxg edm67k8csk6pkxf	2	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams</i> , <i>sextortion</i>)	2023-03-05	2023-03-05
104.	19nvnC9kQJxp5cKZ9C86eis1t GYjoFH3u3	25	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-05	2023-02-18
105.	1MotJuxU8Vj2zvbvQFLq1WN pzQzxFb9vEz	32	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-05	2023-02-25
106.	1A2RNoZEqVP5CgsTw5HMD Y7Qnuq2KnrPg	14	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-05	2023-02-27
107.	1P27Tie1RcLQSXUTwjr8ssSm Loi5AY5zxA	15	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-05	2023-03-01
108.	1Gn8bDVtvpzjRuJYBukem4Jgj hkas2WRUT	40	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-06	2023-02-11
109.	1CrgLZz3fzxT7NxAoJaNVT88 SdEnmFdGii	2	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-07	2023-03-04
110.	bc1quz5m872vte7x9twmveljeu ege6dq05lhg5ttu2	12	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-07	2023-03-01
111.	1ACYLDC1qZt2ZfQJ1DB5H5 ZL7yMnA4EiuH	22	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-07	2023-02-20
112.	bc1q6v3xw8dnkegndkgwgd210t xd6wqqnxcyrzn5jn	8	Meilės sukčiavimas (<i>Romance scam</i>)	2023-03-08	2023-02-08
113.	bc1qhzgmsk4gfxm928s8c7mu9 gxuqu4kpnf9hkfttq	9	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-08	2023-02-08
114.	1oYPT3hrSoK9AzrFMbfWkP XKgLknBuPFq	12	Kenkėjiškų programų paskleidimas, seksualinis	2023-03-08	2023-02-07

			išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)		
115.	3QKUnRhpvikJ3KaD4pv8rK4bhdFYzWGPbi	5	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-08	2023-02-08
116.	1DEjJHJkdpGPP6nT4A3i6hjgiaqXdUd3VS	15	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-08	2023-02-08
117.	3G3zDF9kySTfvjbYmRH3AobruCKY6vYZxC	7	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-08	2023-02-08
118.	17Tx7yk2UJvG2ihhEnW2gzcJomFJ4dDJQT	13	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-08	2023-02-08
119.	bc1qy9rs6z4l56g38jph9fm9rg7gruz635ku6wash8	8	Avansinio mokėjimo sukčiavimas (<i>Advance-fee scam</i>)	2023-03-08	2023-02-08
120.	17hENHuaAjxWmEcMV9u3Z3JQDZcWFv7MoD	32	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-10	2023-02-28
121.	14YLQA98RNJX22W2Prmc7PRQNf6QQf1B1D	3	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-10	2023-03-08

122.	1LmWSVRD2xtPyQeHko1ZC pyTvUmuWF19y5	11	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-11	2023-03-04
123.	1JGF9Nxx8aubhsqipqdtPoUnE sz1vFesYb	19	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-11	2023-03-02
124.	bc1q9hanmksrceyn40868ax30 qdu0srgs3yqq3kea	11	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-11	2023-03-06
125.	bc1qauyc72zfnmud4m23vhgj7v hclm5vgd7q3k2luq	1	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-11	2023-03-11
126.	bc1qkfdjfa4zeze07fvhr5f0ct2z h8yfw7hy5wj30	10	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-12	2023-02-08
127.	bc1qnfzvr7s5e0cy137u5dxfg6gg p822qeyx50x30s	14	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams,</i> <i>sextortion</i>)	2023-03-12	2023-02-08
128.	1JSyEBTz9w2YpGcM2fzcQrx 79Yt5yF6515	17	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams,</i> <i>sextortion</i>)	2023-03-12	2023-02-08
129.	bc1qyceuk79a70vv95en0rfhvf 3kvzs3e747nek04	16	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams,</i> <i>sextortion</i>)	2023-03-12	2023-02-08
130.	18GaQVHRKASCZu9B9oH1g nHENfSHL352G8	34	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje	2023-03-12	2023-02-08

			erdvėje (<i>Malware scams, sextortion</i>)		
131.	13Rj8AREJsA1Trq6i9qZQ8D883NLhRPC8g	10	Meilės sukčiavimas (<i>Romance scam</i>)	2023-03-12	2023-02-08
132.	bc1qpqzy4cgqyfd5gaslznngajgq4jxuryggm0mdr	10	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-12	2023-02-08
133.	bc1qvmg0x7v4c6f0hajs3uru09uqhkiepl4d5vqhev	31	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-12	2023-02-08
134.	3QRXs5pXNa3c63m7prX9wGa6CHM9uawfxZ	58	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-12	2022-12-13
135.	16gcWpgoX6iLTnnB3Wrz2mzGqco8evez7N	26	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-15	2023-02-08
136.	bc1qan8ykykj58uy8g2e7adpkxf e3ldse898dh920a	4	Kenkėjiškų programų paskleidimas, seksualinis išnaudojimas kibernetinėje erdvėje (<i>Malware scams, sextortion</i>)	2023-03-15	2023-03-14
137.	18uRoz4TvnzbhPZYxSNoUE3LTbw7qFCnUr	44	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-15	2023-02-15
138.	1EY6y3Do3ehJj4i1rquyBP9LU6j5WwrAsA	32	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-15	2023-02-21
139.	1ACU7WyXgRMFpf7JJYM27ELzvtqG1uLyCd	22	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-15	2023-02-08
140.	bc1qy2r64yu2d6gl2mr8qsjtaz7va85sralr7j0zhy	25	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-16	2023-03-03

