

MYKOLO ROMERIO UNIVERSITETO
TEISĖS FAKULTETO
TARPTAUTINĖS IR EUROPOS SĄJUNGOS TEISĖS INSTITUTAS

OLIVIJA KAZIMIERA SINKEVIČIŪTĖ
TARPTAUTINĖS TEISĖS STUDIJŲ PROGRAMA

VIRTUALIOS VALIUTOS IR PINIGŲ PLOVIMO PREVENCIJA TARPTAUTINĖS TEISĖS
POŽIŪRIU

Magistro baigiamasis darbas

Darbo vadovas –
Prof. dr. Justinas Žilinskas

Vilnius, 2022

SANTRUMPŲ SĄRAŠAS.....	3
IVADAS	4
1. Virtualios valiutos.....	9
1.1 Virtualių valiutų sąvoka	9
1.2 Virtualių valiutų santykis su realiais pinigais	11
1.3 Virtualių valiutų atskirtis nuo elektroninių pinigų.....	12
1.4 Virtualių valiutų rūšys.....	14
1.4.1 Apibendrinti virtualių valiutų požymiai	17
1.5 Virtualių valiutų technologiniai ypatumai	17
1.5.1 Blokų grandinės technologijos samprata	19
1.5.2 Blokų grandinės technologijos veikimo pagrindai.....	20
1.5.3 Proof-of-Work ir Proof-of-Stake: blokų grandinės technologijos principai patikimumo sprendimo problema.....	22
1.6 Virtualių valiutų rinkos dalyviai.....	23
2. Pinigų plovimas.....	26
2.1 Pinigų plovimo sąvoka.....	26
2.2 Trys pagrindiniai pinigų plovimo ciklo etapai.....	26
2.2.1 Pinigų plovimo metodai	28
2.3 Pinigų plovimo procesas pasitelkiant virtualias valiutas	31
2.3.2 Augantis susirūpinimas: virtualių valiutų panaudojimas terorizmo finansavimui	33
3. PINIGŲ PLOVIMO PANAUDOJANT VIRTUALIAS VALIUTAS TEISINIAI IR REGULIACINIAI MECHANIZMAI.....	35
3.1 Nacionalinis požiūris	36
3.3 Internacionalizacija	41
3.3.1 Pinigų plovimo ir teroristų finansavimo standartų minkštoji normatyvinė struktūra	44
3.3.2 Pinigų plovimo ir teroristų finansavimo standartų minkštosios normatyvinės struktūros poveikis Europos Sąjungos teisei.....	59
3.3.3 AMLD5 veikimo sritis	64
3.3.4 Kova su pinigų plovimu baudžiamosios teisės priemonėmis	70
3.3.5 Reglamentas dėl informacijos, teikiamos pervedant lėšas	73
3.3.6 Tarptautinis bendradarbiavimas.....	74
3.4 Tarptautinių atsiskaitymų banko pozicija ir centrinių bankų skaitmeninės valiutos	76
IŠVADOS.....	80
REKOMENDACIJOS.....	82
LITERATŪROS SĄRAŠAS.....	83
ANOTACIJA	89
ABSTRACT.....	89
SANTRAUKA.....	90
SUMMARY	91
AKADEMINIO SĄŽININGUMO DEKLARACIJA	92

SANTRUMPŲ SĄRAŠAS

AML/CTF – kova su pinigų plovimu/kova su terorizmo finansavimu

AMLD1 – pirmoji kovos su pinigų plovimu direktyva

AMLD2 – antroji kovos su pinigų plovimu direktyva

AMLD3 – trečioji kovos su pinigų plovimu direktyva

AMLD4 – ketvirtoji kovos su pinigų plovimu direktyva

AMLD5 – penktoji kovos su pinigų plovimu direktyva

CBDC – centrinio banko skaitmeninė valiuta

DLT – paskirstytųjų duomenų technologija

EBI – Europos bankininkystės institucija

ECB – Europos centrinis bankas

FATF – Finansinių veiksmų darbo grupė

FŽP – finansinės žvalgybos padaliniai

KYC – pažink savo klientą

TAB – Tarptautinių atsiskaitymų bankas

IVADAS

Tiriama problema. Daugiau nei prieš dešimtmetį autorius slapyvardžiu Satoshi Nakamoto išleido straipsnį pavadinimu „*Bitcoin: A Peer-to-Peer Electronic Cash System*“, kuris sukėlė perversmą finansų sektoriuje. Ši inovacija pasiūlė tai, ko negalėjo pasiūlyti įprastinės finansų įtaigos – sumažinti sandorių sąnaudas, pagerinti klientų patirtį, padidinti perlaidų greitį. Tikriausiai svarbiausi aspektai buvo decentralizuotas sistemos pobūdis bei garantuojamas aukštas anonimiškumo laipsnis.¹ Nenuostabu, jog tokia inovacija sukėlė įvairių suinteresuotųjų šalių reakcijų: viena vertus, smalsumą ir entuziazmą dėl inovacijos potencialo, kita vertus, susirūpinimą ir nepasitikėjimą dėl rizikos ir pasekmių, susijusių su naudojimu.

Šiai dienai tai, kam pagrindą davė S. Nakamoto, įvardinama daugeliu skirtingų terminų, kurie dažnai naudojami kaip sinonimai – kriptovaliutos, kriptoturtas, virtualiosios valiutos, virtualus turtas ar skaitmeninės valiutos. Tačiau nepriklausomai nuo pavadinimo, svarbiausias aspektas, jog tokio pobūdžio turto populiarumas tik didėja, remiantis 2020 m. gruodžio 3 d. duomenimis rinkoje buvo fiksuota daugiau nei 7850 kriptovaliutų, šiai dienai (2022 m. balandžio mėn.) jų yra jau virš 18000 rūšių, todėl ignoruoti virtualių valiutų reikšmės ir vystymosi spartos yra neįmanoma.²

Nors buvo daroma prielaida, jog virtualios valiutos grėsmės tarptautiniam finansiniam stabilumui nekelia, ypač dėl to, kad jų bendra pasaulinė rinkos vertė buvo palyginti nedidelė³, tačiau matome, jog rinkos dydis per nepilnus dvejus metus išaugo beveik 2.5 karto. Be kita ko, remiantis blokų grandinės duomenų bendrovės Chainalysis metine ataskaita, 2021 m. nusikaltėliai išplėvė 8,6 mlrd. dolerių kriptovaliutomis, t. y. 30 % daugiau nei ankstesniais metais.⁴

Pasaulinio masto kontekste tokie skaičiai gali pasirodyti nedideli, tačiau šie skaičiai auga ir galima daryti prielaidą, jog augs lygiai taip pat, kaip ir virtualių valiutų skaičius rinkoje. Todėl tai nepanaikina sunkumų, su kuriais susiduria reguliavimo institucijos. Kai kurie iš klausimų, dėl kurių diskutuoja nacionalinės ir tarptautinės suinteresuotosios šalys, yra susiję su šio turto naudojimu neteisėtais tikslais, taip pat vartotojų apsauga ir net su šio sektoriaus veiklos pasekmėmis aplinkai.

Vienas iš didžiausių pavojų, susijusių su virtualiomis valiutomis, yra jų panaudojimas pinigų plovimo ir terorizmo finansavimo veikloje ir tai išryškėja kaip viena iš pagrindinių

¹ Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

² CoinMarketCap, <https://coinmarketcap.com>

³ Rodrigues, Gustavo; Kurtz, Lahis. Cryptocurrencies and anti-money laundering regulation in the G20. Institute for Research on Internet and Society: Belo Horizonte, 2019

⁴ Chainalysis, The 2021 Crypto Crime Report, 4 psl., 2021, <https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>

nacionalinių ir tarptautinių teisinių tyrimų sričių, kuri pastaruoju metu vis labiau yra dėmesio centre.⁵ Pinigų plovimas teoriškai laikomas nesmurtiniu nusikaltimu, tačiau sėkmingas pinigų plovimas turi gali turėti didelį neigiamą poveikį, nes jis dažnai palaiko ir remia kitas neteisėtas veiklas, kaip prekybą narkotikais ar terorizmą, leidžia perkelti lėšas iš sankcionuotų šalių, todėl suprantamas toks augantis dėmesys.⁶

Kadangi tarptautiniu mastu vienodo sutarimo apie tai, kas yra virtualios valiutos ir virtualaus valiutų paslaugų teikėjai, dėl to išlieka tikimybė, kad pinigų plovėjai galėtų rasti ir pasinaudoti galimomis reguliavimo spragomis. Taip pat ir nacionalinių sistemų skirtumai suteikia galimybę nusikaltėliams pasinaudoti atviru arba nereguliuojamu virtualiu turtu ir toliau plauti pelną.⁷

Šio darbo apimtyje pagrindinis vartojamas terminas bus - virtualios valiutos, nors kaip minėta, šiam reiškiniui gali būti priskirta daugybė įvairių terminų. Toks pasirinkimas nulemtas fakto, jog apibrėžimas virtualios valiutos yra dažniausiai vartojamas tarp reguliatorių ir gali būti traktuojamas plačiausiai.⁸

Baigiamojo darbo aktualumas. Virtualios valiutos nacionaliniams bei tarptautiniams įstatymų leidėjams bei reguliavimo institucijoms kelia kritinius sisteminius iššūkius, susijusius su kovos su pinigų plovimo reguliavimu, taigi svarbus supratimas bei teisės aktų bei praktikos įvertinimas virtualiųjų valiutų atžvilgiu. Be kita ko, skirti ypatingą dėmesį šiai temai taip pat skatina Europos Sąjungos direktyvų dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos raida. Pirmoji direktyva pristatyta dar 1991 m. birželio mėn. įvedė prevencinius veiksmus, tokius kaip: klientų patikrinimas, vartotojų atpažinimas, įtartinų transakcijų ataskaitų rengimas, kas ir šiai dienai išliko nepakitę.⁹ Antroji direktyva, išleista 2001 m. gruodžio mėnesį, suderino ES suderino veiklos kryptį su Tarptautinės kovos su pinigų plovimu organizacijos (angl. *Financial Action Task Force; FAPT*) 40 rekomendacijų.¹⁰ Trečioji direktyva sukoordinavo ES standartus su atnaujintais FAPT standartais.¹¹ Ketvirtoji direktyva buvo išleista

⁵ RODRIGUES, Gustavo; KURTZ, Lahis. Cryptocurrencies and anti-money laundering regulation in the G20. Institute for Research on Internet and Society: Belo Horizonte, 2019

⁶ Nicholas J. Ajello. *Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination*. (2015)

⁷ Velkes, Gabrielle Chasin, International Anti-Money Laundering Regulation Of Virtual Currencies And Assets , 2020

⁸ Blandin, Apolline, et al., Global Cryptoasset Regulatory Landscape Study, 35 psl., 2020 m., <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf>

⁹ COUNCIL DIRECTIVE of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (91/308/EEC)

¹⁰ Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering - Commission Declaration

¹¹ Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

tik po dešimtmečio, kurios metu, pašalino netikslumus, buvusius trečiojoje direktyvoje bei dar labiau sugriežtino kovos su pinigų plovimu taisykles.¹² Šio darbo kontekste aktuali penktoji direktyva (angl. *AMLD5*) pasirodė praėjus tik trims metams po ketvirtosios direktyvos išleidimo bei įvedė naujus reikalavimus virtualioms valiutoms, galutinių naudos gavėjų registrai bei išankstinio mokėjimo kortelių operacijų limitams.¹³ Direktyvoje dėl kovos su pinigų plovimu baudžiamosios teisės priemonėmis pažymima: „<...> *virtualiųjų valiutų naudojimas kelia naujus pavojus ir uždavinius kovos su pinigų plovimu požiūriu. Valstybės narės turėtų užtikrinti, kad būtų tinkamai atsižvelgiama į tuos rizikos veiksnius*“.¹⁴ Tad pastaraisiais metais ypač suintensyvėjęs šių direktyvų plėtojimas suponuoja, jog ši sritis darosi kaip niekada aktuali.

Taigi, virtualių valiutų ir pinigų plovimo tematikos tarptautinės teisės požiūriu aptarimas bei analizė svarbūs tiek finansinių, tiek kibernetinių nusikaltimų prevencijai, taip pat siekiant apsaugoti rinkų vientisumą, suprasti vartotojų poreikius bei reguliatoriams kylančias problemas.

Baigiamojo darbo mokslinis naujumas. Rengiant šį baigiamąjį darbą Lietuvoje nebuvo tiriamųjų darbų, kurių analizės pagrindas būtų šiame darbe keliami probleminiai klausimai, kurie susietų virtualias valiutas ir pinigų plovimo prevencijos teisės srities reglamentavimą tarptautinės teisės atžvilgiu. Nors pinigų plovimo prevencijos institutas yra gerai žinomas, tačiau, galima daryti prielaidą, jog atsižvelgiant į virtualių valiutų naujumą tiek iš privačiojo sektoriaus, tiek iš viešojo sektoriaus perspektyvų, nulėmė neišplėtotą reglamentavimą, todėl pinigų plovimo problematika, kuri tiesiogiai susijusi su virtualių valiutų panaudojimu, yra vis dar retai sutinkamas klausimas.

Baigiamajame darbe tiriamos problemos ištyrimo lygis. Nagrinėjant virtualių valiutų bei su jomis susijusią pinigų plovimo prevenciją tarptautinės teisės požiūriu, aktualūs tarptautiniai teisės aktai, kaip anksčiau aptartos Europos Sąjungos direktyvos dėl pinigų plovimo bei terorizmo finansavimo prevencijos. Be kita ko, ypač aktuali tarpvyriausybinių organizacijų – Tarptautinės kovos su pinigų plovimu organizacijos rekomendacijos bei nuolatos atnaujinami standartai. Be kita ko, svarbu atkreipti dėmesį į Jungtinių tautų vaidmenį pinigų plovimo kovoje bei įvertinti Tarptautinių atsiskaitymų banko poziciją.

Literatūra lietuvių kalba nėra gausi, daugiausiai randami pavieniai straipsniai atskiromis temomis susijusiomis su kriptovaliutomis ar pinigų plovimu. Apie kriptovaliutų teigiamas bei

¹² Europos Parlamento ir Tarybos Direktyva (ES) 2015/849, 2015 m. gegužės 20 d., dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos, kuria iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 ir panaikinama Europos Parlamento ir Tarybos direktyva 2005/60/EB bei Komisijos direktyva 2006/70/EB

¹³ Europos Parlamento ir Tarybos Direktyva (ES) 2018/843, 2018 m. gegužės 30 d, kuria iš dalies keičiama Direktyva (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos ir iš dalies keičiamos direktyvos 2009/138/EB ir 2013/36/ES

¹⁴ Europos Parlamento ir Tarybos Direktyva (ES) 2018/1673, 2018 m. spalio 23 d., dėl kovos su pinigų plovimu baudžiamosios teisės priemonėmis

neigiamas puses straipsnyje „*Kriptovaliutos: privalumai ir trūkumai*” kalba A. Subačius bei R. Subačienė.¹⁵ Taikytinos teisės nustatymą kriptovaliutų sistemų dalyvių santykiams aptaria D. Grigaitis.¹⁶

Literatūra užsienio kalba gausesnė. Pagrindinį dėmesį galima skirti FATF pateiktoms ataskaitoms dėl virtualaus turto ir virtualaus turto paslaugų teikėjų. Be abejo, svarbų pagrindą sudaro ir Europos bankininkystės institucijos nuomonė dėl virtualių valiutų bei Europos Centrinio Banko virtualių valiutų schemų analizė. Skaitmeninių valiutų temą, sampratą, keliamus iššūkius plėtoja profesorius David Lee Kuo Chuen knygoje „*Handbook of Digital Currency*”. Ypač išsamiai ir gausiai tiek AMLD4, tiek AMLD5 taikymo sritis yra aptaręs FinTech srityje besispecializuojantis teisininkas Niels Vandezande.

Baigiamojo darbo reikšmė. Šiame darbe siekiama atlikti kompleksinę apžvalgą, įvertinant virtualių valiutų keliamus probleminius klausimus tarptautinėje pinigų plovimo prevencijos srityje. Be kita ko, bandoma įvertinti kokią įtaką padarė virtualių valiutų prieinamumas pinigų plovimo prevencijos instituto formavimuisi, siekiama pabrėžti galimas reglamentavimo spragas, kurios gali apimti tiek bendrus klausimus, kaip virtualių valiutų sąvokos formavimą, tiek konkrečius klausimus, tokius kaip specifinių rinkos dalyvių reguliavimo problemas.

Išskyrus aktualius klausimus bei atskleidus susijusią problematiką, ne ką mažiau svarbu įvertinti, kaip ir kokiomis teisinio reglamentavimo priemonėmis šie klausimai sprendžiami. Galima teigti, jog darbo pagrindas yra įpareigojančių bei neįpareigojančių tarptautinės teisės normų įtakos pinigų plovimo prevencijos politikos formavimuisi atskleidimas bei įvertinimas.

Baigiamojo darbo originalumas. Baigiamojo darbo originalumo klausimą galima tiesiogiai susieti su šio darbo aktualumu bei naujumu. Darbo apimtyje sutelkiamas dėmesys į vis dar naujai, bet ypač sparčiai besivystančius teisinius santykius virtualių valiutų ir pinigų plovimo prevencijos srityje. Galima teigti, jog šis institutas vis dar yra formavimosi stadijoje ir laiko tėkmėje atsiskleidžia nauji išskylantys iššūkiai. Todėl baigiamajame darbe siekiama parodyti virtualių valiutų ir pinigų plovimo prevencijos teisinio reglamentavimo raidą, analizuojant šiuose santykiuose aktualius klausimus ir jų pokytį, taip pat faktą, jog nėra suformuotos bendros doktrinos probleminių klausimų atžvilgiu.

Tyrimo tikslas. Šiuo darbu siekiama ištirti virtualių valiutų problematiką pinigų plovimo prevencijos kontekste, išnagrinėti, kokią įtaką daro virtualių valiutų naudojimas plėtojant pinigų plovimo prevencijos institutą tarptautinės teisės požiūriu.

¹⁵ Subačius A. and Subačienė R. (2019) “Cryptocurrency: Advantages and Disadvantages”, *Buhalterinės apskaitos teorija ir praktika*,

¹⁶ Grigaitis, Denas, Taikytinos Teisės Nustatymas Kriptovaliutų Sistemų Dalyvių Santykiams Europos Sąjungoje, 2021

Tyrimo uždaviniai. Siekiant kokybiškos darbo analizės, buvo iškelti šie uždaviniai:

1. Išnagrinėti virtualių valiutų sampratą, atskleisti jų pagrindines savybes.
2. Atlikti teorinę pinigų plovimo nusikaltimo analizę, išskirti pagrindinius nusikaltimo etapus bei metodus.
3. Išanalizuoti tarptautinius pinigų plovimo ir terorizmo finansavimo prevencijos reglamentavimo standartus, siekiant atskleisti jų pritaikymą reguliuojant virtualių valiutų rinką.
4. Išanalizuoti ar užtektingai išplėsta AMLD5 taikymo sritis, apimanti tik virtualiųjų valiutų konvertavimo bei depozitinių piniginių paslaugų teikėjus.

Tyrimo metodika. Rašant magistro baigiamąjį darbą, pasitelkti šie metodai:

Sisteminės analizės metodas – naudojantis šiuo metodu siekiama kompleksiskai išanalizuoti virtualių valiutų ir pinigų plovimo prevencijos probleminius klausimus ir pritaikyti sprendimo būdus.

Loginis-analitinis metodas – pasitelkiant šį metodą siekiama atlikti virtualių valiutų bei pinigų plovimo prevencijos teisinio reglamentavimo santykį, įvertinant teisinių santykių reguliavimo pokytį laike.

Lingvistinis metodas – taikytas aiškinant tarptautinės teisės normas aktualias darbo kontekste.

Tyrimo struktūra. Tyrimo pagrindą sudaro šios dalys: įvadas, dėstomoji dalis, išvados. Bendroji dalis skirta išanalizuoti virtualių valiutų, pinigų plovimo prevencijos sampratą, veikimo mechanizmus. Suprasti technologijas, kurių pagrindu veikia virtualios valiutos, klasifikuoti jų vietą rinkoje.

Specialiosios darbo dalies paskirtis apžvelgti teisinio reguliavimo metodus tarptautiniu lygmeniu, taikomas praktikas. Ištirti Europos Sąjungos bei tarptautinę reglamentavimo sistemą.

Aptarus pirmąją bei antrąją dalis, suformuojamos išvados. Pateikiamas literatūros sąrašas, anotacija, darbo santraukos lietuvių bei anglų kalbomis.

Ginamieji teiginiai.

1. Vieningos tarptautinės virtualių valiutų ir su jomis susijusio pinigų plovimo prevencijos sistemos nebuvimas sukelia kliūčių veiksmingam šios srities reguliavimui.
2. Dabartinės pinigų plovimo prevencijos gairės nėra pakankamos virtualių valiutų operacijoms.
3. Siekiant sumažinti pinigų plovimo galimybes panaudojant virtualias valiutas, svarbu užtikrinti teisinių standartų kūrimą bei unifikavimą tarptautiniu lygmeniu.

