VILNIAUS UNIVERSITETAS

EKONOMIKOS IR VERSLO ADMINISTRAVIMO FAKULTETAS

KRISTINA POTECHINA

4 kursas, Ekonomika, Finansai

BAIGIAMASIS BAKALAURO DARBAS

MANIPULIACIJŲ KRIPTOTURTO RINKOJE PRIEŽASTYS IR PASEKMĖS	**THE CAUSES AND CONSEQUENCES OF MANIPULATIONS IN THE CRYPTO ASSETS MARKET**

Darbo vadovė Jaunesnioji asistentė Daiva Raziūnienė

Vilnius, 2024

TURINYS

ĮVADAS

Nagrinėjamos temos aktualumas. Manipuliacijų kriptoturto rinkoje priežastys ir pasekmės – tai tema, kuri yra labai aktuali šių dienų finansų ir ekonomikos srityse dėl kelių svarbių priežasčių. Viena jų – sparčiai auganti kriptoturto rinka. Paskutiniu metu kriptoturto formos tapo svarbiais investicijų objektais ir įgijo didelį populiarumą rinkoje. Kriptoturtas yra labai dinamiškas, o jo vertė stipriai kinta, todėl labai svarbu suprasti, kaip jį tinkamai įvertinti ir apskaityti. Antroji priežastis – finansinio reguliavimo klausimai. Valstybės ir reguliavimo institucijos visame Pasaulyje stengiasi suprasti, kaip tinkamai reguliuoti kriptoturto rinką ir užtikrinti saugumą bei skaidrumą. Kita priežastis – rizikos ir galimybės. Kriptoturto vertės svyravimai gali turėti didelę riziką ir įtaką įmonės finansams ir pelningumui. Šiuo metu yra daug kalbama apie kriptovaliutas, kriptoturtą, bet niekas nežino, kaip reikėtų tinkamai su juo elgtis. Nėra patvirtintų aiškių įstatymų, gairių, kuriomis remiantis galima būtų tvarkyti apskaitą, registruoti ūkines operacijas apskaitoje.

Mokslinės problematikos tyrimas. Pasak mokslinio straipsnio autorių Sandros Idkinaitės ir Artūro Grumulaičio, kriptovaliutų populiarumas auga (Subačius ir Subačienė, 2019) ir jų naudojimas yra aktyviai įtraukiamas į socialines ir profesines gyvenimo sritis, o tai neabejotinai nulems būtinybę teisės aktų leidėjams atlikti atitinkamus skaitmeninių valiutų sandorių apskaitos ir mokesčių reglamentavimo pakeitimus, pritaikant įstatymus skaitmeninės ekonomikos rinkoms (Idkinaitė ir Grumaitis, 2022). Iki šiol laisva ir nereguliuojama sritis vis labiau atkreipia ir įtakingiausių Pasaulyje bankų priežiūros institucijų dėmesį (Idkinaitė ir Grumaitis, 2022).

O Özgür Ekin Sucu savo straipsnyje rašo, kad kriptovaliutų turtas neturi dėmesio vertos istorijos. Jis tapo labai populiarus pastaraisiais metais. Kriptoturtas, kuris naudoja blokų grandinės infrastruktūrą, išryškėjo dėl savo infrastruktūros ypatybių ir tada patraukė žmonių dėmesį dėl įvairių priežasčių (Sucu, 2022).

I. Česnienė verslo žinioms pateikia dar vieną nuomonę. Ji savo straipsnyje teigia, kad yra labai svarbu, jog kriptoturto įmonės finansų apskaitos specialistas glaudžiai bendradarbiautų su bendrovės kriptooperacijų specialistais. Finansų apskaitą tvarkantys specialistai ir kriptoturto veiklos vykdytojai turi glaudžiai bendrauti, kad vieni kitus suprastų ir kad veiklą vykdantis žmogus žinotų, ko reikia apskaitą tvarkančiam kolegai (I. Česnienė, 2022). Dėl šių priežasčių kriptoturto apskaita ir jo naudojimo galimybių tema „Manipuliacijų kriptoturto rinkoje priežastys ir pasekmės“ yra labai aktuali ir gali suteikti naudingos informacijos įmonių finansų specialistams ar investuotojams (I. Česnienė, 2022).

Darbo temos problematika. Šiame darbe yra analizuojamas kriptoturtas, jo rūšys, naudojimo galimybės bei apskaitos alternatyvos. Taip pat apibrėžiama sąvoka, kas gi yra kriptoturtas, kaip jis atsirado, kokie teisiniai reglamentai naudojami kriptoturtui apskaityti, kaip savo moksliniuose straipsniuose traktuojamas kriptoturtas ir kaip efektyviai ir pelningai gali būti naudojamas kriptoturtas ne tik internetinėje erdvėje, bet ir įmonėje. Tokiu atveju būtų atitinkamas finansinis svertas ar stabilumas. Atskleidžiama ir išaiškinama, kaip kriptoturtas bus reglamentuotas (MiCA)[1] reglamentui įsigaliojus.

Darbo tikslas ir uždaviniai

Tikslas: pateikti kriptoturto teisinę ir mokslinę analizę, išskirti jo rūšis ir naudojimo galimybes bei įvertinti manipuliacijų kriptoturto rinkoje priežastis ir pasekmes.

Uždaviniai:

1. Atskleisti kriptoturto sampratą mokslino ir teisinio reglamentavimo prasme.
2. Išnagrinėti ir įvertinti naująjį Europos Parlamento ir Tarybos reglamentą 2023/1114, patvirtintą 2023 m.
3. Pateikti kriptoturto manipuliacijos sampratą, jo apskaitymo būdus ir aprašyti iš to kylančias problemas.
4. Nustatyti manipuliacijų kriptoturto rinkoje pažeidimus ir pasekmes.

Darbo metodai. Nustatytiems uždaviniams įgyvendinti šiame darbe naudojami įvairūs metodai. Naudotasi dokumentų tyrimo ir analizės metodu, kuriuo siekiama išanalizuoti ir įvertinti MiCA reglamentą; mokslinės literatūros analizės, lingvistiniu, lyginamuoju, sisteminės analizės, loginės dedukcijos analogijos metodais bei teisinio modeliavimo metodais, kurie naudojami analizuotų šaltinių ir duomenų pagrindu išvadoms ir apibendrinimams suformuluoti bei pasiūlymams pateikti.

Darbo struktūra. Šį darbą sudaro trys pagrindinės dalys. Pirmoje dalyje nagrinėjamas kriptoturto konceptas mokslinio ir teisinio reglamentavimo prasme. Nagrinėjamas naujasis Mica reglamentas, aptariamos kriptoturto rūšys ir jo naudojimo galimybės. Taip pat kriptoturto apskaita verslo ir tarptautiniuose standartuose, manipuliacijos samprata kriptoturto rinkoje. Antroje dalyje aprašomas tyrimo metodas, kurio pagalba aiškintasi manipuliacijos kriptoturto rinkoje priežastys ir pasekmės. Trečioje dalyje aptariami tyrimo rezultatai.

---

1. 2023 m. gegužės 16 d. Europos Valdovų Taryba oficialiai patvirtino Reglamentą dėl kriptoturto (Kriptoturtas - Consilium (europa.eu))

1. KRIPTOTURTO SAMPRATA

1.1. Kriptoturto sąvoka moksliniame kontekste

Virtualios valiutos arba kriptoturtas sparčiai auga tokių išsivysčiusių šalių ekonomikoje kaip JK, JAV ir Japonija. Šių šalių motyvai kriptoturto atžvilgiu yra sukurti efektyvų skaitmeninės mokėjimo sistemos būdą, kuris bus visuotinai priimtas, ir turės tikrą vertę (fizinę ar piniginę) pagal savo gimtąją valiutą. Pirmoji kriptovaliuta Bitcoin (BTC) šiandien susiduria su konkurencija su naujai išleistomis „Altcoins“ arba „Alternatyviomis monetomis“, pvz., Ripple (XRP), Ethereum (ETH) ir kt., BTC užimama rinka (rinkos viršutinė riba) nuolat mažėja ir svyruoja nuo 30 % iki 35 % visos rinkos kapitalizacijos. Naujai išleisti „Altcoins“ yra techniškai efektyvios ir turi skirtingų motyvų auditoriją, palyginti su BTC. Taip pat šios monetos turi didžiulę augimo lygio potencialą per tam tikrą laiką, palyginti su BTC. BTC kainos yra labai aukštos ir jos augimo lygis yra žemas, palyginti su naujai sukurtomis monetomis (A. K. Yadava, 2018).

Autorių Vivian A. Maese, Alan W Avery, Benjamin A. Naftalis, Stephen P Wink, and Yvette D. Valdez nuomone, griežto vieno apibrėžimo, kuris galėtų paaiškinti kriptoturtą, nėra. Jų nuomone, tai yra „mainų priemonė, kuri veikia kaip pinigai. Ją galima iškeisti į prekes ar paslaugas“.

Luther & White[1], 2014; Šurda[2], 2014 mano, kad „kriptoturtą galima laikyti skaitmenine mainų priemone ir decentralizuota mokėjimo sistema“.

Pasak Demertzis, Maria Wolff, Guntram B., „kriptoturtas iš esmės gali būti suskirstytas į tuos, kurie neatspindi jokio realaus turto, ir tuos, kurie atspindi realų turtą arba turi pagrindą“ (Demertzis, Maria Wolff, Guntram B., 2018).

„Kriptoturtas yra didėjanti turto klasė ir vis dažniau manoma, kad jis gali turėti daug naudos finansų sektoriui, įskaitant sąnaudų mažinimą, efektyvumo padidėjimą ir finansinių paslaugų kokybės bei skaidrumo gerinimą“, savo straipsnyje mini Agata Ferreiraa ir Philipp Sandner. (Ferreiraa, Sandner, 2021).

---

1. Luther & White, 2014 Can Bitcoin Become a Major Currency (Can Bitcoin Become a Major Currency? by William J. Luther, Lawrence H. White :: SSRN)

2. Šurda, 2014 Making Money: The Philosophy of Crisis Capitalism (Making Money– The Philosophy of Crisis Capitalism - Ole Bjerg - Google knygos).

Sąvoka „kriptoturtas“ vartojama ir kriptovaliutoms, ir kriptovaliutų žetonams įvardinti. „Kriptografinis turtas yra decentralizuoto valdymo modelis, leidžiantis susitarti dėl bendros sąvokos tikrovę nepasitikėjimo stokojančioje aplinkoje“ mano H. Hamledari ir M. Ficher (Hesam Hamledari, Martin Fischer, 2021).

Mokslininkų teigimu, kriptoturtas yra skaitmeninė vertė, kurią galima iškeisti į prekes arba paslaugas ir jis gali turėti realų pagrindą. Kriptoturtas gali turėti naudos finansų sektoriui. Vadinasi, galima traktuoti, jog įmonės gali įsigyti kriptoturto ir tai bus finansiškai naudingas pasirinkimas. Kriptoturtas apima ir kriptovaliutas, ir kriptovaliutų žetonus.

1.2. Kriptoturto teisinis reglamentavimas

Apie kriptoturtą kalba ne tik mokslininkai savo moksliniuose straipsniuose, bet ir institucijos, kurios yra glaudžiai susijusios su kriptoturtu.

Kriptoturtas pagal Europos centrinio banko (toliau – ECB) paaiškinimą yra „skaitmeninės vertės arba teisių išraiška“.

Kriptoturtas yra skaitmeninis turtas, kuris gali būti naudojamas investicijoms arba kaip mainų priemonė. Kitaip nei tradicinėje bankininkystėje, centrinio registro nereikia – kriptoturtas yra pagrįstas paskirstytojo registro technologija, kuri leidžia saugiai registruoti operacijas kompiuterių tinkle. Kriptoturtas yra privatus (Europos Parlamentas, 2023).

Pagal Europos Parlamento ir Tarybos reglamentą „kriptoturtas – viena iš pagrindinių blokų grandinės technologijų finansų srityje. Nuo 2018 m. kovo mėn., kai paskelbė „FinTech“ srities veiksmų planą, Europos komisija (toliau – Komisija) nagrinėja kriptoturto teikiamas galimybes ir keliamas problemas“ (Europos Parlamento ir Tarybos reglamentas, 2020). 2017 m. smarkiai išaugus kriptoturto rinkos kapitalizacijai, 2017 m. gruodžio mėn. Europos bankininkystės institucijai (EBI) ir Europos vertybinių popierių ir rinkų institucijai (ESMA) nustatė, kad reikia daugiau priežiūros ir kontrolės kripptoturto rinkoje. 2018 m. „FinTech“ srities veiksmų plane Komisija įgaliojo EBI ir ESMA įvertinti, ar kriptoturtui galima taikyti dabartinę ES finansinių paslaugų reglamentavimo sistemą ir ar ji tam tinkama (Europos Parlamento ir tarybos reglamentas, 2020). 2019 m. sausio mėn. Europos Parlamento ir tarybos reglamente teigiama, kad kai kurių rūšių kriptoturtas patenka į Europos Sąjungos (toliau – ES) teisės aktų taikymo sritį, tačiau šiuos teisės aktus veiksmingai taikyti šiam turtui ne visada paprasta. Be to pastebima, kad galiojančių ES teisės aktų nuostatos gali suvaržyti PRT naudojimą. Kartu EBI ir ESMA pabrėžė, kad dauguma kriptoturto nepatenka į ES finansinių paslaugų teisės aktų (išskyrus ES teisės aktus, skirtus kovai su pinigų plovimu ir teroristų

finansavimu) taikymo sritį, todėl jam negalioja su vartotojų ir investuotojų apsauga, rinkos vientisumu ir kt. susijusios nuostatos, nors tokia rizika kriptoturtui būdinga (Europos Parlamento ir Tarybos reglamentas, 2020). Keletas valstybių narių neseniai priėmė teisės aktus, skirtus atvejams, kai kriptoturtas lemia rinkos susiskaidymą (Europos Parlamento ir Tarybos reglamentas, 2020). „Neseniai atsirado palyginti naujas kriptoturto pogrupis – vadinamoji stabilizuotoji virtualioji valiuta – kuris atkreipė viso pasaulio visuomenės ir reguliavimo institucijų dėmesį. Nors kriptoturto rinka tebėra kukli ir šiuo metu nekelia grėsmės finansiniam stabilumui, ji gali pasikeisti išleidus pasaulinę stabilizuotąją virtualiąją valiutą, kurią siekiama plačiau naudoti įtraukiant jos vertę stabilizuojančias savybes ir išnaudojant tinklo poveikį, kurį lemia šį turtą skatinančios įmonės“ (Europos Parlamento ir Tarybos reglamentas, 2020).

Nuo 2025 m. įsigalios europinio kriptoturto rinkų reglamento (angl. MiCA) reikalavimai, tačiau „Lietuvos Respublika nelaukdama įsigaliosiančio reglamento jau 2022 m. birželio 30 d. pritarė Finansų ministerijos kartu su Lietuvos banku, Finansinių nusikaltimų tyrimo tarnyba, Vidaus reikalų ministerija bei Pinigų plovimo prevencijos kompetencijų centru parengtiems Pinigų plovimo ir teroristų finansavimo prevencijos įstatymo pakeitimams, kuriais siekiama kriptoturto sektoriuje didinti skaidrumą, stiprinti rizikų valdymą ir išsamiau reglamentuoti paslaugų tiekėjų veiklos sąlygas, sukuriant prielaidas tvariam sektoriaus vystymuisi“ (Finansų ministerija, 2022). Taip pat įstatymo projekte „kriptoturto sektoriaus veiklos skaidrumą didinantys pakeitimai numato, jog nuo 2023 m. vasario 1 d. Juridinių asmenų registro tvarkytojas viešai skelbs virtualiųjų valiutų keityklos operatoriaus ir depozitinių virtualiųjų valiutų piniginių operatoriaus veiklą vykdančių asmenų sąrašą, tokiu būdu suteikiant daugiau skaidrumo kriptoturto paslaugų teikėjų rinkai“ (Finansų ministerija, 2022). Įstatymo pakeitimais siekiama numatyti aukštesnius reikalavimus operatorių valdymo ar priežiūros organų nariams arba tokių asmenų naudos gavėjams, įvertinant aukštą vykdomos veiklos riziką (Finansų ministerija, 2022).

Atsirandant vis daugiau įmonių, kurios prekiauja kriptovaliutomis ar teikia panašias paslaugas, Lietuvos bankas griežtina reikalavimus šalyje šias paslaugas teikiančioms įmonėms (Lietuvos bankas, 2023). Kriptoturto sektoriaus veikla yra inovatyvi, tačiau kriptoturtas dažnai yra naudojamas ir kaip pinigų plovimo ir sukčiavimo priemonė (Lietuvos bankas, 2023). Apie šią riziką Lietuvos bankas yra daug kartų įspėjęs ir vartotojus, ir finansų rinkos dalyvius, ir institucijas. Labai svarbu, kad kriptoturto rinka būtų tinkamai kontroliuojama, todėl Lietuvoje būtina griežtinti teisinį reguliavimą ir mes prie to aktyviai prisidedame ekspertine patirtimi rengiant konkrečias priemones, inicijuodami ir teikdami pasiūlymus (Lietuvos banko valdybos pirmininkas Gediminas Šimkus,

2023). Norint kaip įmanoma greičiau pradėti įgyvendinti sugriežtintus reikalavimus, Lietuvos Respublikos finansų ministerija (toliau – FM), Finansinių nusikaltimų tyrimo tarnyba (toliau – FNTT) ir Lietuvos bankas kartu bendradarbiaudami nusprendė pateikti keletą įstatymo pakeitimo projektų. Reglamentai nustatys naujus veiklos vykdymo reikalavimus šių paslaugų teikėjams ir įtvirtins jų licencijavimo procesą. Juos įgyvendinus bus užtikrinama neprofesionaliųjų investuotojų aukšto lygio apsauga bei geriau valdomos kriptoturto paslaugų teikėjų pinigų plovimo ir teroristų finansavimo bei sankcijų vengimo rizikos (Finansų ministerija, 2023). Įstatymų pakeitimai numato, kad už kriptoturto paslaugų teikėjų, su turtu susietų žetonų emitentų ir elektroninių pinigų žetonų emitentų priežiūrą bus atsakingas Lietuvos bankas. Už kriptoturto paslaugų teikėjų pinigų plovimo ir teroristų finansavimo prevencijos (toliau – PPTF) priežiūrą atsakingos institucijos – Lietuvos bankas ir FNTT (Finansų ministerija, 2023). Kriptoturto paslaugų teikėjų licencijavimas yra svarbus ir atsižvelgiant į geopolitinę padėtį regione, kai dėl pradėto karo Ukrainoje daugeliui Vakarų valstybių pritaikius finansines ir kitokias sankcijas Rusijai, jos piliečiams ir juridiniams asmenims apribotos galimybės naudotis daugeliu tradicinių finansinių paslaugų, todėl neatmestina tikimybė, kad jie gali bandyti pasinaudoti virtualiomis valiutomis, siekdami išvengti sankcijų poveikio savo lėšoms (Finansų ministerija, 2023).

Kriptoturtas yra viena iš pagrindinių blokų grandinių, skaitmeninės vertės arba teisių išraiška. Kriptoturtas yra skaitmeninis turtas. Be to, galima suprasti, kad nėra vieningo apibrėžimo, taikomo visam kriptoturtui. Taip pat nėra patvirtinto teisės akto, kuriame būtų tiksliai viskas aprašyta, kas yra kriptoturtas, kaip jis reglamentuojamas ar apskaitomas. Iki 2023 m., kol nebuvo pradėta kalbėti apie naująjį reglamentą, kiekviena valstybė bandė reguliuoti šitą sritį kaip pati išmanė, galvodama, kad elgiasi teisingai investicijų reguliavimo klausimais. Tačiau Europos Sąjunga siekė suvienodinti ir sustiprinti kontrolę. 2023 m. gegužės 16 d. Europos Vadovų Taryba patvirtino reglamentą dėl kriptoturto rinkų (toliau – MiCA), kuris įsigalios 2025 m.

1.3. Europos Sąjungos reguliuojamos kriptoturto rūšys ir jo naudojimo galimybės

Iki 2023 m., kol nebuvo pradėta kalbėti apie naująjį reglamentą, kiekviena valstybė bandė reguliuoti šitą sritį kaip pati išmanė, galvodama, kad elgiasi teisingai investicijų reguliavimo klausimais. Tačiau Europos Sąjunga siekė suvienodinti ir sustiprinti kontrolę. 2023 m. gegužės 16 d. Europos Vadovų Taryba patvirtino reglamentą dėl kriptoturto rinkų (toliau – MiCA), kuris įsigalios 2025 m. Tačiau nuo 2024 m. gruodžio 30 d. kontroliuojančios institucijos turi pradėti parengiamuosius darbus (Europos Vadovų taryba, Europos Sąjungos taryba, 2023).

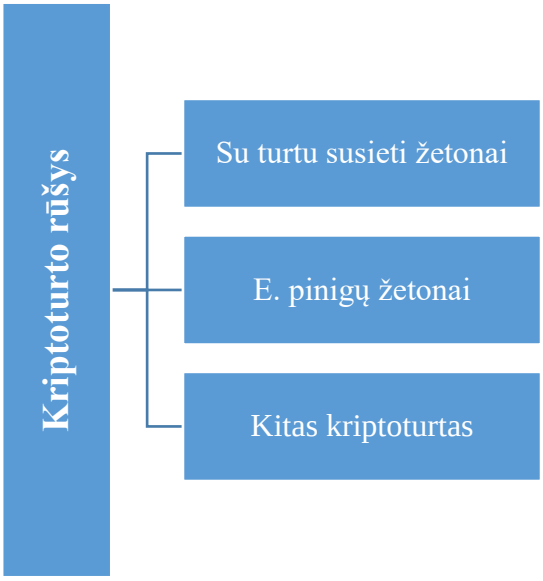
Naujasis ES reglamentas atsirado dėl kriptovaliutų rinkų aplinkybių. Svarbiausias ir pagrindinis kriptovaliutų reguliavimo ES lygmeniu žingsnis buvo įtraukti virtualiąsias valiutas į 2018 m. įsigaliojusią direktyvą dėl Kovos su pinigų plovimu direktyvos. „Monetų siūlymai paskatino augimą rinkoje, kurioje yra įvairių kriptografinių aktyvų (mokėjimo/mainų, investavimo/saugumo, naudingumo ir žetonai). 2019 m. sausio mėn. priežiūros institucijos EBI ir EVPRI nustatė reguliavimo spragas ES lygmeniu. Svetainėje 2020 m. rugsėjį Europos Komisija pristatė MiCA teisės akto projektą. Reglamentas įsigaliojo visose ES šalyse, kurios yra narės“ (Read Oliver, Diefenbach Carolin, 2022).