141.	1KtMqDFfRiZ2EQyY6Bp3nSrt 3zFaFpU54K	35	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-18	2022-12-15
142.	1FkgDn3YegN4uctMkrg6kCD PruTJLQJ6qj	2	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-18	2023-03-17
143.	1Gqj8kFK1KDyrE41LmT1ZHt 5FfzQJTpPc7	28	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-19	2023-02-27
144.	bc1qrxecc52dfktp4qw32fpfmg wzn99udk3chr7va	2531	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-20	2022-02-05
145.	13tJMv5arEGvZwN4jjxCD27z BNwgKJBGGg	20	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-20	2023-03-02
146.	bc1qd4r24fj8a9ltlzy6wvlt8p0s9 72ut6cw2q3x0c	9	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-21	2023-03-10
147.	bc1qlmy9x95cka808gz3ewnhgs fke78z284gq83fhj	5	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-22	2023-03-20
148.	bc1qennuszly66xpjrvysm0xjs4v 5ldf7js5h0378g	6	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-25	2023-03-21
149.	bc1qv8p4l43gpd0anq3nd8vujv3 sjka2lr9z4etqqz	3	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-25	2023-03-24
150.	bc1qkd8h2rdz9t2u5zgl73cwfam ur3792w82t4403v	39	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-26	2023-02-20
151.	1F5RH8dTtzyznsPENTkUzrG6 2BuhbQsXLG	67	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-26	2023-02-14
152.	19v2smbJeqvYvMBnh8ysnNsb D6HqQ22L66	16	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-28	2023-03-15
153.	1iEMKaPqMp6zWv47UcPVzh 7xzJvFvvZgx	190	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-30	2022-11-01
154.	1Fta8uBmpYqa2GLDhMCxqru NEFqWQDCi4T	34	Dovanų įteikimo sukčiavimas (Giveaway scam)	2023-03-30	2023-03-24

155.	bc1q5gnywap4jae38lduwnuma ppjh5xzzga4vgujss	4	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-30	2023-03-28
156.	1CRYYUGRWwDMFaaEHYJ BwL1zwwgpQPdgeK	2	Kenkėjiškų programų paskleidimas (<i>Malware scams</i>)	2023-03-30	2023-03-30
157.	bc1q8xqez70xs7hehxxwnwqj37 7h4hx9dz64w4m04w	5	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-31	2023-03-28
158.	13pZB9AZng9RwCrRBKff8NN NCJa6e5Q4rN	40	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-31	2023-02-23
159.	1MusKqjBk497v4Jf1bkgSpKb4 aUhjzfoqA	509	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-31	2022-11-21
160.	bc1qs8t9fwxy0sajzcfetw6eye2d slpfp87lkgy4pt	22	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-31	2023-03-25
161.	bc1q8zl7425jy96xae7ze46gzsc 0c0vlql92anp7eq	6	Dovanų įteikimo sukčiavimas (<i>Giveaway scam</i>)	2023-03-31	2023-03-26
162.	16nxDUoGWjXx8aNswJE8RH jSSu75UzVtnc	1	Kripto valiutos investavimo sukčiavimas (<i>Crypto investment scam</i>)	2023-03-31	2023-03-31

Priedas Nr. 4. BlockChain.com duomenys tyrimo laikotarpyje

Sudaryta autorės, remiantis Blockchain.com duomenimis.

Nr.	Kripto piniginės adresas	Operacijų skaičius, atliktas kriptovaliutų piniginėje	Lėšos, gautos iš nusikalstamos veikos (BTC (USD))	Išsiųstos lėšos iš kriptovaliutų piniginės (BTC (USD))	2023 m. kovo 31 dienos balansas kriptovaliutų piniginėje (BTC (USD))
1.	bc1qm34lsc65zpw79lxe s69zkqmk6ee3ewf0j77s 3h	805058	38885199.27982424 BTC (\$1 106 609 388 628)	38855245.26869119 BTC (\$1 087 740 443 431)	57822.56241057 BTC (\$1 618 690 016)
2.	1FbN9mgTzppSUGRgB s1o7N8FpPQVfoRrKd	16	0.32124036 BTC (\$9 151.24)	0.32124036 BTC (\$8 916.82)	0.00000000 BTC (\$0.00)
3.	1P8Bb873JUzSS7Jp4E Dx8UwaQakGAWhq9S	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
4.	bc1qmx76pwe64u2mxy 4fdjw8rtxj3ehvdnafgraul 2	2	0.00197211 BTC (\$55.79)	0.00197211 BTC (\$54.54)	0.00000000 BTC (\$0.00)
5.	bc1qgg5kjkagkr2yk7us l5fajlu9032gryxxmjfys	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
6.	bc1q0tj9nn8vjz996vw5y wd0mwc240n8zefuejax5 2	3	0.00156375 BTC (\$44.37)	0.00156375 BTC (\$43.34)	0.00000000 BTC (\$0.00)
7.	bc1qaad67kkffvnuqe0q3 vsldcncc5e5zpg2vjhe9m	81619	1996.97713985 BTC (\$56 659 014)	2012.36714069 BTC (\$55 917 167)	0.17327070 BTC (\$4 814.62)
8.	34tiPzriGj3kbYsW28Xg E8nHwk18XDBX7E	479	3.62627225 BTC (\$102 441)	2.34721512 BTC (\$65 222.61)	1.30791772 BTC (\$36 343.41)