1. Virtualios valiutos

Pirmajame skyriuje bus siekiama išanalizuoti virtualių valiutų klausimą apibrėžiant virtualių valiutų sąvoką, jos kitimą laike, atskleidžiant pagrindines virtualių valiutų savybes, atsakant į klausimą, ar virtualias valiutas galima prilyginti realiems pinigams. Be kita ko, svarbus ir blokų grandinės technologijos apžvelgimas, kurios pagrindu veikia didžioji dalis reguliacinių iššūkių keliančių virtualių valiutų, įvertinant blokų grandinės funkcionalumą, pagrindinius rinkos dalyvius.

1.1 Virtualių valiutų sąvoka

Visų pirma, siekiant išnagrinėti virtualių valiutų reguliavimą tarptautinės teisės požiūriu, svarbu suprasti virtualių valiutų terminą. Tačiau nustatyti virtualių valiutų sąvoką nėra lengva užduotis, nes iki šios dienos nėra vieningai priimtose bei bendros virtualios valiutos apibrėžties. Pavyzdžiui, Europos Centrinis Bankas (ECB) 2012 m. dokumente *Virtualių valiutų schemos*, virtualias valiutas apibrėžė kaip: „nereguliuojamus skaitmeninius pinigus kuriuos išleidžia ir paprastai kontroliuoja jų kūrėjai, o naudoja ir priima tam tikros virtualios bendruomenės nariai“.¹⁷ Kiek vėliau, po dviejų metų, 2014 m., Europos bankininkystės institucija (EBI), virtualių valiutų sąvoką pateikė kaip: „skaitmeninė vertės išraiška, kurios neišleidžia centrinis bankas ar valdžios institucija ir kuri nebūtinai yra susieta su fiat (įprastine) valiuta¹⁸, bet kurią fiziniai ar juridiniai asmenys priima kaip mainų priemonę ir kurią galima perduoti, saugoti ar ją prekiauti elektroniniu būdu.“¹⁹ Tų pačių metų Finansinių veiksmų darbo grupės pateiktoje apibrėžtyje virtualios valiutos įvardinamos, kaip: “skaitmeninis vertės išraiška, kuriuo galima prekiauti skaitmeniniu būdu ir kuris veikia kaip (1) mainų priemonė ir (arba) (2) apskaitos vienetas ir (arba) (3) vertės saugykla, tačiau neturi teisėtos mokėjimo priemonės statuso (t. y. kai pateikiama kreditoriui, nėra galiojantis ir teisėtas mokėjimo pasiūlymas) jokioje jurisdikcijoje”.²⁰

2015 m. ECB pozicija dėl virtualių valiutų buvo iš dalies pakeista, kai buvo pareikšta, jog žodis *nereguliuojama* turėtų būti išbraukta iš 2012 m. naudotos apibrėžties, pripažįstant, kad

¹⁷ European Central Bank, Virtual Currency Schemes, 5 psl., 2012 m., <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

¹⁸ Fiat pinigai, kaip juos apibūdino Rūta Vainienė knygoje „Ekonomikos terminų žodynas“ yra suprantami, kaip dekretiniai pinigai. Dekretiniai pinigai - yra dekretu išleisti valstybiniai popieriniai pinigai, kurie nepadengti aukso atsargomis bei nekonvertuojami į auksą ir naudojami tik kaip mainų priemonė. Didžioji dauguma šiuolaikinių pinigų yra dekretiniai.

¹⁹ European Banking Authority, EBA Opinion on „virtual currencies“, 5 psl., 2014 m., <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1>

²⁰ FATF; FATF Report Virtual Currencies: Key Definitions and Potential AML/CFT Risks; 4 psl., 2014 m., <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

jurisdikcijos, kuriose virtualių valiutų reguliavimas vykdomas ir tam yra išleisti atitinkami teisės aktai. Todėl sąvoka buvo pakeista į: „*skaitmeninę vertės išraišką, neišleistą centrinio banko, kredito įstaigos ar elektroninių pinigų įstaigos, kuri tam tikromis aplinkybėmis gali būti naudojamas kaip pinigų alternatyva.*“ Be kita ko, siekiant išvengti nesusipratimų dėl teorinių virtualios valiutos pripažinimo apribojimų, buvo atsisakyta frazės: „*naudojama ir pripažįstama tarp konkrečios virtualios bendruomenės narių*“.²¹

Šiai dienai, remiantis Europos Parlamento ir tarybos direktyva (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos virtualiosios valiutos suprantamos kaip: „*skaitmeninė vertės forma, kuri nėra išleista arba užtikrinta centrinio banko ar viešosios valdžios institucijos, nebūtinai susieta su teisės aktais nustatyta valiuta ir neturinti teisinio valiutos ar pinigų statuso, tačiau pripažįstama fizinių arba juridinių asmenų kaip atsiskaitymo priemonė ir galinti būti perduodama, laikoma arba parduodama elektroniniu būdu*“.

²² Pažymėtina, jog Direktyvoje teigiama, jog virtualios valiutos gali būti dažnai sutinkamos kaip mokėjimo priemonė, tačiau jų panaudojimo mastas kur kas platesnis, nes tai gali būti ir mainų ar investavimo priemonė, vertės išsaugojimo produktas.²³

Atkreiptinas dėmesys, jog ir naujausiame FATF dokumente „*Atnaujintos rizikos vertinimu pagrįsto požiūrio gairės. Virtualusis turtas ir virtualiojo turto paslaugų teikėjai*“ yra išskiriamos ne virtualios valiutos, tačiau naudojama virtualaus turto apibrėžtis, kuri skamba taip: „*virtualus turtas - skaitmeninis vertės išraišką, kuriuo galima prekiauti ar perleisti skaitmeniniu būdu ir kuris gali būti naudojamas mokėjimo ar investavimo tikslais. Virtualusis turtas neapima skaitmeninių fiat valiutų, vertybinių popierių ir kito finansinio turto atvaizdų, kurie jau yra įtraukti į kitus FATF Rekomendacijas*“.²⁴

Mokslinėje literatūroje dauguma tyrėjų remiasi pirminiuose teisės šaltiniuose suformuluotomis virtualių valiutų sąvokomis. Tačiau, pavyzdžiui, Dong He et al. virtualias valiutas apibūdina kaip skaitmeniniai vertės pavidalus, kuriuos išleidžia privatūs kūrėjai ir kurie išreikšti savo apskaitos vienetais. Virtualiosios valiutos gali būti gaunamos, saugomos, pasiekiamos ir jomis gali būti atliekami sandoriai elektroniniu būdu, ir jos gali būti naudojamos

²¹ European Central Bank; Virtual currency schemes – a further analysis; 25 psl., 2015 m., <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

²² Europos Parlamento ir tarybos direktyva (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos, kuria iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 ir panaikinama Europos Parlamento ir Tarybos direktyva 2005/60/EB bei Komisijos direktyva 2006/70/EB, 12 psl., 2021 m., <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:02015L0849-20210630&from=EN>

²³ *Ibid.* (10)

²⁴ FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, 21 psl., 2021 m., <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

įvairiais tikslais, jei sandorio šalys sutinka jas naudoti.²⁵ Štai Stefan Mbiyavanga virtualias valiutas įvardina tik kaip skaitmeninis vertės atvaizdavimą, pažymint, jog jų teisinė klasifikacija tebėra prieštaringa.²⁶

Nagrinėjant jau pateiktas virtualių valiutų sąvokas, kaip pažymi, A. Dibrova, svarbu apibrėžti ir klasifikuoti virtualiųjų valiutų aspektus, tačiau apibrėžtis paprastai skiriasi priklausomai nuo konteksto, pavyzdžiui, apmokestinimo, rinkos dalyvių registravimo ir licencijavimo ar kovos su pinigų plovimu, nes virtualios valiutos tiksliai neatitinka jokios esamos klasifikacijos. Taip pat atkreipia dėmesį, jog virtualioji valiuta nėra nei užsienio valiuta, nei tradicinė prekė, nei tiesiog mokėjimų tinklas.²⁷

Apibendrinant, šių apibrėžimų analizė yra ypač svarbi, nes terminas virtualios valiutos gali būti dalinai klaidinantis, leidžiantis padaryti prielaidą, jog virtuali valiuta galėtų būtų leidžiama valstybinių institucijų ir pripažįstama kaip realūs, įteisinti pinigai. Iš pateiktų apibrėžčių matoma, jog sąvoka nereguliuojami skaitmeniniai pinigai buvo pakeista į skaitmeninė vertės išraišką, neišleistą centrinio banko ar kitų įstaigų. Galima būtų teigti, jog tokie skirtumai ir sąvokos kitimas laike parodo, jog reguliuojančios institucijos nuolatos analizuoja virtualių valiutų sampratą ir stengiasi, jog terminas geriausiai atspindėtų virtualių valiutų prigimtį bei galimą panaudojimą.

1.2 Virtualių valiutų santykis su realiais pinigais

Vienas iš dažniausiai kylančių klausimų ar virtualios valiutos pasižymi tokiomis pat savybėmis, kaip ir tikri pinigai. Tad siekiant atsakyti į klausimą, ar virtualios gali būti priskiriamos pinigams pirmiausia reikia apibrėžti pinigų sąvoką, o tai gali padėti padaryti trys populiariausios pinigų teorijos.

Remiantis pirmąja teorija, vadinama *metalistika*, pinigai turi būti susieti su pagrindiniu daiktu, turinčiu nepriklausomą rinkos vertę. Kaip sufleruoja šios teorijos pavadinimas, pinigus buvo bandoma susieti su metalais, ypač tokiu tauriuoju metalu, kaip auksas.²⁸ Įdomu pastebėti, jog yra autorių, teigiančių, kad virtualias valiutas, konkrečiau, tikriausiai geriausiai žinomą virtualią valiutą - Bitcoin, įkvėpė ne kas kita, o *metalistika*. Ši teorija grindžiama mintimi, jog brangiųjų metalų prieinamumas ir metalo gavybos kaštai turėtų automatiškai nustatyti ribą, kiek pinigų galima sukurti. Žvelgiant iš virtualių valiutų perspektyvos, tai turėtų būti interpretuojama taip, kiek

²⁵ He, Dong, et al., Virtual Currencies and Beyond: Initial Considerations, IMF STAFF DISCUSSION NOTE, 7 psl., 2016

²⁶ Mbiyavanga, Stefan, CRYPTOLAUNDERING: ANTI-MONEY LAUNDERING REGULATION OF VIRTUAL CURRENCY EXCHANGES, 2019

²⁷ Dibrova, Alina, Virtual currency: new step in monetary development, 5th International Conference On Leadership, Technology, Innovation And Business Management, 2016

²⁸ Goodhart, Charles A.E, The two concepts of money: implications for the analysis of optimal currency areas, 1998

galima tokios rūšies turto sukurti, nes, pavyzdžiui, bitkoinų skaičius yra ribotas, taip bitkoinas yra „kasamas“, o ne „kalamas“.²⁹

Antroji pinigų teorija yra žinoma kaip *chartalizmas*. Šios požiūrio pagrindas yra suvokimas pinigų, kaip teisinio valstybės kūrinio, tad galima suprasti, jog atsakomybė už veikiančią pinigų sistemą taip pat yra priskiriama valstybei. Ir tol, kol tokių pinigų egzistavimas yra juridškai įteisintas, visai nesvarbu jų kilmė, ar tai būtų fiziniai pinigai, pagaminti iš popieriaus ar metalo, ar virtualūs vienetai.³⁰

Tikriausiai geriausiai žinoma ir plačiausiai pripažinta yra trečioji pinigų teorija, vadinama *funkcionalizmu*. Apibrėžimas grindžiamas supratimu, jog siekiant, kad pinigai galėtų būti laikomi pinigais, turi atlikti tam tikras funkcijas. Pagal šią teoriją, tokių funkcijų yra trys: buvimas mokėjimo priemone, apskaitos vienetu ir kad pinigų vertė neturėtų per daug svyruoti. Terminas mokėjimo priemonė turėtų reikšti, kai pirkėjas tikslingai duoda pardavėjui pinigus, o ne kai jie abu suranda daiktą ar paslaugą, kuria galėtų apsieisti.³¹

Atsižvelgus į tris pateiktas teorijas, bendrai žinoma, jog virtualios valiutos nėra susietos su konkrečia preke ar valstybine valiuta, todėl galima teigti, jog pačios iš savęs, savo prigimties neturi vertės. Neegzistuoja joks teisinis mechanizmas, kuris virtualias valiutas galėtų priversti jas priimti, kaip mokėjimo formą. Dėl šios priežasties, jos paremtos tik visišku pasitikėjimu, o virtualių valiutų vertė nulemiama jų cirkuliavimu elektroninėje erdvėje. Taip pat virtualios valiutos vis dar nėra plačiai paplitusi mokėjimo priemonė, kuria būtų atsiskaitoma už prekes ar paslaugas. Be kita ko, virtualių valiutų vertė yra per daug nepastovi ir svyruojanti. Todėl galima būtų teigti, jog virtualios valiutos neatitinka nei vienos iš pateiktų pinigų teorijų ir neturėtų būti laikomos pinigais.

1.3 Virtualių valiutų atskirtis nuo elektroninių pinigų

Kitas svarbus aspektas virtualių valiutų identifikacijoje – atskyrimas nuo elektroninių pinigų. Kaip minėta prieš tai, įprastos valiutos yra teisėta mokėjimo priemonė, kuri leidžiama ir palaikoma vyriausybių. Tačiau kyla klausimas, kokie yra virtualių valiutų ir elektroninių pinigų skirtumai. Pirmiausia, atsakant į klausimą, kas yra elektroniniai pinigai, Europos Parlamento ir Tarybos Direktyvoje 2009/110/EB pateikiamas toks apibrėžimas: „išleidėjui pateikiamu reikalavimu išreikšta, elektroninėse, įskaitant, magnetines, laikmenose saugoma piniginė vertė,

²⁹ Swartz, Lana. What Was Bitcoin, What Will It Be? Cultural Studies. Volume 32, Issue 4. 2018 m.

³⁰ Wray, L. Randall, From the State Theory of Money to Modern Money Theory: An Alternative to Economic Orthodoxy, 2014

³¹ Palley, Thomas I. (2018): The evolution of money debate: Functionalism versus chartalism, Schumpeterian dynamics, Gresham's fallacy, and how history constrains public finance, FMM Working Paper, No. 34, Hans-Böckler-Stiftung, Macroeconomic Policy Institute (IMK), Forum for Macroeconomics and Macroeconomic Policies (FFM), Düsseldorf

*kuri išleidžiama gavus lėšas, skirta mokėjimo operacijoms, kaip apibrėžta Direktyvos 2007/64/EB 4 straipsnio 5 punkte, atlikti ir priimama fizinių arba juridinių asmenų, neskaitant elektroninių pinigų išleidėjo”.*³²

Remiantis ECB pateikta sąvoka, elektroniniai pinigai taip pat įvardinami kaip elektroninė piniginių vertės laikmena techniniame įrenginyje, kuri gali būti naudojama mokėjimams atlikti su tiek su fiziniais, tiek su juridiniais asmenimis. Tokio tipo įtaisui nereikia banko sąskaitos, kad būtų galima atlikti operacijas, nes yra iš anksto apmokėta priemonė. Priklausomai nuo piniginei vertei saugoti naudojamos technologijos, elektroninių pinigų priemonės gali būti aparatinės arba programinės įrangos.³³

Kalbant apie aparatinę įrangą pagrįstus produktus, vertė, už kurią galima nupirkti, saugoma fiziniame įrenginyje, kuris priklauso asmeniui, pavyzdžiui, lustinėje kortelėje. Tokioms piniginėms vertėms perversi paprastai naudojami prietaisų skaitytuvai, nereikalaujantys, jog realiu laiku būtų tinklo prieiga prie nutolusio serverio. Kitu atveju, programine įranga pagrįstoms prekėms naudojama specializuota programinė įranga, kaip pavyzdžiui, esanti nešiojamuosiuose kompiuteriuose. Siekiant perduoti vertę, įrenginiai turėtų užmegzti interneto ryšį su nuotoliniu serveriu, siekiant įsigyti prekę ar paslaugą.³⁴

Taigi, apibendrinant, elektroniniai pinigai apibūdinami kaip vertė, kuri saugoma elektroniniu būdu, išleidžiama mainais už lėšas ir kurią kaip mokėjimo būdą priima kitos šalys. Elektroninių pinigų sistemose elektroninių pinigų ir *fiat* valiutos, už kurią jie išleisti, ryšys yra tiesioginis, nes lėšos nurodomos tos valiutos vienetais, kaip kad eurai ar JAV doleriais. Priešingai, virtualiųjų valiutų sistemose apskaitos vienetas neturi faktinio ekvivalento *fiat* pinigais. Taip pat skirtingai nei virtualios valiutos, elektroniniai pinigai nėra atskira valiuta ir juos reguliuoja ta pati centrinė institucija, kuri reguliuoja pagrindinę nacionalinę valiutą.³⁵

G. A. Acuña su A. S. Pulla išskiria, jog pagrindinis skirtumas tarp virtualiosios valiutos ir elektroninių pinigų yra tas, kad antrieji neturi teisėtos mokėjimo priemonės statuso. Kita vertus, elektroniniai pinigai yra *fiat* valiuta su elektronine reprezentacija. Šis skirtumas lemia specialios teisinės sistemos būtinybę ir kitas svarbias pasekmes. Pirma, virtualiosios valiutos schemoje pastebimas tradicinių finansų subjektų, tokių kaip centriniai bankai, nebuvimas. Už skaitmeninių valiutų veikimo priežiūrą atsakingi jų emitentai. Tai reiškia, kad tipinis finansų sektoriaus reguliavimas netaikomas. Antra, tarp skaitmeninės valiutos ir *fiat* valiutos nėra teisinio ryšio.

³² Europos Parlamento ir Tarybos Direktyva 2009/110/EB, dėl elektroninių pinigų įstaigų steigimosi, veiklos ir riziką ribojančios priežiūros, iš dalies keičianti Direktyvas 2005/60/EB ir 2006/48/EB ir panaikinanti Direktyvą 2000/46/EB, 2009 m. rugsėjo 16 d., 2 str. 2 d.