Europos komisija savo memorandume įtraukė šį pasiūlymą, kad galėtų sudaryti sąlygas plėtoti ir remti skaitmeninį finansinį potencialą, skatinti konkurenciją ar inovacijas. Kartu sumažinti riziką. Patvirtinus šį reglamentą, pasiektas tikslas – užtikrinti finansinį stabilumą. Kadangi kriptoturtas nuolat kinta, todėl šis reglamentas – puiki priemonė jį užtikrinti (Europos Vadovų Taryba, Europos Sąjungos Taryba, 2023). Šiame reglamente yra išskiriamos trys kriptoturto rūšys, kurias reguliuos ES:

1. Su turtu susieti žetonai.
2. E. pinigų žetonai (elektroninių pinigų žetonai).
3. Kitas kriptoturtas. Gali būti produkto žetonai.

1 paveikslas

Kriptoturto rūšys



Šaltinis: sudaryta autorės (remiantis Europos centrinio banko duomenimis)

Su turtu susieti žetonai – tai „stabilus kriptoturtas, nes yra susietas su keliomis valiutomis, kurios yra teisiškai pripažįstamos oficialia mokėjimo priemone (t. y. turi teisėtos valiutos „dekretinių pinigų“ statusą), su viena ar keliomis biržos prekėmis, su vienu ar keliais kriptoturto vienetais arba tokio turto krepšeliu. Jie naudojami kaip mokėjimo priemonė perkant prekes ir paslaugas ir kaip vertės išsaugojimo priemonė“ (Europos Vadovų Taryba, 2023). Pasak Bankera ir advokatų kontoros TGS Baltic, „su turtu susieti žetonai yra kriptoturto tipas (angl. asset-referenced token), kuris siekia išlaikyti stabilią vertę susiejant ją ne tik su teisėtomis valiutomis, bet ir su vienos ar kelių žaliavų, vieno arba kelių kriptoturto žetonų vertėmis ar kelių priemonių deriniais“ („Bankera“ ir advokatų kontora „TGS Baltic“, 2023). Dar vieną paaiškinimą pateikia Start a company in Europe Accounting & Consulting. Teigiama, kad su turtu susieti žetonai – tai kriptoturto tipas, kurio vertybė – siekimas išlaikyti juos stabilius. Su turtu susieti žetonai yra teisėta mokėjimo priemonė, vienos ar kelių prekių ar vienos ar kelių kriptovaliutų derinio vertė. MiCa reikalauja, kad ART emisijos subjektai atitiktų griežtus kapitalo reikalavimus, korporatyvinio valdymo standartus ir užtikrintų skaidrumą dėl tokeno vertę užtikrinančių turtų (Start a company in Europe Accounting & Consulting, 2023).

Antroji kriptoturto rūšis yra **e. pinigų žetonai** (elektroninių pinigų žetonai). „Jie išlaiko stabilią vertę, nes yra susieti su vienos rūšies dekretiniais pinigais ir yra elektroniniai monetų ir banknotų pakaitalai. Pirmumo teisė suteikiama kaip mokėjimo priemonė“ (Europos vadovų Taryba, 2023). Šiai stabilios vertės žetonų grupei priskiriami „elektroninių pinigų žetonai (angl. e-money token), kurių stabilią vertę siekiama išlaikyti susiejant ją su euru ar kita teisėta valiuta. Tai savo pranešime skaitė Bankera ir advokatų kontoros TGS Baltic specialistai („Bankera“ ir advokatų kontora „TGS Baltic“, 2023). EMT arba elektroninių pinigų žetonai – tai kriptoturto rūšis, kurios pagrindinis tikslas – būti naudojama kaip mainų priemone. Ja siekiama palaikyti stabilų vertės lygį. EMT emisijos subjektai turi atitikti reikalavimus, panašius į tuos, kurie taikomi tradiciniams elektroninių pinigų išdavėjams Europos Sąjungoje, įskaitant kapitalo reikalavimus, licencijavimą ir korporatyvinį valdymą (Start a company in Europe Accounting & Consulting, 2023). Taigi, reguliavimo institucijos siekia užtikrinti, kad vartotojai ir investuotojai būtų tinkamai informuoti apie kiekvieno kriptoturto tipo rizikas ir ypatybes, su kuriomis jie susiduria (Start a company in Europe Accounting & Consulting, 2023).

Trečioji kriptoturto rūšis, kurią reglamentuos naujasis reglamentas, yra **kitas kriptoturtas.** Kitas kriptoturtas gali būti – produkto žetonai (Europos Vadovų Taryba, 2023). Taisyklėmis kriptoturto emitentams ir paslaugų teikėjams nustatomi reikalavimai dėl:

- sandorių leidimo ir priežiūros;
- skaidrumo;
- kriptoturto poveikio aplinkai atskleidimo.

Apskaičiuota, kad kai kurioms kriptoturto rūšims per metus suvartojama energija apima tiek, kiek jos suvartoja kai kurios vidutinio dydžio šalys (Europos Vadovų Taryba, 2023). „Tai yra prekių ir paslaugų žetonai (angl. utility token), kuriais galima atsiskaityti už prekes ir paslaugas blokų grandinės pagrindu veikiančioje platformoje. Kiekvienai iš šių grupių taikomos skirtingos taisyklės“. Taip teigia advokatų kontoros specialistai („Bankera“ ir advokatų kontora „TGS Baltic“, 2023) „„Utility“ tokenai arba prekių ir paslaugų žetonas, yra specifinė kriptovaliutų klasė. Jie sukurti tam, kad suteiktų tam tikrą funkcionalumą konkrečioje blokų grandinės platformoje arba aplikacijoje“ (Start a company in Europe Accounting & Consulting, 2023). Pagal MiCa reglamentą, jeigu „utility“ tokenai neatitinka kriptovaliutų apibrėžimų, tokių kaip ART ar EMT, jie gali likti neįtraukti į griežtus šio reglamento reikalavimus. Vis dėlto, priklausomai nuo tokeno struktūros ir funkcionalumo, jis vis tiek gali patekti po kitų įstatymų ir reglamentų reguliavimu (Start a company in Europe Accounting & Consulting, 2023).

2023 m. gegužės 16 d. Europos Vadovų Taryba patvirtino reglamentą dėl kriptoturto rinkų stebėsenos ir didesnės kontrolės. Kontroliuojamos bus trys kriptoturto rūšys. Pirmoji su turtu susieti žetonai – tai stabilus kriptoturtas, nes yra susietas su keliomis valiutomis, kurios yra teisiškai pripažįstamos oficialia mokėjimo priemone. Antroji kriptoturto rūšis yra e. pinigų žetonai (elektroninių pinigų žetonai). Jais siekiama palaikyti stabilų vertės lygį. EMT emisijos subjektai turi atitikti reikalavimus, panašius į tuos, kurie taikomi tradiciniams elektroninių pinigų išdavėjams Europos Sąjungoje, įskaitant kapitalo reikalavimus, licencijavimą ir korporatyvinį valdymą. Trečioji kriptoturto rūšis, kurią reglamentuos naujasis reglamentas, yra kitas kriptoturtas. Kitas kriptoturtas gali būti – produkto žetonai. Taisyklėmis kriptoturto emitentams ir paslaugų teikėjams nustatomi reikalavimai dėl: sandorių leidimo ir priežiūros., skaidrumo, kriptoturto poveikio aplinkai atskleidimo.

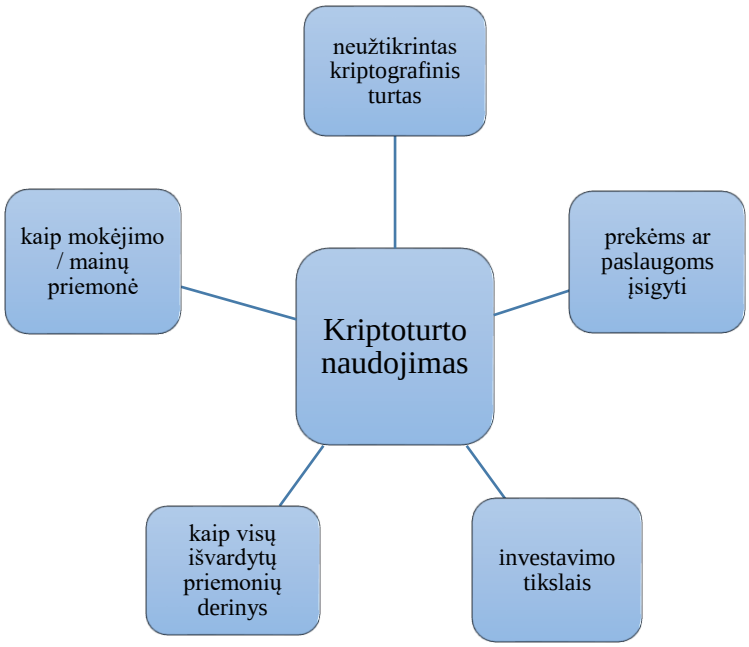
1.4. Kriptoturto naudojimo galimybės

Kriptoturtas reglamentuos su turtu susietus žetonus, e. pinigų žetonus (elektroninių pinigų žetonai) ir kitą kriptoturtą. Taip pat bus aptariama, kaip minėtos turto rūšys bus naudojamos. Kiekviena kriptoturto rūšis turi ir skirtingas naudojimo galimybes (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022). Literatūroje aprašomos penkios naudojimo galimybės:

kaip mokėjimo / mainų priemonė, investavimo tikslais, neužtikrintas kriptografinis turtas, prekėms ar paslaugoms įsigyti (panašiai kaip kuponai, dar vadinami produkto žetonais), kaip visų išvardytų priemonių derinys. Tam, kad galima būtų išsiaiškinti, kaip veikia šie mechanizmai, kiekviena iš kriptoturto naudojimo galimybių analizuojama žemiau esančioje lentelėje.

2 paveikslas

Kriptoturto naudojimas



Šaltinis: sudaryta autorės

Kaip mokėjimo / mainų priemonė (vadinamoji kriptovaliuta). Kriptografinis turtas gali padidinti finansinių paslaugų veiksmingumą, tačiau kelia riziką, kurią valdžios institucijos turėtų spręsti. Iš pradžių sukurtas mokėjimams demokratizuoti, tam tikras kriptografinis turtas, naudojamas tokiose srityse kaip mokėjimai, skolos ir nuosavybės vertybinių popierių išleidimas, prekybos finansavimas ir procesai po sandorio sudarymo (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022). Mažos apimties viešųjų ir privačių subjektų atlikti eksperimentai parodė, kad kai kurie kriptografiniai aktyvai gali padidinti finansinių paslaugų efektyvumą per tarpininkavimą, sumažinti sąnaudas ir pagreitinti procesus (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022). Tačiau kriptografinis turtas yra įvairus, todėl reikia atsižvelgti į individualią riziką ir naudą. „Nors kai kurie kriptografinio turto vienetai gali tapti investavimo ar decentralizuojančių funkcijų, pavyzdžiui, saugojimo, skolinimo ar mokėjimų,

įrankiais, daugelis jų gali kelti didelę riziką rinkos vientisumui, vartotojų apsaugai, finansiniam vientisumui ir vis dažniau – finansiniam stabilumui“ (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022). Nors decentralizacija yra pagrindinė kriptovaliutų ekosistemos koncepcija, praktiškai dauguma vartotojų prie savo kriptovaliutų turto jungiasi per centralizuotus subjektus, kurie teikia lengvai naudojamas sąsajas. Daugelis šių subjektų turi informacijos apie savo naudotojus ir gali priimti arba blokuoti sandorius iš tam tikrų adresų arba gali dalytis sandorių duomenimis su kitomis organizacijomis (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022). Šie subjektai apima biržas ir pinigines ir atlieka svarbų vaidmenį kriptovaliutų turto rinkose. Piniginių paslaugų teikėjai – panašiai kaip bankai ir elektroninių mokėjimų piniginės – laiko turtą vartotojų vardu ir inicijuoja pervedimus (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022). Kai turtas perduodamas šiems subjektams, vartotojai pasitiki centralizuotu subjektu. Panašiai kaip vertybinių popierių biržos – palengvina prekybą rinkose ir registruoja per savo platformas atliktus sandorius. Ir šiuo atveju naudotojai turi pasitikėti centralizuotais subjektais dėl savo duomenų ir turto mainų. Daugelis šių subjektų išaugo ir siūlo keletą produktų ir paslaugų kaip vieno langelio principu veikiančią parduotuvę (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022). „Be to, potencialūs kritinių paslaugų teikėjai gali taip pat suteikti centralizavimo galimybes, o daugelio kriptovaliutų turto turėjimas gali būti sutelktas kelių „banginių“ rankose. Balio fintech darbotvarkė (BFA) – TVF ir Pasaulio banko kartu parengta orientacinė fintech sistema – gali padėti valdžios institucijoms orientuotis svarbiuose kriptoturto politikos klausimuose. BFA sudaro 12 politikos elementų, padedančių valdžios institucijoms vadovautis, kaip išnaudoti fintech teikiamą naudą ir kartu mažinti jų keliamą riziką“ (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022).

Kriptovaliuta yra virtuali, skaitmeninė valiuta, kuria galima atlikti elektroninius mokėjimus, persiųsti lėšas internetu. Didžiausią kriptovaliutų turto dalį sudaro kriptovaliutos, o bitkoinas yra populiariausias ir užima didžiausią vaidmenį rinkoje. Kriptovaliutų dalis pasaulinėse mokėjimo operacijose yra nedidelė. Europos centrinio banko duomenimis, kasdien pasaulyje atliekama apie 284 000 bitkoinų operacijų, plg. su 330 mln. mažmeninių mokėjimų euro zonoje. Iš pradžių buvo keičiamasi bitkoinais ir vyriausybės remiamomis valiutomis. Dominuoja Didžiosios Britanijos svaras, kuris ir dabar yra plačiau pasklidęs tarp valiutų. Geografinę bitkoinų lokalizaciją sunku nustatyti, nes bitkoinai „gyvena“ internete (Demertzis, Maria; Wolff, Guntram B., 2018). Šiandien kriptovaliutos, tokios kaip Bitcoin ar Ethereum, vis dažniau naudojamos kaip alternatyva tradicinėms bankų mokėjimo sistemoms. Kai kuriose interneto parduotuvėse ir fizinėse Pasaulio parduotuvėse

galima sumokėti kriptovaliuta už prekes ar paslaugas (Demertzis, Maria; Wolff, Guntram B., 2018). Kaip atsiskaitymo priemonė, kriptovaliutos turi tam tikrų privalumų. Pavyzdžiui, jos leidžia atlikti greitus ir pigius tarptautinius pavedimus, nes paprastai nėra papildomų tarpininkų ar aukščių transakcijos mokesčių. Be to, kriptovaliutos dažniausiai yra decentralizuotos. Tai reiškia, kad jos nekontroliuoja jokia centrinė institucija, pavyzdžiui, centrinis bankas, todėl jų naudojimas gali būti laisvesnis ir nepriklausomas“ (Demertzis, Maria; Wolff, Guntram B., 2018). Vis dėlto kriptovaliutos ir jų naudojimas kaip atsiskaitymo priemonės sparčiai auga ir tampa vis populiaresnės visame Pasaulyje (Demertzis, Maria; Wolff, Guntram B., 2018).

Investavimo tikslais (pvz., suteikiamos nuosavybės teisės). Dėl kriptovaliutos plėtros ji tapo pelningu lėšų investavimo objektu. Taigi rinkoje atsiranda naujų investavimo metodų ir būdų, o tai sukelia daugelio investuotojų susidomėjimą ir yra susiję su kriptovaliutos, kaip investicijos, gyvavimo ciklu (Koval et al., 2018). Pagrindiniai investavimo į kriptovaliutą būdai: a) spekuliacija kursu – kriptovaliutos pirkimas ir tolesnis jos pardavimas; b) kasyba – galingų kompiuterių, „fermų“, naudojimas sprendžiant sudėtingus matematinius uždavinius kriptovaliutai kurti; c) debesų kasyba – skaičiavimo galios pirkimas už nuomą; d) ICO – kriptovaliutos išleidimas, kurio metu galima surinkti lėšų investiciniam projektui plėtoti. Pelningiausias, bet kartu ir rizikingiausias investavimo būdas yra ICO. Palyginti saugus ir mažiau pelningas – kasyba. Spekuliacijos kurso būdas yra mažiau saugus, tačiau pelningesnis už kasybą. Norint nustatyti kriptovaliutos, kaip investavimo priemonės, naudojimo perspektyvas ir riziką, būtina apsvarstyti pagrindinius kriptovaliutos privalumus ir trūkumus (Olena Bondarenko, Oksana Kichuk Andrii Antonov, 2019). Literatūroje galima rasti informacijos apie investicinių portfelių, kuriuose yra kriptovaliutų optimizavimas. Galima išskirti keletą darbų, pavyzdžiui, (Carpenterio, 2016), kuris analizavo bitkoinų portfelį. Taip pat kelis Amerikos rinkos indeksus, atspindinčius akcijas, žaliavas, iždo obligacijas, nekilnojamąjį turtą ir užsienio akcijas. Šiam portfeliui optimizuoti buvo naudojamas Markowitz modelis ir autorius parodė, kad šio kriptoaktyvo įtraukimas pagerina portfelio rezultatus. Taip atsitinka net ir tada, kai tikėtiną vidutinę bitkoino grąžą baudžiame koeficientu, atsižvelgdami į prielaidą, kad praeityje (nuo 2012 m. sausio mėn. iki 2016 m. gegužės mėn.) gautas didelis pelnas gali nepasikartoti ateityje. (Chan, Chu, Nadarajah ir Osterrieder 2017 m.) analizavo pagrindinių kriptovaliutų kainų statistines savybes nuo 2014 m. birželio mėn. iki 2017 m. vasario mėn. ir, remdamiesi šia informacija, modeliavo tolydžius tikimybių pasiskirstymus, bandydami numatyti būsimą kainų elgseną. Kita vertus, (Trimborn, Li ir Hardle 2018) siūlo Markowitz metodiką, prie kurios prideda likvidumo apribojimą. Tai daroma apribojant į kriptovaliutas investuojamą sumą, kad būtų galima greitai koreguoti portfelio poziciją,

atsižvelgiant į tai, kad Amerikos investuotojo prekybos kriptovaliutomis apimtis yra daug mažesnė, palyginti su tokiais indeksais kaip S&P500. Be to, (Klabbers, 2017) įvertino portfelius su JAV, Europos ir Azijos rinkų indeksais, naudodamas istorinius 2010-2016 m. duomenis, ir, atlikdamas Monte Karlo modeliavimą, sugeneravo naujus pasiskirstymus Markovičiui taikyti. Jie padarė išvadą, kad įtraukus bitkoinus į portfelius, padidėjo grąža, bet nebūtinai sumažėjo rizika (Javier Gutierrez Castroa, Edison Americo Huarsaya Titob, Luiz Eduardo Teixeira Brandaob, and Leonardo Lima Gomes, 2020).

Yra keletas žetonų, kurie gali būti laikomi ir naudojami kaip investavimo priemonė. Vienas iš jų:

Neužtikrintas kriptografinis turtas. Šis kriptografinis turtas yra perleidžiamas. Visų pirma, skirtas naudoti kaip mainų priemonė, nors jis dažnai yra decentralizuotas. Yra pavyzdžių, kai nepadengtas kriptografinis turtas yra centralizuotai išleidžiamas ir kontroliuojamas. (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022). Dauguma nepadengtų kriptografinių aktyvų yra šiuo metu naudojamas spekuliacijai, o ne mokėjimo tikslais. Ryškūs pavyzdžiai yra bitkoinas ir eteris (nors kai kuriose jurisdikcijose, kuriose galioja plačios vertybinių popierių apibrėžtys, tai gali būti laikomi vertybinių popierių žetonais). Dar viena žetonų rūšis tinkama investavimui t. y. **saugumo žetonai**. Nors saugumo žetono apibrėžtis įvairiose jurisdikcijose skiriasi, tai yra žetonai, suteikiantys turėtojui teises, panašias į tradicinių vertybinių popierių teises, pvz. emitento pelno dalį.

Stabilios monetos. Šio tipo kriptografinio turto tikslas – stabili kainos vertė. Paprastai šio tikslo siekiama kriptovaliutą susiejant su vienu turtu arba turto krepšeliu, pavyzdžiui, fiat fondais, žaliavomis, tokiomis kaip auksas, arba kitu kriptovaliutų turtu. Kaip žinoma, žmonės taip pat investuoja į auksą tikėdamiesi, kad jo vertė liks stabili (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022).

Prekėms ar paslaugoms įsigyti (panašiai kaip kuponai, dar vadinami produkto žetonais). Produkto žetonai yra populiari prekybos priemonė, kuri leidžia įsigyti prekes ar paslaugas su specialiais žetonais. Šiuos žetonus galima gauti įsigijus tam tikrą prekę arba atlikus tam tikrą paslaugą (Monika di Angelo, Gernot Salzer TU Wien, 2020). Tokiu būdu pardavėjai gali teikti specialius pasiūlymus savo klientams. Pavyzdžiui, klientas gali gauti žetoną, kai įsigyja tam tikrą prekę arba paslaugą. Vėliau šį žetoną gali panaudoti kitos prekės ar paslaugos įsigijimui su tam tikru nuolaidos tarifu. Produkto žetonai gali būti naudojami įvairiose srityse, pavyzdžiui, restoranuose, grožio salonuose, sveikatingumo centruose, sporto klubuose ir pan. Jie leidžia klientams gauti tam tikras

privilegijas ar nuolaidas ir tuo pačiu metu skatina grįžtamąjį klientų srautą (Monika di Angelo, Gernot Salzer TU Wien, 2020).

Moksliniuose straipsniuose rašoma, jog produkto žetonai yra veiksmingas būdas klientams pritraukti ir padidinti pardavimus. Žetonai, kaip mainų priemonė, gali būti kaip valiuta. Šiuo atžvilgiu jie taip pat gali būti vadinami dApp vietine valiuta. Iš esmės kriptovaliutų žetonai yra naudojami ne tik mainams, bet ir panaudojant jų svarbiausią savybę – tai, kad juos galima programuoti. Šiuo atžvilgiu jie naudojami įjungti tam tikras dApp išmaniosios sutarties funkcijas. Be to, žetonai gali būti susieti su už grandinės ribų esančiu turtu. Jie gali tarnauti kaip lėšų rinkimo, išankstinio užsakymo ar investavimo priemonės. Taip pat ekosistemai ar bendruomenei kurti (Monika di Angelo, Gernot Salzer TU Wien, 2020). Žetonų kūrimas ant esamos blokų grandinės vykdomas per išmaniąsias sutartis, vadinamąsias žetonų sutartis. Tai yra plačiai paplitęs taikymo tipas, kodavimo modeliai. Yra gerosios praktikos pavyzdžių, kai kodavimo modeliai yra lengvai prieinami. Be to, yra žetonų sutarčių gamyklų, veikiančių grandinėje arba kaip žiniatinklio paslauga. Žetonų įsigijimas skiriasi. Pavyzdžiui, jų galima įsigyti per pirminį monetų siūlymą (ICO) arba kriptovaliutų biržoje, prekiaujama grandinėje arba gaunama laisvai per kriptovaliutų išmetimą (angl. air drop). Arba kaip atlygį už paslaugą ar elgesį. Žetono vertė daugiausia priklauso nuo pasiūlos, paklausos ir dalyvaujančios bendruomenės pasitikėjimo juo, kuris yra grindžiamas patikimumu ir siūlomomis įsigyti paslaugomis (Monika di Angelo, Gernot Salzer TU Wien, 2020). Taip pat žetonai gali būti skirstomi į keletą rūšių, kur **komunalinių paslaugų žetonai** suteikia žetono turėtojui prieigą prie esamo ar būsimo produkto ar paslaugos. Paprastai jie yra skirti tik vienam tinklui (t. y. emitentui) arba uždaram tinklui, susijusiam su emitentu. Pavyzdžiui, žetonizuota parduotuvės kortelė arba tam tikri žaidimų žetonai gali būti laikomi komunalinių paslaugų žetonais (Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, 2022).