9.	DANbgdXKLWuzP7d7 113BYVyGupuzD4CCi	-	-	-	-
10.	3FPD9TtnGdqHnc3RVq SSY16fjL5XtHFokL	123	1.38520175 BTC (\$39 131.69)	1.06951970 BTC (\$29 718.99)	0.31568205 BTC (\$8 771.93)
11.	1Q22EJNqor9f1KUoTo ahDBg1XBL5QGp998	2	0.12164300 BTC (\$3 441.30)	0.00000000 BTC (\$0.00)	0.12164300 BTC (\$3 380.33)
12.	1252NnPXaxc3tkTCGD mvfbXNcU4mfPCCyo	7546	26.54028231 BTC (\$746 165)	26.58419959 BTC (\$738 683)	0.00136631 BTC (\$37.97)
13.	bc1q98jf2h6nn0cchfapkt fltkjmql0q7pp0ceh2e	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
14.	bc1qu9dnf40nzm9a6uce dullm2egat35n55zs8jec9	2	0.06031939 BTC (\$1 697.06)	0.06031939 BTC (\$1 674.74)	0.00000000 BTC (\$0.00)
15.	bc1qft68zdrgrqamaq4ch fl5h4qzptc02zkd2jrcjs	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
16.	3KQRDQiKBzK9p6CV kGWfGFLex8NDun6g AH	2	0.05689500 BTC (\$1 598.78)	0.05689500 BTC (\$1 579.66)	0.00000000 BTC (\$0.00)
17.	1MKjuerdKXjWKwMw RZnj5PcX16YikxvSv8	443	1.07947145 BTC (\$30 699.39)	1.07947145 BTC (\$29 953.12)	0.00000000 BTC (\$0.00)
18.	12nEVuGNtRFMVjeV mLtD4nt2sHX68S47yH	16	0.55015490 BTC (\$15 646.01)	0.51337250 BTC (\$14 233.40)	0.03678240 BTC (\$1 019.80)
19.	1LPEXXSN1t4buFWG K7AbJiA57hCKAcJaAT	2	0.04712000 BTC (\$1 339.47)	0.00000000 BTC (\$0.00)	0.04712000 BTC (\$1 306.01)
20.	bc1q87nhmmdza2xyfx2 5vufpf7gmp80nga28zv4 9hj	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)

21.	bc1qw6k0gshwz2u639y 2wvua5gfthse6ztkj9nztd v	2	0.05000000 BTC (\$1 398.57)	0.05000000 BTC (\$1 386.20)	0.00000000 BTC (\$0.00)
22.	1MTz9A2NH6DXxjYy EmhVc2sBhtJnngenPK	213	1.56923841 BTC (\$43 794.05)	1.56923841 BTC \$43 539.23	0.00000000 BTC (\$0.00)
23.	146MDjQY2TCQXF9Y Qx4jeV3j5JKQx283cA	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
24.	1P4DZNDv9CjhyrMKD N3pt9TSBiVt5UDYRW	246	0.97149132 BTC (\$27 130.49)	0.97849277 BTC (\$27 148.72)	0.00000000 BTC (\$0.00)
25.	bc1qqmun3g4cq4vvr2zv v4sd543nxcemdjk89pkv 6l	2	0.00644215 BTC (\$180.01)	0.00644215 BTC (\$178.59)	0.00000000 BTC (\$0.00)
26.	1NGTAxhLipEp2JfvVh 2q1uQ8UpKhyxQ1zJ	2	0.00623897 BTC (\$174.33)	0.00623897 BTC (\$172.96)	0.00000000 BTC (\$0.00)
27.	14kZFBztXBYHaVskcG UgYU2UTxVJU97N81	44	0.07620941 BTC (\$2 130.08)	0.07769776 BTC (\$2 152.56)	0.00000000 BTC (\$0.00)
28.	bc1qtw9jqxszv55v4s5m 5pja0shrk50ft8wadzllw w	2	0.00004056 BTC (\$1.13)	0.00004056 BTC (\$1.12)	0.00000000 BTC (\$0.00)
29.	bc1qrygp87s80gkvyaxh ks9r2pzjh54xa5aa2xptwl	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
30.	1DEoL2Rs2U83skQWc 3ffzRWHdoSbp1pHWy	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
31.	19NodFVNkEnx9gnWa RXcm7m7XcRnBxUFrv	2	0.04264076 BTC (\$1 191.58)	0.04264076 BTC (\$1 181.33)	0.00000000 BTC (\$0.00)

32.	bc1qwv8lt083rqvunnr3n n22jlx7us5phw4lx5yz m	2	0.03962380 BTC (\$1 106.86)	0.03962380 BTC (\$1 098.50)	0.00000000 BTC (\$0.00)
33.	bc1qmmtyguygh3kxqy 68yd2nms0uzq4dhvexlp s7u	6	0.07310441 BTC (\$2 042.88)	0.07310441 BTC (\$2 029.40)	0.00000000 BTC (\$0.00)
34.	1A9A9LAoMRUu9xB MYWgutckVWwiciuWk w6Z	2	0.04050000 BTC (\$1 145.79)	0.00000000 BTC (\$0.00)	0.04050000 (\$1 124.72)
35.	1J9YpD5861cN4NC2g UKpBvWYp42v3DfVP U	5	0.10118868 BTC (\$2 873.61)	0.10118868 BTC (\$2 810.09)	0.00000000 BTC (\$0.00)
36.	bc1qgmaey0tql50fq2ap6 0smjul3tn652u4wegu33 x	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
37.	bc1qqmfqf5vk7rv09fgxh 7n372s0f985s8sug7r99v	15	0.17683702 BTC (\$4 944.67)	0.17683702 BTC (\$4 910.90)	0.00000000 BTC (\$0.00)
38.	18wJeJiu4MxDT2Ts8XJ S665vsstiSv6CNK	18	3.32097960 BTC (\$92 767.78)	3.32097960 BTC (\$92 325.56)	0.00000000 BTC (\$0.00)
39.	1GEqAtWBpe4vaLsbizb aPXKmRzkfwH7Swf	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
40.	bc1qmelshl4npl9hsmzau 6ffw5r6qurlam9naydn5j	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
41.	bc1qddyea4408jcz2aelvj gegj9ltxw5ym3z20mma u	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
42.	35nAb8UizXBLVnv5Cb 3u8VgKzf62nYug1f	13	0.04406613 BTC (\$1 231.51)	0.04153248 BTC (\$1 154.62)	0.00253365 BTC (\$70.44)