³³ Electronic Money; European Central Bank;

https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html

³⁴ *Ibid.*

³⁵ CGAP, Bitcoin Versus Electronic Money, 3 psl., 2014 m., <https://www.cgap.org/sites/default/files/Brief-Bitcoin-versus-Electronic-Money-Jan-2014.pdf>

Trečia, skaitmeninė valiuta denominuojama kitaip nei *fiat* valiuta. Taip yra todėl, kad visiška virtualiųjų valiutų kontrolė suteikiama jos emitentui.³⁶

1.4 Virtualių valiutų rūšys

Iš aukščiau pateiktų sąvokų, virtualios valiutos apibrėžiamos pakankamai plačiai, taip yra dėl to, jog sąvokos galėtų būti taikomos visoms virtualioms valiutoms, nors tarp jų yra nemažų skirtumų. Šie skirtumai matomi analizuojant ECB klasifikaciją, kuri remiasi ryšiu su ekonomika arba kitaip įvardinant, kaip *fiat* pinigai galėtų būti keičiami į virtualias valiutas. Tad trys išskiriamos grupės yra: 1. uždaros virtualiųjų valiutų schemas; 2. virtualiųjų valiutų schemas su vienakrypčiais srautais; 3. virtualiųjų valiutų schemas su dvikrypčiais srautais.³⁷

Visų pirma, uždaros virtualiųjų valiutų schemas į kurias nepatenka jokie realūs pinigai yra laikomos beveik neturinčiomis ryšio su realia ekonomika. Dažnai jos žinomos tik kaip egzistuojančios žaidimuose ar kitose uždaroje bendruomenėse. Tokias valiutas galima išleisti tik perkant virtualioje bendruomenėje siūlomas virtualias prekes ir paslaugas, o ja neturėtų būti prekiaujama už tos bendruomenės ribų. Geriausiai iliustruoti uždaras virtualiųjų valiutų schemas galėtų *World of Warcraft (WoW)* žaidimas, kuriame auksas yra virtuali valiuta, reikalingas kaip mainų priemonė, leidžianti žaidėjams pasiekti kitus, aukštesnius lygius. Taip pat ir pačiame žaidime yra sudaroma galimybė užsidirbti minėtojo aukso. Pirkti ir parduoti *WoW* auksą realiame pasaulyje griežtai draudžiama pagal žaidimo kūrėjų nustatytas sąlygas.³⁸

Antroji virtualiosios valiutos rūšis vadinama - virtualiųjų valiutų schemas su vienakrypčiais srautais, kuriuose virtualias valiutas galima įsigyti už realius pinigus pagal nustatytą kursą, tačiau jų negalima keisti ar jomis prekiauti su kitais naudotojais. Konvertavimo sąlygas nustato sistemos savininkas. Tokio tipo schema leidžia grynuosius pinigus pirmiausia naudoti virtualioms prekėms ir paslaugoms pirkti, tačiau jie taip pat gali būti naudojami realioms produktams ar paslaugoms pirkti. Šioje situacijoje geras pavyzdys būtų Nintendo sukurta virtualių pinigų sistema, vadinama *Nintendo taškais*, kurią galima išleisti Nintendo parduotuvėse ir žaidimuose. Vartotojai gali įsigyti taškų kortele internetu arba parduotuvėje naudodami *Nintendo taškų* kortelę, tačiau taškų negalima iškeisti į grynuosius pinigus.³⁹ Tokios vienakryptės schemas virtualiosios valiutos gali būti laikomos keliančiomis tarpinę riziką, daugiausia naudotojams ir

³⁶ Acuña, Gonzalo Arias, Pulla, Andres Sanchez, The Digital Currency Challenge for the Regulatory Regime, Centro de Estudios en Derecho Informático • Universidad de Chile, ISSN 0719-2584, vol. 5 núm. 2 (2016), pągs. 173-209

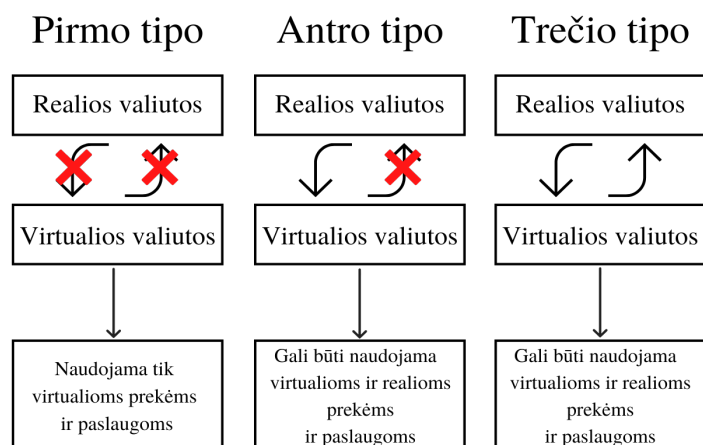
³⁷ European Central Bank; Virtual currency schemes – a further analysis; 6 psl., 2015 m., <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

³⁸ *Ibid.*

³⁹ European Central Bank, Virtual Currency Schemes, 14 psl., 2012 m., <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

kitiems rinkos dalyviams. Nors galimas teisėtų mokėjimo priemonių keitimas į virtualiąją valiutą didina rizikos lygį, bendrą riziką vis tiek galima laikyti vidutine, nes vienakryptes schemas paprastai kontroliuoja centrinis subjektas.⁴⁰

Schemas su dvikrypčiais srautais yra trečioji ir paskutinė virtualiosios valiutos forma. Vartotojai gali pirkti ir parduoti virtualias valiutas pagal savo valiutos kursą. Išitraukimo į realų pasaulį požiūriu tokios virtualios valiutos yra identiškos bet kuriai kitai konvertuojamai valiutai. Šios sistemos leidžia pirkti tiek virtualius, tiek fizinius produktus ir paslaugas. *Lindeno doleris (L\$)* yra viena iš tokių valiutos rūšių, naudojama virtualiame pasaulyje *Second Life*. *Second Life* turi savo „ekonomiką“, kurioje naudotojai gali tarpusavyje prekiauti produktais ir paslaugomis. Tam jiems reikia *Lindeno* dolerių, kuriuos gali įsigyti už realius pinigus, o jų kainą nustato valiutų prekybos rinka. Vartotojai gali iškeisti savo *Linden Dollars* į tikrus pinigus juos parduodami.⁴¹ Šios virtualios valiutos su dvikrypčiais srautais dėl konvertuojamo pobūdžio turi didžiausią rizikos potencialą. Todėl naudotojai ir kiti rinkos dalyviai gali susidurti su papildoma rizika, pavyzdžiui, nepastovumu, anonimiškumu ir nesąžiningais rinkos dalyviais. Augant šio tipo virtualių valiutų pripažinimui ir didėjant sandorių apimčiai, jos gali kelia grėsmę bendram rinkos ir kainų stabilumui, o tai didina riziką rinkoms ir reguliavimo institucijoms.⁴²



Pav. nr. 1 Virtualių valiutų schemas. Adaptuota iš European Central Bank, *Virtual Currency Schemes*, 2012

Kaip matyti, ECB skirsto virtualiąsias valiutas pagal *fiat* pinigų srautus į virtualiųjų valiutų sektorių ir iš jo. Pagal šį scenarijų FATF atsižvelgia į virtualiosios valiutos gebėjimą būti pakeistai į *fiat* pinigus, taip pat į virtualiosios valiutos organizacinę struktūrą. Konvertuojamos bei

⁴⁰ Vandezande, Niels, Virtual currencies under EU anti-money laundering law, 2017

⁴¹ European Central Bank, Virtual Currency Schemes, 14 psl., 2012 m.,

<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

⁴² Vandezande, Niels, Virtual currencies under EU anti-money laundering law, 2017

nekonvertuojamos virtualiosios valiutos skirstomos į dvi grupes: centralizuotas ir necentralizuotas.⁴³

Konvertuojamosios virtualios valiutos, dar vadinamos atviromis virtualiomis valiutomis, gali turėti tokią pačią vertę kaip ir tikri pinigai ir gali būti už juos parduodami. Du pavyzdžiai - bitkoinai ir minėtieji *Linden doleriai*. Nekonvertuojamoji virtualioji valiuta, dar vadinama uždarąja virtualia valiuta, apsiriboja naudojimu vienoje virtualioje srityje, pavyzdžiui, masiniuose daugelio žaidėjų internetiniuose vaidmenų žaidimuose, ir pagal jos naudojimą kontroliuojančius teisės aktus negali būti iškeista į fiat pinigus, pavyzdžiui, kaip taip pat jau minėtas *World of Warcraft* auksas.⁴⁴

Visos nekonvertuojamos virtualiosios valiutos pagal apibrėžimą yra centralizuotos: jas išleidžia centrinė įstaiga, kuri nustato apribojimus, pagal kurias valiutos yra nekonvertuojamos. Kita vertus, konvertuojamosios virtualiosios valiutos skirstomos į centralizuotas arba decentralizuotas. Konvertuojamųjų centralizuotų virtualiųjų valiutų sistemą kontroliuoja viena administracinė institucija. Administratorius yra trečioji šalis, kuri išleidžia pinigus, nustato jų naudojimo taisykles, tvarko centrinę mokėjimų apskaitą ir turi teisę išpirkti valiutą, t. y. išimti ją iš apyvartos. Keičiamos virtualiosios valiutos kursas gali būti kintamas, tokiu atveju jį nustato virtualiosios valiutos pasiūla ir paklausa rinkoje. Tačiau jis gali būti ir fiksuotas - administratorius nustato fiksuotą vertę *fiat* pinigais arba kitu tikru vertės matu, pavyzdžiui, auksu.⁴⁵

Decentralizuotos virtualiosios valiutos, kitaip yra vadinamos kriptovaliutomis - tai paskirstytos atviro kodo, matematikos pagrindu sukurtos lygiavertės virtualiosios valiutos, neturinčios centrinės administruojančios institucijos, centrinės stebėsenos ar priežiūros. Tokių valiutų pavyzdžiai yra geriausia žinomas *Bitcoin*, taip pat *LiteCoin* ar *Ripple*.⁴⁶

Taigi apibendrinant, palyginus ECB ir FATF klasifikaciją, skirtingai nei ECB, FATF pagal grupavimą tiek uždaras, tiek vienkryptes virtualias valiutas laiko nekonvertuojamomis. ECB klasifikacija remiasi į santykį su realia ekonomika, kai tuo metu FATF remiasi į valiutos gebėjimą būti konvertuotai. O atsižvelgiant į valiutų pobūdį ir santykį su ekonomika ar gebėjimą būti konvertuojamoms, galima nustatyti tokių virtualių valiutų keliamas grėsmes.

⁴³ FATF, Virtual Currencies, Key Definitions and Potential AML/CTF Risk, 4 psl., 2014 m., <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

⁴⁴ *Ibid.*

⁴⁵ *Ibid.*, 5 psl.

⁴⁶ *Ibid.*, 5 psl.

1.4.1 Apibendrinti virtualių valiutų požymiai

Atsižvelgiant į tai, kas išdėstyta pirmiau, akivaizdu, kad universalaus virtualių valiutų apibrėžimo nėra. Galima matyti bendrą tendenciją ir sutarimą, kad virtualios valiutos yra skaitmeninė vertės išraiška ir galima išskirti šias joms būdingas savybes:

- Virtualios valiutos egzistuoja tik elektroniniu, skaitmeniniu pavidalu, yra skaitmeninės vertės atvaizdavimo forma
- Virtualios valiutos yra sukurtos privačių asmenų
- Virtualios valiutos gali būti centralizuotos arba decentralizuotos, neturinčios vieno reguliatoriaus
- Lengvai juda tarp valstybių, nėra apribotos šalių sienų

1.5 Virtualiųjų valiutų technologiniai ypatumai

Kitas svarbus uždavinys yra suprasti virtualių valiutų technologinį veikimo pagrindą. 2022 m. sausio mėn. duomenimis rinkoje buvo daugiau nei 17 000 virtualių valiutų ir akivaizdu, kad jų skaičius tik didėja.⁴⁷ Didžioji dalis egzistuojančių virtualių valiutų, tarp jų žinoma, didžiausią rinkos dalį, t. y. daugiau nei 40% užimantis Bitcoin, yra sukurta remiantis *blockchain* arba kitaip vadinama blokų grandinės technologija. Atsižvelgiant į blokų grandinės technologijos populiarumą ir naudojimo dažnumą, todėl svarbu aptarti būtent paskirstytųjų duomenų technologijos mechanizmą, blokų grandinės technologijos sampratą, veikimo principus.

Terminas blokų grandinės technologija reiškia tam tikrą paskirstytųjų duomenų technologiją (angl. *distributed ledger technology*, DLT). Pasak Pasaulio banko grupės, DLT technologija sukurta siekiant užtikrinti, kad bet kokios rūšies turtą internetu perleistų tik tikrieji jo savininkai ir kad toks turtas nebūtų perleistas daugiau nei vieną kartą. Šiame kontekste turtas yra apibrėžiamas kaip virtuali nuosavybė, turinti piniginę vertę.⁴⁸

DLT sąlyginai yra naujas duomenų rinkimo ir platinimo įvairiose duomenų saugyklose (registruose) metodas, kai visi duomenys yra identiški ir juos tvarko bei kontroliuoja paskirstytas kompiuterių sistemų, vadinamų mazgais, tinklas. Paskirstytąją duomenų bazę, pasižyminčią tam tikromis savybėmis, galima laikyti DLT. Šioje vietoje atsižvelgiant, kad yra blokų grandinė - tai tam tikra paskirstyta duomenų rūšis, kurioje naudojami kriptografiniai ir algoritminiai metodai,

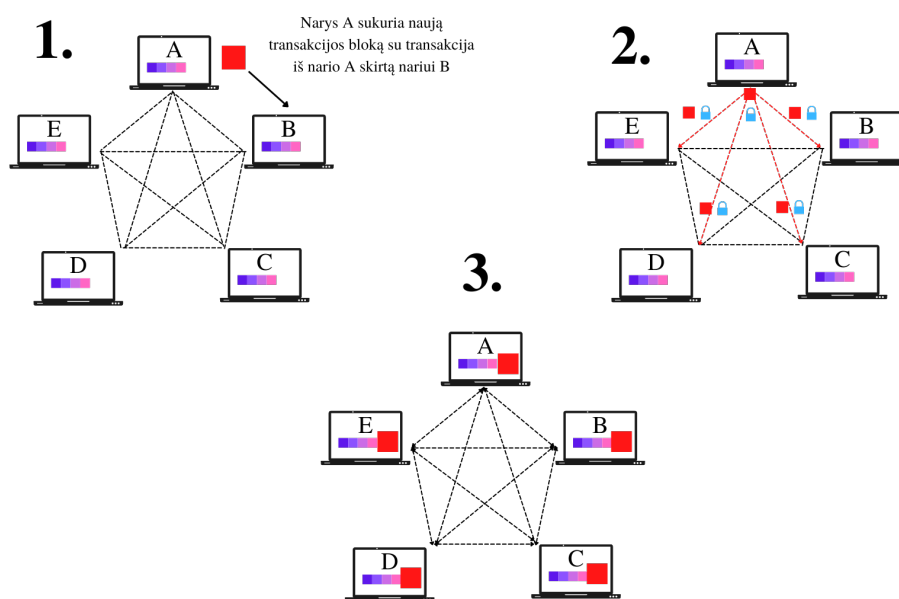
⁴⁷ Coin Market Cap, <https://coinmarketcap.com>

⁴⁸ International Bank for Reconstruction and Development / The World Bank, Distributed Ledger Technology (DLT) and Blockchain, 1 psl., 2017 m., <https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=5>

kad būtų sukurta ir patvirtinta nuolat didėjanti duomenų struktūra, kuri yra vadinamųjų sandorių blokų grandinė - blokų registras.⁴⁹

Vienas iš narių (mazgų) inicijuoja naujus duomenų bazės papildymus, sukurdamas naują duomenų bloką, pavyzdžiui, sandorių įrašų rinkinį ir išplatina informaciją apie šį naują duomenų bloką visame tinkle, užšifruodamas duomenis, kad sandorių duomenys būtų konfidencialūs, o bloko galiojimą bendrai nustato visi tinklo nariai, taikydami iš anksto nustatytą algoritminį patvirtinimo metodą, dar vadinamą konsensuso metodą. Tik patvirtinus naują bloką visi dalyviai gali jį įtraukti į savo atitinkamus registrus. Kiekvienas registro pakeitimas yra replikuojamas visame tinkle, taip užtikrinant, kad kiekvienas tinklo narys visada turėtų pilną, identišką paskirtų duomenų kopiją. Šis metodas gali būti naudojamas bet kokio turto, kurį galima atvaizduoti skaitmeniniu būdu, sandorių apskaitai.⁵⁰

Tad du pagrindiniai ir DLT pagrįstos infrastruktūros požymiai yra: galimybė saugoti, registruoti ir keisti informacija skaitmeniniu pavidalu tarp skirtingų sandorio šalių be centrinio registratoriaus ir užtikrinti, kad nebūtų dvigubo išleidimo, kai tas pats turtas negalėtų būti siunčiamas kelioms šalims.



Pav. nr. 2 DLT paremtų blokų grandinės technologijos veikimo principas. **1.** Blokų grandinėmis grindžiamos DLT sistemos yra sudarytos iš duomenų blokų grandinės, kurią sudaro tik priedai. Vienas iš narių (mazgų) inicijuoja naujus duomenų bazės papildymus, sukurdamas naują duomenų bloką, apimantį daugybę sandorių įrašų. **2.** Informacija apie šį naują duomenų bloką dalijamasi visame tinkle, kuriame yra užšifruoti duomenys, kad sandorio duomenys nebūtų viešai skelbiami. **3.** Visi tinklo dalyviai kolektyviai nustato bloko galiojimą pagal iš anksto nustatytą algoritminį patvirtinimo metodą (konsensuso mechanizmą). Tik po patvirtinimo visi dalyviai įtraukia naują bloką į savo atitinkamus registrus. Naudojant šį mechanizmą kiekvienas registro duomenų pakeitimas kopijuojamas visame tinkle ir kiekvienas tinklo narys bet kuriuo metu turi pilną, identišką visos duomenų kopiją. *Adaptuota iš The World Bank, Distributed Ledger Technology (DLT) and Blockchain, 2017*

⁴⁹ *Ibid.*

⁵⁰ *Ibid.*

1.5.1 Blokų grandinės technologijos samprata

Aptarus paskirstytųjų duomenų technologiją, svarbu išsiaiškinti blokų grandinės veikimo principą. Kaip jau minėta anksčiau, blokų grandinė yra tam tikra paskirstytųjų duomenų technologijos rūšis. Pačią blokų grandinės technologiją apibendrintai galima būtų įvardinti, kaip paskirstytųjų duomenų technologiją, kurioje kriptografija ir specializuotos matematinės procedūros naudojamos generuoti ir patvirtinti nuolat didėjančią duomenų struktūrą, į kurią galima tik įtraukti duomenis, sandorių blokų pavidalu, ir iš kurios negalima ištrinti esamų duomenų.⁵¹ Blokų grandinės technologiją galima laikyti daugialype technologija.

Pirmiausia, prieš tai minėtas konsensusas pasiekiamas leidimų neturinčiose arba kitaip atvirose, blokų grandinėse, taikant decentralizuotą protokolą teoriškai dalyvaujant neribotam dalyvių (mazgų) skaičiui. Išskyrus pseudoniminį identifikatorių, leidimo neturinčiuose protokoluose nereikia, kad asmuo atskleistų savo tapatybę. Be to, dalyviai gali laisvai gauti naujus identifikatorius, atsisakyti senųjų, valdyti daugybę identifikatorių ir bet kuriuo metu prisijungti prie tinklo arba iš jo pasitraukti, nereikalaudami išankstinio centrinės institucijos leidimo. Šioje vietoje, reikalingas tik kompiuteris su programine įranga. Dėl to atvirosiomis blokų grandinėmis negalima pilnai pasitikėti jų kontekste, nes jų nariai išlieka anonimiški ir dažnai nepasiekiami blokų grandinei nepriklausančioms teisėsaugos organizacijoms, pavyzdžiui, reguliavimo institucijų arba pasiekimo kaina yra labai aukšta ir kelianti technologinių iššūkių.⁵²

Leidimais grindžiamoms blokų grandinėms, skirtingai nei blokų grandinėms be leidimų, prieš prisijungiant prie tinklo reikia, kad mazgai būtų patvirtinti tinklo administratoriaus. Kadangi patvirtinimo procedūra paprastai reikalauja, kad mazgai būtų visiškai atviri dėl savo tapatybės, leidimais grindžiamų blokų grandinių konsensuso procesai reiškia bent tam tikrą pasitikėjimą.⁵³ Tokių projektų, kaip *Ethereum* ir *Hyperledger* debiutas 2013 m., kartu su sparčiu bitkoinų plitimu, paskatino pirmaujančius pasaulio įsteigti R3 Corda, kurios misija – „*kurti bankininkystės ateitį ir naują prekybos pasaulį*“.⁵⁴ R3 Corda yra keičiamo dydžio, leidimais pagrįsta tarp vartotojų paskirstytųjų duomenų technologijos platforma, leidžianti kurti taikomas programas, skatinančias ir užtikrinančias skaitmeninį pasitikėjimą tarp šalių reguliuojamose rinkose.⁵⁵

⁵¹ Singh, Sunil Kumar *et al.*, *Blockchain Technology: Introduction, Integration and Security Issues with IoT*, 2021 m.,

⁵² Bakos, Yannis, Halaburda, Hanna, *Permissioned vs Permissionless Blockchains: Tradeoffs in Trust and Performance*, Working Paper, 2021 m.

⁵³ *Ibid.*

⁵⁴ Helliard, Christine V. *et al.*, *Permissionless and permissioned blockchain diffusion*, *International Journal of Information Management*, 2020 m.

⁵⁵ Corda, <https://www.corda.net>

	Leidimų neturinčios blokų grandinės	Leidimus turinčios blokų grandinės
Administratorius	Nėra jokio centrinio administratoriaus	Turi tam tikrą išorinį administravimą
Prieiga	Prisijungti gali kiekvienas	Prisijungti gali iš anksto atrinkti dalyviai
Pasitikėjimo lygmuo	Tinklo nariai neprivalo pasitikėti vieni kitais	Aukštesnis pasitikėjimo lygmuo tarp narių
Atvirtumas	Registras yra atvirtas ir prieinamas visiems tinklo nariams	Galimi skirtingi registro atvirumo ir skaidrumo lygiai
Saugumas	Saugumas dėl plataus pasiskirstymo dideliame tinkle	Saugumas naudojant prieigos kontrolę kartu su DLT mažesnio masto tinkluose
Identifikavimas	Vartotojo tapatybė anoniminė arba apsaugota slaptyvardžiais	Savininkas ir (arba) administratorius paprastai reikalauja patvirtinti tapatybę
Turtas	Paprastai: kriptovaliutos. Tačiau galimi ir tokie variantai, kai naudojamas žetonas, kuris gali atstovauti bet kokią turtą	Bet koks turtas
Teisėta nuosavybė	Teisinės problemos dėl nuosavybės nebuvimo, nes joks juridinis subjektas nevaldo ir nekontroliuoja registro	Didesnis teisinis nuosavybės aiškumas, nes savininkas ir (arba) administratorius paprastai yra juridinis asmuo.
Pavyzdžiai	Bitcoin	R3's Corda, Hyperledger

Lentelė nr. 1 Leidimus turinčių bei leidimų neturinčių blokų grandinių palyginimas. Adaptuota iš *The World Bank, Distributed Ledger Technology (DLT) and Blockchain, 2017*

1.5.2 Blokų grandinės technologijos veikimo pagrindai

Išsiaiškinus technologijos sampratą, blokų grandinės veikimo principą lengviausiai iliustruoti bei perteikti pasinaudojant Bitcoin veikimo mechanizmu.