Kaip visų išvardytų priemonių derinys. Ši naudojimo priemonė gali būti derinama, pavyzdžiui, kaip mokėjimo priemonė naudojant žetonus arba kaip mainų priemonė naudojant žetonus.

Kriptoturtas gali būti naudojimas kaip mokėjimo / mainų priemonė, investavimo tiksliais, prekėms ar paslaugoms įsigyti. Kaip mokėjimo / mainų priemonė, Toks kriptografinis turtas gali padidinti finansinių paslaugų veiksmingumą, tačiau kelia riziką, kurią valdžios institucijos turėtų spręsti. Iš pradžių sukurtas mokėjimams demokratizuoti, tam tikras kriptografinis turtas, naudojamas tokiose srityse kaip mokėjimai, skolos ir nuosavybės vertybinių popierių išleidimas, prekybos finansavimas ir procesai po sandorio sudarymo. Investavimo tikslais (pvz., suteikiamos nuosavybės

teisės). Dėl kriptovaliutos plėtros ji tapo pelningu lėšų investavimo objektu. Taigi rinkoje atsiranda naujų investavimo metodų ir būdų, o tai sukelia daugelio investuotojų susidomėjimą ir yra susiję su kriptovaliutos, kaip investicijos, gyvavimo ciklu. Neužtikrintas kriptografinis turtas. Šis kriptografinis turtas yra perleidžiamas. Visų pirma, skirtas naudoti kaip mainų priemonė, ir nors jis dažnai yra decentralizuotas. Yra pavyzdžių, kai nepadengtas kriptografinis turtas yra centralizuotai išleidžiamas ir kontroliuojamas Tai yra keletas iš daugelio galimybių, kurias gali suteikti kriptoturtas. Kadangi ši sritis sparčiai auga, todėl galima tikėtis dar daug įvairių pokyčių ateityje, pavyzdžiui, kriptovaliutų mainų norint atsiskaityti už prekes ar paslaugas ar kad atsirastų galimybė užstatyti kriptovaliutas paliekant galimybę jas išpirkti esant poreikiui.

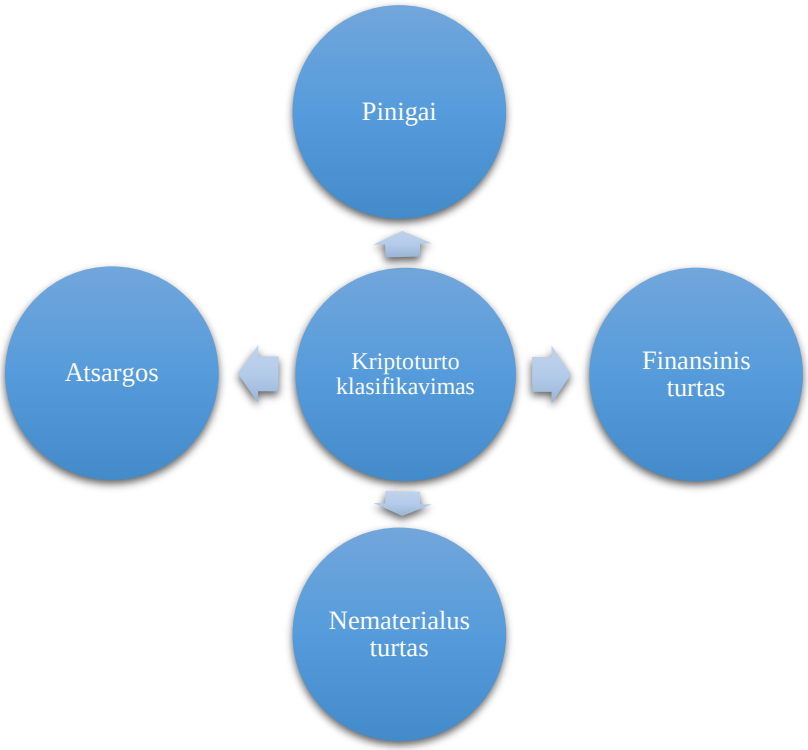
1.5. Kriptoturto apskaita pagal tarptautinius finansinės apskaitos reikalavimus

Atsiradus kriptoturtui, atsirado nauja veiklos sritis, todėl apskaitos reikalavimai gali skirtis priklausomai nuo šalies teisės aktų ir reguliavimo politikos. Grynieji pinigai, pinigų ekvivalentai, valiuta, prekės, atsargos, finansinės investicijos ar nematerialusis turtas yra apskaitos dalis (Kurauskienė Natalija; Subačienė Rasa, 2020). Įstatymų leidybos būtinybė – skaitmeninės ekonomikos reglamentavimo ir jos koregavimo pagal apskaitos standartus aprašai. Kriptoturtui iškilo daug klausimų dėl jo įteisinimo, apmokestinimo, gautų pajamų ir patirtų išlaidų, sąnaudų operacijų registravimų apskaitoje. Nei nacionaliniai, nei tarptautiniai apskaitos standartai atskirai kriptovaliutos apskaitos nereglamentuoja (Kriptoturto ir pirminio kriptoturto žetonų platinimas, 2018). (Kurauskienė Natalija; Subačienė Rasa, 2020). Ir nors yra išleistos kriptovaliutos ir žetonų apskaitos rekomendacijos Lietuvoje bei didžiojo ketverto tarptautinių audito, apskaitos bei konsultacines paslaugas teikiančių įmonių šios valiutos apskaitos, Tarptautinės finansinės apskaitos standartai (toliau – TFAS), aiškinimo komiteto įžvalgos bei rekomendacijos, tačiau ir šios įžvalgos numato, jog apskaitant kriptoturtą, pirmiausia reikėtų vadovautis turto apskaitai keliamais reikalavimais (Kurauskienė Natalija; Subačienė Rasa, 2020). Kriptografinio turto klasifikavimui apskaitos tikslais reikėtų atsižvelgti į tokias charakteristikas, kaip pirminis kriptografinio turto tikslas bei kokia yra kriptografinio turto jam būdinga vertė. Tokiu būdu galima išgryninti kiekvienos kriptovaliutos turėjimo pagrindą (Kriptoturto ir pirminio kriptoturto žetonų platinimas, 2018), (Kurauskienė Natalija; Subačienė Rasa, 2020). Kriptoturto klasifikacija nėra baigtinė, tuo pat metu TFAS ilgą laiką nereglamentavo ataskaitų teikimo ir informacijos apie operacijas su kriptografiniu turtu. Būtų naudinga žinoti kriptoturto savikainos formavimo, klasifikavimo, perkainojimo po pripažinimo, operacijų nutraukimo pripažinimo būdus. Taigi, tokios problemos buvo išspręstos praktika, pagrįsta

profesiniu sprendimu, ir mokslinių tyrimų aplinkoje buvo įvairių prielaidų suklasifikuoti kriptoturtą (Korableva ir kt., 2018).

3 paveikslas

Kriptoturto klasifikavimas



Šaltinis: sudaryta autorės

Pinigai. Kriptoturtas yra laikomas mokėjimo priemone, kai įmonės priima skaitmeninius pinigus už prekes ar paslaugas. Tačiau nėra įrodymų, kad kriptovaliutų turtas yra pripažįstamas pinigais pagal TFAS finansinėse ataskaitose. O Nacionalinių apskaitos įstatymų lygmeniu kriptovaliutų turtas laikomas alternatyvia mokėjimo priemone (Tatiana Morozova, Ravil Akhmadeev, Liubov Lehoux, Alexei Yumashev, Galina Meshkova, Marina Lukiyanova, 2020).

Atsargos. Pagal TFAS išaiškinimą, atsargos tai – turtas, kuris yra: a) laikomas parduoti įprastinės veiklos metu; b) yra šiuo metu gaminamas, numatant jį parduoti; c) žaliavos ar medžiagos, kurios bus sunaudotos gamybos proceso metu arba teikiant paslaugas (Europos Parlamento ir Tarybos reglamentas, 2008).

Nematerialusis turtas. Kriptoturto, priskiriamo nematerialiajam turtui, apskaitos politika turi esminių praktinių problemų su vertinimu po pirminio pripažinimo. Tam tikrų tipų kriptoturtui

yra aktyvi rinka ir tokio turto kainas galima patikimai nustatyti. Toks nematerialusis turtas gali būti vertinamas kaina, vyraujančia tuo laikotarpiu, kai tokio turto rinka egzistavo. Pasinaudodamos šia galimybe, įmonės gali išpūsti savo turto vertę konkrečiam verslo tikslui pasiekti. Pagal TFAS skaitmeninis turtas turėtų būti apskaitomas 38-jame TFAS. Pagal išaiškinimą nematerialusis turtas apskaitomas tokiu turtu, kuris neturi fizinio pagrindo (Tatiana Morozova, Ravil Akhmadeev, Liubov Lehoux, Alexei Yumashev, Galina Meshkova, Marina Lukiyanova, 2020).

Finansinis turtas. Pagal TFAS finansinis turtas turi būti apskaitomas 32-jame standarte kaip finansinės priemonės. Pateikimas: finansinė priemonė – tai bet kuri sutartis, dėl kurios pas vieną ūkio subjektą atsiranda finansinis turtas, o pas kitą – finansinis įsipareigojimas ar nuosavybės priemonė. Finansinis turtas – bet kuris turtas, kuris yra: a) pinigai; b) kito ūkio subjekto nuosavybės priemonė; c) sutartinė teisė (Europos Parlamento ir Tarybos reglamentas, 2008).

Kriptoturtas klasifikuojamas į pinigus, atsargas, nematerialųjį turtą ir finansinį turtą. Pinigai yra laikomi mokėjimo priemone, kai įmonės priima skaitmeninius pinigus už prekes ar paslaugas. Pagal TFAS išaiškinimą, atsargos – tai turtas, kuris yra: a) laikomas parduoti įprastinės veiklos metu; b) yra šiuo metu gaminamas, numatant jį parduoti; c) žaliavos ar medžiagos, kurios bus sunaudotos gamybos proceso metu arba teikiant paslaugas. Kriptoturto, priskiriamo nematerialiajam turtui, apskaitos politika turi esminių praktinių problemų su vertinimu po pirminio pripažinimo. Toks nematerialusis turtas gali būti vertinamas kaina, vyraujančia tuo laikotarpiu, kai tokio turto rinka egzistavo. Pagal TFAS finansinis turtas turi būti apskaitomas 32-jame standarte kaip finansinės priemonės. Pateikimas: finansinė priemonė – tai bet kuri sutartis, dėl kurios pas vieną ūkio subjektą atsiranda finansinis turtas, o pas kitą – finansinis įsipareigojimas ar nuosavybės priemonė.

1.6. Kriptoturto apskaita pagal verslo apskaitos standartus

Apžvelgiant verslo apskaitos standartus (toliau – VAS), pagal 1-ojo VAS „Finansinė atskaitomybė“ metodines rekomendacijas, 28 punktą, įmonė turi nustatyti tokią apskaitos politiką, pagal kurią „finansinėse ataskaitose pateikiami rodikliai teisingai parodytų finansinę būklę, veiklos rezultatus ir pinigų srautus“. Visi elektroninėje erdvėje vykdomi sandoriai, kol nėra kriptoturto teisinio reglamentavimo, gali būti registruojami pagal jų ekonominę prasmę. Įmonė turi pati nustatyti savo apskaitos politikoje, kuriam balanso straipsniui priskirti kriptoturtą, „pagal savo ekonominę prasmę nurodytas sąlygas, ekonominės naudos ar įsipareigojimų tikėtinumą“ (Kriptoturto ir pirminio kriptoturto žetonų platinimas, 2018), (Kurauskienė Natalija; Subačienė Rasa, 2020). Šiuo standartu galima būtų naudotis, jei kriptoturtas būtų naudojamas kaip atsiskaitymo priemonė. Jeigu kriptoturtas

naudojamas atsiskaitymo – įsigijimo tikslais, tada patartina naudoti 22-ojo VAS 4 punkto nuostatą. Registruojant kriptoturto įsigijimą pirminio pripažinimo metu ir įvertinant jį kitais ataskaitiniais laikotarpiais, svarbu įmonės apskaitos politikoje apibrėžti, kokiu šaltiniu bus naudojamasi nustatant kriptoturto tikrąją vertę (Audito, apskaitos, turto vertinimo ir nemokumo valdymo tarnyba, 2018). Kriptoturtu šalių susitarimu gali būti atsiskaitoma už kitą įsigyjamą turtą (paslaugas). Jei įmonė naudoja kriptoturtą kaip atsiskaitymo priemonę už turto (paslaugų) įsigijimą, atsiskaičius už šį turtą (paslaugas), jis nurašomas, užregistruojamas gautas turtas (paslaugos) ir sandorio rezultatas, t. y. pelnas arba nuostoliai, jei tokie yra (Audito, apskaitos, turto vertinimo ir nemokumo valdymo tarnyba, 2018). Nors kriptovaliutų apskaita susiaurėjo iki bendro požiūrio, būtent kaip nematerialusis turtas (38 TAS) arba atsargos (2 TAS), ši nuomonė vis dar labai tikėtina, kad vystytis, nes kriptovaliutų turtas yra naujas, o kriptovaliutų turto sąlygų ir teisinių sąlygų bei jų įtakos ekonominio pobūdžio pokyčiai vis dar yra labai atviri. Papildomai, reguliuotojų politika pakeis kriptovaliutų turėtojus. Kriptovaliutų turtas bus priimtas visiškai arba iš dalies arba netgi bus aiškiai uždraustas. Kriptovaliutų buvimas gali būti neteisėtas. Nors šiuo metu yra daug įrodymų, patvirtinančių faktą, kad kai kuriose šalyse kriptovaliutų turtas buvo priimtas kaip priemonė mokėjimams. Bent jau subjektams, kurie šiuo metu investuoja į kriptovaliutą arba prekiauja kriptoturtu, gali naudoti šią nuorodą įrašydami ją į savo finansines ataskaitas. Ateityje tikimasi, kad pagal tarptautinius standartus bus išleistos specialios gairės arba oficialūs pareiškimai su kriptovaliutų apskaita susijusioms institucijoms, kad kriptoturto apskaita galėtų tapti standartų nuoroda įvairiose šalyse (I Gede Githa Adhi Pramana1 Sekar Mayangsari, Lin Oktris, 2023).

Apibendrinant galima teigti, kad kriptoturto, kuris naudojamas kaip atsiskaitymo priemonė, įsigijimo savikaina nustatoma pagal už ją sumokėtą ar mokėtiną pinigų sumą. Jei jos įsigijimo metu nuskaitomi mokėjimai tarpininkams, tokie nuskaitymai neturėtų būti rodomi atskirai, o vadovaujantis 18-uoju VAS turėtų būti įskaitomi į kriptoturto įsigijimo savikainą.

1.7. Manipuliacijų kriptoturto rinkoje samprata ir būdai

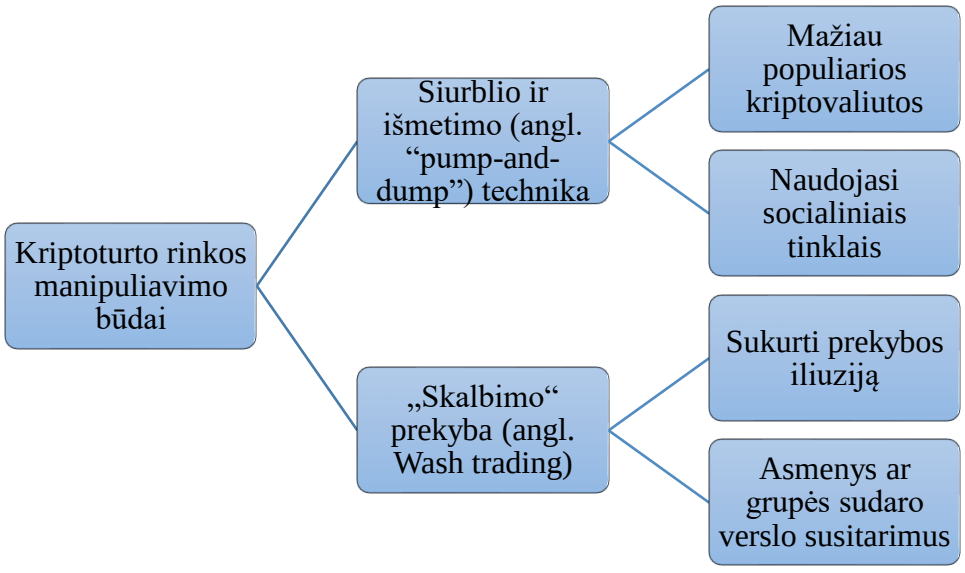
Manipuliacija rinkoje reiškia, kad prekybos strategijos yra skirtos sumažinti ekonominį efektyvumą, siekiama sumažindami rizikos perdavimo rinkos likvidumą. Be to, rinkos manipuliacija kenkia kainų nustatymo tikslumui, nes kainos tampa mažiau tikslios kaip efektyvaus išteklių signalo paskirstymas (Kyle ir Viswanathan 2008). Pavyzdžiui, gauti naudos iš viešai neatskleistos informacijos prekyboje, sumažina kainų efektyvumą ir rinkos likvidumą dėl informacijos asimetrijos. Decentralizuotas kriptovaliutų pobūdis ir silpnas blokų grandinės

ekosistemos reguliavimas veikia neigiamai kriptovaliutų rinkas, nes jos yra pažeidžiamos įvairių rūšių sukčiavimo būdais ir manipuliavimu. Keli mokslininkai išnagrinėjo, kaip kriptovaliutas paveikė įvairios sukčiavimo formos. Pavyzdžiui, Vasek ir Moore'as (2015), pateikė pirmąją empirinę Bitcoin pagrindu sukurtą sukčiavimo analizę ir Ponzi schemų tyrimą reklamos svetainėje bitclontalk.com (2019). Bartoletti ir kt. (2018 m.) sukūrė Ponzi schemą – prognozavimo modelį, susijusį su kriptovaliutu sukčiavimu rinkoje. Tyrėjai naudojosi duomenų gavybos metodais, skirtais sukurti klasifikatorių, kuris veiksmingai identifikuoja Bitcoin adresus, susijusius su Ponzi schemomis. Kriptovaliutų populiarumas ir atskleidimas paskatino daugybę pritaikomumo tyrimų specialių manipuliavimo rinkoje schemų, skirtų kriptovaliutų rinkoms. Mokslininkai ištyrė be kita ko, siurbimo ir išmetimo (angl. pump-and-dump) schemų poveikius (Chen ir kt., 2019b; Hamrick ir kt., 2021; Mansourifar ir kt. 2020 m.; Xu ir Livshits 2019), plovimo prekyba (angl. wash trading) (Aloosh ir li 2019; Cong ir kt. 2020; Pennec ir kt. 2021), įtartina botų veikla mainuose su Gokso kalnu (Gandal ir kt., 2018) ir pirmaujanti (Bernhardt) ir Taub 2008; Daianas ir kt. 2020) kaip manipuliavimo kriptovaliutų rinka formas. Kitos formos manipuliacijos panaudoja specifines faktinių kriptovaliutų savybes (F. Eigelshoven, A. Ullrich, & D. Parry., 2021).

Yra du manipuliavimo būdai, kurie dažniausiai naudojami kriptovaliutų rinkose – Siurblio ir išmetimo prekyba (angl. pump and dump) ir „Skalbimo“ prekyba (agnl. wash).

4 paveikslas

Kriptoturto rinkos manipuliavimo būdai.



Šaltinis: sudaryta autorės, remiantis Cunjak, I. (2022).

Siurblio ir išmetimo (angl. „pump-and-dump“) technika yra įprasta kriptovaliutų rinkose, o ne reguliuojamose finansų rinkose, kur tai draudžia įstatymai. Šios manipuliavimo technikos veikimo būdas kriptovaliutų rinkose šiek tiek skiriasi nuo naudojamo tradicinėse finansų rinkose. Pump ir dump manipuliavimo organizatoriai naudojasi socialiniais tinklais, tokiais kaip Reddit, Discord ar Telegram, kur dalyviai suskirstomi į grupes (Barnes, 2018). Šios grupės turi skirtingą narių skaičių. Šių grupių manipuliavimo objektas yra mažiau populiarios kriptovaliutos, turinčios mažą rinkos kapitalizaciją ir mažą prekybos apimtį (I. Cunjak, 2022). Prekyba pagrįstomis manipuliavimo kainomis teorijose, kai manipuliatorius negali veikti kitaip nei pirkdamas ir parduodamas turtą, manipuliatorius pirmiausia turi nusipirkti tikslinį turtą, kad „perpumpuotų“ (angl. „pump“) jo kainą. Kaip išoriniai investuotojai seka, manipuliatorius gali parduoti už didesnę kainą, kad gautų pelno. Manipuliatoriai gali pasipelnyti tik tuo atveju, jei jų pirkimo poveikis kainai yra didesnis nei parduodant (T. Li, D. Shin, & B. Wang, 2021).

„Skalbimo“ prekyba (angl. Wash trading) yra vienas iš įprastų manipuliavimo būdų tradicinėse finansų rinkose, kurio tikslas – sukurti prekybos apimties iliuziją, kuri sumažina finansų rinkų vientisumą ir pasitikėjimą jomis. Pagrindinis plovimo prekybos technikos bruožas yra tai, kad asmenys ar grupės sudaro verslo susitarimus pagal susitarimą ir tuo pat metu pasirodo kaip tam tikros finansinės priemonės pirkėjai ir pardavėjai. Šios manipuliavimo technikos įgyvendinimas nekeičia tikrosios prekybos objekto nuosavybės, o tik sukuria iliuziją, kad tam tikros prekybos priemonės rinkos aktyvumas didėja ir taip klaidina kitus rinkos dalyvius (Cao, Li, Coleman, Belatreche ir McGinnity, 2016). „Wash“ prekyba taip pat vyksta kriptovaliutų rinkose, o tai patvirtina faktinio kriptovaliutų prekybos apimties pateikimo patirtis. Paklausos iliuzijos kūrimo strategija kriptovaliutų rinkoje, skirtingai nei tradicinėse finansų rinkose, įgyvendinama keliais būdais: melagingas sandorių paskelbimas, kad kriptovaliutų biržos tiesiog paskelbtų sandorius, kurių realybėje neįvyko, biržos, prekiaujančios kriptovaliutomis, taip pat dalyvauja perkant ir parduodant savo platformoje, taip padidindamos prekybos apimtį, biržos sumoka už vadinamąją plovimo prekybą tiesiogiai trečiajai šaliai, dalyvaujančiai didinant prekybos apimtį ir kai kurios biržos suteikia tam tikros naudos kitoms biržoms kriptovaliutų rinkose, kurios generuoja didesnes prekybos apimtis (Hougan et al., 2019, p. 36), (I. Cunjak, 2022). Prekyba plovimu (angl. Wash trading) gali būti didelis iššūkis reguliuotojams, nes dėl unikalių kriptovaliutų pramonės ypatybių tradiciniai bandymai tampa neveiksmingais (L.W. Cong, X. Li, K. Tang, & Y. Yang, 2023).