43.	bc1qncny3ytyl32dxldgef yr4sqt3zyq3z0vxcrs7	1284	17.95233759 BTC (\$501 359)	18.02255121 BTC (\$501 032)	0.00000000 BTC (\$0.00)
44.	bc1qex8e73ymss2rzs0rn avx4v5y4dzfz8ly8vlaph	7	0.16239300 BTC (\$4 536.26)	18.02255121 BTC (\$500 892)	0.00000000 BTC (\$0.00)
45.	1JrrsiUghATTytNJVRz 5UwSfsERczoQ3x4	4	0.28635623 BTC (\$7 997.14)	0.28635623 BTC (\$7 958.57)	0.00000000 BTC (\$0.00)
46.	14u9zyQuEhDS437pspa 5V6oFcgecajEywv	491	2.88783409 BTC (\$80 613.37)	2.88783409 BTC (\$80 260.30)	0.00000000 BTC (\$0.00)
47.	bc1q5q57dsrn4nm00w0 c0yq92gfmf42g6n9ykcc wg	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
48.	bc1q5xl5tz6ecw6v8un8e xvt4ds9ca389lr32g4fxv	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
49.	1EALokrANLmtk4p97 A4pAFwkgjw42bEQ4J	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
50.	bc1q44q8fjrp3m0l0rqt0 73q3a9m79cexk5my6m e8	86	0.16529170 BTC (\$4 612.27)	0.17218103 BTC (\$4 786.34)	0.00000000 BTC (\$0.00)
51.	1E25R2mHg4J6oYMs3 BvswT39HRbV1HuvsN	33	6.18771617 BTC (\$172 699)	6.18771617 BTC (\$171 831)	0.00000000 BTC (\$0.00)
52.	3Pdd4L75gaH8u68wEB cticpUPjf2MU97pH	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
53.	1JNfuUu61dBoN3eH23 MZsryWanWky9MT78	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)

54.	1JPRCLsmvC8oAttCjG wthNTAogpaA5yHqk	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
55.	1LGgfryxMwUUCEHk Ruey86fCa66g1aUogr	131	0.05279250 BTC (\$1 473.24)	0.05279250 BTC (\$1 464.74)	0.00000000 BTC (\$0.00)
56.	bc1qz0hwyvdrq5xvfwc m9m5eg7kjktsux4r058 v6g	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
57.	bc1qm5lk7pk866xq8ph mv27k9fkys0h2nv725eg vwx	12	0.08944471 BTC (\$2 501.03)	0.08944471 BTC (\$2 481.67)	0.00000000 BTC (\$0.00)
58.	bc1q2dgh9v48t2r3sust2 m7g6f8xynd74wd6pu3p ct	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
59.	bc1qhfdvn656wzegrdxw p9dkwthu40gz3lqxvwr2 nd	2	0.07055345 BTC (\$2 005.61)	0.07055345 BTC (\$1 957.53)	0.00000000 BTC (\$0.00)
60.	1H3vScyEmRXfTG7bFt Hzy3dwKTWwKcxLPj	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
61.	bc1qzgrrrt60p0zz6k8gqj9 3udejudhzwrnx2hhgxrv	2	0.06105131 BTC (\$1 703.95)	0.06105131 BTC (\$1 693.89)	0.00000000 BTC (\$0.00)
62.	12qusMrNaac75kHFW MKPQuuSn7L44xozvV	2333	37.13664071 BTC (\$1 043 190)	37.16880799 BTC (\$1 031 260)	0.00000000 BTC (\$0.00)
63.	1PNWAfgoNQhTR2jCp cSPL6P5XrCxCoqB3	3	0.19059775 BTC (\$5 358.48)	0.00000000 BTC (\$0.00)	0.19059775 (\$5 283.97)
64.	183uCvqjaBnCqGkZ4u RJ7Sj9yQDwRgmytp	2	0.88620600 BTC (\$24 914.87)	0.88620600 BTC (\$24 568.42)	0.00000000 BTC (\$0.00)

65.	bc1qsmrpfvsl677t9qh9yfvla3zzzeuxrsmmlyyd	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
66.	TEAWsY2JCsjAxix5Bsem6DiM8HCP65iJP	-	-	-	-
67.	bc1qd6hcw002yjne29c3lf0kjegxl9unyh0hn4a77u	16	0.20172059 BTC (\$5 669.41)	0.20172059 BTC (\$5 587.77)	0.00000000 BTC (\$0.00)
68.	1L3xeyqmrAGHFAxkZEgH9gfreHaMB2md3t	4	0.00846859 BTC (\$238.04)	0.00846859 BTC (\$234.58)	0.00000000 BTC (\$0.00)
69.	bc1qjgkqcsnk449dwj0m ayp4kc87lewtczxnlxyz5	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
70.	bc1q49yed4s2lmd5axkznlak0k00srstg0xcrx9gs	10	0.19667897 BTC (\$5 530.26)	0.19667897 BTC (\$5 444.48)	0.00000000 BTC (\$0.00)
71.	bc1q4rmqwdul3g2kdtlr5td99e6c2ep83udf595azv	112	0.73098756 BTC (\$20 555.19)	0.73098756 BTC (\$20 235.24)	0.00000000 BTC (\$0.00)
72.	1JqqCaSoAYwAL52LNtwjsG6LcwAHexEyXP	6	0.04260735 BTC (\$1 198.05)	0.04260735 BTC (\$1 179.02)	0.00000000 BTC (\$0.00)
73.	155h175vaFRMcDZ9XpkHdRm7t95PG5NNvs	10	0.05240592 BTC (\$1 465.35)	0.05240592 BTC (\$1 447.66)	0.00000000 BTC (\$0.00)
74.	bc1q9k4xlnzqknqsxuzpqttslg20fdr7g43d79g46l	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
75.	bc1q6tru0m2v3uy889ngky4q6cvrm8r028g99yn0pe	1	48.84929500 BTC (\$1 365 889)	0.00000000 BTC (\$0.00)	48.84929500 (\$1 349 415)