Pirmiausia, bitkoinai pagrįsti kriptografiniais įrodymais, o ne pasitikėjimu trečiąja šalimi, kad ši palengvintų internetinį sandorį tarp dviejų sutinkančių šalių. Kiekvienam sandoriui apsaugoti naudojamas skaitmeninis parašas. Tai reikėtų suprasti taip, kad kiekvienas sandoris

(sukurtas naujas blokas), siunčiamas su gavėjo viešuoju raktu, kuris naudojamas dviem tikslais: pirma, kaip viešai žinomas blokų grandinės tinklo adresas, ir, antra, skaitmeniniam parašui patikrinti, taip patvirtinant siuntėjo tapatybę. Taigi sandoris skaitmeniniu parašu pasirašomas siuntėjo privačiuoju raktu, kuris yra užšifruotas, ir taip sandoris skaitmeniniu parašu pasirašomas siuntėjo. Norėdamas gauti prieigą prie turto, savininkas turi įrodyti, kad turi privatųjį raktą.⁵⁶ Naudodamas siuntėjo viešąjį raktą, skaitmeninį turtą gaunantis subjektas patvirtina skaitmeninį parašą, taigi ir atitinkamo privataus rakto nuosavybę. Kiekvienas sandoris transliuojamas visiems Bitcoin tinklo mazgams ir po patikrinimo užregistruojamas viešajame registre, kitaip tariant, į blokų grandinę įtraukiamas naujas blokas. Kiekvienas sandoris turi būti patikrintas prieš jį registruojant, o tai reiškia, kad prieš registruodamas kiekvieną sandorį tikrintojas turi patvirtinti du dalykus:

1. Siuntėjas yra kriptovaliutos savininkas - tikrinamas sandorio skaitmeninis parašas.
2. Siuntėjas savo sąskaitoje turi pakankamą kriptovaliutų kiekį: kiekvienas sandoris tikrinamas pagal siuntėjo sąskaitą, viešąjį raktą ir viešąjį registrą, siekiant įsitikinti, kad siuntėjas savo sąskaitoje turi pakankamai turto.⁵⁷

Vartotojų viešieji bei privatieji raktai gali būti saugomi skaitmeninėse arba elektroninėse piniginėse, kurios išskiriamos į *šaltąsias* bei *karštojas* saugyklas. Šaltoji saugykla skirta padėti apsaugoti saugomą virtualią valiutą nuo įsilaužimų ir vagysčių, nes yra naudojama neprisijungus prie interneto. Karštoji saugykla reiškia internetinę piniginę, tad kadangi ji prijungta prie interneto, karštoji saugykla yra labiau pažeidžiama įsilaužimo ir (arba) vagystės atžvilgiu.⁵⁸

Akivaizdu, kad vienas iš svarbiausių šios technologijos išskirtinumų yra tas, kad ji pašalina tarpininką ir taip decentralizuoja sistemą. Įprastomis aplinkybėmis finansų įstaigos, pavyzdžiui, bankai ir mokėjimo įstaigos, veikia kaip patikima trečioji šalis, kuri apdoroja elektroninius sandorius ir tarpininkauja juos atliekant. Tokios patikimos trečiosios šalys yra atsakingos už sandorių patvirtinimą, apsaugą ir išsaugojimą. Taip yra todėl, kad kiekviename internetiniame sandoryje garantuotai yra tam tikras sukčiavimo procentas, dėl kurio reikia finansinio sandorio tarpininkavimo, todėl didėja sandorių sąnaudos.⁵⁹

⁵⁶ International Bank for Reconstruction and Development / The World Bank, Distributed Ledger Technology (DLT) and Blockchain, 9 psl., 2017 m., <https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=5>

⁵⁷ Crosby, Michael, et al., BlockChain Technology Beyond Bitcoin, Sutardja Center for Entrepreneurship & Technology Technical Report, 6-7 psl., 2015 m.

⁵⁸ FATF, Virtual Currencies, Key Definitions and Potential AML/CTF Risk, 7 psl., 2014 m., <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

⁵⁹ Crosby, Michael, et al., BlockChain Technology Beyond Bitcoin, Sutardja Center for Entrepreneurship & Technology Technical Report, 6 psl., 2015 m.

1.5.3 *Proof-of-Work* ir *Proof-of-Stake*: blokų grandinės technologijos principai patikimumo sprendimo problema

TAB Mokėjimų ir rinkos infrastruktūrų komitetas įspėjo, kad virtualiosios valiutos, pagrįstos paskirstytų duomenų technologija, turi pasiekti tinklo dalyvių sutarimą, kad būtų užtikrintas registro unikalumas, o tinkle būtų platinama tik viena registro versija su sandorių ir likučių istorija. Virtualiųjų valiutų pripažinimui gali kilti pavojus, jei ilgą laiką išliks daug pagrindinio registro versijų arba jei sutarimo mechanizmai bus neteisingi. Kai kurie dalyviai gali siekti gauti naudos iš registro įvesdami netikrus sandorius ir priversdami kitus dalyvius patvirtinti netikrų duomenų autentiškumą.⁶⁰ Todėl šioje vietoje ypač svarbus anksčiau jau minėtas konsensuso mechanizmas, kuris yra neatsiejama blokų grandinės technologijos dalis, nes bet kuris blokų grandinės tinklo dalyvis gali teikti pasiūlymą į grandinę įtraukti naujus duomenis. Tad siekiant užtikrinti, jog naujai siūloma informacija yra patikima ir galiojanti, tinklo mazgai privalo pasiekti konsensuą. Pats mechanizmas yra iš anksto nustatytas algoritminis patvirtinimo metodas ir svarbus tam, kad blokai grandinėje būtų išdėstomi teisingai, nes vienu metu sistemoje gali būti sukurtas didelis skaičius naujų blokų, taip pat siekiant užtikrinti, kad nebūtų dvigubo išleidimo, kai tas pats turtas nebūtų pervedamas daugiau nei vieną kartą. Šioje vietoje yra du geriausiai žinomi konsensuso principo pasiekimo būdai: (1) *Proof-of-Work* (liet. *darbo įrodymo*) ir (2) *Proof-of-Stake* (liet. *statymo įrodymo*).⁶¹

Šifravimo ir skaičiavimo galios derinys darbo įrodymo sistemoje užtikrina konsensuą ir palaiko blokų grandinėje saugomų duomenų teisėtumą - šis procesas vadinamas kasyba (angl. *mining*). Siekdami įrodyti, kad blokas galioja ir kad darbas buvo atliktas, tinklo mazgai, dar vadinami kasėjais, naudoja skaičiavimo galią sandoriams patvirtinti ir įsitikinti, kad siuntėjas turi pakankamai išteklių ir neišlaidauja du kartus. Jie dažnai varžosi sprenddami protokolo kriptografinius uždavinius, kurie laikui bėgant tampa vis sudėtingesni ir reikalauja vis daugiau elektros energijos. Šiuo atveju laikoma, kad pirmasis uždavinį išsprendęs kasėjas įvykdė užduotį ir gauna protokolo atlygį bei teisę surinkti visus sandorių mokesčius.⁶² Šiuo principu pagrįstas ir bitkoinas.

Proof-of-Stake protokolas yra PoW alternatyva. Jis suteikia sprendimų priėmimo teisę sistemos suinteresuotosioms šalims, kurios vadinamos nebe kasėjais, o kaldintojais arba

⁶⁰ Bank for International Settlements, Committee on payments and market infrastructures, Digital currencies, 8 psl., 2015 m., <https://www.bis.org/cpmi/publ/d137.pdf>

⁶¹ European Parliament, Prof. Dr. Robby HOUBEN, Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion, 18 psl., 2018, <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>

⁶² Seang, Sothearath, Torre, Dominique, Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies, 2019 m.

tvirtintojais. Skirtingai nei PoW protokolas, kuris leidžia bet kam tapti kasėju ir dalyvauti procese, PoS protokolas draudžia bet kam prisijungti prie tinklo. Mazgai gali dalyvauti kaldinimo procese, tikrinti sandorius ir gaminti blokus tik tada, jei turi grynujų pinigų arba indėlį tinkle. Be kita ko, nuo PoW metodo, šioje situacijoje kriptografiniams galvosūkiams spręsti nereikia jokios skaičiavimo galios. Valiutų generavimo procese nėra jokio formalaus mokėjimo, nes tvirtintojai gauna mokesčius iš naudotojų ir jiems atlyginama taip pat, kaip ir tradiciniam tarpininkui. Dėl to, kad tvirtintojai uždirba tik mokesčius už sandorius, galima išvengti situacijos, kai generuojami tušti blokai, nes tvirtintojai skatinami įtraukti kuo daugiau galiojančių sandorių, kad gautų kuo didesnę naudą.⁶³

1.6 Virtualių valiutų rinkos dalyviai

Kovos su pinigų plovimu ir terorizmo finansavimu taisyklės gali būti nukreiptos į kriptovaliutos emitentą, kaip pirmąjį galimą adresatą. Kriptovaliutą galima inicijuoti dviem būdais. Pirmiausia iniciatorius - vienas asmuo arba asmenų grupė gali sukurti naują blokų grandinę ir nemokamai išdalyti naujas virtualias valiutas. Antra, naujai sukurtas virtualias valiutas emitentas gali parduoti kaip dalį pirminio monetų siūlymo (angl. *Initial Coin Offering, ICO*), skirto lėšoms pritraukti. Dauguma pirkėjų už virtualias valiutas moka kitomis virtualiomis valiutomis. Tam tikrais atvejais pirkėjas turi galimybę atsiskaityti ir *fiat* pinigais. Platinamos virtualios valiutos gali būti sukurti remiantis nauja ir savita blokų grandine arba prekybai naudojamos esamos blokų grandinės technologijos.⁶⁴

Virtualių valiutų rinka savo dalyvių pobūdžiu stipriai skiriasi nuo mums įprastų finansinių rinkų dalyvių. Visuomenėje tikriausiai geriausiai žinomi *kasėjai*, tačiau yra žymiai daugiau dalyvių, kaip, pavyzdžiui, prekybos platformos, piniginės paslaugų teikėjai ir kita. Jų identifikavimas yra svarbus ir reguliacinei analizei.⁶⁵

Vartotojai FATF rizikos vertinimu pagrįsto požiūrio į virtualiąsias valiutas vadove apibūdinami kaip asmenys, kurie gauna virtualiąją valiutą ir naudoja ją realioms ar virtualiems produktams ar paslaugoms pirkti arba pervedimams kitam asmeniui asmeniniam naudojimui perduoti, arba kurie virtualiąją valiutą laiko kaip investiciją. Šie naudotojai turi tris virtualios valiutos įsigijimo galimybes. Pirmiausia, įsigydami virtualią valiutą už realius pinigus per keityklas arba virtualios valiutos administratorių. Antrasis būdas - kai asmuo užsiima veikla,

⁶³ *Ibid.*

⁶⁴ Haffke, Lars, et al. Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them, 2020

⁶⁵ European Parliament, Prof. Dr. Robby HOUBEN, Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion, 24 psl., 2018, <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>

pavyzdžiui, prekiauja produktais ar paslaugomis, ir gauna užmokestį virtualia valiuta. Galiausiai, naudojant decentralizuotas virtualiąsias valiutas, naudotojai gali gauti valiutą ją kasdami.⁶⁶ Taip pat virtualių valiutų gavimas yra galimas dovanos pavidalu, iš kito virtualios valiutos naudotojo.

Kasėjais (angl. *miners*) gali būti fiziniai arba juridiniai asmenys. Jų dalyvavimą decentralizuotame virtualiosios valiutos tinkle apibrėžia tai, kad jie naudoja specializuotą programinę įrangą matematinėms lygtims spręsti pagal darbo įrodymo mechanizmą, kuriuo patvirtinami virtualiosios valiutos sandoriai.⁶⁷ Dėl šios priežasties, kasėjai yra labai svarbūs virtualių valiutų sistemos komponentai, nes jie atsakingi už nepatvirtintų sandorių sujungimą į naujus blokus ir jų įtraukimą į viešą registrą (blokų grandinę). Kiekvienas teisėtas blokas, kurį kasėjas įtraukia į blokų grandinę, suteikia ne tik atlygį, bet ir apsaugo nuo dvigubo išleidimo rizikos.⁶⁸ Kasėjai tuo pat metu gali būti ir vartotojais, kai jie ir generuoja virtualias valiutas savo tikslams. Tačiau kasėjai neapsiriboja buvimu tik vartotojais, jie taip pat gali dalyvauti rinkoje kaip virtualios valiutos keityklos, t. y. parduodami savo iškastą virtualią valiutą už realius pinigus arba už kitos rūšies virtualią valiutą.⁶⁹

Nuo kasėjų pereinant prie keityklų - keitykla taip gali būti fizinis arba juridinis asmuo, kuris už mokesť prekiauja virtualiosiomis valiutomis ir keičia jas į realias valiutas, kitas virtualiąsias valiutas ir kartais net tauriuosius metalus. Keityklos dažnai leidžia naudoti įvairius mokėjimo būdus, įskaitant grynuosius pinigus, pervedimus ir kitas virtualiąsias valiutas. Asmenys dažnai naudojami keityklomis savo virtualiųjų valiutų sąskaitoms papildyti ir lėšoms atsiimti.⁷⁰ Keityklų sektorius buvo pirmasis virtualių valiutų versle ir tebėra vienas iš didžiausių tiek pagal įmonių dydį, tiek pagal darbuotojų skaičių. Taip pat, keityklos yra labai svarbios virtualių valiutų ekonomikai, nes jos yra prekybos, likvidumo ir kainų nustatymo platforma.⁷¹

Kalbant apie piniginių paslaugų teikėjus, pirmiausiai derėtų apibrėžti virtualiąsias pinigines kaip mechanizmą, kuris, kaip minėta, gali būti arba nebūti susietas su internetu ir yra skirtas virtualiajai valiutai laikyti, saugoti arba pervesti. Piniginių paslaugų teikėjas - tai subjektas, siūlantis pinigines paslaugas virtualiosioms valiutomis. Be to, kaip minėta anksčiau, piniginėje gali būti naudotojo privatūs raktai, kurie leidžia naudotojui išleisti virtualiąją valiutą, susietą su virtualiosios valiutos adresu blokų grandinėje. Piniginės teikėjas sudaro sąlygas dalyvauti virtualiųjų valiutų sistemoje, supaprastindamas virtualiųjų valiutų operacijas naudotojams, keitykloms ir prekiautojams.⁷² Be to, kad piniginėse gali būti suteikiama naudotojo sąsaja, skirta

⁶⁶ FATF, Guidance for risk-based approach, Virtual Currencies, 29 psl., 2015

⁶⁷ FATF, Virtual Currencies, Key Definitions and Potential AML/CTF Risk, 7 psl., 2014

⁶⁸ Hileman, Garrick, Rauchs, Michel, Global Cryptocurrency Benchmarking Study, 86 psl., 2017, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-04-20-global-cryptocurrency-benchmarking-study.pdf>

⁶⁹ FATF, Virtual Currencies, Key Definitions and Potential AML/CTF Risk, 7 psl., 2014

⁷⁰ FATF, Guidance for risk-based approach, Virtual Currencies, 29 psl., 2015

⁷¹ Hileman, Garrick, Rauchs, Michel, Global Cryptocurrency Benchmarking Study, 28 psl., 2017,

⁷² FATF, Virtual Currencies, Key Definitions and Potential AML/CTF Risk, 8 psl., 2014

virtualių valiutų turimų lėšų likučiui stebėti, jos gali būti panaudojamos ir tam tikroms funkcijoms automatizuoti, pavyzdžiui, apskaičiuoti, kokį mokestį reikia sumokėti, kad būtų pasiektas pageidaujamas sandorio patvirtinimo laikas.⁷³

Prekybos platformos veikia kaip rinkos, jungiančios virtualiųjų valiutų pirkėjus ir pardavėjus, suteikdamos jiems galimybę mainytis ir siūlyti vieni kitiems virtualias valiutas, tačiau pačios nedalyvauja jokioje virtualiųjų valiutų prekyboje ar pardavime.⁷⁴

Galiausiai, maišymo paslaugų teikėjai, gali padėti išlaikyti sandorių anonimiškumą. Tokios paslaugos keičia daugelio virtualių valiutų savininkų srautus, kad būtų paslėptas tikrasis lėšų šaltinis ir būtų sunku nustatyti ryšį tarp siuntėjo ir gavėjo. Šis metodas buvo sukurtas atsižvelgiant, kad virtualiųjų valiutų sandoriai yra viešai registruojami, todėl jei pavyksta nustatyti neteisėtą sandorį, tampa sąlyginai lengva atsekti visus ankstesnius dviejų sąskaitų kontaktus. Pasinaudojus maišymo paslaugų teikėjų tarpininkavimu, tarp dviejų pradinių adresų nebelieka jokio ryšio.⁷⁵

⁷³ Hileman, Garrick, Rauchs, Michel, Global Cryptocurrency Benchmarking Study, 48 psl., 2017

⁷⁴ European Central Bank; Virtual currency schemes – a further analysis, 8 psl., 2015

⁷⁵ Sofia Del Monaco, Money mules and tumblers: money laundering during the cryptocurrency era, EUDIFIN RESEARCH WORKING PAPER NO. 10, 12 psl., 2020,
https://www.unive.it/pag/fileadmin/user_upload/dipartimenti/economia/doc-eng/eudifin/wp/WP10.pdf

2. Pinigų plovimas

Aptarus virtualias valiutas, išsiaiškinus jų sąvoką bei veikimo principą, ši darbo dalis skiriama teorinei pinigų plovimo nusikaltimo analizei. Bus pradedama nuo pinigų plovimo termino aptarimo, jo reikšmės, taip pat apibūdinamas pinigų plovimo procesas, nusikaltėlių taikomos strategijos bei metodai. Be kita ko bus paaiškinamas pinigų plovimo procesas pasitelkiant virtualias valiutas, identifikuojami reguliaciniai iššūkiai.

2.1 Pinigų plovimo sąvoka

Visų pirma, reikėtų suprasti, kas yra pinigų plovimas. Taigi, pinigų plovimo sąvoka pati pakankamai gerai paaiškina savo reikšmę, nes paprastai tariant, pinigų plovimas yra būdas, kaip nešvarius pinigus paversti švariais. Išplečiant aiškinimą, tai nusikalstamu būdu įgautų pajamų šaltinių nuslėpimas, siekiant lėšas panaudoti teisėtai ar neteisėtai veiklai vykdyti.⁷⁶

Viename iš žinomiausių, Sertifikuotų kovos su pinigų plovimu specialistų asociacijos (angl. *Association of Certified Anti-Money Laundering Specialists*, ACAMS), studijų vadove aprašant, kas yra pinigų plovimas, aiškinama, kai iš nusikalstamos veiklos gaunamas didelis pelnas, joje dalyvaujantis asmuo ar grupė ieško būdų, kaip panaudoti lėšas neatkreipiant dėmesio į pagrindinę veiklą ar asmenis, dalyvavusius gaunant tokį pelną. Nusikaltėliai šio tikslo siekia slėpdami lėšų šaltinį, keisdami jų formą arba perkeldami pinigus į vietą, kur mažiau tikėtina, kad jie patrauks dėmesį. Nusikalstama veikla, dėl kurios plaunami pinigai (t. y. pirminiai nusikaltimai), gali būti, bet neapsiriboti: neteisėtas ginklų pardavimas, prekyba narkotikais, kontrabanda ir kita su organizuotu nusikalstamumu susijusi veikla, turto pasisavinimas, prekyba pasinaudojant viešai neatskleista informacija, kyšininkavimas ir kompiuterinio sukčiavimo schemas.⁷⁷ Be kita ko, daugiau nei prieš 30 metų įkurta tarptautinė institucija FATF, dar savo veiklos pradžioje sugebėjo įrodyti, jog pinigų plovimas nėra susijęs tik su grynujų pinigų operacijomis. Pinigų plovimas gali būti vykdomas praktiškai per bet kokią priemonę, finansų įstaigą ar verslą.⁷⁸

2.2 Trys pagrindiniai pinigų plovimo ciklo etapai

Pinigų plovimo nusikaltimas pats iš savęs gali būti pavadintas daugiasluoksniu nusikaltimu, dažnai susijęs su sudėtingais sandoriais, kuriuos sunku atskirti. Tačiau įprasta manyti, kad pinigų plovimas vyksta trimis etapais:

⁷⁶ ACAMS, Study Guide, Cams Certification Exam, 1 psl., 2016 m.