Manipuliacija rinkoje reiškia, kad prekybos strategijas yra skirtos sumažinti ekonominį efektyvumą, siekiama sumažindami rizikos perdavimo rinkos likvidumą. Kriptovaliutų

manipuliavimo rinkoje egzistuoja du pagrindiniai rinkos manipuliavimo būdai: siurblio ir išmetimo (angl. „pump-and-dump“) technika ir „skalbimo“ prekyba (angl. Wash trading). Siurblio ir išmetimo (angl. „pump-and-dump“) technika daugiau orientuota į socialinius tinklus ir į ne tokias žinomas kriptovaliutas. „Skalbimo“ prekyba, toks manipuliavimo būdas, kurio tikslas – sukurti iliuziją ir ją pardavus, užsidirbti.

2. MANIPULIACIJŲ KRIPTOTURTU TYRIMO METODOLOGIJA

Tyrimo metodu vadinamas toks metodas, kuris taikomas renkant spausdintame ar rašytiniame tekste, filmavimo juostoje ar magnetinėje erdvėje užfiksuotą informaciją. Tyrimo metodai gali būti labai įvairūs, priklausomai nuo tyrimo tikslų, temos, objekto ir kitų faktorių, kuriuos norima atskleisti savo tyrime. Taip pat tyrimu gali būti vadinamas sistemingas veiksmas, kurio pagrindinis tikslas – gilinti žinias apie tam tikrą reiškinį ar problemą. Tyrimą galima atlikti įvairiose srityse, pagrindžiant objektyviu duomenų surinkimu ar analize. Vieni iš populiariausių tyrimo metodų gali būti:

1. Anketinė apklausa. Tai apklausa, kurioje respondentai atsako į klausimus, kurie yra sudaryti ir pateikti iš anksto. Anketine apklausa galima apimti tiesioginį informacijos surinkimą iš dominančių žmonių grupių ar organizacijų (S. Roopa, MS. Rani, 2012). Anketinės apklausos metodas padeda informacijos surinkėjui gauti tikslią, labai konkrečią informaciją. Anketinės apklausos pagalba galima atlikti įvairius skaičiavimus ar analizes.

2. Interviu. Tai tiesioginis pokalbis su respondentu. Interviu metu galima gauti išsamesnę ir detalesnę informaciją norimam tyrimui atlikti (K. Kreiner, J. Mouritsen, 2006).

3. Eksperimentas. Tai bandomasis tyrimas, kurio metu leidžiama nustatyti priežastinį ryšį tarp tam tikrų dviejų kintamųjų. Eksperimentinė analizė nagrinėja tą tikimybę reagavimo dažnio arba greičio atžvilgiu (B. F. Skinner, 1966).

4. Stebėjimas. Kai tyrėjas tiesiog stebi ir vertina tam tikrą veiklą arba elgesį. Stebėjimas gali būti laikomas pačiu kasdieninio socialinio bendravimo pagrindu: dalyvaudami socialiniame gyvenime, jie stropiai stebi ir komentuoja kitų elgesį. Stebėjimas taip pat yra vienas iš svarbiausių socialinių mokslų tyrimo metodų ir kartu vienas sudėtingiausių. Tai gali būti pagrindinis projekto metodas arba vienas iš kelių papildomų kokybinių metodų. Tai mokslinis metodas. Jis turi būti vykdomas sistemingai, daugiausia dėmesio skiriant konkretiems tyrimo klausimams (M. Ciesielska, K. W. Boström & M. Öhlander, 2017).

5. Dokumentų analizė. Metodas, kai tyrėjas analizuoja rašytinius dokumentus, archyvus ar kitas publikacijas. Fischer (2006) dokumentų analizę apibrėžia kaip sistemingą dokumentų – tiek spausdintos, tiek elektroninės medžiagos – peržiūros ar vertinimo procedūrą. Kaip ir bet kurie kiti analizės metodai, kokybinė tyrimo dokumentų analizė reikalauja, kad duomenys būtų išnagrinėti ir interpretuojami siekiant sukurti prasmę, įgyti supratimo ir plėtoti empirines žinias (Denzin, 2017). Be dokumentų yra tokių šaltinių kaip interviu, stebėjimas dalyvaujant ar nedalyvaujant, užsimena Patton

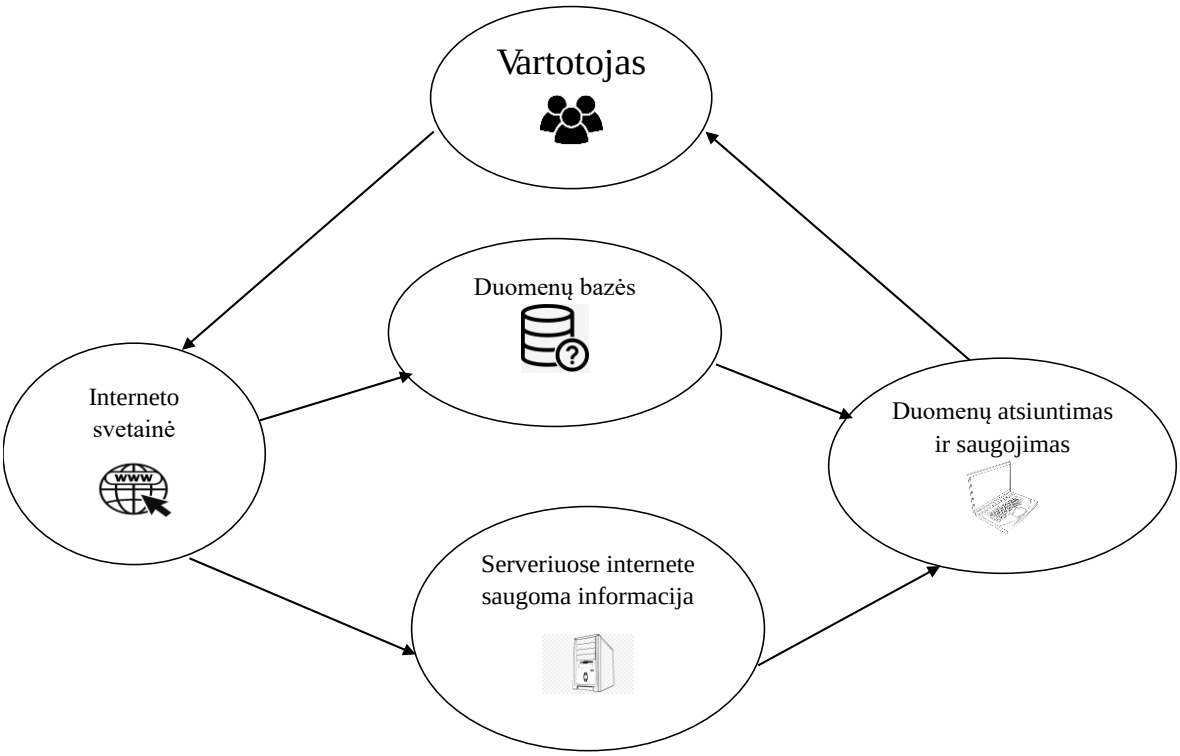
(1990). Nagrinėdamas informaciją, surinktą naudojant skirtingus metodus, tyrėjas gali patvirtinti duomenų rinkinių išvadas ir taip sumažinti galimų paklaidų, kurios gali egzistuoti viename tyrime, poveikį.

Nagrinėjant darbo temą ir siekiant atskleisti, kokie pažeidimai buvo daromi kriptoturto apskaitoje, naudojami internetiniuose puslapiuose rasti priežiūros institucijų pateikti pranešimai, moksliniai straipsniai ir aktualūs mokslininkų darbai. Temai išsiaiškinti naudojamos tokios internetinės platformos kaip Claritive (internetinis puslapis: Web of Science Master Journal List - WoS MJL by Clarivate), Vilniaus universiteto biblioteka (internetinis puslapis: Vilniaus universiteto biblioteka (vu.lt)) ar Google Scholar (internetinis puslapis: „Google“ mokslinčius). Visa informacija buvo renkama naudojantis Vilniaus universiteto skirtu VPN serveriu. Naudojant raktinius žodžius, tokius kaip apskaita, kriptoturtas, pažeidimai, pasekmės, crypto assets, accounting, fine, violations. Buvo atrinkti priežiūros institucijų ir mokslininkų straipsniai, kurie atitiko šiuos kriterijus. Duomenų rinkimą galima apibūdinti 1 pav. pavaizduota schema. Naudojant internetines svetaines, įvairius serverius pagal raktinius žodžius surinkta informacija, reikalinga tyrimui atlikti. Visa informacija išsaugota kompiuterio vidinėje atmintyje.

Tyrimui atlikti pasirinktas dokumentų analizės metodas. Dokumentų analizė daugeliui tyrinėtojų rekomenduojama dėl to, kad yra paprasta, efektyvi, ekonomiška ir lengvai valdoma. Pagrindinis jos pranašumas yra dokumentų prieinamumas. Paprastai tyrėjui tai mažai kainuoja arba visai nekainuoja. Dirbant su dokumentiniais duomenimis, o ne duomenimis, surinktais iš žmonių, retai kada reikalingas sutikimas pasiekti duomenis, todėl mokslininkai gali apeiti poreikį teikti paraiškas dėl patvirtinimo atlikti tyrimą. Tai procesas, galintis sukelti komplikacijų arba vėluoti. Tai nereiškia, kad asmenys, nagrinėjantys dokumentus, neturi jokių rūpesčių, tačiau jie gali gauti prieigą prie dokumentų, kurie gali būti konfidencialūs. Kitas privalumas yra nepastebimas dokumentinės analizės pobūdis, todėl dokumentas, kaip duomenų šaltinis, neatkreipia dėmesio į tyrėjo buvimą, nes jie gali ramiai dirbti užkulisiuose. Kaip kokybinis tyrimo metodas, dokumentų analizė dažnai pasirenkama kaip antrasis arba papildomas duomenų rinkimo būdas, siekiant sustiprinti tyrimą naudojant kelių metodų trianguliacijos formą. Trianguliacija yra metodas, naudojamas tyrimo išvadų patikimumui ir pagrįstumui padidinti (Educational Administration: Theory and Practice, 2018). 2015-2024 m. laikotarpiu surinkti ir analizuoti duomenys leidžia aiškiai matyti, kokiais mastais buvo vykdomi kriptoturto praradimai.

5 paveikslas

Duomenų paieškos ir surinkimo sistemos modelis



Šaltinis: sudaryta autorės, remiantis N. Kaanichea, M. Laurent, 2017.

Atliekant tyrimus galima naudotis įvairiais tyrimo metodais, pradedant anketine apklausa, interviu, eksperimentu, stebėjimu ir dokumentų analize ir baigiant kiekybinio ir kokybinio tyrimo metodais bei tyrimų apžvalga. Ne visus tyrimo metodus galima naudoti kartu, nes tyrimo pasirinkimas priklauso nuo pasirinktos temos analizavimo. Tyrimui atlikti pasirinktas dokumentų analizės metodas. Dokumentų analizė daugeliui tyrinėtojų rekomenduojama dėl to, kad yra paprasta, efektyvi, ekonomiška ir lengvai valdoma. Pagrindinis jos pranašumas yra dokumentų prieinamumas. Paprastai tyrėjui tai mažai kainuoja arba visai nekainuoja. Dirbant su dokumentiniais duomenimis, o ne duomenimis, surinktais iš žmonių, retai kada reikalingas sutikimas pasiekti duomenis, todėl mokslininkai gali apeiti poreikį teikti paraiškas dėl patvirtinimo atlikti tyrimą. Tai procesas, galintis sukelti komplikacijų arba vėluoti. Tai nereiškia, kad asmenys, nagrinėjantys dokumentus, neturi jokių rūpesčių, tačiau jie gali gauti prieigą prie dokumentų, kurie gali būti konfidencialūs.

3. KRIPTOTURTO APSKAITOS PAŽEIDIMŲ IR PASEKMIŲ ANALIZĖ

3.1. Kriptoturto apskaitos pažeidimų apžvalga

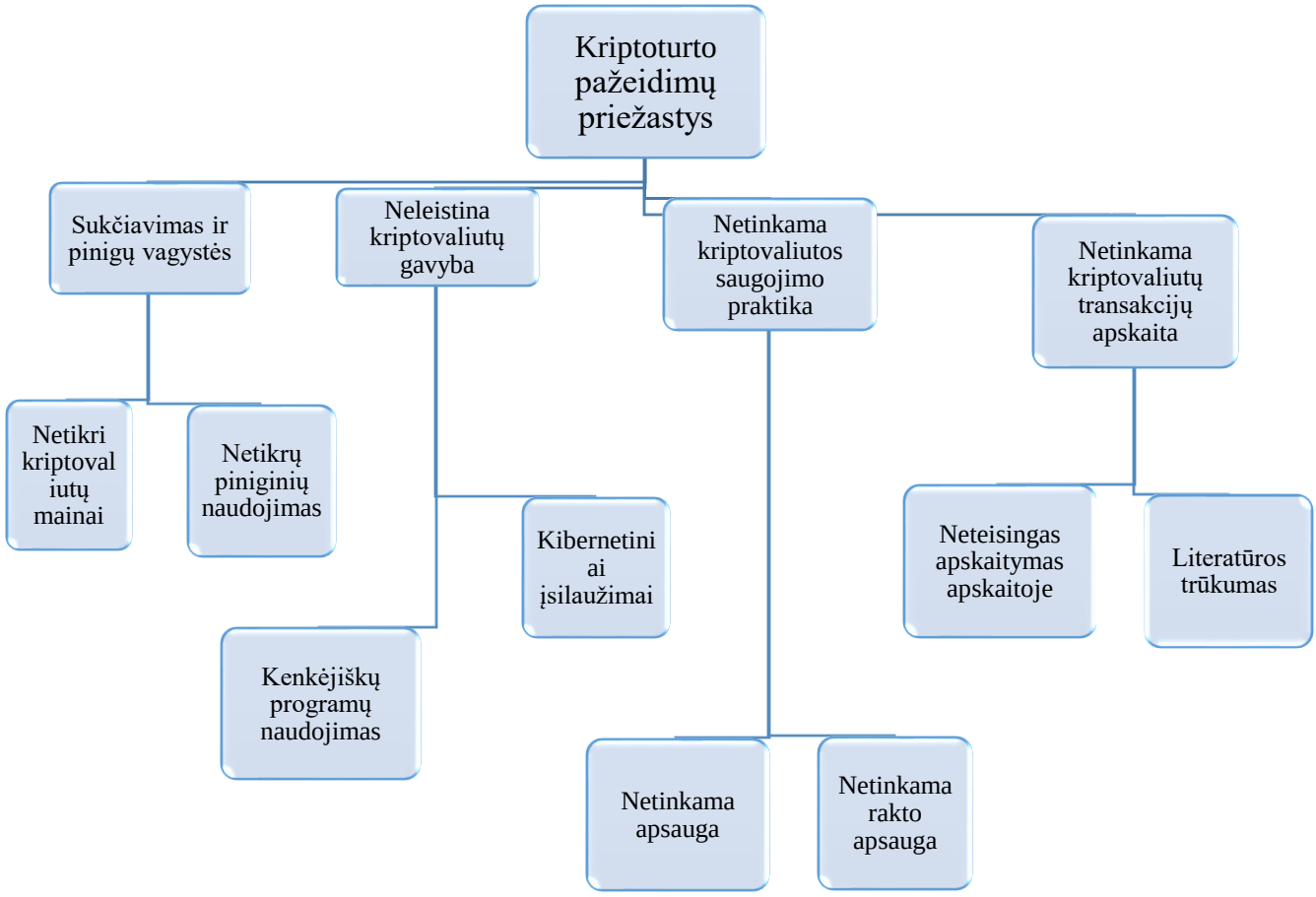
Egzistuoja mažiausiai 1500 kriptovaliutų, tačiau didžioji dauguma kriptovaliutų operacijų atliekama tik keliomis iš jų. 2018 m. gegužės pabaigoje kriptovaliutų rinkos vertė sudarė apie 330 mlrd. USD (Demertzis, M. Wolf and B. Guntram, 2018). 2008 m. pradėjus naudoti Bitcoin, „blockchain“ technologija atvėrė kelią tarpininkavimui. Nuo to laiko buvo išleista arba sukurta daugiau nei 2 000 kriptovaliutų aktyvų, įskaitant naujų tipų turtą, pvz., stabilias monetas, kurių vertė būtų stabili, ir būtų galima palyginti su fiat valiuta (angl. fiat currency) . Daugiausia dėmesio skiriant stabilioms monetoms, jomis siekiama tiesiogiai spręsti ekstremalių kriptovaliutų ir kito rizikingo finansinio turto kainų nepastovumo problemą. Stabilios monetos yra susietos su fiat valiuta (angl. fiat currency), žaliavomis, kitais kriptovaliutų turtais ar indeksais. Jie taip pat gali pasikliauti algoritmais, kurie dinamiškai koreguoja jų pasiūlą, kad stabilizuotų jų rinkos vertę. Stabilios monetos yra pagrįstos paskirstytos knygos arba blokų grandinės technologija, todėl jos turi daug kriptovaliutų savybių. Pasaulyje buvo išleista arba kuriama mažiausiai 200 stabilių monetų. Bendra stabiliųjų monetų rinkos kapitalizacija šiuo metu yra apie 114 milijardų JAV dolerių, o tai sudaro apie 8% visos 1,5 USD vertės kriptovaliutų rinkos. Bendra stabiliųjų monetų pasiūla 2021 m. išaugo daugiau nei dešimt kartų nuo maždaug 10 mlrd. USD 2020 m. gegužės mėn. (T. Pelagidis & E. Kostika, 2022).

Lietuvoje 2020 m. įsisteigė 8 naujos virtualiųjų valiutų paslaugų teikėjų įmonės, 2021 metais – 188 įmonės, o per kelis pirmuosius 2022 metų mėnesius – dar per 40 įmonių. Registrų centro duomenimis 2022 metų kovo 16 d. Lietuvoje iš viso veikė 252 virtualiųjų valiutų paslaugų teikėjų įmonės (Pinigų plovimo prevencijos kompetencijų centras, 2022). Lietuvoje šiuo metu pastebimas itin spartus kriptovaliutų veikla užsiimančių ir besisteigiančių naujų įmonių skaičiaus augimas. Tačiau spartus kriptoturto rinkos segmento augimas ir nuolat atsirandantys nauji produktai reikalauja papildomo atsakingų institucijų dėmesio, siekiant valdyti rizikas, susijusias su pinigų plovimu (Pinigų plovimo prevencijos kompetencijų centras, 2022). Į tai atsižvelgiant buvo inicijuoti įstatymo pakeitimai, kuriais siekiama užtikrinti efektyvesnį šio sektoriaus reguliavimą nelaukiant, kol įsigalios šiuo metu ES institucijose finalizuojamas reglamentas dėl kriptoturto rinkų (angl. Markets in Crypto Assets regulation, MiCA). Tikėtasi, kad europinis reguliavimas bus priimtas dar 2022 metais. Numatoma jo taikymo data – 2025 metai (Pinigų plovimo prevencijos kompetencijų centras, 2022).

Atsiranda kriptoturto apskaitos pažeidimų, su kuriais susiduria daug kriptovaliutų biržų ir kriptovaliutų platintojų. Kadangi kriptoturto apskaita palyginti visai naujas dalykas, todėl pažeidimai atsiranda dėl šių priežasčių: dėl per mažos praktikos sąskaitų tvarkyme, netinkamo duomenų saugojimo ir mainų vykdymo. Išskiriama keletas dažniausių kriptoturto pažeidimo priežasčių:

6 paveikslas

Kriptoturto pažeidimų priežastys



Šaltinis: sudarytas autorės

Sukčiavimas ir pinigų vagystė. Tai vienas iš dažniausių kriptoturto apskaitos pažeidimų. Gali įvykti per netikrus kriptovaliutos mainus arba naudojant pavojingas kriptovaliutos pinigines programas. Mokslinėje literatūroje yra trys šalių grupės, kurios vykdo skirtingą politiką kriptovaliutų reguliavimui: 1) šalys, kuriose yra absoliutus draudimas; 2) šalys, kuriose nėra specialiai sukurta reguliavimo politika; 3) šalys, kurios reguliuoja virtualias valiutas kaip nacionalinę valiutą. Pirmai

grupei priklauso Pietų Korėja, Kinija, Tailandas ir Rusija, kurios draudžia arba nustato griežtus virtualių valiutų apribojimus. 2018 metais Pietų Korėjos reguliavimo institucijos planavo uždaryti visas virtualias valiutų biržas ir uždrausti prekybą kriptovaliutomis, naudotis anoniminėmis banko sąskaitomis. Tačiau buvo nuspręsta atsisakyti šio plano. Kinijos centrinis bankas atmetė teisėtos mokėjimo priemonės statusą bitkoinams (BTC) (Riley ir Dayu, 2013; Apakhayev ir kt., 2018). 2017 m. rugsėjo mėn. Kinijos vyriausybė sustabdė visas virtualios valiutos keitimo operacijas ir uždraudė rinkti lėšas dėl pirmosios kriptovaliutų vagystės. 2013 m. liepos mėn. Tailando bankas nusprendė, kad BTC yra neteisėta. Tačiau 2019 m. planavo visiškai uždrausti BTC (O. Kreminsky, O. Kuzmenko, A. Antoniuk. O. Smahlo, 2021 m.). Antrajai šalių grupei priklauso šalys, kuriose nėra specialios reguliavimo politikos: 27 šalys, įskaitant Aldernį, Argentiną, Belgiją, Kanadą, Čilę, Kroatiją, Kiprą, Daniją, Estiją, Prancūziją, Graikiją, Honkongą, Indiją, Indoneziją, Airiją, Italiją, Japoniją, Malaiziją, Maltą, Nyderlandus, Naująją Zelandiją, Nikaragvą, Lenkiją, Portugaliją, Singapūrą, Taivaną ir Turkiją (O. Kreminsky, O. Kuzmenko, A. Antoniuk. O. Smahlo, 2021 m.).