76.	bc1qy32vvr6xjd90px78e c227ln358wpwhxfe0zt9 d	12	0.04043853 BTC (\$1 129.72)	0.04043853 BTC (\$1 117.08)	0.00000000 BTC (\$0.00)
77.	bc1qnpn5fuf7sdmlvvg8x qmqka85w6hcfnc14gx9s d	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
78.	bc1qvghr24v9ujlye8df4 kprsm97exas4a0yganu3 m	2	0.02317953 BTC (\$647.38)	0.02317953 BTC (\$639.98)	0.00000000 BTC (\$0.00)
79.	bc1q77722q3alsdccum7 vw07e518dxgpsdnpucz z	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
80.	bc1qv563ugqsy3gnvadx hy07u846akzcyv6kk3wl ke	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
81.	bc1qdhazy5ma8d9n3z4t qqkc6dfax7uwfz56t6yan y	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
82.	bc1qzgrrt60p0zz6k8gqj9 3udejudhzwrms2hhgxrv	2	0.06105131 BTC (\$1 701.85)	0.06105131 BTC (\$1 685.85)	0.00000000 BTC (\$0.00)
83.	bc1quttcc59z92wv5k0qx 5avtd93zhkzkwpentfay7	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
84.	1H3vScyEmRXfTG7bFt Hzy3dwKTWwKcxLP	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
85.	1MRUpyvGTeJ1pyhm WFLvspjc1AHwKRbrx R	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
86.	1L15W6b9vkkV81xW5 HDtmMBycrdiettHEL	63954	75559.06274038 BTC (\$2 111 442 850)	75982.32742009 BTC (\$2 095 689 847)	65.41719854 BTC (\$1 804 290)

87.	bc1qknxyy28eksdxsup8 e4vyfdsa8t47umep5jpze k	1	0.02236109 BTC (\$624.54)	0.00000000 BTC (\$0.00)	0.02236109 BTC (\$616.75)
88.	bc1qk2ldv9tw6psv7sjjh0 exjwjtj4d9r5ym8ea8rmt	1	20.84947846 BTC (\$582 702)	0.00000000 BTC (\$0.00)	20.84947846 BTC (\$570 139)
89.	15LZSP9wiNvxHJTJY DDnQ5E5VUUj3KUR7 8	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
90.	3KLqBYexJHsqcxGNR wDbAvX5V6d3tsYzqX	152	0.87942473 BTC (\$24 541.75)	0.87942473 BTC (\$24 048.31)	0.00000000 BTC (\$0.00)
91.	bc1q73lm30rgv6h9wy42 y88t0r8prjh919pzpvvm9 c	6	0.17980000 BTC (\$5 017.61)	0.17980000 BTC (\$4 909.45)	0.00000000 BTC (\$0.00)
92.	1DF32oFXRecv5Sdovi DChBHfQtxM6k3gAj	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
93.	18gcvrjDju719nQNXhJ xRAaw25Vj6M6i4W	2	0.01085493 BTC (\$303.12)	0.00000000 BTC (\$0.00)	0.01085493 BTC (\$296.39)
94.	bc1qglp4zkaj6r9qzvsvx5 t6gnsvcz6v6yzgjk46v5	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
95.	17M2VxWxNFXDjTm mzbaSmhnugtGYwsVk GG	2	0.00014892 BTC (\$4.16)	0.00014892 BTC (\$4.09)	0.00000000 BTC (\$0.00)
96.	bc1qsavrtsnj4f4an3lj3gy 8nrfs7zyh63alkp3vw	10	0.07136890 BTC (\$1 992.98)	0.07136890 BTC (\$1 961.14)	0.00000000 BTC (\$0.00)
97.	1LbUexNYyMckM8f4m P8XLMbpAsRe3N9Xo M	22	0.19336112 BTC (\$5 396.80)	0.19336112 BTC (\$5 313.35)	0.00000000 BTC (\$0.00)

98.	bc1qr9me5t7excnrx6u4c tav7vtqghwhxr6ndufeys	1	0.00120000 BTC (\$33.51)	0.00000000 BTC (\$0.00)	0.00120000 BTC (\$32.89)
99.	1FtUsNNy7kSHTxozts2 ubsUojL8FBRLPYi	5	0.11499855 BTC (\$3 233.56)	0.11499855 BTC (\$3 151.68)	0.00000000 BTC (\$0.00)
100.	16NVQ7DjNYgGbGU7 HtSMLsvnmGsqLnXG WV	5	0.01338298 BTC (\$376.09)	0.01325358 BTC (\$363.23)	0.00012940 BTC (\$3.55)
101.	14kf3JpjQLBHFEGGcU pKLWRLq8YbTPhKT4	1	0.00196686 BTC (\$55.29)	0.00000000 BTC (\$0.00)	0.00196686 BTC (\$53.98)
102.	14dv87kYBem3Foi7Cz Q6nTZ5BMpK8bGtTv	16	1.29591463 BTC (\$36 197.73)	1.29571224 BTC (\$35 548.47)	0.00020239 BTC (\$5.55)
103.	bc1qk6gludgv5h6keydq qcrapxgedm67k8csk6pk sf	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
104.	19nvnC9kQJxp5cKZ9C 86eisltGYjoFH3u3	12	0.25650018 BTC (\$7 210.65)	0.25650018 BTC (\$7 022.25)	0.00000000 BTC (\$0.00)
105.	1MotJuxU8Vj2zvbvQF Lq1WNpzQzxFb9vEz	1	0.00621155 BTC (\$173.70)	0.00000000 BTC (\$0.00)	0.00621155 BTC (\$170.05)
106.	1A2RNoZEqVP5CgsTw 5HMDY7Qnuq2KnvrPg	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
107.	1P27Tie1RcLQSXUTwj r8ssSmLoi5AY5zxA	28	1.52610434 BTC (\$42 869.20)	1.52610434 BTC (\$41 789.12)	0.00000000 BTC (\$0.00)
108.	1Gn8bDVtzipzjRuJYBuk em4Jgjhkas2WRUT	11	0.30281304 BTC (\$8 516.47)	0.30281304 BTC (\$8 300.99)	0.00000000 BTC (\$0.00)