⁷⁷ *Ibid.*

⁷⁸ *Ibid.*

- Pirmasis etapas - **įdarbinimas, įdėjimas**
- Antrasis etapas – **sluoksniavimas, užmaskavimas**
- Trečiasis etapas – **integracija**

Pirmuoju etapu lėšos patenka į finansų sistemą (vykdomas įdėjimas), antruoju etapu atliekami sudėtingi finansiniai sandoriai, kuriais siekiama paslėpti turto pėdsakus ir užtikrinti anonimiškumą (sluoksniavimas), o paskutiniuoju etapu pinigai integruojami į teisėtą ekonominę ir finansinę sistemą ir prilyginami visam kitam sistemos turtui (integracija).⁷⁹

Įdėjimas, visų pirma, reiškia fizinį disponavimą grynaisiais pinigais ar kitomis vertybėmis, gautomis neteisėtais veiksmais. Šio etapo metu pinigų plovėjas neteisėtai gautą naudą įtraukia į finansų sistemą. Dažnai tai atliekama cirkuliuojant pinigines lėšas per oficialias finansų įstaigas, kazino ir kitas vietas bei užsienio įmones. Patekimo į apyvartą pavyzdžiai galėtų būti tokie:

- Lėšų maišymas: neteisėtų ir teisėtų lėšų derinimas, pavyzdžiui, pinigų, gautų iš neteisėto narkotikų pardavimo, įnešimas į vietinį restoraną, turintį didelį grynųjų pinigų srautą.
- Užsienio valiutos keitimas: Užsienio valiutos pirkimas naudojant nelegaliai gautus pinigus.
- Sumų padalinimas: Nedidelių grynųjų pinigų įmokų darymas ir jų perkėlimas į įvairias banko sąskaitas, siekiant išvengti prievolių teikti ataskaitas.
- Valiutos kontrabanda: grynųjų pinigų ar kitų piniginių priemonių gabenimas per valstybės sieną.
- Paskolos: Teisėtos paskolos gražinamos išplautais grynaisiais pinigais.⁸⁰

Po pirmojo grynųjų pinigų pervedimo prasideda **sluoksniavimo ir maskavimo** etapas. Kaip nurodyta anksčiau, šio etapo tikslas - nuslėpti nusikaltimo pelną taip, kad nebūtų žinomas grynųjų pinigų šaltinis ir dabartinė būklė. Paprastai tai neteisėtai gautus pinigus investuoti į ką nors teisėto, kad lėšos atrodytų švarios. Kitais atvejais reikia daug sudėtingesnės sandorių grandinės.

Antrasis etapas apima nusikalstamu būdu gautų pajamų pavertimą kita forma ir sudėtingų finansinių operacijų sluoksnių sukūrimą, siekiant nuslėpti piniginių lėšų šaltinį ir nuosavybę. Antrąjį etapą geriausiai atspindi toliau pateikti pavyzdžiai:

- Elektroninių pinigų pervedimas tarp šalių ir jų sklaida sudėtingose finansinėse schemose
- Lėšų pervedimai tarp finansų įstaigų arba tarp sąskaitų toje pačioje įstaigoje
- Grynųjų pinigų konvertavimas į pinigines priemones

⁷⁹ GOPAC, Anti Money Laundering Action Guide for Parliamentarians, 6 psl., 2012 m., http://www.gopacnetwork.org/Docs/GOPAC_AML_ActionGuide_EN.pdf

⁸⁰ ACAMS, Study Guide, Cams Certification Exam, 2016 m.

- Didelės vertės prekių perpardavimas ir iš anksto apmokėtos prieigos ar sukauptos vertės daiktų perpardavimas

- Investavimas į nekilnojamąjį turtą ar kitus teisėtus verslus
- Investavimas į akcijas, obligacijas ir gyvybės draudimo produktus
- Fiktyvių bendrovių steigimas siekiant nuslėpti galutinį faktinį savininką ir jo turtą⁸¹

Paskutinis etapas yra **integracija** - neteisėto turto pakartotinis įtraukimas į sistemą per įprastą įmonės ar asmeninę veiklą. Šis etapas apima išplautų pinigų naudojimą tariamai teisėtiems sandoriams, siekiant sukurti teisėtumo iliuziją. Pavyzdžiui, pinigų plovėjas gali investuoti į nekilnojamąjį turtą, bankų įmones ir pan. Integracijos proceso metu gana sunku atskirti teisėtą ir neteisėtą turtą. Šis etapas leidžia pinigų plovėjui didinti savo turtą naudojant nusikalstamos veiklos pelną. Integraciją dažnai sunku aptikti tol, kol neatsiranda didelių neatitikimų tarp asmens ar įmonės tikrojo darbo, verslo ar investicinių operacijų ir jų pajamų ar turto.⁸²

2.2.1 Pinigų plovimo metodai

Pinigų plovimas, kitaip nei dauguma kitų nusikaltimų, vykdomų visame pasaulyje, išsiskiria pasižymėjimu daugybe skirtingų metodų, taip pat dideliu skaičiumi įvairių dalyvių ar vietų, kur gali būti vykdomas. Tad, nors nusikaltėliai nuolatos atranda naujų būdų, kai nuslėpti neteisėtu būdu įgautas lėšas, kaip, pavyzdžiui, panaudojant virtualias valiutas, tačiau tik žinant tradicinius pinigų plovimo metodus, teisminės ir reguliacinės institucijos, galės veiksmingai užkirsti kelią pinigų plovimui.

Teigiama, kad grynujų pinigų kontrabanda yra viena iš pirmųjų pinigų plovimo formų, taip pat labai veiksmingas ir dažnai naudojamas plovimo būdas. Kontrabanda apima didelių grynujų pinigų sumų slėpimą bagaže, automobiliuose, laivuose ar kroviniuose, tačiau tuo neapsiriboja. Sluoksniavimo procesas prasideda, kai gryniesi pinigai pasiekia šalį, kurioje galioja griežtos banko paslapties taisyklės.⁸³

Dar viena pinigų plovimo rūšis vadinama smurfingu (angl. *smurfing*) - tai didelio finansinio sandorio padalijimas į kelis mažesnius sandorius, siekiant išvengti reguliavimo arba teisėsaugos institucijų patikrinimo. Paprastai kiekvieno sandorio vertė yra mažesnė už tam tikrą teisės aktais nustatytą ribą, dėl kurios finansų įstaigai nereikia pranešti apie įtartinus sandorius ir (arba) veiklą vyriausybinei institucijai.⁸⁴

⁸¹ ACAMS, Study Guide, Cams Certification Exam, 2016 m.

⁸² *Ibid.*

⁸³ Kevin, Sullivan, Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business Managers, 2015 m.

⁸⁴ European Police Office, Why is cash still king?, 51 psl., 2015 m.,

Į smurfingą panašus būdas, vadinamas struktūrizavimu, kurio metu dideli banko įnašai padalijami į kelis mažesnius įnašus, kad būtų išvengta finansų įstaigų pranešimo apie įtartą veiklą reikalavimų.⁸⁵

Pinigų plovimas per azartinių lošimų įstaigas yra vienas iš dažniausių būdų neteisėtai gautas pajamas paslėpti ir sluoksniuoti.⁸⁶ Natūralu, kad kazino yra daug grynųjų pinigų turinčios įmonės, kurios ne kartą buvo išnaudotos nusikalstamu būdu gautam pelnui plauti. Kiti įtaisai, pavyzdžiui, lošimo automatai, šiuolaikiniais laikais vis dar populiarūs pinigų plovimui, nes jie nereguliuojami: nėra krupjė ar kitų žaidėjų, kurie galėtų stebėti kitus žaidėjus ar vieni kitus.⁸⁷

Šešėlinės įmonės, kaip jos kartais vadinamos, yra juridiniai asmenys, kurios naudojami dėl teisėtų priežasčių, pavyzdžiui, kito verslo subjekto akcijoms ar nematerialiajam turtui laikyti. Tačiau jomis gali piktnaudžiauti neteisėtos įmonės, neturinčios tikro ekonominio tikslo, ir dažnai jas naudoja nusikaltėliai pinigų plovimo veiklai, tokiai kaip investicinių fondų schemoms, mokesčių vengimui ir vidiniam įmonių sukčiavimui. Dažnai fiktyvios įmonės naudojamos fiktyvioms sąskaitoms faktūroms, fiktyviems konsultavimo mokesčiams ir fiktyvioms paskoloms gauti.⁸⁸

Taip pat, nekilnojamojo turto sandoriai dažnai naudojami pinigų plovimo operacijose. Šiais sandoriais gali būti slepiami nusikalstamų lėšų šaltiniai, nes nekilnojamas turtas perkamas ir parduodamas fiktyviais vardais arba per fiktyvias bendroves, todėl jis gali būti patogus užstatas vėlesniems sandoriams ir pinigų plovimui.⁸⁹

Be to, prekių pirkimas gali taip pat būti naudojamas neteisėtiems mokėjimams nuslėpti. Auksas yra viena populiariausių tokių prekių, nes jis visame pasaulyje pripažįstamas kaip vertybė, suteikia anonimiškumo, greitai keičia formą ir leidžia dubliuoti sąskaitas faktūras, padirbti siuntas ir atlikti kitus nusikalstamus veiksmus. Panašus atvejis ir su meno kūrinių ir kitais vertingais daiktais, pavyzdžiui, reti pašto ženklai, gali būti patrauklūs plovimo tikslais dėl to, kad lengva sukurti netikrus pardavimo sertifikatus arba gauti jų kopijas. Taip pat, daiktai gali būti lengvai perduodami visame pasaulyje arba perparduodami už rinkos vertę siekiant įvykdyti integraciją.⁹⁰

Pinigų plovėjai taip pat gali naudotis valiutų keityklomis arba jas steigti, o tai ypač svarbu, kai kalbama apie virtualiąsias valiutas. Jei nusikaltėliai įsteigia savo valiutos keityklą, jie gali

⁸⁵ *Ibid.*

⁸⁶ Kevin, Sullivan, *Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business Managers*, 2015 m.

⁸⁷ European Police Office, *Why is cash still king?*, 39 psl., 2015

⁸⁸ FATF, *Money laundering using trust and company service providers*, 34 psl., 2010 m., <https://www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf>

⁸⁹ Reuter, Peter, Truman, Edwin M., *Chasing dirty money: The fight against money laundering*, 2004 m., Institute for international economics

⁹⁰ *Ibid.*

lengvai sukurti iliuziją, kad turi daugiau klientų nei iš tikrųjų, ir papildyti savo pajamas neteisėtai įgytu turtu. Jei įmonėms reikia tik nedidelių pinigų kiekių, kuriuos reikia iškeisti, jie gali samdyti asmenis keisti valiutas jau esamose keityklose.⁹¹

Įmonių susijungimai ir įsigijimai taip pat yra tiek pinigų plovimo sluoksniavimo, tiek ir integravimo metodas. Dėl galimybės manipuliuoti pinigų srautais, šių sandorių kainos yra gana subjektyvios, ypač įsigyjant sunkumų turinčias įmones. Tačiau taikant šį metodą pinigų plovėjams neretai kyla rizika, kad mokesčių institucijos ir komercinės veiklos priežiūros institucijos gali nuodugniai išanalizuoti sandorius.⁹²

Nelegalūs pinigai gali būti naudojami teisėtų įmonių, ypač restoranų ir barų, pinigų srautams papildyti. Papildomos lėšos tiesiog įnešamos į kasą, o vėliau nuo to sumokami mokesčiai. Įmonėse, kuriose yra daugiau sandorių dokumentacijos, sąskaitos faktūros gali būti modifikuojamos, siekiant sukurti autentiškumo įspūdį. Pavyzdžiui, naudotų automobilių prekybos įmonė gali suteikti pirkėjui nuolaidą mainais į mokėjimą grynaisiais pinigais, o tada išrašyti sąskaitą faktūrą su pradine pardavimo kaina, taip paaiškindama papildomų neteisėtų pinigų atsiradimą.

Šiek tiek pažangesnė strategija gali leisti nusikaltėliui gauti dvigubą naudą įsteigus fiktyvią, su viešai pardavinėjamomis akcijomis, bendrovę, kurios tikslas yra tikra komercinė veikla - pirma, plaunant grynuosius pinigus, sumaišytus su verslo lėšomis, ir, antra, parduodant šios bendrovės akcijas nieko neįtariantiems investuotojams.⁹³

Galiausiai, pinigų plovimas gali būti vykdomas naudojant iš anksto virtualiomis valiutomis papildytas kredito korteles. Kripto valiutų kortelės iš esmės yra iš anksto apmokėtos Visa arba Mastercard kortelės, kurias išduoda licencijuotas kortelių leidėjas. Tai kortelės, kurios palaiko oficialias valiutas ir kurias galutiniams naudotojams siūlo kortelių teikėjas, sudaręs sutartį su kortelių leidėju arba pats esantis kortelių leidėjas. Šios kortelės gali būti apibūdinamos kaip fizinės arba virtualios, priklausomai nuo to, ar jos išduodamos fiziškai, ar skaitmeniniu būdu, ir vėliau naudojamos perkant internetu arba parduotuvėse, kuriose priimami Visa arba Mastercard mokėjimai, taip pat grynujų pinigų išėmimui bankomatuose. Dažnai šios kortelės įsigyjamos naudojant suklastotus asmens tapatybės dokumentus, o tai apsunkina sandorių analizę, paslepia tikrąjį kortelės savininką ir skatina sandorių neskaidrumą.⁹⁴

⁹¹ Teichmann, F. M. Johannes, Twelve methods of money laundering, Journal of Money Laundering Control, 2017 m.

⁹² *Ibid.*

⁹³ Reuter, Peter, Truman, Edwin M., Chasing dirty money: The fight against money laundering, 2004 m., Institute for international economics

⁹⁴ Sanz-Bas, David, Carlos del Rosal, Sergio Luis Nández Alonso, and Miguel Ángel Echarte Fernández. 2021. Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. *Laws* 10: 57.

2.3 Pinigų plovimo procesas pasitelkiant virtualias valiutas

Išanalizavus dažniausiai sutinkamus pinigų plovimo metodus, šio darbo kontekste svarbu įsigilinti, kaip pinigų plovimas galėtų būti vykdomas pasitelkiant virtualias valiutas. Šiais laikais tai ypač aktualu, nes blokų grandinės bendrovės Chainalysis ataskaitoje teigiama, jog 2021 m. pasinaudodami virtualiomis valiutomis, nusikaltėliai išplovė maždaug 8,6 mlrd. dolerių. Žadą atima ne tik pats skaičius, bet ir faktas, jog tai yra 30 % daugiau nei ankstesniais metais.⁹⁵ Virtualios valiutos išties patrauklios nusikaltėliams, visų pirma dėl savo pseudoanoniškumo ir paprastumo, kuriuo naudotojai gali akimirksniu siųsti lėšas į bet kurią pasaulio vietą, nepaisant jos skaidrumo ir atsekamumo, todėl su virtualioms valiutomis pagrindinis susijęs nusikaltimas yra pinigų plovimas.⁹⁶ Ir nors finansų įstaigos per pastaruosius 40 metų palaipsniui įgijo žinių ir metodų, kaip kovoti su tradiciniu pinigų plovimu, virtualios valiutos, konkrečiau kalbant kriptovaliutos, egzistuoja tik nuo maždaug nuo 2008 m. ir vis dar yra naujas bei sudėtingas klausimas daugeliui.⁹⁷

Dažniausias skaitmeninis pinigų plovimo būdas, kai nusikaltėliai įsigyja virtualių valiutų virtualių valiutų keityklose arba už grynuosius pinigus, arba atsiskaitydami debeto kortele virtualios valiutos bankomatuose. Dažnai pirmenybė teikiama pirmajam būdai, atsižvelgiant į tai, kad dauguma virtualių valiutų bankomatų paslaugų teikėjų yra reguliuojamos organizacijos, kurioms taikomos galiojančios kovos su pinigų plovimu taisyklės. Kai sukčiai per virtualių valiutų valiutos keityklas įsigyja norimos valiutos, jie dažnai pasitelkia tarpininkus (angl. *strawman*), turinčius nepriekaištingą reputaciją, legaliai dirbančius asmenis. O siekdami dar labiau apsaugoti savo anonimiškumą, nusikaltėliai naudoja pseudonimus, anonimines pinigines ir virtualius privačius tinklus (VPN).⁹⁸

Kai tarpininkams suteikiamas patvirtinimas vykdyti skaitmeninius mainus, lėšos pirminėms monetoms (pvz., pvz., *Bitcoin*, *Etherum*) pirkti, skiriamos realia valiuta arba banko pavedimais. Vėliau šios pirminės valiutos naudojamos pirkti alternatyvias monetas, atitinkančias tam tikrus kriterijus, pavyzdžiui, užtikrina didesnę anonimiškumą. Siekdami užmaskuoti pirminės monetos pirkimą, nusikaltėliai taiko taktiką, vadinamą maišymu (angl. *mixing*, *tumbling*).⁹⁹ Tai apima naudojimą tokių paslaugų teikėjų, kaip *Bitmixer* ar *Helix*, kurie suteikia galimybę tikruosius

⁹⁵ Chainalysis, The 2022 Crypto Crime Report, 10 psl., <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>

⁹⁶ Chainalysis, The 2021 Crypto Crime Report, 4 psl., 2021, <https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>

⁹⁷ Sprenger, Pascal, Balsiger, Franziska, Anti Money Laundering Times: cryptocurrencies – game changers in many ways, KPMG, 2018 m., <https://assets.kpmg/content/dam/kpmg/ch/pdf/anti-money-laundering-in-times-of-cryptocurrency.pdf>

⁹⁸ *Ibid.*

⁹⁹ *Ibid.*

monetų adresus pakeisti į laikinus skaitmeninių piniginių adresus, kad suklaidentų blokų grandinę ir apribotų atsekamumą. Be to, yra papildomas metodas, kai fiktyvūs gavėjų adresai naudojami siekiant nukreipti sandorius į atsarginius adresus ir taip sutrikdyti registrą.¹⁰⁰

Kitame etape sumaišytos pirminės monetos pervedamos į virtualių valiutų keityklas, kad būtų galima įsigyti alternatyvių monetų, su aukštesniu privatumo lygmeniu, tokių, kaip *Verge*, *Monero*, *Dash* ar pan. Pavyzdžiui, *Monero* blokų grandinėje nerodomas nei siuntėjas, nei gavėjas, nei sandorių vertė. Joje naudojami vadinamieji slaptieji adresai arba nauji adresai, kurie skirti naudoti tik vieną kartą, siekiant užtikrinti, kad tik siuntėjas ir gavėjas turėtų prieigą prie sandorio duomenų, taip pat pasitelkiama žiedinio parašo kriptografijos forma, leidžianti pasirašyti sandorius tarp grupės naudotojų taip, kad pašaliniai asmenys negalėtų iššifruoti atskiro sandorį pasirašiusio asmens.¹⁰¹

Taigi pinigų plovėjai naudoja sluoksniavimą, kuris apima papildomų, aukštesnio privatumo lygmens monetų, kodavimo ir skaitmeninių adresų naudojimą, kad neteisėtai gautas lėšas pinigus paruoštų pakartotiniam integravimui į įprastą finansų sistemą. Išplovę neteisėtai įgautus pinigus, nusikaltėliai turi daugybę galimybių konvertuoti juos į teisėtą valiutą. Vienas iš integracijos būdų - alternatyvias monetas konvertuoti į pirmines monetas, o vėliau į realią valiutą, kurią galima pervesti į susietą banko sąskaitą. Antrasis būdas - turimas virtualias valiutas pervesti į fizinę, su internetu nesusietą, virtualios valiutos piniginę arba atspausdinti QR kodą, kurį galima pateikti bet kuriam gavėjui visame pasaulyje.¹⁰² Taigi nusikaltėliai turi nemažai būdų, kuriuos derindami tarpusavyje, gali vykdyti pinigų plovimą pasitelkiant virtualias valiutas.