Neleistina kriptovaliutos gavyba. Tai toks pažeidimas, kai kai kurie asmenys gali bandyti gauti kriptovaliutą neleistinai, naudojant kenkėjiškas programas arba kibernetinius įsilaužimus į kriptovaliutos mainus ar pinigines. Kibernetinė valiuta yra internetinės vertės saugykla, kuri naudojama ir kuriama tuo pačiu tikslu kaip ir fizinė valiuta. Tačiau kibernetinė valiuta neturi fizinio atvaizdo realybėje – kuriama, saugoma ir vykdoma elektroniniu būdu. Kibernetinės valiutos pervedimai vyksta akimirksniu ir be sienų. Daugelis jų buvo sukurta taip, kad vartotojai galėtų atlikti operacijas santykinai anonimiškai. Šie jų funkcionalumo elementai ne tik suteikia įdomių galimybių finansinių technologijų (fintech) naujovėms, bet ir sukuria daugybę iššūkių finansų sektoriaus reguliavimo institucijoms ir teisėsaugos institucijoms. Kibernetinės valiutos, tokios kaip Bitcoin, buvo siejamos su internetine narkotikų pramone (Martin, 2014), pinigų plovimu (ML) ir terorizmo finansavimu (Irwin ir Milad, 2016; Pflaum ir Hateley, 2014). Kriptovaliutos buvo siejamos su kibernetine nusikalstama veika tamsiose internetinėse rinkose, tokiose kaip Silk Road, Alphabay ir Valhalla. Šios platformos leidžia vartotojams įsigyti elektroninių nusikaltimų paslaugą, įsilaužimo įrankius, kenkėjiškas programas, pavogtus kredito kortelių duomenis ir pažeistus vartotojo vardų ir slaptažodžių derinius naudojant Bitcoin. Kriptovaliutos taip pat prisidėjo prie pasaulinių išpirkos programų atakų palengvinimo. 2017 m. gegužės mėn. išpirkos reikalaujančios programinės įrangos ataka, žinoma kaip WannaCry, labai greitai išplito visame pasaulyje. „WannaCry“, vadinamas „didžiausiu išpirkos programų protrūkiu istorijoje“ (F-Secure, 2017). Ši ataka buvo ypatingai žalinga,

nes tai buvo ne tik išpirkos reikalaujanti programa, bet ir „kirminas“, kuris ieškojo kitų kompiuterių ir sistemų, kad galėtų jas užkrėsti (A. S.M. Irwin, A. B. Turner, 2018).

Netinkama kriptovaliutos saugojimo praktika. Dažnai žmonės saugo savo kriptovaliutą netinkamai, palikdami ją atvirai prieigai prie interneto ir taip padėdami kibernetiniams nusikaltėliams plėsti veiklą. Pastaraisiais metais kriptovaliutos sulaukia vis didesnio susidomėjimo. Pagrindinė technologija „Blockchain“ perkelia atsakomybę už turto apsaugą galutiniam vartotojui ir reikalauja, kad jis tvarkytų savo (privačius) raktus. Mažai dėmesio buvo skiriama priežiūrai, kaip kriptovaliutų vartotojai praktiškai susidoroja su raktų valdymo iššūkiais ir kaip tam pasirenka įrankius. Mokslinio straipsnio autoriai M. Fröhlich, F. Gutjahr, Fl. Alt, Authors Info & Claims, norėdami užpildyti šią spragą, atliko pusiau struktūruotus interviu (M. Fröhlich, F. Gutjahr, Fl. Alt, Authors Info & Claims, 2020).

Netinkama kriptovaliutų transakcijų apskaita. Netinkama kriptovaliutos transakcijų apskaita gali sukelti netikslumų ir neskaidrumų, kurie gali būti išnaudojami finansinių nusikaltimų metu. Kriptovaliutos yra reiškinys, kuris pastaraisiais metais atsiranda vis dažniau ir yra plačiai naudojamas tiek fizinių asmenų, tiek subjektų. Jų technologinės ypatybės suintrigavo daugelį, todėl gerokai išaugo turimų kriptovaliutų skaičius ir išaugo jų naudojimo sritys. Vis daugiau įmonių pradėjo naudoti kriptovaliutas, pavyzdžiui, investuoti arba priimti jas kaip mokėjimo priemonę. Dėl to apskaitos standartų kūrėjams skubiai prireikė gairių, kaip reglamentuoti, kaip jie traktuojami finansinėse ataskaitose. Dėl tokių gairių trūkumo, praktikoje buvo taikomi įvairūs apskaitos metodai, dėl kurių finansinių ataskaitų rengėjams kilo didelių iššūkių. Iki šiol gaires finansinių ataskaitų rengėjams sudarė didžiųjų apskaitos įmonių ataskaitos ir vietos apskaitos reguliavimo institucijų rekomendacijos. Literatūros trūkumas ir galimos pasekmės rinkai lėmė, jog skubiai reikia gairių, kad būtų išvengta pasekmių apskaitos tvarkymo rinkoje. Be to, dėl šių iššūkių gali atsirasti galimybių valdyti pajamas arba gali padidėti informacijos asimetrija tarp suinteresuotųjų šalių ir subjektų (P. Hyytiä, E. Sundqvist, 2019).

Pastaraisiais metais kriptoturto įmonių vis daugėjo, todėl atsirando ir pažeidimų. Pagrindiniais kriptoturto apskaitos pažeidimais pripažįstami šie: sukčiavimas ir pinigų vagystė, neleistina kriptovaliutos gavyba, netinkama kriptovaliutos saugojimo praktika, netinkama kriptovaliutų transakcijų apskaita. Dėl apskaitos gairių trūkumo atsiranda problemų dėl kriptoturto apskaitos valdymo.

3.2. Kriptoturto apskaitos pažeidimai ir pasekmės Lietuvoje

Siekiant geriau įsisavinti ir suprasti kriptoturto apskaitos pažeidimų problemas, būtina apžvelgti kriptoturto apskaitos pažeidimus Lietuvoje. 1 lentelėje pateikiama informacija apie Lietuvoje, Lietuvos banko skirtas nuobaudas 2015-2024 m. už nuosavo kapitalo pažeidimus.

1 lentelė

Lietuvos banko skirtos baudos už nuosavo kapitalo pažeidimus

Eil. Nr.	**Laikotarpis**	**Įstaigų pavadinimai**	**Poveikio priemonė Bauda Eur**
1.	2019-07-01	„NomuPay Europe“, UAB	17,2 tūkst.
2.	2020-06-29	„Via Payments“, UAB	120 tūkst.
3.	2020-08-31	„SatchelPay“, UAB	5 tūkst.
4.	2021-05-07	„Via Payments“, UAB	15 tūkst.
5.	2021-06-10	„Valyuz“, UAB	15 tūkst.
6.	2021-11-29	„Bebawa“, UAB	4 tūkst.
7.	2021-12-14	„SHIFT Financial Services LT“, UAB	16 tūkst.
8.	2022-11-22	„Secure Nordic Payments“, UAB	28 tūkst.
9.	2023-03-07	„Amber Payments“, UAB	2 tūkst.
10.	2023-04-03	„PCS Transfer“, UAB	6 tūkst.
11.	2023-04-05	„Finansinės paslaugos „Contis““, UAB	180 tūkst.
12.	2023-05-16	„Stanhope Financial“, UAB	9 tūkst.
13.	2023-08-22	„SatchelPay“, UAB	25 tūkst.
14.	2023-11-14	„Stanhope Financial“, UAB	48 tūkst.
15.	2024-03-19	„Flywire Europe“, UAB	40 tūkst.

Šaltinis: sudarytas autorės, remiantis Lietuvos banku (2015-2024 m.)

Didžiausia bauda už minėtą laikotarpį buvo skirta „Finansinės paslaugos „Contis““, UAB dėl nuosavo kapitalo reikalavimų nesilaikymo. Įstaiga toje pačioje sąskaitoje laikė ne tik klientų, partnerių lėšas, bet ir nuosavo kapitalo poreikį, kurį be to ir neteisingai buvo paskaičiavę. Už minėtus pažeitimus įtaigai buvo skirta 180 tūkst. Eur bauda.

2 lentelė

Lietuvos banko skirtos baudos už klientų pažinimo, informacijos surinkimo ir vertinimo pažeidimus 2015-2024 m. laikotarpiu

Eil. Nr.	**Laikotarpis**	**Įstaigų pavadinimai**	**Poveikio priemonė Bauda Eur**
1.	2015-08-10	„Paysera LT“, UAB	11,7 tūkst.
2.	2018-05-28	„Secure Nordic Payments“, UAB	19,7 tūkst.
3.	2020-02-24	„deVere E-Money“, UAB	30 tūkst.
4.	2020-05-28	„ConnectPay“, UAB	110 tūkst.
5.	2020-11-13	„Paysera LT“, UAB	370 tūkst.
6.	2021-05-19	„Forexlita“, UAB	5 tūkst.
7.	2021-06-23	„Payswix“, UAB (buvęs *GlobalNetint*, UAB)	350 tūkst.
8.	2021-12-14	„Wallter“, UAB	280 tūkst.
9.	2022-03-15	„Revolut Bank“, UAB	50 tūkst.
10.	2022-03-29	„Revolut Payments“, UAB	150 tūkst.
11.	2022-09-06	„Paysera LT“, UAB	100 tūkst.
12.	2022-10-25	„Best Finance“, UAB	109 tūkst.
13	2023-04-25	„Verified Payments“, UAB	110 tūkst.
14.	2023-05-30	„Via Payments“, UAB	100 tūkst.
15.	2023-06-06	„Wittix“, UAB	55 tūkst.
16.	2024-03-12	„Secure Nordic Payments“, UAB	210 tūkst.

Šaltinis: sudarytas autorės, remiantis Lietuvos banku (2015-2024 m.)

Minėtu laikotarpiu už klientų pažinimą, informacijos surinkimą ir vertinimą didžiausia bauda skirta „Payswix“, UAB (buvęs GlobalNetint, UAB) net 350 tūkst. Eur. Lietuvos banko Finansų rinkos priežiūros tarnyba atliko elektroninių pinigų įstaigos „Payswix“, UAB (buvęs GlobalNetint, UAB) patikrinimą ir nustatė daugybinių įstatymų pažeidimų, už kuriuos skyrė 350 tūkst. Eur baudą ir apribojo jos veiklą. Lietuvos bankas skyrė „Payswix“, UAB (buvęs GlobalNetint, UAB) piniginę baudą ir laikinai, kol pašalins pinigų plovimo ir teroristų finansavimo prevenciją reglamentuojančių teisės aktų pažeidimus, uždraudė pradėti dalykinius santykius su klientais, kurių veikla susijusi su didesne pinigų plovimo ir teroristų finansavimo rizika. Be to, bendrovė laikinai neteko teisės leisti elektroninius pinigus ir teikti mokėjimo paslaugas tam tikrų teritorijų klientams. Bendrovė pažeidė Pinigų plovimo ir teroristų finansavimo prevencijos įstatymo reikalavimus – netinkamai vertino klientų keliamą pinigų plovimo ir teroristų finansavimo riziką, ne visais atvejais užtikrino, kad klientų tapatybės nustatymas nuotoliniu būdu atitiktų teisės aktų reikalavimus. „Payswix“, UAB (buvęs

GlobalNetint, UAB), tikrindama klientų pateiktus dokumentus ir informaciją apie naudos gavėjus, ne visais atvejais rėmėsi patikimo ir nepriklausomo šaltinio informacija. Bendrovė taip pat nebuvo įdiegusi tinkamų procedūrų, skirtų nustatyti, ar klientas ir naudos gavėjas yra politiškai pažeidžiami (paveikiami) asmenys. Lietuvos banko atlikto patikrinimo metu buvo nustatyta, kad „Payswix“, UAB (buvęs GlobalNetint, UAB) neužtikrino, kad didesnės rizikos grupės klientams būtų taikomos sustiprinto tapatybės nustatymo priemonės, neatnaujino klientų pažinimo informacijos, netinkamai vykdė nuolatinę klientų dalykinių santykių ir operacijų stebėseną (Lietuvos bankas, 2022 m.).

3 lentelė

Lietuvos banko skirtos baudos už finansinius apskaitos pažeidimus 2015-2024 m. laikotarpiu

Eil. Nr.	**Laikotarpis**	**Įstaigų pavadinimai**	**Pažeidimo pavadinimas**	**Poveikio priemonė Bauda Eur**
1.	2019-07-22	„deVere E-Money“, UAB	Bankui teikė neteisingą informaciją apie klientų lėšų likučius kredito įstaigose.	21,6 tūkst.
2.	2019-08-19	„PanPay Europe“, UAB	Klientų pinigus laikė ne kredito įstaigoje.	16,8 tūkst.
3.	2019-10-21	„Secure Nordic Payments“, UAB	Bendrovė laiku neįvykdė dalies klientų pateiktų mokėjimo nurodymų ir lėšų įskaitymo operacijų.	245,1 tūkst.
4.	2019-12-02	„SatchelPay“, UAB	Dalį klientų lėšų laikė elektroninių pinigų ir mokėjimo įstaigose bei ES šalies banke, tačiau ne klientų lėšoms saugoti skirtose sąskaitose.	23 tūkst. Eur
5.	2020-01-27	„Glocash Payment“, UAB	Už netinkamą klientų lėšų laikymą.	17 tūkst. Eur.
6.	2020-05-14	„Secure Nordic Payments“, UAB	Už netinkamą mokėjimo operacijų vykdymą.	22 tūkst. Eur
7.	2022-07-21	„Via Payments“, UAB	Bauda už laiku nepateiktas finansines ataskaitas.	20 tūkst. Eur
8.	2022-07-21	„Secure Nordic Payments“, UAB	Bauda už laiku nepateiktas finansines ataskaitas.	10 tūkst. Eur
9.	2022-08-09	„Blender Lithuania“, UAB	Nesudarė sutarties su audito įmone dėl metinės finansinės atskaitomybės audito, nepatvirtino metinių finansinių ataskaitų	10 tūkst. Eur
10.	2020-09-25	„Wallter“, UAB	Bendrovė ne tik netinkamai laikė klientų lėšas, bet ir slėpė šį faktą teikdama Lietuvos bankui tikrovės neatitinkančią informaciją.	90 tūkst. Eur

11.	2022-11-10	„Revolut Bank“, UAB	Įmonė per nustatytus terminus nepatvirtino ir nepateikė audituotų metinių finansinių ataskaitų rinkinio bei auditoriaus išvados.	70 tūkst. Eur
12.	2023-06-06	UAB „Nexpay“	Nesilaikė reikalavimų dėl kliento dalykinių santykių ir sandorių (operacijų) stebėsenos.	125 tūkst. Eur
13.	2023-10-17	„Blue Emi LT“, UAB	Teisės aktuose nustatytus terminus nepatvirtino metinių finansinių ataskaitų rinkinio ir nepriėmė sprendimo dėl pelno (nuostolio) paskirstymo, nepateikė Lietuvos bankui šių dokumentų.	6 tūkst. Eur
14.	2023-04-11	„Glocash Payment“, UAB	Neužtikrino vidaus audito funkcijos – nuo 2020 m. nebuvo atlikusi teisės aktų reikalavimus atitinkančio vidaus audito.	10 tūkst. Eur
15.	2024-01-23	„Revolut Bank“, UAB	Bankas pažeidė didelių pozicijų limito reikalavimą.	200 tūkst. Eur

Šaltinis: sudarytas autorės, remiantis Lietuvos banku (2015-2024 m.)

Dižiausią baudą Lietuvos bankas skyrė „Secure Nordic Payments“, UAB (anksčiau vadinosi UAB MisterTango) bendrovei – 245,1 tūkst. Eur. Pinigų plovimo ir teroristų finansavimo prevencijai finansų įstaigose Lietuvos bankas skiria ir ateityje skirs ypatingą dėmesį. „Secure Nordic Payments“, UAB (anksčiau vadinosi UAB MisterTango) bendrovėje rasta šiurkščių ir sistemingų pažeidimų. Kai kurie iš jų buvo pakartotiniai. Lietuvos bankas ir anksčiau buvo nustatęs, kad ši elektroninių pinigų įstaiga nesilaiko Pinigų plovimo ir teroristų finansavimo prevencijos įstatymo reikalavimų, bet ji nesiėmė tinkamų priemonių trūkumams pašalinti. Klientų atliekamų mokėjimo operacijų stebėsenos procesai reglamentuoti formaliai, neužtikrinant jų tinkamo įgyvendinimo. Įstaiga neįvertino rizikų, susijusių su jos veikla, neturėjo vidaus audito procedūrų ir tikrinamuoju laikotarpiu nebuvo atlikusi pinigų plovimo ir teroristų finansavimo prevencijos srities audito. „Secure Nordic Payments“, UAB (anksčiau vadinosi UAB MisterTango) už pinigų plovimo ir teroristų finansavimo prevencijos reikalavimų pažeidimus baudžiama trečią kartą (anksčiau bausta 2016 ir 2018 m.) (Lietuvos bankas, 2019 m.).

4 lentelė

Lietuvos banko skirtos baudos už kitus kriptoturto apskaitos pažeidimus 2015-2024 m. laikotarpiu

Eil. Nr.	Laikotarpis	Įstaigų pavadinimai	Pažeidimo pavadinimas	Poveikio priemonė (Piniginė, bauda)
1.	2015-11-02	„Lietuvos paštas“, AB	Pažeidimas dėl veiklą reglamentuojančių teisės aktų nesilaikymo – nepranešė priežiūros institucijai apie numatomus vadovų pasikeitimus	19,7 tūkst. Eur
2.	2018-09-19	„Pervesk“, UAB	Bendrovė aplaidžiai vertino klientų riziką: neturėjo tinkamų ir jų veiklai adekvačių rizikos valdymo vidaus taisyklių	244 tūkst. Eur
3.	2020-04-03	“Majestic Financial”, UAB	Įstaiga neužtikrino vidaus kontrolės pinigų plovimo ir teroristų finansavimo prevencijos srityje – tinkamo darbuotojų ir atsakingų asmenų funkcijų pasiskirstymo.	9 tūkst. Eur
4.	2020-12-08	„Wittix”, UAB	Įstaigos administracijos vadovas ne tik neužtikrino, kad tinkamai veiktų vidaus kontrolės sistema ir būtų tinkamai užkardomos rizikos.	28 tūkst. Eur
5.	2021-02-10	„Verse Payments Lithuania”, UAB	Netinkamai įgyvendino klientų lėšų saugojimo reikalavimus ir teik neteisingą informaciją Lietuvos bankui apie lėšų likučius.	30 tūkst. Eur
6.	2021-06-11	„Zen.com”, UAB	Lietuvos Bankui teikė neteisingą informaciją apie valiutas, kuriomis buvo laikomos bendrovės klientų ir nuosavos lėšos.	60 tūkst. Eur
7.	2022-02-08	„Transactive Systems”, UAB	Įmonė tinkamai neapsaugojo klientų lėšų ir teikė neteisingą informaciją.	20 tūkst. Eur
8.	2022-09-20	„Perlas Finance“, UAB	Neužtikrino vidaus politikos ir vidaus kontrolės procedūrų,	40 tūkst. Eur.
9.	2022-11-08	„Phooenix Payments“, UAB	Neturėjo klientų lėšų apsaugos kontrolės mechanizmo, toje pačioje sąskaitoje laikė ne tik klientų, bet ir nuosavas lėšas.	90 tūkst. Eur
10.	2023-04-25	„Via Payments”, UAB	Netinkamai atliko poveikio veiklai analizę.	70 tūkst. Eur
11.	2023-05-30	„Transactive Systems”, UAB	Netinkamai vykdė pinigų plovimo ir teroristų finansavimo prevencijos reikalavimus ir neužtikrino, kad vidaus kontrolės sistemos būtų efektyvi.	280 tūkst. Eur
12.	2023-06-13	„Finci“, UAB	Nebuvo įtvirtintos priemonės, skirtos kliento sandoriams patikrinti.	30 tūkst. Eur
13.	2023-08-29	„Roltena”, UAB	Įstaiga netikrino, ar klientai, jų atstovai, naudos gavėjai nepatenka tarptautinių sankcijų apimtį.	8 tūkst. Eur
14.	2023-11-07	„Exchangelt“, UAB	Įstaiga nebuvo nustačius vidaus politikos bei vidaus kontrolės procedūrų dėl atitikties ir audito.	45 tūkst. Eur

15.	2023-11-21	Finansinės paslaugos „Contis", UAB	Neužtikrino efektyvių platintojų rizikos vertinimo procesų, tinkamai nesiaiškino klientų portfelio,	840 tūkst. Eur
16.	2023-12-12	„Valyuz", UAB	Įstaigos vidaus kontrolės procedūros, susijusios su sustiprintu kliento tapatybės nustatymu, turėjo trūkumų.	55 tūkst. Eur
17.	2023-12-19	„NexPay", UAB	Bauda už netinkamą informavimą apie kibernetinį incidentą.	50 tūkst. Eur

Šaltinis: sudarytas autorės, remiantis Lietuvos banku (2015-2024 m.)

Atlikęs patikrinimą, Lietuvos bankas nustatė, kad elektroninių pinigų įstaiga UAB „Finansinės paslaugos „Contis" nesilaikė pinigų plovimo ir teroristų finansavimo prevencijos bei informacijos saugumo ir veiklos tęstinumo rizikos valdymo reikalavimų. Įstaigai skirta 840 tūkst. Eur bauda ir ji įpareigota pašalinti pažeidimus bei veiklos trūkumus. Be to, įstaigai iki atskiro Lietuvos banko sprendimo nustatyta apribojimų dėl verslo plėtros. UAB „Finansinės paslaugos „Contis", vykdydama veiklą per elektroninių pinigų platintojus (toliau – platintojai), delegavo jiems funkcijas, susijusias su pinigų plovimo ir teroristų finansavimo prevencijos priemonių įgyvendinimu, tačiau nekontroliavo, kad platintojai šias funkcijas tinkamai įgyvendintų (Lietuvos bankas, 2023 m.). Tai didžiausia bauda skirta Lietuvos banko per visą tiriamąjį laikotarpį.

2015-2022 m. laikotarpiu Lietuvos bankas skyrė baudas už nuosavo kapitalo reikalavimų nesilaikymą. Įstaigos netikrino, ar klientai, jų atstovai, naudos gavėjai nepatenka į tarptautinių sankcijų apimtį; ar netinkamai taikė sustiprintos klientų tapatybės nustatymo priemones didesnės rizikos klientams, ypač nustatant jų turto ir lėšų šaltinį, ir netinkamai atliko poveikio veiklai analizę.

2023-2024 m. laikotarpiu Lietuvos bankas „Nexpay" UAB įstaigai skyrė 125 tūkst. Eur baudą ir įspėjimą. Įspėjimas skirtas už tai, kad patikrinimo metu įstaiga ne visada Lietuvos bankui teikė išsamią ir tikslią informaciją, nesilaikė nustatytų terminų, o tai apsunkino patikrinimo procesą. Įstaiga pažeidė teisės aktų reikalavimus dėl kliento dalykinių santykių ir sandorių (operacijų) stebėsenos – tikrintu laikotarpiu įstaigos vidaus procedūrose nustatytas kliento dalykinių santykių ir operacijų stebėsenos reglamentavimas ir praktikoje įdiegti sprendimai nebuvo pakankami (Lietuvos bankas, 2023 m.).