109.	1CrgLZz3fzxT7NxAoJa NVT88SdEnmFdGii	9	0.61141267 BTC (\$17 162.03)	0.61141267 BTC (\$16 760.60)	0.00000000 BTC (\$0.00)
110.	bc1quz5m872vte7x9tw mveljeuege6dq05lhg5ttu 2	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
111.	1ACYLDC1qZt2ZfQJ1 DB5H5ZL7yMnA4EiuH	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
112.	bc1q6v3xw8dnkegndkg wgd2l0txd6wqqnxcyrzn 5jn	18	0.04333693 BTC (\$1 217.23)	0.04325491 BTC (\$1 184.9)	0.00008202 BTC (\$2.25)
113.	bc1qhzgmsk4gfxm928s8 c7mu9gxuqu4kpnf9hkftt q	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
114.	1oYPT3hrSoK9AzcFMb fWkPXXgLknBuPFq	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
115.	3QKUnRhpvikJ3KaD4p v8rK4bhdFYzWGPbi	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
116.	1DEjJHJkdpGPP6nT4A 3i6hjgiaqXdUd3VS	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
117.	3G3zDF9kySTfvjbYmR H3AobruCKY6vYZxC	16	0.01890019 BTC (\$530.88)	0.01890019 BTC (\$519.17)	0.00000000 BTC (\$0.00)
118.	17Tx7yk2UJvG2ihhEn W2gzczJomFJ4dDJQT	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
119.	bc1qy9rs6z4l56g38jph9f m9rg7gruz635ku6wash8	149	0.86956454 BTC (\$24 373.99)	0.87430401 BTC (\$24 016.40)	0.00186885 BTC (\$51.34)

120.	17hENHuaAjsxWmEcM V9u3Z3JQDZcWFv7M oD	2	0.00046434 BTC (\$13.04)	0.00046434 BTC (\$12.79)	0.00000000 BTC (\$0.00)
121.	14YLQA98RNJX22W2 Prmc7PRQNf6QQf1B1 D	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
122.	1LmWSVRD2xtPyQeH ko1ZCpyTvUmuWF19y 5	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
123.	1JGF9Nxx8aubhsqipqdt PoUnEsz1vFesYb		0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
124.	bc1q9hanmksrceyeyn408 68ax30qdu0srgs3yqq3ke a	18	0.04251416 BTC (\$1 196.44)	0.04079448 BTC (\$1 125.11)	0.00167508 BTC (\$46.15)
125.	bc1qauyc72zfnmud4m2 3vhgj7vhclm5vgd7q3k2l uq	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
126.	bc1qkfdjfa4zeze07fvhr 5f0ct2zh8yfw7hy5wj30	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
127.	bc1qnfzvr7s5e0cy137u5 dxfg6ggp822qeyx50x30 s	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
128.	1JSyEBTz9w2YpGcM2 fzcQrx79Yt5yF6515	1449	11.24815229 BTC (\$316 653)	11.36087133 BTC (\$312 962)	0.00000000 BTC (\$0.00)
129.	bc1qyceeuk79a70vv95e n0rfhvf3kvzs3e747nek0 4	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)

130.	18GaQVHRKASCZu9B9oH1gnHENfSHL352G8	1	0.07703209 BTC (\$2 165.01)	0.00000000 BTC (\$0.00)	0.07703209 BTC (\$2 122.04)
131.	13Rj8AREJsA1Trq6i9qZQ8D883NLhRPC8g	16	2.39232592 BTC (\$67 263.83)	2.11410685 BTC (\$58 238.21)	0.27821907 BTC (\$7 664.22)
132.	bc1qpqzy4cgqyfd5gaslznngajq4jxuryggm0mdr	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
133.	bc1qvmg0x7v4c6f0hajs3uru09uqhkuelp14d5vqhev	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
134.	3QRXs5pXNa3c63m7prX9wGa6CHM9uawfxZ	14	0.00485989 BTC (\$136.00)	0.00485989 BTC (\$133.89)	0.00000000 BTC (\$0.00)
135.	16gcWpgoX6iLTnnB3Wrz2mzGqco8evez7N	20	2.27026594 BTC (\$63 958.41)	2.27026594 BTC (\$62 544.67)	0.00000000 BTC (\$0.00)
136.	bc1qan8ykykj58uy8g2e7adpkxfe3ldse898dh920a	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
137.	18uRoz4TvnzbhPZYxSNoUE3LTbw7qFCnUr	7	0.08108464 BTC (\$2 266.75)	0.08108464 BTC (\$2 233.15)	0.00000000 BTC (\$0.00)
138.	1EY6y3Do3ehJj4i1rqybP9LU6j5WwrAsA	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
139.	1ACU7WyXgRMFpf7JYm27ELzvtqG1uLyCd	27	0.81891818 BTC (\$23 053.88)	0.81891818 BTC (\$22 568.39)	0.00000000 BTC (\$0.00)
140.	bc1qy2r64yu2d6gl2mr8qsjtaz7va85sralr7j0zhy	4	0.25752834 BTC (\$7 249.96)	0.25752834 BTC (\$7 092.58)	0.00000000 BTC (\$0.00)