2.3.1 Virtualių valiutų keliama reguliaciniai iššūkiai

Virtualios valiutos išties kelia nemažai susirūpinimo įvairioms reguliacinėms ar finansų veiklą vykdančioms įstaigoms. Pagrindinius sunkumus galima apibendrintai būtų įvardinti kaip šiuos:

Didesnis anonimiškumas arba galimybė naudotis anonimiškumą didinančiomis priemonėmis. Sandoriai dažnai prieinami internete ir atsekami iš vienos piniginės į kitą, tačiau susieti konkretų adresą ar piniginę su tam tikru asmeniu yra sudėtinga. Prie sunkumų prisideda ir tai, kad yra metodų, specialiai skirtų srautų atsekamumui apsunkinti. Jie apima anonimiškumą didinančius elementus, kaip minėtus maišytuvus ar kelių lygių šifravimą, slapčius adresus ir žiedinius parašus, ribojant prieinamos informacijos kiekį, įskaitant informaciją apie sandorio vertę

¹⁰⁰ Investopedia, Monero (XMR) Cryptocurrency, <https://www.investopedia.com/tech/introduction-monero-xmr/>

¹⁰¹ *Ibid.*

¹⁰² Sprenger, Pascal, Balsiger, Franziska, Anti Money Laundering Times: cryptocurrencies – game changers in many ways, KPMG, 2018 m., <https://assets.kpmg/content/dam/kpmg/ch/pdf/anti-money-laundering-in-times-of-cryptocurrency.pdf>

ir sandorio šalis. Kai kurie antrinę informaciją taip pat naudoja tapatybės paslėpimui, kaip kad, neleisdami nustatyti IP adresų, geolokacijos duomenų, įrenginio identifikatorių.¹⁰³

Tarpvalstybinis pobūdis ir centrinio administratoriaus nebuvimas. Virtualiosios valiutos judėjimas suteikia galimybę greitai keistis skirtingomis virtualiosiomis valiutomis, siekiant sudėtingiau užmaskuoti lėšų kilmę tarpvalstybiniame kontekste. Virtualiosios valiutos paslaugų teikėjas gali fiziškai būti vienoje jurisdikcijoje, būti registruotas kitoje, patalpinti savo serverį dar kitoje ir teikti paslaugas visame pasaulyje be centrinio valdymo administratoriaus. Tai apsunkina neteisėtų sandorių prevenciją ir finansinės žvalgybos duomenų, gautų iš pranešimų apie įtartinus sandorius, analizę, nes informacija apie atvejus gali būti fragmentiška įvairiose šalyse. Tai taip pat apsunkina teisėsaugos veiksmus, nes paprastai nėra vieno subjekto, kuris galėtų atlikti tyrimą ir į kurį būtų nukreiptas.¹⁰⁴

Nevienodas vidaus kovos su pinigų plovimu ir teroristų finansavimu priemonių taikymas. Dauguma šalių dar tik pradeda įgyvendinti atitinkamus FATF standartus, o tai sukuria didelį reguliavimo arbitražo potencialą, todėl nusikaltėliams suteikiama galimybė pasinaudoti virtualiųjų valiutų paslaugų teikėjais, įsikūrusiais arba veikiančiais šalyse, kuriose nėra arba yra minimalios virtualiųjų valiutų ir virtualiųjų valiutų paslaugų teikėjų kovos su pinigų plovimu ir terorizmo prevencija taisyklės.¹⁰⁵

2.3.2 Augantis susirūpinimas: virtualių valiutų panaudojimas terorizmo finansavimui

Atskirai galima būtų išskirti dar vieną problemą, kurią gilina virtualių valiutų naudojimas. Štai 2020 m. vyriausybės agentūros visame pasaulyje nustatė, ištyrė ir patraukė baudžiamojon atsakomybėn daugiau nei bet kada anksčiau terorizmo finansavimo schemų naudojant virtualiąsias valiutas. Bene garsiausias tų metų atvejis įvyko, kai JAV teisingumo departamentas atskleidė didžiausią kada nors iš teroristinės organizacijos konfiskuotą kriptovaliutų sumą. Atlikdamos tyrimą dėl daugelio atskirų virtualiosios valiutos įnašų operacijų, JAV vyriausybės agentūros iš teroristinėms organizacijoms ir jų finansiniams tarpininkams priklausiusių piniginių surinko daugiau kaip 1 mln. dolerių bitkoinų pavidalu.¹⁰⁶

Pirmąją kampaniją vykdė Hamas karinis sparnas Al-Qassam Brigades, kai 2019-2020 m. į ją buvo pervesta dešimčių tūkstančių dolerių vertės bitkoinų. Antrąją kampaniją vykdė Al-Qaeda

¹⁰³International Monetary Fund, Schwarz, N. Schwarz et al., Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism, 4 psl., 2021

¹⁰⁴ *Ibid.*

¹⁰⁵ *Ibid.*

¹⁰⁶ Chainalysis, The 2021 Crypto Crime Report, 93 psl., 2021 m., <https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>

ir kelios su ja susijusios grupuotės Sirijoje, kurios naudojos Idlibe, Sirijoje, įsikūrusia virtualių valiutų keitykla *BitcoinTransfer*, kad išplautų aukas ir paskirstytų jas tarp dalyvaujančių grupių.¹⁰⁷

Al Qaeda pavyzdys puikiai iliustruoja, koks sudėtingas yra šis procesas, nes jame dalyvauja žmonių grupės, turinčios sudėtingus tinklus ir net kelias pinigų rinkimo infrastruktūras. Teroristinės grupės internete dažnai prisistatydavo kaip labdaros organizacijos, skirtos Sirijai, tačiau daugelyje jų žinučių ir privačių pranešimų buvo aiškiai matyti, kad aukos bus naudojamos džihadistų grupių ginklams įsigyti. Tarp dalyvavusių teroristinių organizacijų buvo ir šios:

Malhama Tactical - privatus karinis rangovas iš Uzbekistano, rengęs mokymus kelioms teroristinėms grupuotėms Sirijoje ir kovojęs kartu su jomis.

Al Sadaqah - socialinėje žiniasklaidoje aktyviai veikianti Sirijos organizacija, kuri skelbiasi esanti labdaros organizacija, tačiau yra įsitraukusi į terorizmo finansavimą.

Al Ikhwa - teroristinė organizacija, dokumentais patvirtintais ryšiais susijusi su tokiomis teroristinėmis grupuotėmis kaip *Hay'at Tahrir al-Sham*.

Taip pat buvo bendraujama ir lėšų rinkimas vykdomas tokiuose socialiniuose tinkluose, kaip *Telegram*.¹⁰⁸

Visos šios organizacijos naudojo daugiasluoksnes operacijas, kad nuslėptų šių mokėjimų pervedimą į pagrindinį adresų centrą, iš kurio pinigai vėliau paskirstomi kitoms organizacijoms. Atlikus blokų grandinės tyrimus nustatyta, kad pagrindinis centras buvo *BitcoinTransfer* keitykla. Nuo 2018 m. gruodžio mėn. iki 2020 m. liepos mėn. per *BitcoinTransfer* buvo atlikta sandorių už maždaug 280 000 JAV dolerių, kurių didžioji dalis buvo susijusi su terorizmo finansavimu.¹⁰⁹

¹⁰⁷ *Ibid.* 95 psl.

¹⁰⁸ *Ibid.* 97 psl.

¹⁰⁹ *Ibid.* 97 psl.

3. PINIGŲ PLOVIMO PANAUDOJANT VIRTUALIAS VALIUTAS TEISINIAI IR REGULIACINIAI MECHANIZMAI

Pirmoje darbo dalyje atlikus virtualių valiutų sąvokų, jų atskirties nuo realių pinigų analizę, taip pat supratęs veikimo mechanizmus bei išsiaiškinęs pinigų plovimo apibrėžtį ir dažniausiai taikomus metodus, svarbu aptarti pinigų plovimo prevencijos priemones bei jų teisinę raidą. Dėl šios priežasties, antroje darbo dalyje bus siekiama apžvelgti pinigų plovimo teisinio reglamentavimo pakopas, siekiant pateikti išvadas apie šiuo metu galiojantį reguliavimą, įvertinti jo efektyvumą.

Galima teigti, jog reguliacinė raida geriausiai atspindi laike kilusias problemas, jų sprendimo būdus bei galimai leidžia prognozuoti ateities tendencijas. Tai ypač svarbu kalbant apie virtualias valiutas, atsižvelgiant į jų sąlyginę naujumą tiek rinkoje tarp vartotojų, tiek įstatymų atžvilgiu tarptautiniu lygmeniu. Gerai reguliuojamų finansų sistemų ir paslaugų plėtra yra esminis bet kokios veiksmingos ir išsamios pinigų plovimo ir teroristų finansavimo politikos bruožas. Labai svarbu išlaikyti subalansuotą požiūrį į kovos su pinigų plovimu ir terorizmo finansavimu politiką, kuri gali turėti nenumatytą poveikį - išstumti teisėtas įmones ir klientus iš finansų sistemos. Atsižvelgiant į tai, pinigų plovimo bei pinigų plovimo, kuris apima virtualias valiutas, reglamentavimą galima būtų išskirti į šias grupes:

1. Nacionalinio lygmens teisinė sistema, kuri apima tam tikras taisykles, išdėstytas konkrečios šalies vidaus teisėje, kaip valstybės atsakingos institucijos turėtų reglamentuoja virtualias valiutas bei sprendžia su jomis susijusias pinigų plovimo keliamas problemas bei rizikas.

2. Tarptautinio lygmens teisinė sistema, kuri šiame kontekste galėtų būti išskirta į dvi grupes. Pirmiausia - minkštąją teisę (angl. *soft law*), kurią galima apibūdinti kaip įvairių neįpareigojančių normatyvinių priemonių rinkiniu, kurias šiuolaikiniuose tarptautiniuose santykiuose naudoja valstybės ir tarptautinės organizacijos. Švelniosios teisės pavyzdžiai galėtų būti rekomendacijos, gairės, elgesio kodeksai, neįpareigojančios rezoliucijos ir standartai. Antra - griežtąją teisę (angl. *hard law*), kuri reiškia teisiškai privalomus, įpareigojančius instrumentus, kurie tarptautinėje teisėje dažnai pasireiškia tarptautinių sutarčių forma.

Taigi, šioje darbo dalyje bus siekiama aptarti anksčiau nurodytas teisinio reglamentavimo grupes pinigų plovimo ir virtualių valiutų tematika, išskirti keliamus iššūkius. Be kita ko, bus aptartas *minkštosios* bei *kietosios* teisės panaudojimas pinigų plovimo problematikoje, tarpusavio santykis.

3.1 Nacionalinis požiūris

Virtualioms valiutoms populiarėjant visame pasaulyje, ypač greitai keičiasi ir jų priežiūrai bei reguliacijai, susijusiais su pinigų plovimu, numatyti teisės aktai. Nacionalinėse teisės sistemose įtvirtinami įstatymai, reglamentuojantys kompetentingų institucijų veiksmus sprendžiant pinigų plovimo bei virtualių valiutų reguliavimo problematiką. Valstybių teisinės sistemos lygmeniu šio darbo kontekste galima būtų atsižvelgti į šias kategorijas: kaip yra reglamentuojamos virtualios valiutos bei jų keityklos ir kokie teisės aktai tai daro. Taip pat, papildomai galima išskirti modelius, kuriuos šalys taiko valstybės viduje šio klausimo reguliavimui.

Visų pirma, svarbu atsakyti į klausimą ar virtualios valiutos, konkrečiai trečiajam tipui priskiriamos kriptovaliutos, yra laikomos teisėta mokėjimo priemone? Šis klausimas tiesiogiai susijęs su pirmoje darbo dalyje aptarta pinigų samprata bei apibūdinta virtualių valiutų sąvoka. Šiai dienai, didžioji dalis valstybių virtualių valiutų nelaiko teisėta atsiskaitymo priemone. Pavyzdžiui, Jungtinių Valstijų Iždo Departamento biurui priklausantis Finansinių nusikaltimų vykdymo tinklas (angl. *Financial Crimes Enforcement Network, FinCEN*), virtualias valiutas supranta, kaip mainų priemonę, kuri gali veikti kaip valiuta, tačiau neturi visų „tikrosios“ valiutos požymių, įskaitant teisėtą mokėjimo priemonės statusą.¹¹⁰ Tačiau įdomu pažymėti, jog 2018 m. byloje *Wisconsin Central Ltd. v. United States*, buvo paminėtas bitkoinas. Byla pati iš savęs nebuvo susijusi su bitkoino reguliavimo ar teisiniu statusu, teisėjas Stephen Breyer savo atskiरोjoje nuomonėje pasisakė už „platesnį pinigų supratimą“ ir bitkoinas buvo panaudotas kaip besikeičiančios pinigų prigimtys pavyzdys ir buvo išsakyta teorija, kad „galbūt vieną dieną darbuotojams bus mokama bitkoinais ar kita kriptovaliuta“.¹¹¹

Panašios nuomonės kaip ir Jungtinės Amerikos Valstijos laikosi ir dauguma kitų valstybių, kaip Kanada, Indija, Singapūras, Pietų Korėja ir kt., nepripažindamos virtualių valiutų, kaip teisėtą mokėjimo priemonę arba atsižvelgiant į Kinijos atvejį – išvis jas draudžiant. Tačiau tokios valstybės kaip Japonija ar Australija virtualias valiutas traktuoja kaip teisėtą nuosavybės tipą. Australijos vyriausybė teigia, jog su bitkoinu ar kitomis į jį panašiomis virtualiomis valiutomis susiję sandoriai gali turėti mokestinių pasekmių ir šios rinkos dalyviai turi tvarkyti įrašus, kurie susiję su tokių valiutų sandoriais.¹¹² Atsižvelgiant apie mokestinę į virtualių valiutų pusę, 2015 m. Europos Sąjungos Teisingumo Teismas byloje *Skatteverket v. David Hedqvist*, nusprendė, jog nors

¹¹⁰ FinCEN, *FinCEN Guidance, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, 2019, 7 psl., <https://www.fincen.gov/sites/default/files/201905/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>

¹¹¹ Supreme Court of The United States, *Wisconsin Central Ltd. Et Al. v. United States*, 2017, https://www.supremecourt.gov/opinions/17pdf/17-530_6537.pdf

¹¹² Australian Government, Australian Taxation Office, *Tax treatment of cryptocurrencies*, 2020, <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/>

PVM taikomas visose Europos Sąjungos valstybėse narėse tačiau iki to laiko ES nebuvo nuoseklaus požiūrio, nes vienose valstybėse bitkoinai buvo apmokestinami PVM, kitur - neapmokestinami. Tad minėtuojų sprendimu padėtis buvo pakeista ir pareikalauta, kad valstybės narės neapmokestintų bitkoino tiekimo PVM.¹¹³

Atkreiptinas dėmesys, jog 2021 m. Salvadoras tapo pirmąją valstybe pasaulyje, kuri bitkoiną pripažino teisėta mokėjimo priemone.¹¹⁴ Tačiau Tarptautinis valiutos fondas patarė valdžios institucijoms sumažinti teisės aktų dėl bitkoinų taikymo sritį, nesuteikiant šiai virtualiai valiutai teisėtos valiutos statuso, nes kriptovaliutos kaip teisėtos mokėjimo priemonės priėmimas kelia didelę riziką finansų ir rinkos vientisumui, finansiniam stabilumui.¹¹⁵ Šalies prezidentas Nayib Bukele į tai atsako, jog tai būdas pasiūlyti skaitmeninę bankininkystę didžiajai daliai gyventojų (apie 70 proc.), kurie dar nesinaudoja banko paslaugomis.¹¹⁶

Antrasis svarbus klausimas, kaip šalys nacionaliniu lygmeniu reguliuoja virtualių valiutų keityklas. Kaip ir pirmasis klausimas, tai taip tiesiogiai susijęs su pirmąja darbo dalimi, kurioje aptariamas pinigų plovimo procesas pasitelkiant virtualias valiutas, nes dažniausiai nusikaltėliai virtualias valiutas, kurias vėliau panaudoja pinigų plovimo nusikaltimo vykdyme, įsigyja virtualių valiutų keityklose. Tačiau požiūris į tą patį objektą net valstybės viduje gali būti fragmentuotas. Kaip pavyzdys galėtų būti, jog Jungtinėse Amerikos Valstijose kriptovaliutų keityklų veikla yra teisėta ir reguliuojama, o joms taikomas Bankų slaptumo įstatymas (angl. *Bank Secrecy Act, BSA*). Dėl to, kad FinCEN virtualių valiutų keityklų paslaugų teikėjus priskiria tai pačiai reguliavimo kategorijai kaip ir tradicinius pinigų pardavėjus ir jiems taikomos visos tos pačios taisyklės. Tuo tarpu, Jungtinių Valstijų Vertybinių popierių ir biržos komisija (angl. *Securities and Exchange Commission*) pareiškė, kad kriptovaliutos yra laikomos vertybiniais popieriais ir kad vertybinių popierių taisyklės taikomos visoms skaitmeninėms piniginėms ir keitykloms. Kita vertus, Prekių ateities sandorių komisija (angl. *The Commodities Futures Trading Commission*,) laikosi paprastesnio požiūrio, bitkoinus klasifikuodama kaip biržos prekes ir leisdama viešai prekiauti kriptovaliutų išvestinėmis finansinėmis priemonėmis.¹¹⁷ Panašiai ir daugelyje kitų pasaulio valstybių, virtualių valiutų keityklos yra laikomos legaliomis ir prižiūrimos įvairių reguliacinių kūnų. Tačiau, didžiausia savo gyventojų skaičiumi valstybė – Kinija – ir vėl išsiskiria. 2021 m.

¹¹³ Europos Teisingumo Teismas, *Skatteverket v. David Hedqvist*, C-264/14, 2015

¹¹⁴ The Wall Street Journal, *El Salvador Becomes First Country to Adopt Bitcoin as National Currency*, 2021, <https://www.wsj.com/articles/bitcoin-comes-to-el-salvador-first-country-to-adopt-crypto-as-national-currency-11631005200>

¹¹⁵ International Monetary Fund, *PRESS RELEASE NO. 22/13, IMF Executive Board Concludes 2021 Article IV Consultation with El Salvador*, 2022, <https://www.imf.org/en/News/Articles/2022/01/25/pr2213-el-salvador-imf-executive-board-concludes-2021-article-iv-consultation>

¹¹⁶ EuroNews, *The IMF warns El Salvador to drop Bitcoin as a legal currency*, 2022, <https://www.euronews.com/next/2022/01/26/the-imf-warns-el-salvador-to-drop-bitcoin-as-a-legal-currency>

¹¹⁷ S. Sackheim, Michael, et. al., *The Virtual Currency Regulation Review: USA*, 4th edition, The Law Reviews, 2021

šalis uždraudė bet kokią vietinę kriptovaliutų kasybą, o kiek vėliau iš esmės uždraudė naudotis visomis kriptovaliutų keityklomis, kurios apėmė tiek tarptautines, tiek vietines keityklas.¹¹⁸ Panašiai buvo pasielgta ir Indijoje, kai Indijos rezervų bankas uždraudė bankams ir kitoms reguliuojamoms finansų įstaigoms prekiauti virtualiosiomis valiutomis arba vykdyti atsiskaitymus jomis. Dėl plačios šios taisyklės taikymo srities prekyba virtualiomis valiutomis šalies keityklose buvo uždrausta, o veikusios keityklos buvo priverstos nutraukti verslą. Tačiau 2020 m. valstybės Aukščiausiasis Teismas pripažino draudimą neteisėtu ir jį panaikino, leisdamas keitykloms atnaujinti savo veiklą.¹¹⁹

Galiausiai, kalbant apie nacionalinį reglamentavimo lygmenį, svarbu įvertinti ir jau egzistuojančius, valstybių taikomus virtualių valiutų reguliavimo metodus. Tam tikri metodai gali būti derinami ir (arba) laikui bėgant skirtis, atsižvelgiant į konkrečios rinkos reguliavimo institucijų tikslus. Pažymėtina, jog nėra vieno bendro, visuotinai paplitusio pasaulinio virtualių valiutų reguliavimo modelio, kaip bus matoma vėlesnėje analizėje, esamų virtualių valiutų reguliavimo režimai daugiausia dėmesio skiria *fiat* valiutų ir virtualių valiutų tarpusavio sąveikai.