Dar viena įmonė, kuriai Lietuvos bankas skyrė 55 tūkst. Eur baudą yra „Wittix" UAB. Lietuvos bankas nustatė, kad elektroninių pinigų įstaiga „Wittix" UAB pažeidė tarptautinių finansinių sankcijų, ribojamųjų priemonių įgyvendinimo bei pinigų plovimo ir teroristų finansavimo prevencijos reikalavimus. Įstaiga taip pat neužtikrino, kad klientų, jų atstovų ir naudos gavėjų tapatybė (įskaitant

sustiprintą patikrą) būtų nustatoma pagal teisės aktuose nustatytus reikalavimus. Atrinktų klientų bylų duomenys parodė, kad įstaiga ne visais atvejais tinkamai nustatydavo kliento naudos gavėjo tapatybę (Lietuvos bankas, 2023 m.).

Lietuvos bankas elektroninių pinigų įstaigos „Finci“ UAB patikrinimo metu nustatė Pinigų plovimo ir teroristų finansavimo prevencijos įstatymo pažeidimų. Tikrintu laikotarpiu įstaigos vidaus kontrolės procedūros, susijusios su tarptautinių sankcijų įgyvendinimu, turėjo reikšmingų trūkumų – nebuvo aprašytas praktikoje taikomas tarptautinių sankcijų įgyvendinimo procesas, nebuvo įtvirtintos priemonės, skirtos nustatyti, ar kliento vykdomi sandoriai ir operacijos nepatenka į tarptautinių ribojamųjų priemonių (nustatančių sektorinius, prekybos, tam tikrų paslaugų ribojimus) sąrašą, netaikė tarptautinių sankcijų stebėsenos sistemos kontrolės priemonių (Lietuvos bankas, 2023 m.).

„TransferGo Lithuania“ UAB įdiegtos kliento dalykinių santykių ir operacijų (sandorių) stebėsenos priemonės buvo nepakankamos, kad būtų tinkamai valdoma pinigų plovimo ir teroristų finansavimo rizika. Vykdydama operacijų stebėseną, įstaiga ne visada užtikrindavo, kad operacijos (sandoriai) atitiktų jos turimas žinias apie klientą, jo verslą, rizikos pobūdį ir lėšų šaltinį. Be to, įstaiga pranešimus apie įtartinas operacijas ir sandorius teikė ne teisės aktų nustatyta tvarka (Lietuvos bankas, 2023 m.).

„Payrnet“ UAB neturėjo visų duomenų, kiek klientų – galutinių vartotojų – naudojosi jos paslaugomis: nekontroliavo informacijos apie galutinių vartotojų mokėjimo operacijų duomenis ir negalėjo nustatyti tikslios galutinių vartotojų lėšų sumos. Taip pat nesaugojo pagrindinių galutinių vartotojų duomenų, būtinų siekiant užtikrinti pinigų plovimo ir teroristų finansavimo prevenciją (Lietuvos bankas, 2023 m.).

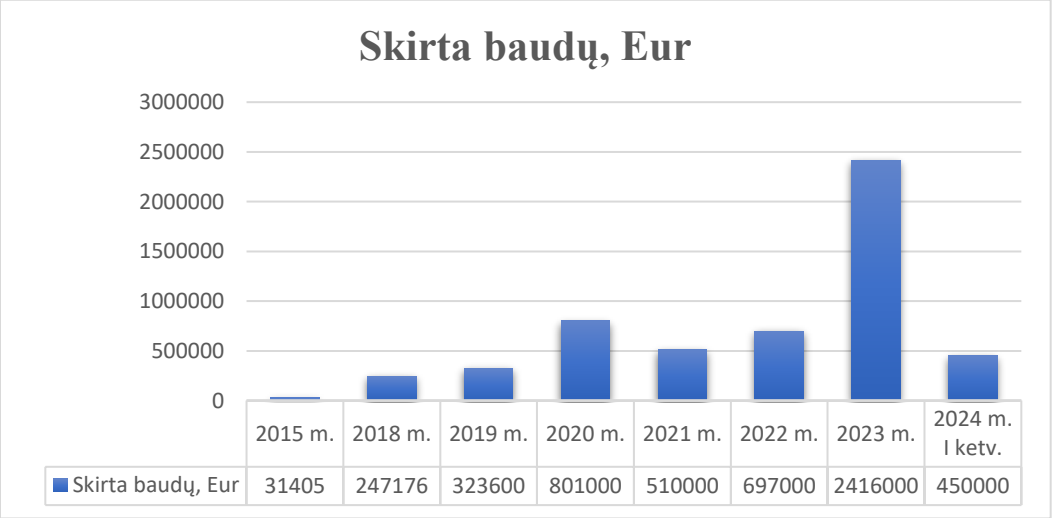
2024 m. Lietuvos bankas patikrinimo metu nustatė tokių pažeidimų: įstaiga neužtikrino patikimos ir efektyvios pinigų plovimo ir teroristų finansavimo prevencijos vidaus kontrolės, nesilaikė reikalavimų nustatydama klientų ir naudos gavėjų tapatybę, neužtikrino klientų dalykinių santykių ir sandorių (operacijų) stebėsenos, nesilaikė nuosavo kapitalo reikalavimų, neatskyrė ir neapsaugojo klientų lėšų, teikė Lietuvos bankui neteisingą informaciją, laiku nepateikė priežiūrai skirtų ataskaitų. Įstaigai laikinai uždrausta užmegzti naujus dalykinius santykius su didesnės pinigų plovimo ir teroristų finansavimo rizikos klientais ir juridiniais asmenimis, kurių vykdoma veikla susijusi su finansinėmis paslaugomis, lošimais ir kriptoturtu (Lietuvos bankas, 2024 m.).

Lietuvos bankas nustatė, kad mokėjimo įstaiga Flywire Europe UAB 2023 m. III ir IV ketvirtį nesilaikė nuosavo kapitalo reikalavimų, kurių privalo laikytis nuolat. Už šį pažeidimą Lietuvos bankas įstaigai skyrė 40 tūkst. Eur baudą.

Per 2014-2024 m. laikotarpį Lietuvos bankas skyrė rekordinę baudą už pažeidimą įstaigai UAB „Finansinės paslaugos „Contis“, kuri nesilaikė pinigų plovimo ir teroristų finansavimo prevencijos bei informacijos saugumo ir veiklos tęstinumo rizikos valdymo reikalavimų. Įstaigai skirta 840 tūkst. Eur bauda ir ji įpareigota pašalinti pažeidimus bei veiklos trūkumus. Be to, įstaigai iki atskiro Lietuvos banko sprendimo nustatyta apribojimų dėl verslo plėtros.

7 paveikslas

Lietuvos banko skirtos baudos už kriptoturto apskaitos pažeidimus 2015-2024 m.



Šaltinis: sudarytas autorės, remiantis Lietuvos banku (2015-2024 m. I ketv.)

Pagal 7 pav. surinktus ir pateiktus duomenis nuo 2015-2020 m. laikotarpiu matoma ryški kilimo tendencija. 2015-2020 m. laikotarpiu buvo patikrinta daugiau įmonių nei 2021 m. arba skirtų baudų vidurkis buvo didesnis dėl padarytų šiurkščių pažeidimų. 2021 m. lyginant su 2020 m. skirtų baudų sumažėjo. Galima manyti, kad tam įtakos turėjo mažesnis tikrintų įstaigų skaičius arba skirtų baudų dydis. Tačiau nuo 2021 m. vėl regima kilimo tendencija. Pagrindinis pažeidimas, dėl kurio įstaigoms buvo skirtos baudos, yra susijusios su klientų pinigų plovimo ir teroristų finansavimo rizikos vertinimu ir valdymu. Kiekviena įstaiga, laiku neatlikusi analitikos, nepatikrinusi abejotinų kriptoturto operacijų, prisidėjo prie nusikaltimo. Tai patikrinus atsakingoms institucijoms už operacijų teisingumą ir teisėtumą, buvo skirta bauda už pažeidimus.

3.3. Kriptoturto pasisavinimai 2019-2023 metais Jungtinėse Amerikos Valstijose ir Europoje

Federalinio tyrimų biuro „Skundų dėl nusikaltimų internetu centras“ per 2021 m. gavo 34 202 skundus dėl tam tikros rūšies kriptovaliutų neteisėto naudojimo. „Vartotojų finansinės apsaugos biuras“ per 2022 m. turėjo 1870 paskelbtų skundų. Federalinė prekybos komisija pranešė apie daugiau nei 46 000 sukčiavimo atvejų, kurių aukos pareikalavo daugiau nei 1 mlrd. USD dolerių. Vidurkis vienam sukčiavimo atvejui siekė apie 2600 USD dolerių. „Privataus sektoriaus tyrimai“ apskaičiavo, kad 2021 m. Pasauliniu mastu kriptovaliutų nusikaltimų vertė buvo maždaug 14 mlrd. USD, o tai yra beveik dvigubai daugiau nei 7,8 mlrd. Tai sudaro 60 % kriptovaliutų sukčiavimo atvejų per 2020 m. Dažniausiai naudojamas kilimėlio traukimo būdas (angl. a rug pull) yra sukčiavimo rūšis, kai nusikaltėliai sukuria iš pažiūros teisėtą projektą kriptovaliutai nupirkti. Tada suranda patiklius investuotojus, kurie sutinka investuoti į taip vadinamus „projektus“. Užuot panaudoję surinktas lėšas „projektui“ įgyvendinti, kaip buvo žadėta, nusikaltėliai tiesiog atsisako „projekto“ ir dingsta su pavogtomis lėšomis (J. Scharfman, 2023).

Kriptovaliutos pamažu integruojamos į finansinę kultūrą, o nusikalstama veika, susijusi su kriptovaliutomis, tapo šiuolaikinių sukčiavimo schemų dalimi (I. Cunjak, 2022). Įsilaužimų rūšis galima suskirstyti į šias kategorijas:

5 lentelė

Kriptoturto nusikaltimų rūšys

Šaltinis	Nusikaltimo rūšis	Trumpas aprašymas
Cunjak, (2022)	Nuo elektroninės erdvės priklausomi nusikaltimai.	Nusikaltimų kategorija apima atakas, kenkėjiškas kompiuterių išpirkos reikalaujančias programas.
Charoenwong, Bernardi (2022)	„Žmogaus klaidos“ įsilaužimas.	Tokio tipo „nulaužimas“ paprastai apima išpirkos el. laiškus arba kenkėjiškas programas.
Chainalysis, (2020)	Išpirkos reikalaujančios programos.	Nusikaltimų būdas, kai užpuolikai įterpia kenkėjišką kompiuterinę programą, siekdami šifruoti failus.
Charoenwong, Bernardi (2022)	Saugumo pažeidimas.	Infrastruktūra be jokios apsaugos.
Cunjak, (2022)	Ponzi schema.	Investuotojams žadamos didelės grąžos su maža rizika.
Tiwari, Gepp & Kumar, (2019)	Sukčiavimas pagal žetonus.	Sukčiavimas, sukčiavimas vertybiniais popieriais, Ponzi schema ir įsilaužimas.
B, Charoenwong M. Bernardi, (2022)	Agentūros problema.	Vidinio darbo priežastys.

Šaltinis: sudarytas autorės, remiantis lentelėje nurodytais šaltiniais

Nuo elektroninės erdvės priklausomi nusikaltimai negali būti įvykdyti be informacinių technologijų ir tam tikro lygio žinių apie jų pritaikymą elektroninėje erdvėje. Ši elektroninių nusikaltimų kategorija apima atakas svetainėse – įsilaužimą, kenkėjiškas kompiuterių programas – kenkėjiškas programas arba šantažuojančias kompiuterių programas, išpirkos reikalaujančias programas. Be šio esminio skirtumo informacinių technologijų naudojimo kontekste, skiriasi ir motyvacija. Nusikalstamų veikų, priklausančių nuo informacinių technologijų, motyvas pirmiausia yra ne finansinė nauda, bet motyvai dažniausiai yra iššūkis, naujų žinių įgijimas, smalsumas ar linksmybės (Weulen Kranenbarg, 2018), (I. Cunjak, 2022).

„Žmogaus klaidos“ (angl. „Human Error“ Hack) / įsilaužimas. Tokio tipo „nulaužimas“ paprastai apima išpirkos el. laiškus arba kenkėjiškas programas į savo sistemą, kuri leidžia įsilaužėliams gauti privačius biržų piniginių raktus (B, Charoenwong M. Bernardi, 2022).

Išpirkos reikalaujančios programos yra vienas iš elektroninių nusikaltimų būdų, kai užpuolikai, t. y. įsilaužėliai, į vartotojo kompiuterį įterpia kenkėjišką kompiuterinę programą, siekdami šifruoti failus. Užpuolikai iš vartotojų prašo išpirkos, dažniausiai kriptovaliutomis, kad jie galėtų vėl pasiekti failus. Apskaičiuota, kad kiekvieną mėnesį sukuriama 1,5 milijono naujų sukčiavimo svetainių (Chainalysis, 2020). Remiantis kibernetinio saugumo tyrimais, yra dviejų tipų išpirkos programinės įrangos atakų pažeidėjai. Pirmąjį tipą sudaro nusikaltėliai, priklausantys organizuotoms nusikalstamoms grupuotėms. Antrasis nusikaltėlių tipas – valstybės veikėjai, organizuojantys daug didesnius išpuolius (I. Cunjak, 2022).

Saugumo pažeidimas (angl. Security Breach). Šis įsilaužimas įvyksta dažniausiai daugiausia dėl to, kad įsilaužėliai gali rasti spragą saugos sistemoje ir išnaudoti visas galimybes, todėl dalis pagrindinės šių mainų infrastruktūros praktiškai yra be jokios apsaugos (B, Charoenwong M. Bernardi, 2022).

Ponzi schema yra sukčiavimo rūšis, kai investuotojams žadamos didelės grąžos su maža rizika arba jos visai nėra. Sukčiavimo organizatoriams ir pirmiesiems investuotojams išmokama vėlesnių investuotojų lėšomis, kai realiai iš verslo projekto gaunama mažai pajamų arba visai negaunama. Ponzi schema veikia tol, kol atsiranda naujų investuotojų arba tol, kol investuotojams nereikia grąžinti pinigų (I. Cunjak, 2022).

Sukčiavimas pagal žetonus. Ši technologija suteikia galimybę palyginti greitai, pigiai ir lengvai gauti lėšų verslumo projektams ar pradiniams monetų pasiūlymams. Pradinis pasiūlymas leidžia investuotojams per tam tikrą laikotarpį įsigyti žetonų mainais į pinigus ar kitas kriptovaliutas.

Žetonai palengvina investuotojų prieigą prie emitento paslaugų, tačiau nesuteikia jiems nuosavybės teisės (Tiwari, Gepp & Kumar, 2019).

Agentūros problema (angl. Agency Problem). Šis įsilaužimo tipas įvyksta ne dėl aplaidumo ar prastesnių saugumo priemonių, o dėl vidinio darbo (B, Charoenwong M. Bernardi, 2022).

6 lentelė

Kriptoturto praradimai 2015-2021 metais

Eil. Nr.	Akcijų biržos pavadinimas	Kriptovaliuta	Prarasta (mln. USD valiuta) suma	Vagystės (įsilaužimo) tipas
1.	Bitstamp	19000 Bitcoin	5,1	Žmogaus klaidos
2.	BTER	7170 Bitcoin	1,75	Agentūros problema
3.	Gatecoin	185000 Ethereum ir 250 Bitcoin	2,0	Saugumo pažeidimas
4.	Bitfinex	119756 Bitcoin	66,0	Saugumo pažeidimas
5.	Yapizon	3816 Bitcoin	5.3	Saugumo pažeidimas
6.	NiceHash	4736 Bitcoin	62,0	Saugumo pažeidimas
7.	Coincheck	523000,00 Nem	500,0	Žmogaus klaidos
8.	Bitgrail	17000,00 Nano	17,0	Saugumo pažeidimas
9.	CoinSecure	438 Bitcoin	3,3	Agentūros problema
10.	Bithumb and Coinrail	10394 Bitcoin, Ripple XRP	71,5	Saugumo pažeidimas
11.	Zaif	5966 Bitcoin, neatskleistos (angl. undisclosed) BCH and MonaCoin	60,0	Saugumo pažeidimas
12.	QuadrigaCX	26350 Bitcoin	9,0	Agentūros problema
13.	Coinbene	100000,00 HPT, NPSX, MXM, and UDOO	100,0	Agentūros problema
14.	Binance	6270 Bitcoin	40,0	Žmogaus klaidos
15.	Bitrue	9300 XRP (Ripple) ir 2500 ADA (Cordano)	39,0	Saugumo pažeidimas
16.	Upbit	342000 Ethereum	51,0	Saugumo pažeidimas
17.	Cashaa	336 Bitcoin	31,0	Žmogaus klaidos
18.	KuCoin	11480 Ethereum ir Bitcoin	281,0	Saugumo pažeidimas
19.	EXMO	422 Bitcoin, Ethereum, Ripple XRP, Zcash (ZEC), Ethereum Classic	10,0	Saugumo pažeidimas
20.	Africrypt	69000 Bitcoin	3,6	Agentūros problema
21.	Poly Network	12964 Bitcoin ir Ethereum	600,0	Saugumo pažeidimas
22.	Liquid Hack	1941 Bitcoin ir Ethereum	91,35	Saugumo pažeidimas
23.	Cream Finance	2102 Ethereum	130,0	Saugumo pažeidimas
24.	Boy x Highspeed Theft	2404 įvairios kriptovaliutos	139,0	Žmogaus klaidos
25.	Badger DAO	2544 Bitcoin ir Ethereum	120,0	Saugumo pažeidimas
26.	Bitmart	4155 Ethereum 20 tokenai Bitcoin BSC tokenai	150,0	Saugumo pažeidimas
27.	AscendEX	1,647 Ethereum 20 tokenai ir Polygon tokenai	77,7	Saugumo pažeidimas
28.	Heco Chain bridge	10145 Ethereum 20 tokenai	100,0	Saugumo pažeidimas

Šaltinis: sudarytas autorės, remiantis B. Charoenwong, M. Bernardi (2022), J. Scharfman, (2022), A. Augusto, R. Belchior ir kiti, (2023)

„Bitstamp“ pažeidimas – 2015 m. sausio mėn. buvo įtraukta daugiapakopė ir tikslinė kenkėjiška programa. Jeigu pažeidimo metodai nėra pažangūs, tai reiškia techninis saugumas labai žemas. Ir jei mainų saugumo platforma yra žema, bendrovė negalės atsilikti prieš sudėtingus nacionalinės valstybės veikėjus (K. Oosthoek, & C. Doerr, 2020).

„BTER“ – 7170 pavogtų bitkoinų buvo paimti iš neprisijungusios kriptovaliutų piniginės, vadinamos „šalta pinigine“, kuri negalėjo būti pasiekiama įsilaužėliams, nes ji nebuvo saugoma prie interneto prijungtame serveryje. Spėjama, kad tai galėjo būti asmens, turinčio fizinę prieigą prie biržos serverių, darbas (St. Millward, 2015).

„Gatecoin“ patyrė paslaugos sutrikimą, kurį sukėlė serverio perkrovimas. Tikėtina, kad pažeidimas yra susijęs su kriptovaliutų vagyste. Kenkėjiška išorinė programa sugebėjo pakeisti sistemą taip, kad Bitcoin ir Ethereum indėlių pervedimai aplenkė šaldymo saugyklą ir pažeidimo laikotarpiu pateko tiesiai į įsilaužėlio karštąją piniginę (B. Charoenwong, M Bernardi, 2022).

„Bitfinex“ – 2016 m. įsilaužėliai naudojo kenkėjiškas programas, kad įsiskverbtų į Bitfinex, Honkonge įsikūrusią kriptovaliutų biržą. Pavogtų beveik 120 000 vienetų Bitcoin vertė tuo metu buvo beveik 66 mln. Tai buvo antras didžiausias tokios mainų platformos saugumo pažeidimas istorijoje. Tačiau, pasak ekspertų, pažeidimas nebuvo padarytas pažeidžiant blockchain sistemą (O. Gulyás., & G. Kiss, 2023).

„Yapizon“. Į Pietų Korėjos biržą Yapizon buvo įsilaužta už 5,3 mln. USD, 3816 BTC. Išsiaiškinta, kad buvo pažeistos keturios bendrovės karštosios piniginės, kurių suma apytiksliai siekė 36 procentus visų biržai priklausančių lėšų (B. Charoenwong, M Bernardi, 2022).

„NiceHash“. Nusikaltimas įvyko 2017 m. gruodžio 6 d., kai Slovėnijoje įsikūrusi kriptovaliutų gavybos įmonė „NiceHash“ pranešė, kad jų sistema buvo pažeista per kibernetinę ataką. „NiceHash“ yra žinoma kaip didžiausia Pasaulyje kriptovaliutų gavybos rinka ir buvo sukurta remiantis bendros ekonomikos koncepcija (D. Gregory, 2018).

„Coincheck“. Antrą pagal dydį nuostolį patyrė Coincheckas nuo išorinio įsilaužimo į jos sistemą 2018 m. sausio mėn. Tai buvo rekordinis (530 mln.) kriptovaliutų nuostolis (M. J. Morshed, & P. A. Watters,).

„Bitgrail“. Tai buvo Italijoje sukurta platforma, kuri skyrėsi nuo Bitcoin ir buvo vadinama „Nano“. Buvo įtariama, kad tiek platforma, tiek platformą valdančios korporacijos direktorius

sukčiavo ir pagrobė didžiulį kiekį monetų, kurių vertė 2018 metais buvo apie 170 mln. (R. Mangano, 2020).

„CoinSecure“ buvo įsilaužta į Indijos kriptovaliutų biržą „Coinsecure“, iš kurios buvo pavogta maždaug 438 bitkoinai, kurių vertė tuo metu buvo maždaug 3,3 mln. Iš pradžių birža tvirtino, kad lėšos buvo prarastos dėl techninio gedimo, tačiau vėliau pripažino, kad jos buvo pavogtos. Šis įvykis parodė, kad Indijos kriptovaliutų pramonėje reikia griežtesnių kibernetinio saugumo priemonių (D. Parouha, 2023).

„Bithumb and Coinrail“. Pietų Korėjos kriptovaliutų birža patyrė įsilaužimą ir prarado apie 30 procentų savo monetų atsargų. „Bithumb and Coinrail“ savo tinklalapyje pranešė, kad buvo užpulta ir prarado monetų, kurių vertė buvo apie 40 milijonų JAV dolerių (B. Charoenwong, M Bernardi, 2022). Iš kitos Pietų Korėjos kriptovaliutų biržos „Bithumb“, į kurią buvo įsilaužta, pavogta žetonų už 31,5 mln. USD (B. Charoenwong, M Bernardi, 2022).