141.	1KtMqDFfRiZ2EQyY6 Bp3nSrt3zFaFpU54K	52	3.55090734 BTC (\$99 904.85)	3.55090734 BTC (\$97 795.40)	0.00000000 BTC (\$0.00)
142.	1FkgDn3YegN4uctMkr g6kCDPruTJLQJ6qj	9	1.55137526 BTC (\$43 645.96)	1.55137526 BTC (\$42 672.05)	0.00000000 BTC (\$0.00)
143.	1Gqj8kFK1KDyrE41Lm T1ZHt5FfzQJTpPc7	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
144.	bc1qrxeccc52dfktp4qw3 2fpfmgwzn99udk3chr7v a	8	0.00464100 BTC (\$130.57)	0.00459174 BTC (\$126.30)	0.00004926 BTC (\$1.35)
145.	13tJMv5arEGvZwN4jjx CD27zBNwgKJBGGg	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
146.	bc1qd4r24fj8a9ltlzy6wv lt8p0s972ut6cw2q3x0c	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
147.	bc1qlmy9x95cka808gz3 ewnhgsfke78z284gq83f hj	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
148.	bc1qennuszly66xpjrvys m0xjs4v5ldf7js5h0378g	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
149.	bc1qv8p4l43gpd0anq3n d8vujv3sjka2lr9z4etqqz	2	0.00030000 BTC (\$8.43)	0.00030000 BTC (\$8.26)	0.00000000 BTC (\$0.00)
150.	bc1qkd8h2rdz9t2u5zgl7 3cwfamur3792w82t4403 v	33	0.21878848 BTC (\$6 164.95)	0.21764263 BTC (\$5 988.83)	0.00249962 BTC (\$68.78)
151.	1F5RH8dTtzyznsPENT kUzrG62BuhbQsXLG	42	0.73875120 BTC (\$20 730.72)	0.73875120 BTC (\$20 339.8)	0.00000000 BTC (\$0.00)

152.	19v2smbJeqvYvMBnh8 ysnNsbD6HqQ22L66	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
153.	1iEMKaPqMp6zWv47U cPVzh7xzJvFvvZgx	3	0.00110000 BTC (\$30.97)	0.00100000 BTC (\$27.55)	0.00010000 BTC (\$2.75)
154.	1Fta8uBmpYqa2GLDh MCxqruNEFqWQDCi4 T	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
155.	bc1q5gnywap4jae38ldu wnumappjh5xzzga4vguj ss	7	0.06357129 BTC (\$1 806.88)	0.06357129 BTC (\$1 751.35)	0.00000000 BTC (\$0.00)
156.	1CRYYUGRWWdMFa aEHYJBwL1zwwgpQPd geK	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
157.	bc1q8xqez70xs7hehxxw nwqj377h4hx9dz64w4m 04w	1	0.00000890 BTC (\$0.25)	0.00000000 BTC (\$0.00)	0.00000890 BTC (\$0.25)
158.	13pZB9AZng9RwCrRB Kfj8NNNCJa6e5Q4rN	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
159.	1MusKqjbk497v4Jf1bkg SpKb4aUhjzfoqA	8	0.15589185 BTC (\$4 366.33)	0.15589185 BTC (\$4 296.60)	0.00000000 BTC (\$0.00)
160.	bc1qs8t9fwxy0sajzcfetw 6eye2dslpfp87lkg4pt	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
161.	bc1q8zl7425jy96xae7ze 46gzsc0c0vlq192anp7eq	0	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)	0.00000000 BTC (\$0.00)
162.	16nxDUoGWjXx8aNsw JE8RHjSSu75UzVtnc	10	0.04826518 BTC (\$1 372.29)	0.04826518 BTC (\$1 330.26)	0.00000000 BTC (\$0.00)

Priedas Nr. 5. Statistinių rodiklių „Kriptovaliutų piniginių adresų skaičius“ ir „Kartai, kiek buvo pranešta apie nusikalstamą veiką“ apskaičiavimas

1. Koreliacijos koeficientas:

	<i>Kriptovaliutų piniginių adresų skaičius</i>	<i>Kartai, kiek buvo pranešta apie nusikalstamą veiką</i>
Kriptovaliutų piniginių adresų skaičius	1	
Kartai, kiek buvo pranešta apie nusikalstamą veiką	0.600776	1

2. Regresijos statistika:

- R: 0.600776042
- R kvadratas: 0.360931853
- Pakoreguotas R kvadratas: 0.281048335
- Standartinė paklaida: 21.74944235
- Stebėjimai: 10

ANOVA:

- Laisvės laipsniai (df):
 - Regresija: 1
 - Likutis: 8
 - Viso: 9
- Kvadratinė suma (SS):
 - Regresija: 2137.294061
 - Likutis: 3784.305939
 - Viso: 5921.6
- Vidutinės kvadratinės sumos (MS):
 - Regresija: 2137.294061
 - Likutis: 473.0382423

- F statistika: 4.518226795
- P reikšmė: 0.066243957

Koeficientai:

- Konstanta: 11.06535261
 - Standartinė paklaida: 8.368777214
 - t statistika: 1.322218566
 - P reikšmė: 0.222646589
 - 95% intervalas (žemesnis): -8.233082257
 - 95% intervalas (aukštesnis): 30.36378747
- X Kintamasis 1: 0.01159438
 - Standartinė paklaida: 0.005454608
 - t statistika: 2.125612099
 - P reikšmė: 0.066243957
 - 95% intervalas (žemesnis): -0.000983968
 - 95% intervalas (aukštesnis): 0.024172727

Priedas Nr. 6. Hipotezės 3 skaičiavimas

Stebėjimai (O)			
	Kripto valiutų piniginių adresų skaičius	Kartai, kiek buvo pranešta apie nusikalstamą veiką	Kripto valiutų piniginių adresų skaičiaus ir Kartų, kiek buvo pranešta apie nusikalstamą veiką, suma
Kenkėjiškų programų paskleidimo nusikalstama veika	70	1250	1320
Dovanų įteikimo sukčiavimo nusikalstama veika	54	4174	4228
Seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika	48	933	981
Avansinio mokėjimo sukčiavimo nusikalstama veika	11	37	48
Žvejybos nusikalstama veika	9	421	430
Meilės sukčiavimo nusikalstama veika	6	32	38
Kripto valiutų investavimo sukčiavimo nusikalstama veika	5	10	15
Apgaulingos piniginės nusikalstama veika	4	10	14
Teroristų finansavimo nusikalstama veika	4	1872	1876
Aukojimo sukčiavimo nusikalstama veika	1	2	3
Suma:	212	8741	8953