Vienas iš reguliavimo metodų yra vadinamas „laukimo ir stebėjimo“ - kaip pavadinimas ir atspindi, yra taikoma laukimo ir stebėjimo strategija, kai naujiems sektoriams nesuteikiamas aiškus reguliavimas, kad jie galėtų vystytis. Dažnai derinamos galiojančios taisyklės ir reglamentai bei kruopšti stebėseną, todėl su laiku sukuriamą reguliavimo sistemą, kurioje atsižvelgiama į riziką. Tokiu metodu siekiama užkirsti kelią paveikti naujoves dar prieš joms prasidedant, tačiau reguliaciniai kūnai išlieka budrūs ir pasirengę įsikišti, jei to reikia stabilumui palaikyti.¹²⁰ Robert Herian teigimu, šis reguliavimo metodas labiau atspindi motyvacijos ar energijos stoką visoje reguliavimo aplinkoje, o jurisdikcijos reaguoja skirtingu greičiu kai kurios lėtai, kitos skubiau. Šio teisės mokslininko nuomone, toks laukimo ir stebėjimo politika gali būti priešinga inovatyvumui arba sukurti vakuumą, kurį inovatyvumas greitai užpildo, o tai dažnai aiškiai matyti iš verslininkų ir kitų suinteresuotųjų šalių raginimų, kad valdžia neslopintų inovacijų, ir tuo metu didėja atotrūkis tarp teisės, reguliavimo ir valdymo bei blokų grandinės.¹²¹

Antrasis požiūris, vadinamas licencijavimu, numato, kad virtualiomis valiutomis vykdomoms operacijoms turėtų būti taikomi jų kilmės šalies ir (arba) šalies, kurioje jos vykdomos,

¹¹⁸ Bloomberg, China Widens Ban on Crypto Transactions; Bitcoin Tumbles, 2021, <https://www.bloomberg.com/news/articles/2021-09-24/china-deems-all-crypto-related-transactions-illegal-in-crackdown>

¹¹⁹ Parikh, Vaibhav, Reddy, Jaideep, The Virtual Currency Regulation Review: India, 4th edition, The Law Reviews, 2021

¹²⁰ World Economic Forum, Global Future Council on Cryptocurrencies, Navigating Cryptocurrency Regulation: An Industry Perspective on the Insights and Tools Needed to Shape Balanced Crypto Regulation, Community Paper, 18 psl., 2021 m., https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

¹²¹ Herian, R. Taking Blockchain Seriously. *Law Critique* 29, 163–171 (2018).

licencijavimo įstatymai. Norint vykdyti atitinkamas operacijas toje šalyje, pirmiausia reikia gauti reikiamą licenciją iš institucijos, dažniausiai finansinių paslaugų reguliavimo institucijos. G. Badmus licencijavimą pažymi kaip kokybinį barjerą, atrankos procesą, pabrėžiant, jog, kad sąlygos prieš išduodant licenciją būtų pakankamai griežtos, kad apribotų riziką, kad paslaugų teikėjai būtų įpareigoti laikytis minimalių standartų, bet ne apsunkinančios, kad slopintų inovacijas.¹²² Vienas iš tokių pavyzdžių - Niujorko BitLicence, kurią 2015 m. priėmė Niujorko finansinių paslaugų departamentas. BitLicense reguliavimo sistemoje nurodyta, kad ji apima virtualiųjų valiutų verslo operacijas, kurios daro poveikį Niujorkui arba jo gyventojams. Bet kuri įmonė, vykdanči virtualiosios valiutos verslo operacijas Niujorko valstijoje, arba bet kuris asmuo, gyvenantis, esantis, turintis verslo vietą ar užsiimantis verslu Niujorke, privalo pateikti paraišką BitLicense licencijai gauti.¹²³

Trečioji strategija yra viešojo ir privačiojo sektorių partnerystės strategija, kartais vadinama subalansuota arba rizikos ir proporcingumo metodu. Ši strategija - tai politikos formuotojų, reguliavimo institucijų ir privačiojo sektoriaus bendradarbiavimas kuriant ir įgyvendinant teisės aktus ir reglamentus, kuriais siekiama skatinti kūrybingą finansų sistemą per darbo grupes ir (arba) inovacijų centrus. Reguliuotojams šis požiūris naudingas, nes jie gali geriau suprasti inovatorius ir greičiau prisitaikyti prie sparčiai kintančios aplinkos, o įmonėms šis požiūris naudingas, nes jos gali greičiau prisitaikyti prie reguliuotojams rūpimų klausimų, kad apsaugotų ekosistemos vientisumą ir reputacijos vertę. Ši strategija taikoma ir Europos Sąjungoje.¹²⁴ Reguliavimo institucijų, technologų, saugumo specialistų ir kitų susijusių suinteresuotųjų šalių (pvz., akademinės bendruomenės ir pramonės atstovų) bendradarbiavimas gali padėti priežiūros institucijoms tinkamai suvokti įvairių konsensuso procesų poveikį.¹²⁵ Tačiau, kaip pastebi Eduard Hofert, reguliavimo institucijoms siekiant spręsti valdymo mechanizmų klausimus, taikant bendro reguliavimo režimą tarp privačių tinklus organizuojančių subjektų ir valstybės institucijų, reikia atsižvelgti į ir tai, kad daugumą tinklų jau valdo kūrėjų bendruomenė, kuri vykdo reikšmingą atitinkamos paskirstytųjų duomenų registro kontrolę, ir tvirtintojai, kurie privalo įgyvendinti visus siūlomus protokolo pakeitimus. Todėl priežiūros institucijai gali būti naudingiau sąveikauti su jau

¹²² Badmus, Gbolahan, A Global Guide to a Crypto Exchange Regulatory Framework, Journal of Law, Policy and Globalization, Vol.90, 2019

¹²³ The Commonwealth, Regulatory Guidance on Virtual Currencies, 15 psl., 2019, https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/D16999_GPD_Virtual_Currncs.pdf

¹²⁴ World Economic Forum, Global Future Council on Cryptocurrencies, Navigating Cryptocurrency Regulation: An Industry Perspective on the Insights and Tools Needed to Shape Balanced Crypto Regulation, Community Paper, 18 psl., 2021 m., https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

¹²⁵ Bains, Parma, International Monetary Fund Blockchain Consensus Mechanisms: A Primer for Supervisors, 18 psl., 2022

egzistuojančiomis valdymo institucijomis, nei lygiagrečiai skatinti institucionalizavimo procesą.¹²⁶

Ribojantis požiūris egzistuoja tada, kai tam tikri arba visi veiksmai naudojant virtualią valiutą yra draudžiami teisės aktais. Šia strategiją taiko ir Kinijos Liaudies Respublika, kuri kaip aptarta anksčiau, visiškai nepripažįsta virtualių valiutų, draudžia jas bei bet kokią susijusią veiklą. Įdomu, jog Pietų Korėjos teisingumo ministerija taip pat svarstė galimybę uždrausti bitkoinus ir kitas virtualiąsias valiutas, tačiau vėliau patikslino, kad tai buvo tiesioginis anoniminės prekybos virtualiosiomis valiutomis apribojimas ir priminimas, kad visose rinkose turi būti laikomasi užsienio valiutos keitimo ir pinigų plovimo taisyklių, o ateityje, jei šios priemonės bus neveiksmingos siekiant užkirsti kelią blogai praktikai Pietų Korėjos virtualiųjų valiutų rinkoje, galimas ir visiškas draudimas.¹²⁷ Tačiau Kavid Singh teigimu, reguliavimo metodas siekiant uždrausti virtualias valiutas yra per daug griežtas. Visų pirma, autorius pabrėžia, jog, pavyzdžiui, bitkoinas padidina finansavimo prieinamumą skurdžiose vietovėse, leidžia atlikti pigias pinigines perlaidas, sumažina sandorių išlaidas įmonėms. Net ir siekiant visiškai uždrausti virtualias valiutas, to beveik neįmanoma užtikrinti. Teisės mokslininko teigimu, toks griežtas požiūris greičiausiai išnaikins tik teisėtus bitkoinų naudojimo būdus, o slaptus sandorius atliekantys naudotojai liks nepalieti.¹²⁸

Visapusiškas reguliavimo metodas apima konkretaus reglamento, skirto reguliuojamų įmonių veiklai prižiūrėti, parengimą ir vykdymą. Tai gali apimti minėtą licencijos reikalavimą, taip pat ataskaitų teikimo ir kovos su pinigų plovimu bei terorizmo finansavimo reikalavimus finansinių paslaugų teikėjams prievolių vykdymą, taip pat užsienio valiutos keitimo limitus užsienio sandoriams ir kt.¹²⁹

Galiausiai, rinkos savireguliacijos veikla gali turėti didelę įtaką reguliavimo režimų formavimui. Rinkos savireguliacijos idėja yra ta, kad dalyviai dažnai turi daugiau patirties ir žinių nei reguliavimo institucijos, todėl yra motyvuoti kurti veiksmingą ir patikimą sistemą. Šiems režimams būdingas pavojus, kad dalyviai pradės priimti taisykles, kuriomis gina savo, o ne klientų interesus. Todėl egzistuoja nominaliai autoritetingas hibridas - priverstinis savireguliavimas, kai savireguliavimas vyksta stebint oficialioms valdžios reguliavimo institucijoms. Tokiomis aplinkybėmis pramonė atlieka didžiąją dalį savireguliacijos kasdienių pareigų, tačiau reguliavimo

¹²⁶ Hofert, Eduard, Regulating virtual currencies, IMFS Working Paper Series, No. 130, Goethe University Frankfurt, Institute for Monetary and Financial Stability (IMFS), Frankfurt a. M., 2019

¹²⁷ The Commonwealth, Regulatory Guidance on Virtual Currencies, 17 psl., 2019, https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/D16999_GPD_Virtual_Currncs.pdf

¹²⁸ Singh, Kavid, The New Wild West: Preventing Money Laundering in the Bitcoin Network, 2015

¹²⁹ World Economic Forum, Global Future Council on Cryptocurrencies, Navigating Cryptocurrency Regulation: An Industry Perspective on the Insights and Tools Needed to Shape Balanced Crypto Regulation, Community Paper, 18 psl., 2021 m., https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

institucija išlaiko įgaliojimus keisti režimą arba užtikrinti papildomą vykdymą. Šiam modeliui pritaria ir E. Fletcher et al., pažymima, jog privačiojo sektoriaus subjektai neturi įgaliojimų atlikti areštus ar skirti baudas. Todėl reguliavimas turėtų būti įgyvendinamas pritaikant strategiją, kai su įmonės, teikiančios paslaugas virtualiomis valiutomis, pavyzdžiui, pirkimo, pardavimo, pervedimo, mainų ar saugojimo paslaugas, sukurtų bendruomenės standartus ir geriausios praktikos taisyklės. Valstybių vyriausybės šioje vietoje veiktų kaip teisinė jėga ir užtikrintų tam tikrus vykdymo užtikrinimo mechanizmus.¹³⁰

3.3 Internacionalizacija

Pinigų plovimui būdingas tarpvalstybinis pobūdis ir, kaip išskirta pirmoje darbo dalyje, ši nusikalstama veikla pasižymi įvairiapusiškumu. Atsižvelgiant į tai, nacionalinė kovos su pinigų plovimu politika yra ne tik valstybių vidaus reikalas, tačiau persikėlė ir į tarptautinį lygmenį. Būtent tarptautinių teisinių priemonių formavimasis buvo šios tendencijos, pasireiškusių nusikaltimų prevencijos ir kontrolės pastangų globalizacija, pradžia.

Internacionalizacija paprastai suprantama kaip viešojo bei privačiojo sektoriaus bendradarbiavimas, kuris persikelia už nacionalinių ribų. Šio darbo kontekste ši sąvoka gali reikšti pastangas atkreipti tarptautinės bendruomenės dėmesį į pinigų plovimo problemą dėl įvairių priežasčių, iš kurių viena yra ta, kad ji savo pobūdžiu kelia tarptautinę riziką, o realybėje - daugialypę problematiką. Tai susideda iš to, kad pinigų plovimo nusikaltimas daromas peržengiant daugelio skirtingų jurisdikcijų sienas, o pati veikla yra dinamiška, kai pinigai pervedami į įvairias finansų įstaigas tiek šalies viduje, tiek tarptautiniu mastu. Todėl ypač svarbu kalbant apie pinigų plovimo kontrolės valdymą visame pasaulyje, kad valstybės turėtų tą pačią viziją, tikslą ir strategiją. Ne mažiau svarbu sudaryti palankesnes sąlygas tarptautiniam bendradarbiavimui užkertant kelią tokio pobūdžio nusikaltimams ir vykdant baudžiamąjį persekiojimą. Pavyzdžiui, jei viena šalis pinigų plovimą laiko nusikaltimu, o kita - ne, bus sunku palaikyti bendradarbiavimą šioje srityje. Be to, tie patys kriterijai taikomi ir tuo atveju, jei abi šalys nesutampa su ta pačia (-omis) pagrindine (-ėmis) nusikalstama veika (-omis), kuria (-iomis) grindžiama pinigų plovimo nusikalstama veikla. Todėl valstybės, kurios dalyvauja tokioje bendradarbiavimo veikloje kaip ekstradicija ar savitarpio teisinė pagalba, turi laikytis dvigubo baudžiamumo koncepcijos, pagal kurią už nusikalstamą veiką baudžiama pagal įstatymus ir prašančiojoje, ir prašomojoje šalyje.

¹³⁰ Emily Fletcher, Charles Larkin, Shaen Corbet, Countering money laundering and terrorist financing: A case for bitcoin regulation, Research in International Business and Finance, Volume 56, 2021

Todėl ypač svarbu siekti tikslo, kad pinigų plovimo prevencija būtų prižiūrima tarptautiniu mastu.¹³¹

Ženklus žingsnis į priekį tarptautiniu mastu kovojant su pinigų plovimu buvo nulemtas Jungtinių Tautų Vienos konvencijos ir Bazelio bankininkystės reglamentų komitetą. Pirmuoju atveju sprendžiamas pinigų plovimo nusikalstamo komponento internacionalizavimo klausimą, o antruoju - finansinių taisyklių, draudžiančių naudoti finansų sektorius pinigų plovimo tikslams, koncepcijos internacionalizavimo klausimą. Neretai literatūroje galima sutikti, jog remiantis W. Gilmore, šie tarptautiniai dokumentai apibūdinami kaip dvigubas pinigų plovimo sprendimas.¹³² Taip yra dėl to, kad pirmasis dokumentas ragina stiprinti represinę, baudžiamąją teisę pinigų plovimo nusikaltimo atžvilgiu, o antruoju dokumentu pripažįstama, kad finansų sistema gali ir turi atlikti veiksmingą prevencinį vaidmenį, todėl akivaizdžiai matoma, jog pinigų plovimo nusikaltimo reglamentavimas gali būti išskirtas į represinį ir prevencinį.

Tarptautinei prekybai narkotikais ir milžiniškos su ja susijusioms pinigų sumoms, patenkančioms į bankų sistemą, pasiekus epidemijos mastą, Jungtinės Tautos per Jungtinių Tautų narkotikų kontrolės programą (angl. *UNDCP*) žengė pirmąjį žingsnį kovoje su prekyba narkotikais ir pinigų plovimu - pasirašė tarptautinį susitarimą - Jungtinių Tautų konvenciją dėl kovos su neteisėta narkotinių ir psichotropinių medžiagų apyvarta, dar žinomą kaip Vienos konvenciją. Ir nors pačioje konvencijoje daugiausia kalbama apie kovos su neteisėta prekyba narkotikais priemones ir su tuo susijusius teisėsaugos sunkumus, o sąvoka pinigų plovimas nėra tiesiogiai vartojama, nepaisant to, konvencijoje šis terminas apibrėžiamas, o vyriausybės raginamos bausti už tokią praktiką.¹³³ Neteisėtų narkotinių ir psichotropinių medžiagų kriminalizavimą reglamentuoja konvencijos 3 straipsnio 1 dalies a punktas, kuriame reikalaujama, kad kiekviena šalis įpareigojama savo vidaus teisėje nustatyti išsamų su prekyba narkotikais susijusių veiklų sąrašą kaip nusikalstamas veikas. 3 straipsnio 1 dalyje b punkte minimas pinigų plovimo neteisėtumas. Pagal šį straipsnį sąvoka pinigų plovimas apibrėžiama trejopai: pirma, turto pavertimas arba perdavimas, žinant, kad toks turtas gautas iš su narkotikais susijusio nusikaltimo, siekiant nuslėpti arba užmaskuoti neteisėtą turto kilmę arba padėti bet kuriam kitam asmeniui, susijusiam su narkotikais susijusiu nusikaltimu, išvengti teisinių savo veiksmų pasekmių, antra, tikrojo turto pobūdžio, šaltinio, buvimo vietos ar paskirties nuslėpimas arba užmaskavimas ir trečia, turto įgijimas, laikymas ar naudojimas, žinant jo gavimo metu, kad toks turtas gautas iš su

¹³¹ Hanafi, A., The Internationalization Of Anti-Money Laundering and The Compliance Of States. *Jurnal Hukum IUS QUIA IUSTUM*, 20(3), 343–361, 2016

¹³² Ebikake, Emmanuel, Money laundering: an assessment of soft law as a technique for repressive and preventive anti-money laundering control, *Journal of Money Laundering Control*, Vol 19, 2016

¹³³ Al-Zaqibh, Ahmad Aqeil Mohamad, International Laws on Money Laundering, *International Journal of Social Science and Humanity*, Vol. 3, No. 1, 2013

narkotikais susijusios nusikalstamos veikos.¹³⁴ Be to, ši tarptautinė sutartis padėjo pagrindą tarptautiniam bendradarbiavimui konfiskavimo, ekstradicijos ir savitarpio teisinės pagalbos srityse skatinti ir taip tapo daugelio tarpvyriausybinių pastangų, pavyzdžiui, G7, Finansinių veiksmų darbo grupės ir kitų tarptautinių sutarčių, pavyzdžiui, Strasbūro konvencijos, Palermo konvencijos ir ES direktyvų, pagrindu.¹³⁵

Priešingai nuo Vienos konvencijos, Bazelio komiteto paskelbtos gairės dėl finansų sektoriaus reguliavimo, nėra teisiškai įpareigojančios. Minėtomis gairėmis siekiama, jog būtų tinkamai identifikuojami visi su jų įstaigomis sandorius sudarantys asmenys, taip pat bendra prasme atgrasoma nuo sandorių, kurie neatrodo teisėti ir galiausiai, kad būtų bendradarbiaujama su teisėsaugos institucijomis. Šis komitetas yra ypač svarbi pinigų plovimo nusikaltimo internacionalizacijos dalis, nes sukūrė vieną iš svarbiausių koncepcijų, pinigų plovimo nustatymui bei veiksmingai kovai su juo, vadinama – „pažink savo klientą“ (angl. *Know Your Customer, KYC*).¹³⁶

Tiek šio darbo, tiek bendrame pinigų plovimo prevencijos kontekste, kliento tapatybės įrodymas yra ypač svarbus bankams ar finansų įstaigoms prieš pradedant bendradarbiauti su savo klientais ir pagal kurį bankai ar finansų įstaigos privalo sustabdyti įtartinus sandorius ir apie juos pranešti, identifikuoju klientą.¹³⁷ Kiekvienoje institucijoje gali būti taikomas skirtingas metodai, tačiau dažniausiai jie būna gana panašūs. Visų pirma, pateikiami tokie dokumentai, kaip asmens tapatybės patvirtinančius dokumentus, taip pat gyvenamąją vietą įrodantys dokumentai. Be to, gali būti prašoma pateikti asmens nuotrauką, siekiant patikrinti ar asmens tapatybės dokumente esančios nuotrauka atitinka su kliento pateikiama nuotrauka. Tokiu būdu siekiama užtikrinti, kad asmuo nepavogė kito asmens tapatybės. Pagal griežtesnius atrankos kriterijus gali būti reikalaujama atlikti pokalbį arba atsakyti į klausimus apie savo praeitį ir pateikti tai patvirtinančius dokumentus.¹³⁸

Kaip jau minėta, kiekvieno kliento tapatybės, jurisdikcijos ir tikslų patvirtinimas yra labai svarbus kovos su pinigų plovimu programų etapas. Nepaisant virtualioms valiutoms būdingos rizikos, įmonės, teikiančios virtualių valiutų paslaugas, turėtų užtikrinti, kad jų taisyklės ir procesai leistų šią pagrindinę veiklą vykdyti taip pat užtikrintai, kaip ir teikiant įprastines paslaugas.

¹³⁴ United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Vienna, 1988

¹³⁵ Hanafi, A., The Internationalization Of Anti-Money Laundering and The Compliance Of States. *Jurnal Hukum IUS QUIA IUSTUM*, 20(3), 343–361, 2016

¹³⁶ BIS, Report by a working group comprised of members of the Basle Committee on Banking Supervision and the Offshore Group of Banking Supervisors, The Supervision of Cross-Border Banking, 1996

¹³⁷ Biryukov, Alex; Khovratovich, Dmitry; Tikhomirov, Sergei (2018): Privacy-preserving KYC on Ethereum. In: W. Prinz & P. Hoschka (Eds.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies (ISSN 2510-2591)

¹³⁸ Know Your Customer (KYC) verification guide for cryptocurrency trading, <https://bitgap.com/blog/know-your-customer-kyc-verification-guide-for-cryptocurrency-trading/>

Pagrindinė kliūtis, trukdanti priimti daugumą virtualiųjų valiutų, yra jų turėtojų pseudoanonimiškumas, todėl virtualiųjų valiutų paslaugų teikėjai neturėtų užmegzti santykių su klientu prieš tai nepatikrinę tikrosios kliento tapatybės.¹³⁹

Šiai dienai, virtualių valiutų paslaugai, leidžiančiai keisti virtualią valiutą į *fiat* valiutą, reikia atlikti deramą klientų patikrinimą. *Coinfirm* atliktas tyrimas parodė, kad didžioji dalis virtualių valiutų keityklų nėra susitvarkę savo pinigų plovimo prevencijos politikos. Buvo parodyta, kad 69 % iš 216 tirtų virtualių valiutų keityklų neturi išsamių ir skaidrių KYC procedūrų - neatsiejamos patikimos pinigų plovimo prevencijos programos dalies.¹⁴⁰

Atsižvelgiant į tai, Europos Komisija siekia sugriežtinti taikomas taisykles virtualių paslaugų teikėjams, kad tokios įmonės gautų, saugotų ir pateiktų informaciją apie pervedimuose dalyvaujančius asmenis, nepriklausomai nuo pervedimo sumos, siekiant lengviau nustatyti įtartinus sandorius ir apie juos pranešti, įšaldyti skaitmeninį turtą ir atgrasyti nuo didelės rizikos sandorių. Teigiama, kad daryti išimtis nedidelės vertės pervedimams nėra tinkama, nes virtualių valiutų naudotojai galėtų apeiti taisykles sukurdami beveik neribotą pervedimų skaičių ir taip vykdyti pinigų plovimo nusikaltimą pasitelkiant virtualias valiutas.¹⁴¹

3.3.1 Pinigų plovimo ir teroristų finansavimo standartų minkštoji normatyvinė struktūra

Nepaisant to, kad tarptautinis pinigų plovimo prevencijos reglamentavimas egzistuoja nuo devintojo dešimtmečio pabaigos, pinigų plovimo ir terorizmo finansavimo reglamentavimas tarptautinėje teisėje vis dar yra retas klausimas. Pasak autoriaus N. Beekarry, šį retumą galima paaiškinti tuo, kad nėra katalizatoriaus, kuris paskatintų pinigų plovimą iškelti į pasaulinės politinės darbotvarkės viršūnę arba, galbūt, dar svarbiau yra tai, kad dėl, kaip W. Gilmore įvardinamos - dvilypės pasaulinės kovos su pinigų plovimu ir teroristų finansavimu reguliavimo sistemos struktūros kyla klausimų dėl teisiškai neįpareigojančių mechanizmų naudingumo.¹⁴²