„Zaif“ incidentas. 2018 m. rugsėjį buvo įsilaužta į karštą Zaifo piniginę ir prarasta apie 60 mln. USD, kai užpuolikas iš bendrovės „karštų piniginių“ pavogė trijų tipų kriptovaliutas. „Karšta piniginė“ yra terminas, vartojamas apibūdinti kriptovaliutų adresus su lengvomis saugumo priemonėmis, kai kriptovaliutų biržoje laikomos lėšos neatidėliotinoms operacijoms, pvz., kai vienos rūšies kriptovaliutos keičiamos į kitos rūšies kriptovaliutas operacijos ir atvirkščiai. Karštosios piniginės priešingybė yra šalta piniginė, kai užpuolikas turi pereiti per kelias autentifikavimo sistemas, kad gautų prieigą prie lėšų (B. Charoenwong, M Bernardi, 2022).

„QuadrigaCX“ buvo didžiausia Kanados kriptovaliutų birža. Ją įkūrė Geraldas Cottenas dar 2013 m. O dabar pavogta daugiau nei 190 milijonų dolerių investuotojų lėšų. Kaip ir daugelis kitų kriptovaliutų biržų, QuadrigaCX nerimavo, kad nusikaltėliai neįsilaužtų. Siekdama apsaugoti savo platformą ir vartotojų lėšas, ji naudojo šaltą piniginę kriptovaliutų turtui saugoti. Keista yra tai, kad Geraldas Cottenas buvo vienintelis asmuo, kuris galėjo pasiekti QuadrigaCX šaltąją piniginę. Niekas kitas įmonėje neturėjo galios ir atsakomybės tvarkyti įmonės (ir vartotojo) lėšas. Tai tapo problema, nes Cotten mirė 2018 m. gruodžio 9 d., keliaudamas po Indiją. Kadangi niekas kitas negali pasiekti piniginės, visas QuadrigaCX turtas oficialiai dingo (K. Werbach, 2018).

„Coinbene“. Kovo mėnesį kriptovaliutų birža Coinbene per tris dienas patyrė 100 milijonų JAV dolerių nuostolį, kuris, kaip manoma, atsirado dėl atakos. Palyginti su kitais įsilaužimais, CoinBene gali būti vienas paslaptingiausių įsilaužimų. Tokie žetonai kaip Huobipool (HPT), Pundi X (NPSX), Maximine (MXM) ir Udoo (UDOO) buvo prarasti įsilaužimo metu (U. W. Chohan, 2018).

„Binance“. Iš didžiausios pasaulyje biržos „Binance“ buvo pavogta bitkoinų už beveik 40 mln. Bendrovė, kuri, kaip manoma, valdo didžiausią pasaulyje kriptovaliutų biržą pagal prekybos apimtis, pareiškė, kad reaguodama į šį įsilaužimą, stengsis padidinti saugumo priemones, procedūras ir praktiką. Per šį incidentą įsilaužėliai įvairiomis priemonėmis taikėsi į didelę grynąją vertę turinčius klientus (B. Charoenwong, M Bernardi, 2022). Įsilaužėlis pasinaudojo programinės įrangos saugumo spraga, kad pavogtų 40 mln. „Bitcoin“ iš „Binance“ (D. Maroz, 2020).

„Bitrue“ yra kriptovaliutų birža Singapūre, kuri 2019 m. birželį prarado 4,2 mln. USD. Įsilaužėliai aplenkė biržos apsaugos sistemą. Sukčiavimas taip pat yra kriptovaliutų pasaulyje. kiekvienam pradiniam monetų pasiūlymui ICO (angl. Initial Coin Offering) yra bent vienas klonas – svetainė. Du Izraelio broliai buvo suimti po trejus metus trukusios paieškos. Tuo tarpu jiedu pavogė 100 milijonų dolerių vertės kriptovaliutų pritraukdami investuotojus, pavyzdžiui, dideles įmones, imituojant kriptovaliutų biržas (M. C. Șcheau, S. L. Crăciunescu, I. Brici, & M. V. Achim, 2020).

„Upbit“ – viena didžiausių kriptovaliutų biržų Pietų Korėjoje, prarado lėšas po to, kai buvo pažeistas jos saugumas, o įsilaužėliai tuo metu atsiėmė 342 000 ETH arba maždaug 51 mln. USD. Buvo spėliojama, kad įsilaužimas buvo vidinio darbo dalis, nes pavogta kriptovaliuta pateko iš biržos šaltos piniginės (B. Charoenwong, M Bernardi, 2022).

„Cashaa“. Jungtinėje Karalystėje įsikūrusi kriptovaliutų birža 2020 m. liepos 11 d. „Cashaa“, „Peer-to-Peer“ prekybos platforma paskelbė, kad dėl įsilaužėlių atakos buvo prarasti 336 bitkoinai. Įsilaužėliai įdiegė kenkėjišką programą į vieną iš biržos kompiuterių, suteikdami įsilaužėliams galimybę ją pasiekti. Bendrovė rado sistemoje įdiegtą kenkėjiškos programos dalį, kuri leido įsilaužėliams inicijuoti mainų pervedimus, pavyzdžiui, išėmimus (A. ShamsulAbd Aziz, N. Azlina Mohd Noor, O. Farouk, Al Mashhour , 2022).

„KuCoin“. 2020 m. rugsėjį į Singapūre įsikūrusią kriptovaliutų biržą „KuCoin“ buvo įsilaužta ir iš įmonės buvo pavogta kriptovaliutų už 281 mln. USD. Atrodė, kad pagrindinė priežastis buvo saugumo pažeidimas (B. Charoenwong, M Bernardi, 2022). Kibernetiniai nusikaltėliai pavogė kriptovaliutą, esančią biržos centralizuotoje piniginėje. Šis pažeidimas išnaudojo centralizuotų mainų saugumo trūkumą (C. A. Makridis, M. Fröwis, K. Sridhar, & R. Böhme, 2023).

„EXMO“. Jungtinėje Karalystėje įsikūrusi kriptovaliutų birža EXMO 2020 m. gruodį aptiko įtartiną pinigų išėmimo veiklą ir sustabdė išėmimus iškart po incidento. Audito ataskaita, gauta iš įsilaužimo, atskleidė „didelius išėmimus“. Skaičiuojama, kad nuostoliai galėjo siekti 10 mln. USD, beveik 5% viso turto (B. Charoenwong, M Bernardi, 2022).

„Africrypt“. Didžiausia kriptovaliutų birža Afrikoje pranešė, kad 2021 m. birželį kriptografinėje erdvėje buvo įvykdyta keletas didelio masto vagysčių, kurių metu buvo pavogtas turtas. Daugelį šių investuotojų nuostolių lydėjo faktinis arba tariamas įmonės steigėjų, dalyvaujančių kriptovaliutų įmonės steigime ir valdyme, dingimas. Tokios situacijos vadinamos pasitraukimo sukčiavimu, nes pagrindinis asmuo arba asmenų grupė, kuriai yra svarbiausias projektas, paprasčiausiai išeina iš projektų ir palieka investuotojus nelaimėje (J. Scharfman, 2022).

„Poly Network“. Decentralizuoti finansai 2021 m. rugpjūtį patyrė didžiausią kada nors užfiksuotą įsilaužimą, nes iš kryžminės grandinės „Poly Network“ buvo išeikvota maždaug kriptovaliutų už 600 mln. USD. Šis incidentas parodo, kokios yra besikuriančios kriptovaliutų kryžminės grandinės platformos ir kaip jos yra pažeidžiamos įvairių atakų vektorių. Įdomu tai, kad išbandymas baigėsi gana teigiamai, nes įsilaužėlis grąžino visas pavogtas lėšas „Poly Network“ (B. Charoenwong, M Bernardi, 2022).

„Liquid“ – viena iš labiausiai žinomų Japonijos biržų visame pasaulyje, taip pat patyrė įsilaužimą. Buvo pasisavinta 1941 Bitcoin ir Ethereum kriptovaliutų už daugiau nei 91 mln. USD. Pagrindinė „Liquid“ operacijų ir technologijų komanda sužinojo apie neteisėtą prieigą prie kai kurių savo „karštų“ piniginių ir netrukus perkėlė turtą, kuris nebuvo paveiktas (B. Charoenwong, M Bernardi, 2022).

„Cream Finance“. 2021 m. spalį buvo pranešta, kad buvo įsilaužta į „Cream Finance“ platformą. Įsilaužėliai sugebėjo išnaudoti „Cream Finance“ platformos greitųjų paskolų sistemą, kad pavogtų visus platformos „Ethereum“ pagrindu veikiančius žetonus už 130 mln.. Įsilaužėlis naudojo greitas paskolas, kurios iš esmės buvo būdas, leidžiantis vartotojams pasiskolinti pinigų iš skolinimo platformos nededant užstatų ir grąžinant pasiskolintą sumą to paties sandorio metu (J. Scharfman, 2023).

„Boy x Highspeed“ (BXH). BXH įsilaužimas įvyko, nes užpuolikas pasiekė administratoriaus privatų raktą per sukčiavimo ataką. Tokie įsilaužimai verčia pagalvoti, kaip pagerinti raktų valdymų strategijas, pavyzdžiui, naudojant aparatinės įrangos pinigines. Kiti švelninimo būdai yra tikrintuvų skaičiaus ir slenksčių padidėjimas kelių parašų piniginėse ir decentralizavimas, kai vienas subjektas neturėtų turėti prieigos prie kelių kriptografinių raktų. Be to, raktai gali būti apsaugoti naudojant papildomas autentifikavimo procedūras – simetrinius raktus arba slaptažodžius (A. Augusto, R. Belchior ir kiti, 2023).

„BadgerDAO“ yra decentralizuota autonominė organizacija, orientuota į Bitcoin įtraukimą į DeFi. 2021 m. spalį buvo pranešta, kad į BadgerDAO buvo įsilaužta ir pavogta Bitcoin ir Ethereum

kriptovaliutų už 120 mln. Įsilaužimo analizė parodė, kad įsilaužėliai galėjo įterpti kenkėjišką kodą į Badger svetainės vartotojo sąsajos dalį. Suaktyvinus kenkėjiškus scenarijus, jis perimtų operacijas ir tuo pat metu inicijuotų prašymą perkelti žetonus į nusikaltėlio piniginę (J. Scharfman, 2022).

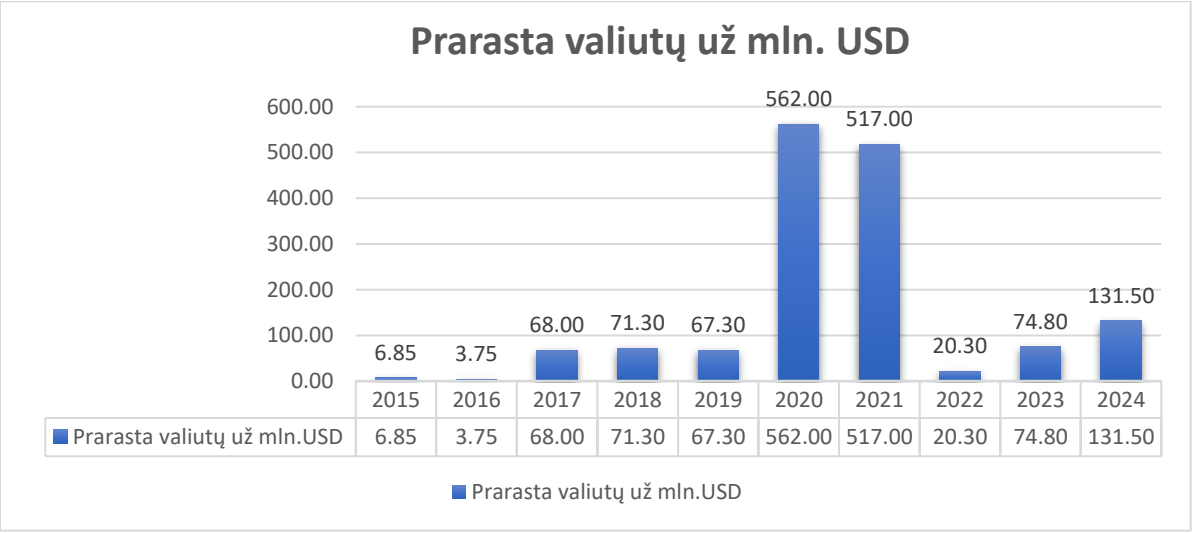
„Bitmart“. Dažniausiai pažeidimas vyksta per privačių raktų įsiskverbimą į mainų „karštąją piniginę“. 2021 m. gruodžio mėn., viena iš patikimiausių prekybos platformų, „Bitmart“ patyrė didelio masto saugumo pažeidimą. Pavogtas privatumo raktas, naudojamas norint pasiekti „Bitmart“ karštąją piniginę, todėl buvo atimta maždaug 150 mln. USD vertės žetonų (A. Aspris, A.H. Dyhrberg ir kiti, 2022).

„Ascendex“. 2021 m. gruodžio mėn. buvo pranešta, kad į Singapūre įsikūrusią kriptovaliutų biržą „Ascendex“ buvo įsilaužta iš „karštų piniginių“ (angl. hot wallets) ir atlikta daugybė neteisėtų operacijų už 77 mln. Analizė parodė, kad įsilaužimas išplito per tris skirtingas grandines. Tiksliau, „Ethereum“ už 60 mln. USD, „Binance Smart Chain“ už 9,2 mln. USD ir „Polygon“ už 8,5 mln. Nors įsilaužimas buvo susijęs su įvairiomis virtualiomis valiutomis, didžiausia įsilaužimo dalis buvo altkoinas, pavadintas Taraxa (TARA), kurio vertė 10,8 mln. (J. Scharfman, 2023).

„Heco Chain bridge“ 2023 m. rugsėjo kriptovaliutų pramonė patyrė beveik 1 mlrd. dolerių nuostolių dėl įsilaužimų, spragų ir sukčiavimų. Šie įsilaužimai apėmė daugiau nei 100 mln. dolerių skaitmeninio turto nuostolių, o vien dėl įsilaužimo į Heco Chain bridge buvo pavogta daugiau nei 80 mln. dolerių (J. McKay, 2023).

8 paveikslas

Kriptoturto praradimai USD 2015-2023 metais



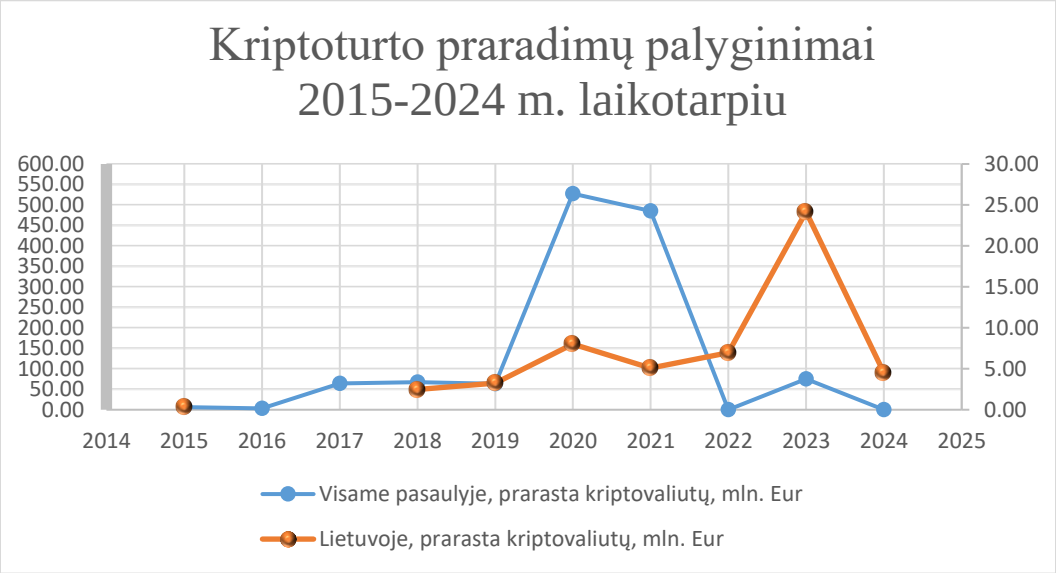
Šaltinis: sudaryta autorės, remiantis 3 lentelės duomenimis

Apibendrinant pagal 3 pav. pateiktus duomenis galima pastebėti, kad per minėtą 2015-2023 m. laikotarpį buvo prarasta kriptovaliutų už įspūdingas sumas. 2020 m. jos siekė net 562 mln. USD. Tokios didelės kriptovaliutų vagystės įvyko todėl, kad buvo nesilaikoma saugumo reikalavimų dėl žmogaus padarytų klaidų ar dėl apsaugos pažeidimų. Todėl ir įvyko tokios stambios kriptovaliutų vagystės per minėtą laikotarpį. Visos šios vagystės skaudžiai atsiliepė dabartinei kriptoturto rinkai. Po šių vagysčių dalyviai gali įsivertinti ir stengtis, kad toks įvykis daugiau nepasikartotų arba pasekmės būtų kuo įmanoma švelnesnės.

3.4. Kriptoturto praradimų palygimas

Atlikus kriptoturto praradimų analizę, galima palyginti gautus rezultatus. Per tyrimo laikotarpį buvo prarasta įvairių kriptovaliutų: nuo žymiausių Bitcoin, Ethereum, Ripple ar Bitcoin Cash iki tokių kaip Zec, Ada, Hpt, Npx, Mxm ar Udoo. Pagrindinės priežastys, dėl kurių vyko kriptovaliutų praradimai – tai įsilaužimai naudojant kenkėjiškas programas ar įvykus techniniams gedimams. 7 pav. pateikiamas palyginimas Lietuvoje prarastų kriptovaliutų ir visame Pasaulyje.

9 paveikslas
Kriptoturto praradimų palyginimai 2015-2024 metais



Šaltinis: sudaryta autorės

Apibendrinant III skyrių pastebima, kad pažeidimai atsiranda dėl šių priežasčių: nuo elektroninės erdvės priklausomi nusikaltimai negali būti įvykdyti be informacinių technologijų ir tam tikro lygio žinių apie jų pritaikymą elektroninėje erdvėje. Ši elektroninių nusikaltimų kategorija apima atakas svetainėse – įsilaužimą, kenkėjiškas kompiuterių programas. „Žmogaus klaidos“ (angl. „Human Error“ Hack) įsilaužimas – tokio tipo „nulaužimas“ paprastai apima išpirkos el. laiškus arba kenkėjiškas programas. Išpirkos reikalaujančios programos yra vienas iš elektroninių nusikaltimų būdų, kai užpuolikai, t. y. įsilaužėliai į vartotojo kompiuterį įterpia kenkėjišką kompiuterinę programą, siekdami šifruoti failus. Saugumo pažeidimas (angl. Security Breach) – šis įsilaužimas įvyksta dažniausiai, daugiausia dėl to, kad įsilaužėliai gali rasti spragą saugos sistemoje. Ponzi schema yra sukčiavimo rūšis, kai investuotojams žadamos didelės grąžos su maža rizika arba jos visai nėra. Sukčiavimas pagal žetonus – ši technologija suteikia galimybę palyginti greitai, pigiai ir lengvai gauti lėšų verslumo projektams ar pradiniams monetų pasiūlymams. Agentūros problema (angl. Agency Problem) – paskutinis įsilaužimo tipas įvyksta ne dėl aplaidumo ar prastesnių saugumo priemonių, o dėl vidinio darbo apsaugos nesilaikymo. O dėl to investuotojai ir įstaigos patiria didelių nuostolių. Siekdami apsisaugoti, stengiasi kaip įmanoma naujinti apsaugos sistemas ar diegti naujas, kurios užtikrintų saugumą.

IŠVADOS

1. Kriptoturtas yra skaitmeninis turtas, kuris neturi fizinės formos, neatitinka nei finansinės priemonės, nei grynųjų pinigų sąvokos, todėl kriptoturtą labai sunku apskaityti. Kriptoturtą galima iškeisti į prekes arba paslaugas. Jis yra mainų priemonė, kuria elektroninėje erdvėje naudojasi ne tik juridiniai, bet ir fiziniai asmenys. Kriptoturto sąvoka vartojama kriptovaliutoms ir kriptovaliutų žetonams apibūdinti, kadangi tai yra virtuali valiuta. Kriptoturtas gali turėti naudos finansų sektoriui, nes teisingai investavus įmonė gali gauti pelną.

2. Nuo 2025 m. pradėsiantis veikti reglamentas atneš daugiau aiškumo ir skaidrumo finansų rinkos dalyviams, kaip reikėtų elgtis su kriptoturtu. Naujasis teisės aktas reglamentuos tris kriptoturto rūšis: su turtu susieti žetonai, kuriais galima atsiskaityti už prekes ir paslaugas, stabilus kriptoturtas, e. pinigų žetonai (elektroninių pinigų žetonai), kurie turi stabilią vertę ir pirmumo teisė teikiama kaip mokėjimo priemonei. Paskutinė kriptoturto rūšis – kitas kriptoturtas pvz.: produkto žetonai. Jais galima atsiskaityti už prekes ir paslaugas.

3. Kriptoturtas gali būti naudojamas: kaip mokėjimo/mainų priemonė (vadinamoji kriptovaliuta). Taip pat skaitmeninė valiuta, kurią galima atlikti per internetinius mokėjimus, investavimo tikslais (pvz., suteikiamos nuosavybės teisės); neužtikrintas kriptografinis turtas, prekėms ar paslaugoms įsigyti (panašiai kaip kuponai, dar vadinami produkto žetonais), arba kaip visų išvardytų priemonių derinys. Šiuolaikiniame pasaulyje viskas nuolat keičiasi, tai visko gali būti, kad kriptoturto panaudojimas greitu laiku bus ne tik šios keturios esamos galimybės. Kriptoturtą galima klasifikuoti į pinigus, atsargas, nematerialųjį turtą ir finansinį turtą. Gairių, metodinių rekomendacijų dėka, jį galima teisingai apskaityti. Tačiau tvarkant apskaitą, atsiranda ir daug neaiškumų, kaip teisingai tai padaryti.

4. Kriptoturto manipuliacijų rinkoje praradimų priežastys yra šios: nuo elektroninės erdvės priklausomi nusikaltimai, „žmogaus klaidos“ (angl. „Human Error“ Hack), saugumo pažeidimas (angl. Security Breach), Ponzi schema, sukčiavimas pagal žetonus, agentūros problema (angl. Agency Problem). Paskutinis įsilaužimo tipas įvyksta ne dėl aplaidumo ar prastesnių saugumo priemonių, o dėl vidinio darbo apsaugos nesilaikymo. Šioms priežastims suvaldyti nuolat vyksta sistemų naujinimai, kad būtų išvengta kriptoturto praradimų.