Tikimybė (E)		
	Kripto valiutų piniginių adresų skaičius	Kartai, kiek buvo pranešta apie nusikalstamą veiką
Kenkėjiškų programų paskleidimo nusikalstama veika	31,25656	1288,743
Dovanų įteikimo sukčiavimo nusikalstama veika	100,1157	4127,884
Seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika	23,22931	957,7707
Avansinio mokėjimo sukčiavimo nusikalstama veika	1,136602	46,8634
Žvejybos nusikalstama veika	10,18206	419,8179
Meilės sukčiavimo nusikalstama veika	0,89981	37,10019
Kripto valiutų investavimo sukčiavimo nusikalstama veika	0,355188	14,64481
Apgaulingos piniginės nusikalstama veika	0,331509	13,66849
Teroristų finansavimo nusikalstama veika	44,4222	1831,578
Aukojimo sukčiavimo nusikalstama veika	0,071038	2,928962

(O-E)²/E		
	Kripto valiutų piniginių adresų skaičius	Kartai, kiek buvo pranešta apie nusikalstamą veiką
Kenkėjiškų programų paskleidimo nusikalstama veika	48,02364	1,164742
Dovanų įteikimo sukčiavimo nusikalstama veika	21,24201	0,515194
Seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika	26,41435	0,640641
Avansinio mokėjimo sukčiavimo nusikalstama veika	85,59425	2,075962
Žvejybos nusikalstama veika	0,137229	0,003328
Meilės sukčiavimo nusikalstama veika	28,90825	0,701127
Kripto valiutų investavimo sukčiavimo nusikalstama veika	60,74041	1,473169
Apgaulingos piniginės nusikalstama veika	40,59566	0,984588
Teroristų finansavimo nusikalstama veika	36,78239	0,892102
Aukojimo sukčiavimo nusikalstama veika	12,14808	0,294634

x²	369,3317557
df	9
p-value	4,7381

Priedas Nr. 7. Statistinių rodiklių „Pirma kartą pateiktas pranešimas“ ir „Paskutinį kartą pateiktas pranešimas“ apskaičiavimas

1. Koreliacijos koeficientas

	<i>pirma karta pateiktas pranešimas</i>	<i>paskutinį kartą pateiktas pranešimas</i>
Pirmą kartą pateiktas pranešimas	1	
Paskutinį kartą pateiktas pranešimas	0.142475723	1

2. Regresijos statistika

- R: 0,142475723
- R kvadratas: 0,020299332
- Pakoreguotas R kvadratas: 0,014176203
- Standartinė paklaida: 135,7392641
- Stebėjimai: 162

ANOVA:

- Laisvės laipsniai (df):
 - Regresija: 1
 - Likutis: 160
 - Viso: 161
- Kvadratinė suma (SS):
 - Regresija: 61082,85106
 - Likutis: 2948023,649

- Viso: 3009106,5
- Vidutinės kvadratinės sumos (MS):
 - Regresija: 61082,85106
 - Likutis: 18425,14781
- F statistika: 3,315189
- P reikšmė: 0.070510733

Koeficientai:

- Konstanta: -58530,75992
 - Standartinė paklaida: 56829,39689
 - t statistika: -1,02993808
 - P reikšmė: 0,304593
 - 95% intervalas (žemesnis): -170763,2245
 - 95% intervalas (aukštesnis): 53701,70465
- X Kintamasis 1: 2,299791708
 - Standartinė paklaida: 1,263090138
 - t statistika: 1,820766103
 - P reikšmė: 0,070511
 - 95% intervalas (žemesnis): -0,194686975
 - 95% intervalas (aukštesnis): 4,794270391

Priedas Nr. 8. Hipotezės 4 skaičiavimai

Nusikalstama veika	Kriptovaliutų piniginių adresų skaičius	Kartai, kiek buvo pranešta apie nusikalstamą veiką	Kriptovaliutos	Kriptovaliutų piniginių adresų skaičius procentine dalis	Kartai, kiek buvo pranešta apie nusikalstamą veiką procentine dalis	Kriptovaliutų procentinė dalis
Kenkėjiškų programų paskleidimo nusikalstama veika	70	1250	2049.197757	33.01887	14.30042	0.002634
Dovanų įteikimo sukčiavimo nusikalstama veika	54	4174	24.45660824	25.4717	47.75197	3.14E-05
Seksualinio išnaudojimo kibernetinėje erdvėje nusikalstama veika	48	933	2047.107044	22.64151	10.67384	0.002632
Avansinio mokėjimo sukčiavimo nusikalstama veika	11	37	104.7932327	5.188679	0.423293	0.000135
Žvejybos nusikalstama veika	9	421	38855247.32	4.245283	4.816383	49.94843
Meilės sukčiavimo nusikalstama veika	6	32	20.96937019	2.830189	0.366091	2.7E-05

Kripto valiutų investavimo sukčiavimo nusikalstama veika	5	10	2.10820151	2.358491	0.114403	2.71E-06
Apgaulingos piniginės nusikalstama veika	4	10	0.49845445	1.886792	0.114403	6.41E-07
Teroristų finansavimo nusikalstama veika	4	1872	38931227.6	1.886792	21.41631	50.04611
Aukojimo sukčiavimo nusikalstama veika	1	2	0	0.471698	0.022881	0
Suma:	212	8 741	77 790 724,04	100	100	100