REKOMENDACIJOS

Kriptoturtas užima vis didesnę finansų rinkos dalį. Didesnis susidomėjimas ir prekyba kriptoturtu verčia visus finansų rinkos dalyvius labiau domėtis, kaip tinkamai apskaityti kriptoturtą, kokie reikalavimai tam keliami. Šiuo metu yra mažai informacijos, kaip tinkamai tvarkyti apskaitą. Be to, nuomonių yra labai įvairių ir sunku suprasti, kuri yra teisinga. Rekomenduojama turėti daugiau gairių šiai naujai platformai apskaityti. Taip pat seminarų, mokymų, kurių metu galima būtų diskutuoti ir prieiti prie vieningos nuomonės. Atsiradus literatūrai, kuri padės vesti apskaitą, įstaigų finansų specialistai galės lengviau atsikvėpti, nes patvirtintos tvarkos nepaliks vietos interpretacijai, o pradėjus galioti naujajam reglamentui, vyriausybė bus įpareigota teikti įvairiapusę pagalbą, kad įstaigos galėtų susitvarkyti savo kriptoturto apskaitą pagal galiojančius teisės aktus ar patvirtintas gaires.

Kriptovaliutų praradimai gali turėti įvairių pasekmių, pavyzdžiui finansinių, nes po kriptovaliutos praradimo ji gali pabrangti arba prarasti pasitikėjimą, nes po kriptovaliutos praradimo kurį laiką gali būti sunku pasitikėti rinkomis. Arba galima psichologinė pasekmė, nes praradus didelę sumą pinigų, galima patirti stresą. Kad taip neatsitiktų, kriptovaliutų biržos stengiasi užtikrinti saugumą, ypač tada, kai ta kriptovaliutų birža buvo praradusi didelį kiekį kriptovaliutų. Būtų naudinga apsaugos priemones testuoti ne rečiau kaip kas pusmetį, nes kriptovaliutų birža gali apsaugoti save ir investuotojus nuo milžiniškų nuostolių.

LITERATŪROS SĄRAŠAS

Abd Aziz, A. S., Noor, N. A. M., & Al Mashhour, O. F. (2022). *The money of the future: A study of the legal challenges facing cryptocurrencies. BiLD Law Journal, 7(1s), 21-33.* 34743_33f7d302d3a2433c31fb62bb9acdfb20.pdf (lb.lt)

Armstrong, C. (2021). *Key methods used in qualitative document analysis. OSF Preprints, 1-9.*

Aspris, A., Dyhrberg, A. H., Putniņš, T. J., & Foley, S. (2022). *Digital Assets and Markets: A Transaction-Cost analysis of market architectures.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4301258

Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., & Hardjono, T. (2023). Sok: *Security and privacy of blockchain interoperability. Authorea Preprints.* https://www.techrxiv.org/doi/full/10.36227/techrxiv.24595764.v1

Bondarenko, O., Kichuk, O., & Antonov, A. (2019). *The possibilities of using investment tools based on cryptocurrency in the development of the national economy. Baltic Journal of Economic Studies, 5(2), 10-17.* View of THE POSSIBILITIES OF USING INVESTMENT TOOLS BASED ON CRYPTOCURRENCY IN THE DEVELOPMENT OF THE NATIONAL ECONOMY (baltijapublishing.lv)

Bullmann, D., Klemm, J., & Pinna, A. (2019). *In search for stability in crypto-assets: are stablecoins the solution?. Available at SSRN 3444847.* In Search for Stability in Crypto-Assets: Are Stablecoins the Solution? by Dirk Bullmann, Jonas Klemm, Andrea Pinna :: SSRN

Cao, Y., Li, Y., Coleman, S., Belatreche, A., & McGinnity, T. M. (2015). *Detecting wash trade in financial market using digraphs and dynamic programming. IEEE transactions on neural networks and learning systems, 27(11), 2351-2363.* https://ieeexplore.ieee.org/abstract/document/7298451/

Castro, J. G., Tito, E. A. H., Brandão, L. E. T., & Gomes, L. L. (2020). Crypto-assets portfolio optimization under the omega measure. The Engineering Economist, 65(2), 114-134.Crypto-assets portfolio optimization under the omega measure (tandfonline.com)

Cardno, C. (2018). *Policy Document Analysis: A practical educational leadership tool and a qualitative research method. Educational Administration: Theory & Practice, 24(4), 623-640.* https://eric.ed.gov/?id=EJ1305631

Chohan, U. W. (2018). *The problems of cryptocurrency thefts and exchange shutdowns. Available at SSRN 3131702.* https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3131702

Ciesielska, M., Boström, K. W., & Öhlander, M. (2018*). Observation methods. Qualitative methodologies in organization studies: Volume II: Methods and possibilities, 33-52.* https://link.springer.com/chapter/10.1007/978-3-319-65442-3_2

Cong, L. W., Li, X., Tang, K., & Yang, Y. (2023). *Crypto Wash Trading-Online Appendices. Available at SSRN 4529817.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4529817

Cunjak, I. (2022). *Crypto-Assets Illicit Activities: Theoretical Approach with Empirical Review. International E-Journal of Criminal Sciences, (17).* https://ojs.ehu.eus/index.php/inecs/article/view/23830

Cunjak, I. (2022). *Crypto-Assets Illicit Activities: Theoretical Approach with Empirical Review. International E-Journal of Criminal Sciences, (17).* https://ojs.ehu.eus/index.php/inecs/article/view/23830

Demertzis, M., & Wolff, G. B. (2018). *The economic potential and risks of crypto assets: is a regulatory framework needed? (No. 2018/14). Bruegel Policy Contribution*. The economic potential and risks of crypto assets: Is a regulatory framework needed? (econstor.eu)

Di Angelo, M., & Salzer, G. (2020, August). *Tokens, types, and standards: identification and utilization in Ethereum. In 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) (pp. 1-10). IEEE.* IEEE Xplore Full-Text PDF:

Eigelshoven, F., Ullrich, A., & Parry, D. (2021, December). Cryptocurrency Market Manipulation-A Systematic Literature Review. In ICIS.

Europos vadovų taryba (2023). Europos Sąjungos taryba. *Infografikas. Kriptoturtas.* Kriptoturtas - Consilium (europa.eu)

Europos parlamento ir tarybos dėl kriptoturto rinkų, kuriuo iš dalies keičiama Direktyva (ES) 2019/1937.

Europos Vadovų taryba (2023). *Europos Sąjungos taryba. Infografikas. Kriptoturtas.* eurlex.europa.eu/legalcontent/LT/TXT/HTML/?uri=CELEX:52020PC0593&from=EN Kriptoturtas - Consilium (europa.eu)

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, 43, 105632*. Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure - ScienceDirect

Finansų ministerija (2023). *Kripto paslaugų teikėjų laukia reguliavimo pokyčiai.* Finansų ministerija: Kripto paslaugų teikėjų laukia reguliavimo pokyčiai - Lietuvos Respublikos finansų ministerija (lrv.lt)

Fröhlich, M., Gutjahr, F., & Alt, F. (2020, July*). Don't lose your coin! Investigating Security Practices of Cryptocurrency Users. In Proceedings of the 2020 ACM Designing Interactive Systems Conference (pp. 1751-1763)*. https://dl.acm.org/doi/abs/10.1145/3357236.3395535

Gregory, D. (2018). *Cryptocurrency and its forensic significance (Doctoral dissertation, Murdoch University).* https://researchportal.murdoch.edu.au/esploro/outputs/graduate/Cryptocurrency-and-its-forensic-significance/991005541378807891

Gulyás, O., & Kiss, G. (2023). *Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, 84-90.* https://www.sciencedirect.com/science/article/pii/S1877050923002752

Hamledari, H., & Fischer, M. (2021). *The application of blockchain-based crypto assets for integrating the physical and financial supply chains in the construction & engineering industry. Automation in construction, 127, 103711.*The application of blockchain-based crypto assets for integrating the physical and financial supply chains in the construction & engineering industry (sciencedirectassets.com)

Houben, R., & Snyers, A. (2020). Crypto-assets: Key developments, regulatory concerns and responses. Crypto-assets - Key developments, regulatory concerns and responses (uantwerpen.be)

Howell, S. T., Niessner, M., & Yermack, D. (2020). *Initial coin offerings: Financing growth with cryptocurrency token sales. The Review of Financial Studies, 33(9), 3925-3974.*Initial Coin Offerings (jstor.org)

Idkinaitė, S., & Grumulaitis, A. (2023). *Kripto turto apmokestinimas Lietuvoje ir užsienyje: vertinimai, siūlymai tobulinimui. Teisės mokslo pavasaris 2022, 40-58.* https://www.zurnalai.vu.lt/open-series/article/download/31637/30501/73958

Inga Česnienė (2022). *Apskaita kriptoturto įmonėse – kompleksinis ir žinių reikalaujantis procesas.* Apskaita kriptoturto įmonėse – kompleksinis ir žinių reikalaujantis procesas - Verslo žinios (vz.lt)

Irwin, A. S., & Turner, A. B. (2018). *Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. Journal of money laundering control, 21(3), 297-313.* https://www.emerald.com/insight/content/doi/10.1108/JMLC-07-2017-0031/full/html

Yadava, A. K. (2018). *Prevalence of Crypto-currencies: A Critical Review of Their Functioning and Impact on Indian Economy. International Journal of Research in Economics and Social Sciences (IJRESS), 8(1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431718*

Kaaniche, N., & Laurent, M. (2017). *Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Computer Communications, 111, 120-141.* https://www.sciencedirect.com/science/article/pii/S014036641730796X

Kreiner, K., & Mouritsen, J. (2006). *The analytical interview, relevance beyond reflexivity. Teoksessa: The Art of Science, toim. Tengblad–Solli–Charnlawska 153–176. Liber.* Art_of_Science2f.indd (researchgate.net)

Kurauskienė, N., & Subačienė, R. (2020). *Evaluation of alternatives of cryptocurrency accounting. Buhalterinės apskaitos teorija ir praktika, (22).* Kriptovaliutos apskaitos alternatyvų vertinimas (redalyc.org)

Laucius, G. (2023). *Naujasis kriptoturto veiklos reglamentavimas Lietuvoje ir Europos Sąjungoje. Teisė, 128, 115-132.* Kriptovaliutų įtaka ES teisėkūrai | Naujienos | Europos Parlamentas (europa.eu)

Li, T., Shin, D., & Wang, B. (2021). *Cryptocurrency pump-and-dump schemes. Available at SSRN 3267041.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3267041

Lietuvos banko pozicija (2022) *Kriptoturto ir pirminio kriptoturto žetonų platinimas.* https://www.lb.lt/lt/naujienos/lietuvos-banko-valdybos-nutarimai-pozicija-del-virtualiojo-turto

Lietuvos bankų Finansų rinkos priežiūros komiteto sprendimai. *https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi_2tqYkO2FAxWxg_0HHRDmDK0QFnoECBIQAQ&url=https%3A%2F%2Fwww.lb.lt%2Flt%2Fnaujienos%2Flietuvos-banko-finansu-rinkos-prieziuros-komiteto-sprendimai-52&usg=AOvVaw0QnOhyqpQnIwM91f1jPkIv&opi=89978449*

Lietuvos Respublikos vidaus reikalų ministerija (2023). *Vyriausybė griežtina pinigų plovimo prevenciją ir kriptoturto paslaugų teikėjų priežiūrą.* Vyriausybė griežtina pinigų plovimo prevenciją ir kriptoturto paslaugų teikėjų priežiūrą - Lietuvos Respublikos vidaus reikalų ministerija (lrv.lt)

Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas. 1997 m. birželio 19 d. Nr. VIII-275. Suvestinė redakcija nuo 2022-11-10 iki 2023-12-31. VIII-275 Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas (lrs.lt)

Lietuvos respublikos Finansų ministerija (2022). *Kriptoturto sektoriaus veiklos skaidrumą didinantys įstatymo pakeitimai.*

Patvirtini kriptoturto sektoriaus veiklos skaidrumą didinantys įstatymo pakeitimai | Lietuvos Respublikos finansų ministerija (lrv.lt)

Luther, W. J., & White, L. H. (2014). *Can Bitcoin become a major currency?* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446604

Makridis, C. A., Fröwis, M., Sridhar, K., & Böhme, R. (2023). *The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. Journal of Corporate Finance, 79, 102358.* https://www.sciencedirect.com/science/article/pii/S092911992300007X

Mangano, R. (2020). *Cryptocurrencies, cybersecurity and bankruptcy law: how global issues are globalizing national remedies. University of Miami International and Comparative Law Review, 27(2), 355.* https://repository.law.miami.edu/umiclr/vol27/iss2/8/

McKay, J. (2022). *DeFi-ing cyber attacks.* https://tellingstorieswithdata.com/inputs/pdfs/final_paper-2022-jack_mckay.pdf

Millward S. Nearly $2M in bitcoins feared lost after Chinese cryptocurrency exchange hack. https://www.techinasia.com/bitcoins-lost-after-china-cryptocurrency-exchange-hack-bter

Moroz, D. J., Aronoff, D. J., Narula, N., & Parkes, D. C. (2020). *Double-spend counterattacks: Threat of retaliation in proof-of-work systems. arXiv preprint arXiv:2002.10736.* https://arxiv.org/abs/2002.10736

Morozova, T., Akhmadeev, R., Lehoux, L., Yumashev, A., Meshkova, G., & Lukiyanova, M. *Crypto asset assessment models in financial reporting content typologies (2020) Entrepreneurship and Sustainability Issues, 7 (3). doi, 10, 2196-2212.*The Concept of Infamy In Roman Law (jssidoi.org)

Morshed, M. J., & Watters, P. A. *An Empirical Analysis of Blockchain Cybersecurity Incidents.* https://www.researchgate.net/profile/Alex-Ng-11/publication/337647279_An_Empirical_Analysis_of_Blockchain_Cybersecurity_Incidents/links/5e087691a6fdcc2837460279/An-Empirical-Analysis-of-Blockchain-Cybersecurity-Incidents.pdf

Oosthoek, K., & Doerr, C. (2020). *Cyber security threats to Bitcoin exchanges: Adversary exploitation and laundering techniques. IEEE Transactions on Network and Service Management, 18(2), 1616-1628.* https://ieeexplore.ieee.org/abstract/document/9300238

Parma Bains, A. I., Melo, F., & Sugimoto, N. (2022*). Regulating the Crypto Ecosystem*. Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets in: FinTech Notes Volume 2022 Issue 007 (2022) (imf.org)

Parouha, D. (2023). Law, *Technology and Cryptocurrency. Indian J. Integrated Rsch. L., 3, 1.* https://eric.ed.gov/?id=EJ1305631

Pelagidis, T., & Kostika, E. (2022). *Investigating the role of central banks in the interconnection between financial markets and cryptoassets. Journal of Industrial and Business Economics, 49(3), 481-507.* https://link.springer.com/article/10.1007/s40812-022-00227-z

Pramana, I. G. G. A., Mayangsari, S., & Oktris, L. (2023). *Accounting Analysis for Crypto-Assets Based on IFRS. Jurnal Magister Akuntansi Trisakti, 10(1), 19-44.* ACCOUNTING ANALYSIS FOR CRYPTO-ASSETS BASED ON IFRS | Jurnal Magister Akuntansi Trisakti

Read, O., & Diefenbach, C. (2022). The Path to the EU Regulation Markets in Crypto-assets (MiCA) (No. 13/2022). wifin Working Paper. The Path to the EU Regulation Markets in Crypto-assets (MiCA) (econstor.eu)

Roopa, S., & Rani, M. S. (2012). *Questionnaire designing for a survey. Journal of Indian Orthodontic Society, 46(4_suppl1), 273-277.* https://journals.sagepub.com/doi/pdf/10.5005/jp-journals-10021-1104

Scharfman, J. (2023). *Cryptocurrency Exchange Fraud and Hacks. In The Cryptocurrency and Digital Asset Fraud Casebook (pp. 17-33). Cham: Springer International Publishing.* https://link.springer.com/chapter/10.1007/978-3-031-23679-2_2

Scharfman, J. (2023). *Decentralized finance (defi) fraud and hacks: Part 2. In The Cryptocurrency and Digital Asset Fraud Casebook (pp. 97-110). Cham: Springer International Publishing.* https://link.springer.com/chapter/10.1007/978-3-031-23679-2_7

Scharfman, J. (2023). *Introduction to cryptocurrency and digital asset fraud and crime. In The Cryptocurrency and Digital Asset Fraud Casebook (pp. 1-16). Cham: Springer International Publishing.* https://link.springer.com/chapter/10.1007/978-3-031-23679-2_1

Scharfman, J., & Scharfman, J. (2022*). Cryptocurrency regulatory framework and regulatory reporting. Cryptocurrency Compliance and Operations: Digital Assets, Blockchain and DeFi, 115-135.* https://link.springer.com/chapter/10.1007/978-3-030-88000-2_6

Șcheau, M. C., Crăciunescu, S. L., Brici, I., & Achim, M. V. (2020). *A cryptocurrency spectrum short analysis. Journal of Risk and Financial Management, 13(8), 184.* https://www.mdpi.com/1911-8074/13/8/184

Skinner, B. F. (1966). What is the experimental analysis of behavior?. Journal of the Experimental Analysis of behavior, 9(3), 213. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1338181/pdf/jeabehav00169-0039.pdf

Söderberg, G. (2018). *Are Bitcoin and other crypto-assets money. Economic Commentaries, 5, 14.* Are Bitcoin and other crypto-assets money? (riksbank.se)

Start a company in Europe Accounting & Consulting (2023). *Mica reglamentas dėl kriptovaliutų rinkų.* MiCA reglamentas dėl kriptovaliutų rinkų (eestifirma.ee)

Subačienė, R., & Kurauskienė, N. (2020). *Kriptovaliutos apskaitos alternatyvų vertinimas. Buhalterinės apskaitos teorija ir praktika, 22, 1-12.*Lituanistika | Kriptovaliutos apskaitos alternatyvų vertinimas / Natalija Kurauskienė, Rasa Subačienė

Sundqvist, E., & Hyytiä, P. (2019). *Accounting for Cryptocurrencies-A Nightmare for Accountants*. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1331799&dswid=-2501

Sucu, Ö. E. (2022). Crypto-Assets: Classification Problem For An Emerging Asset Class. Digitalization In Business And Economy (Blockchain, Cryptocurrencies, Industry 4.0, Digital Transformation),107.researchgate.net/profile/Ozan-Goenuellue/publication/364356068_DIGITALIZATION_IN_BUSINESS_AND_ECONOMY_Blockchain_Cryptocurrencies_Industry_40_Digital_Transformation/links/634f0d4a6e0d367d91a88788/DIGITALIZATION-IN-BUSINESS-AND-ECONOMY-Blockchain-Cryptocurrencies-Industry-40-Digital-Transformation.pdf#page=115

Trimborn, S., Li, M., & Härdle, W. K. (2020*). Investing with cryptocurrencies—A liquidity constrained investment approach. Journal of Financial Econometrics, 18(2), 280-306.* Investing with Cryptocurrencies—a Liquidity Constrained Investment Approach* | Journal of Financial Econometrics | Oxford Academic (oup.com)

Verstein, A. (2019). *Crypto Assets and Insider Trading Law's Domain. Iowa L. Rev., 105, 1.*Law Journal Library - HeinOnline.org

Weng, S. S., & Chang, H. L. (2008). *Using ontology network analysis for research document recommendation. Expert Systems with Applications, 34(3), 1857-1869.* https://www.sciencedirect.com/science/article/pii/S0957417407000620?ref=pdf_download&fr=RR-2&rr=87d215dd698bbc0f

Werbach, K. (2018). *Trust, but verify: Why the blockchain needs the law. Berkeley Technology Law Journal, 33(2), 487-550.* https://www.coincola.com/blog/what-happened-to-quadrigacx-how-to-avoid-it/

Wong, K. Y., Casey, R. G., & Wahl, F. M. (1982). *Document analysis system. IBM journal of research and development, 26(6), 647-656.* https://ieeexplore.ieee.org/abstract/document/5390486/

SANTRAUKA

Šiame bakalauriniame darbe analizuotas kriptoturtas, jo galimybės, naujasis Mica reglamentas, manipuliacijų kriptoturto rinkoje pasekmės ir priežastys. Pirmoje darbo dalyje pristatoma kriptoturto sąvoka, kurią savo moksliniuose straipsniuose naudoja mokslininkai, siekdami kuo tiksliau ją apibūdinti ir pristatyti. Taip pat aptariama, kaip kriptoturtas traktuojamas teisiniu požiūriu. Pateikiami apibrėžimai, kad galima būtų aiškiau suprasti jo sąvoką. Pateikiamos kriptoturto rūšys, kurias nuo 2024 m. gruodžio 30 d. pradės kontroliuoti naujas Mica reglamentas. Pristatomos ir aprašomos rūšys, kurioms bus skiriamas didesnis dėmesys, nes iki šiol kiekviena šalis kriptoturto turinčias įstaigas kontroliavo taip, kaip kiekvienai atrodė teisingai. Baigiamajame darbe pristatomos kriptoturto naudojimo galimybės, kaip panaudojant vieną ar kitą būdą galima būtų atsiskaityti už prekes ar paslaugas, galbūt atlikti mainus ar investuoti. Aprašoma kriptoturto apskaita. Kadangi kriptoturtas palyginti nauja veiklos sritis, todėl daug įstaigų susiduria su sunkumais, kaip teisingai vesti kriptoturto apskaitą. Pristatoma, kokiu turto klasifikavimo modeliu turėtų vadovautis įstaigos, tvarkydamos kriptoturto apskaitą. Analizuojami ir tarptautinės finansinės ir verslo apskaitos standartai. Antroje dalyje aprašomi tyrimo metodai. Pasirenkamas ir aprašomas metodas, kurio pagalba su analizuojami duomenys. Trečioje dalyje analizuojamos priežastys, dėl kurių atsiradimo buvo prarasta nemažai kriptoturto įvairiomis kriptovaliutomis tiek Lietuvoje, tiek visame Pasaulyje. Darbo rezultatai rodo, jog didžiausias dėmesys, kuris yra skiriamas kriptoturtui apsaugoti, yra visiškai pagrįstas, nes peržvelgus kriptoturto praradimų istoriją, galima suskaičiuoti milijardus prarastų įvairių kriptovaliutų.

SUMMARY

This bachelor's thesis analyzes crypto-assets, its possibilities, the new Mica regulation, the consequences and causes of manipulation in the cryptocurrency market. The first part of the work introduces the concept of crypto assets, which is used by researchers in their scientific articles to describe and present it as accurately as possible. It also discusses how crypto - assets are treated from a legal perspective. Definitions are provided to clarify the understanding of the concept. The types of crypto - assets, that will be regulated by the new Mica regulation from 30 December 2024. The types that will receive more attention are introduced and described, as until now each country has controlled crypto-asset institutions as they saw fit. The thesis presents the possibilities of using crypto-assets, how one or the other method can be used to pay for goods or services, perhaps exchange or invest. Crypto asset accounting is described. Since crypto-assets are a relatively new field of activity, many institutions face difficulties in how to correctly keep records of crypto-assets. It is presented which asset classification model institutions should follow when managing crypto-asset accounting. International financial and business accounting standards are also analyzed. The second part describes the research methods. The method used to analyze the data is selected and described. The third part analyzes the reasons that led to the loss of a significant amount of crypto assets in various cryptocurrencies both in Lithuania and around the world. The results of the work show that the greatest attention that is paid to the protection of crypto-assets is completely justified, because after reviewing the history of losses of crypto-assets, it is possible to count billions of lost various cryptocurrencies.