Minkštosios, neįpareigojančios teisės funkcija pinigų plovimo prevencijos srityje sutelkta į visuotinį prevencinių kovos su pinigų plovimu priemonių, kurios galiausiai virsta nacionaliniais kovos su pinigų plovimu teisės aktais, įgyvendinimą. Pasitelkiant prevenciją pinigų plovimo srityje siekiama sumažinti žalingą pinigų plovimo poveikį finansų sistemai, užkertant kelią pinigų

¹³⁹ Holman, Daniel, Stettner, Barbara, Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches, ICLG TO: ANTI-MONEY LAUNDERING, 2018

¹⁴⁰ Leigh Cuen, Most Crypto Exchanges Still Don't Have Clear KYC Policies: Report, <https://www.coindesk.com/markets/2019/03/27/most-crypto-exchanges-still-dont-have-clear-kyc-policies-report/>

¹⁴¹ European Parliament, Crypto assets: new rules to stop illicit flows in the EU, Press Releases, 2022, <https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu>

¹⁴² Beekarry, Navin, The International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law

plovimo plitimui. Šios neprivalomos kilmės neoficialios iniciatyvos įteisina tarptautinių subjektų ir suinteresuotų vidaus institucijų dalyvavimą priimant nacionalinius sprendimus, nes skatina reikšmingą konvergenciją dėl jose įtvirtintų principų.¹⁴³

Devintajame dešimtmetyje įsteigta FATF padarė didžiausią įtaką kovos su pinigų plovimu politikos formavime. Iš pradžių ši organizacija buvo įkurta siekiant skatinti tarptautinį bendradarbiavimą pinigų plovimo srityje, ypač siekiant susigrąžinti iš pinigų plovimo gautą pelną. Vėliau išaugus tarptautinio radikalaus islamo terorizmo mastams, šioje srityje buvo parengta daugiau tarptautinių priemonių, taip pat išplėsti FATF įgaliojimai. Glaudesnis tarptautinis bendradarbiavimas, taip pat *minkštųjų* ir *kiėtųjų* tarptautinių teisės aktų šioje srityje plitimas padėjo plisti ir kovos su pinigų plovimu ir teroristų finansavimo baudžiamiesiems įstatymams.¹⁴⁴ Šiai dienai, FATF, kuriai dabar priklauso 37 nariai ir dvi regioninės organizacijos, yra laikomas svarbiausiu tarpvyriausybinio tinklu kovos su pinigų plovimu srityje. Valdymas pasitelkiant tarpvyriausybinius tinklus turi keletą privalumų, ypač tinkami tarpvalstybiniais klausimams spręsti. Be to, jie paprastai garantuoja, kad jų nariai turi didelę specializacijos lygį, taip pat ir dėl nuolatinio keitimosi informacija. Galiausiai jie paprastai yra lankstesni ir veiksmingesni nei tradicinės ir labiau struktūruotos daugiašalės tarptautinės organizacijos, pavyzdžiui, Jungtinės Tautos ir Pasaulio prekybos organizacija.¹⁴⁵

FATF kaip organizacija, nuo pat įkūrimo reguliariai tobulina savo standartus, atsižvelgdama į kylančius pavojus, tokius kaip virtualaus turto reguliavimą. FATF stebi valstybes, kad patikrintų, ar jos visapusiškai ir veiksmingai laikosi FATF reikalavimų.¹⁴⁶ Tačiau nepateikia jokių rekomendacijų dėl institucinės priežiūros struktūros. Institucinės struktūros ir kitos priemonės, kurias šalys naudoja rizikos vertinimu pagrįstai priežiūrai vykdyti ir vykdymo užtikrinimui užtikrinti, turėtų būti pritaikytos prie kiekvienos jurisdikcijos unikalių aplinkybių. Tai gali apimti esamą institucinę ir reguliavimo sistemą, pavyzdžiui, pagrindinių sektorių riziką ribojančią priežiūrą, reguliuojamų sektorių dydį ir sudėtingumą, jų pažeidžiamumo pinigų plovimo ir terorizmo rizikos laipsnį, taip pat grėsmes ir pažeidžiamumą.¹⁴⁷

Neabejotinai, FATF nuo pat pradžių buvo aktyviausia tarptautinė organizacija, sprendžianti virtualiųjų valiutų keliamas pinigų plovimo grėsmes, ir jau 2015 m., reaguodama į tai, kad jurisdikcijos visame pasaulyje pradėjo reguliuoti virtualiąsias valiutas, remdamasi pagrindiniais FATF standartais, išdėstė ir pateikė šalims gaires, kaip spręsti su virtualiosiomis

¹⁴³ Ebikake, Emmanuel, Money laundering: an assessment of soft law as a technique for repressive and preventive anti-money laundering control, Journal of Money Laundering Control, Vol 19, 2016

¹⁴⁴ Borlini, Leonardo, Montanaro, Francesco, The Evolution of The Eu Law Against Criminal Finance: The “Hardening” Of Fatf Standards Within The EU, 2017

¹⁴⁵ Ibid.

¹⁴⁶ FATF, Who we are, <https://www.fatf-gafi.org/about/whoweare/>

¹⁴⁷ FATF, Risk based supervision, 7 psl., 2021 m., <https://www.fatf-gafi.org/media/fatf/documents/Guidance-Risk-Based-Supervision.pdf>

valiutomis susijusias pinigų plovimo problemas. Gairės, visų pirma, buvo skirtos virtualiųjų valiutų keitykloms, atsižvelgiant į tai, kad tai buvo taškas, per kurį patenkama į finansų sistemą, kuri jau yra reguliuojama. Pirmosios ataskaitos metu buvo atkreiptas dėmesys tik į aštuonias rekomendacijas iš originaliųjų keturiasdešimt. 2015 m. gairių kontekste prevencinės kovos su pinigų plovimu priemonės galima būtų išskirti į kelias sritis:

AML/CFT (angl. *anti-money laundering, counter terrorism financing*, liet. kova su pinigų plovimu/kova su terorizmo finansavimu) **politikos formavimas ir jos koordinavimas:** Šių standartų reguliavimo perimetras toks jog, visų pirma, šalys buvo paragintos atlikti koordinuotą virtualiųjų valiutų produktų ir paslaugų rizikos vertinimą, skatinti viešojo ir privačiojo sektorių bendradarbiavimą, siekiant padėti kompetentingoms institucijoms reguliuoti konvertuojamąsias virtualiąsias valiutas ir realių valiutų keitimo platformas, ir įgyvendinti sustiprinto deramo patikrinimo priemones, nes dėl virtualių valiutų anonimiškumo ir sunkumų tinkamai nustatyti dalyvio tapatybę decentralizuotos virtualios valiutos laikomos keliančiomis didesnę pinigų plovimo ir (arba) terorizmo finansavimo riziką (1 rekomendacija).¹⁴⁸ Be kita ko, vyriausybės buvo skatinamos bendradarbiauti ir koordinuoti AML/CFT politiką, susijusią su virtualiosiomis valiutomis. Šalys galėjo apsvarstyti galimybę sukurti mechanizmus, pavyzdžiui, tarpžinybines darbo grupes, kad politikos formuotojai, reguliavimo institucijos, priežiūros institucijos, finansinės žvalgybos padaliniai (FŽP) ir teisėsaugos institucijos galėtų bendradarbiauti tarpusavyje ir su visomis kitomis kompetentingomis institucijomis, siekdamos parengti ir įgyvendinti veiksmingą politiką, taisykles ir kitas priemones, skirtas su pinigų plovimu ir teroristų finansavimu susijusiems rizikos veiksniams šalinti (2 rekomendacija).¹⁴⁹

Papildomos priemonės konkretiems klientams ir veiklai: šiuo atveju, konkreti veikla turėtų būti suprantama, kaip virtualiųjų valiutų keitimo tarp virtualiųjų valiutų ir *fiat* valiutų paslauga, kurią vykdo fiziniai arba juridiniai asmenys, užtikrinant, jog jie laikytųsi taikomų kovos su pinigų plovimu ir teroristų finansavimo įstatymų. Tai turėtų apimti tokių šalyje veikiančių paslaugų stebėseną, siekiant užtikrinti, kad būtų laikomasi registracijos ar licencijavimo reikalavimų ir kitų atitinkamų kovos su pinigų plovimu ir (arba) kovos su teroristų finansavimu priemonių (14 rekomendacija).¹⁵⁰ Be kita, šalims, prieš pradedant prekiauti naujais produktais ar kurti naujas technologijas, rekomenduota nustatyti ir įvertinti su naujais produktais, įskaitant virtualias valiutas, susijusią pinigų plovimo ir terorizmo riziką, o šalies finansų įstaigoms imtis tinkamų priemonių šiai rizikai valdyti ir mažinti (15 rekomendacija).¹⁵¹ Rizika veiksmingai

¹⁴⁸ FATF, Guidance for risk-based approach, Virtual Currencies, 8 psl., 2015 m., <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

¹⁴⁹ *Ibid.* 9 psl.

¹⁵⁰ *Ibid.* 10 psl.

¹⁵¹ *Ibid.*

mažinama ir valdoma galėjo būti nustatant konkrečiai šaliai būdingų bankinių pervedimų standartus. Ypač svarbu šalims buvo užtikrinti, kad konvertuojamosios virtualios valiutos keitykloms atliekant konvertuojamosios virtualios valiutos elektroninius pervedimus, būtų pateikiama būtina siuntėjo ir gavėjo informacija, tokiu būdu palengvinant operacijų dalyvių identifikaciją. Šalys šiuo atžvilgiu galėjo nustatyti *de minimis* kriterijų tarptautinėms bankinėms operacijoms (16 rekomendacija).¹⁵² Taip pat, raginta atkreipti dėmesį ir atidžiau prižiūrėti virtualiųjų valiutų keityklas, ypač tas, kurios vykdo decentralizuotų virtualiųjų valiutų konvertavimą, dėl jų keliamos aukštesnio laipsnio rizikos, kaip apibrėžta pirmoje darbo dalyje (26 rekomendacija).¹⁵³

Ypač svarbu buvo skatinti veiksmingą ir efektyvų tarptautinį bendradarbiavimą tarp valstybių kovojant su pinigų plovimu, su juo susijusiais pagrindiniais nusikaltimais ir teroristų finansavimu, įskaitant abipusę teisinę pagalbą. Be to, buvo teigiama, jog ji padėtų nustatyti, įšaldyti, areštuoti ir konfiskuoti pelną ir nusikalstamas priemones, kurios gali būti virtualių pinigų pavidalo, taip pat teikti veiksmingą ekstradicijos pagalbą (40 rekomendacija).¹⁵⁴

Galiausiai matomas ir **represinis** reguliavimas, reikalaujant, kad vyriausybės nustatytų veiksmingas, proporcingas ir atgrasančias bausmes, tokias kaip baudžiamąsias, civilines ar administracines, nesvarbu fiziniams ar juridiniams asmenims, pažeidusiems atitinkamus kovos su pinigų plovimu ir teroristų finansavimu įstatymus. Tačiau atsižvelgiant į tai, kad virtualiosios valiutos, ypač decentralizuotos, sudaro keletą kliūčių taikyti standartinius teisėsaugos metodus ir sėkmingai nagrinėti bylas (35 rekomendacija).¹⁵⁵ Šiuo atveju, virtualiųjų valiutų keityklų reguliavimas arba registravimas ir klientų identifikavimo, patikrinimo bei registravimo kriterijų taikymas galėtų leisti valstybėms veiksmingiau įgyvendinti sankcijas.

Tačiau ši sistema toli gražu nebuvo be trūkumų. Geriausiai šioms, 2015 m. išleistoms FATF gairėms, kritiką apibendrina Malcolm Campbell-Verduyn, mokslininkas ją išskiria į tris dalis. Visų pirma, problema kyla dėl to, jog FATF šalims siūlo reikalauti, kad finansų ir ne finansų įmonės, dirbdamos su virtualiomis valiutomis, pačios įvertintų pinigų plovimo riziką. Tačiau akcentuojant rinkos iniciatyvas, M. Campbell-Verduyn teigimu, nepastebimos problemos, susijusios su pasiklovimu sektoriaus remiamais duomenimis, taip pat su tuo, kad reguliavimo institucijos gali būti materialiai ir intelektualiai „užvaldytos“ sektoriaus interesų. Dėl šios priežasties, mokslininko teigimu, taikant riziką grindžiamą požiūrį linkstama nepastebėti galimos rizikos, susijusios su pasiklovimu sektoriaus sprendimais.¹⁵⁶

¹⁵² *Ibid.*

¹⁵³ *Ibid.*

¹⁵⁴ *Ibid.* 11 psl.

¹⁵⁵ *Ibid.* 11 psl.

¹⁵⁶ Campbell-Verduyn, M. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime Law Soc Change* 69, 283–305, 2018

Antroji kritikos dalis susijusi su tuo, kad FATF gairėse linkstama pasikliauti „stebuklingais“ technologiniais sprendimais, tikintis, jog rinkos dalyviai gali sukurti taikomųjų programų programavimo sąsajas, kuriomis būtų teikiama kliento identifikavimo informacija, arba trečiųjų šalių skaitmeninės tapatybės sistemos, kurios pačios turėtų būti reguliuojamos. Tačiau nebuvo atsižvelgta, jog dar nebuvo technologijos, kuri leistų imtis tapatybės nustatymo procesų. Be kita ko, tai iš esmės prieštarauja virtualių valiutų bendruomenės taip siekiamai decentralizacijai ir bendru nepasitikėjimu centralizacija.¹⁵⁷

Galiausiai, M. Campbell-Verduyn teigia, jog pabrėžiant didelės rizikos mainus, neatsižvelgiama į platesnį kitų galimai mažesnės rizikos, tačiau vis dėlto svarbių virtualių valiutų ekosistemos centrų rinkinį. Sutelkiant dėmesį į mazgus, t. y. keityklas, neatsižvelgiama į pinigų plovimo potencialą daugybės kitų veikėjų. Pavyzdžiui, siaurai apibrėžiant, kas tiksliai sudaro virtualių valiutų mainus, neatsižvelgiama į tai, kad, pavyzdžiui, kasėjai, taip pat gali būti pagrindiniai mazgai, palengvinantys pinigų plovimą. Nors nurodoma, kad kasybos procesas savaime nėra susijęs su pinigų plovimo problemomis, pelningi sandorių mokesčiai kasėjams, norintiems patvirtinti nesąžiningus sandorius, gali skatinti nusikalstamą elgesį. Toks požiūris potencialiai apriboja FATF gairių taikymo sritį.¹⁵⁸

Po 2015 m., FATF kelis kartus atnaujino savo rekomendacijas, susijusias su virtualių valiutų reguliavimu. Ir dabar, 2021 m. pabaigoje, FATF pateikė atnaujiną rizika paremtą požiūrį į virtualų turtą ir virtualaus turto paslaugų teikėjų reguliavimo vadovą. Lyginant du dokumentus, gairės tapo išsamesnės nei 2015 m., FATF išplėtė savo terminologiją, įvesdama virtualaus turto bei virtualaus turto paslaugų teikėjų sąvokas. Pažymėtina, kad virtualaus turto paslaugų teikėjas turėtų būti suprantamas, kaip: „bet kuris fizinis ar juridinis asmuo, vykdomas verslą vieną ar daugiau nurodytų veiklų ar operacijų kito fizinio ar juridinio asmens naudai arba jo vardu“ ir tai apima:

- Virtualiojo turto ir *fiat* valiutų keitimas;
- Vienos ar daugiau formų virtualiojo turto mainus;
- Virtualaus turto pervedimas ir
- Virtualaus turto ar priemonių saugojimas ir (arba) administravimas, suteikiančių galimybę kontroliuoti virtualųjį turtą;
- Dalyvavimas teikiant finansines paslaugas, susijusias su virtualaus turto siūlymu ir (arba) pardavimu, ir jų teikimas.¹⁵⁹

¹⁵⁷ *Ibid.*

¹⁵⁸ *Ibid.*

¹⁵⁹ FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, 22 psl., 2021 m., <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

Vadovaujantis atnaujintomis gairėmis FATF rekomendacijos turėtų būti taikomos šalims ir kompetentingoms institucijoms, taip pat virtualaus turto paslaugų teikėjams ir kitiems įpareigotiesiems subjektams, kurie vykdo su virtualiu turtu susijusią veiklą, pavyzdžiui, finansų įstaigoms, tokioms kaip bankai. Tačiau G. Soana teigimu, reguliuojamų įpareigotųjų subjektų skaičiaus didinimas nepakeis fakto, kad virtualios leidžia vykdyti *peer-to-peer* sandorius, todėl joks tarpininkas niekada neatliks tos priverstinės kliūties funkcijos, kurią jis atlieka *fiat* rinkoje. Mėginimas pritaikyti paveldėtą reguliavimo metodą naujai priemonei gali duoti tik dalinių ir galiausiai nepatenkinamų rezultatų.¹⁶⁰

Galima teigti, jog beveik visos FATF rekomendacijos dabar yra tiesiogiai taikomos sprendžiant virtualiojo turto ir virtualiojo turto paslaugų teikėjų keliamą pinigų plovimo ir terorizmo riziką, o kitos rekomendacijos vis dar yra aktualios ir taikytinos, nepaisant to, kad yra mažiau tiesiogiai ar aiškiai susijusios su virtualiuoju turtu ar virtualiojo turto paslaugų teikėjais. Toks išplėstinis rekomendacijų taikymas parodo išaugusį poreikį spręsti pinigų plovimo pasitelkiant virtualias valiutas problematiką. Nuo šiol virtualaus turto paslaugų teikėjams taikomi tokie patys bendrieji reguliavimo reikalavimai kaip ir finansų įstaigoms ir kai kurioms nefinansinėms įmonėms bei profesijoms.¹⁶¹

Pastebėtina, kad išskiriamos pagrindinės virtualaus turto pinigų plovimo ir terorizmo finansavimo rizikos yra susijusios su reikalavimų neatitinkančių arba silpnai juos atitinkančių virtualaus turto paslaugų teikėjų problema, taip pat anonimiškumo didinimo metodais.¹⁶² Vieni iš geriausiai žinomų ir darbo teorinėje dalyje aptartų anonimiškumą didinančių instrumentų yra – valiutų virtualių maišytuvai. Kaip pastebi J. Scharfman, naudojimasis kriptovaliutų maišytuvų paslauga pats savaime nebūtinai yra neteisėtas. Taip pat yra nemažai teisėtų priežasčių, dėl kurių žmonės naudojami tokiais paslaugomis, pavyzdžiui, norintys didesnio privatumo. Tačiau tai ypač patogus įrankis nusikaltėliams, siekiantiems plauti lėšas. Maišymo paslaugos naudojimas padeda jiems užmaskuoti lėšų šaltinį, sekti jų sandorius ir paslėpti tapatybę. Todėl suprantama, kodėl FATF atkreipia savo ir visos tarptautinės bendruomenės dėmesį į anonimiškumą didinančius metodus. Vienas iš pavyzdžių, 2019 m. gegužę Europolas kartu su Nyderlandų finansinių nusikaltimų tyrimo tarnyba uždarė maišymo paslaugas teikusį *Bestmixer.io*, kur, kaip įtariama, buvo sumaišyta apie 27 000 bitkoinų, kurių didžioji dalis buvo nusikalstamos kilmės arba paskirties.¹⁶³

¹⁶⁰ Soana, Giulio, *Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?*, Wiley, 2021

¹⁶¹ *Ibid.* 1 psl.

¹⁶² *Ibid.* 12 psl.

¹⁶³ Jason Scharfman, *Cryptocurrency Compliance and Operations, Digital Assets, Blockchain and DeFi*, 210 psl., 2021

Kaip minėta, beveik visos 40 rekomendacijų yra tiesiogiai adaptuojamos virtualiam turtui ir virtualaus turto paslaugų teikėjams. Taigi planas šalims, kaip kovoti su pinigų plovimu, teroristų finansavimu pasitelkiant virtualias valiutas, apima šias pagrindines sritis:

- Pinigų plovimo ir terorizmo finansavimo politika ir koordinavimas
- Pinigų plovimo kriminalizavimas ir nusikalstamu būdu įgytų pajamų konfiskavimas
- Terorizmo finansavimas ir ginklų platinimo finansavimas
- Prevencinės priemonės
- Papildomos priemonės konkreitiems klientams ir veiklai
- Tarptautinis bendradarbiavimas

Pinigų plovimo ir terorizmo finansavimo politika ir koordinavimas: Ši sritis aptariama 1 ir 2 rekomendacijose. 1 rekomendacijoje vyriausybėms rekomenduojama kovojant su pinigų plovimu ir TF taikyti rizika pagrįstą požiūrį, užtikrinti, kad pinigų plovimo ir teroristų finansavimo prevencijos ar mažinimo priemonės atitiktų pavojus, kurie pripažįstami atskirose jurisdikcijose. Reikalaujama, jog šalys sugriežtintų savo reikalavimus, taikomus didesnės rizikos veiklai, susijusiai su virtualiosiomis valiutomis, atsižvelgiant į finansinės veiklos rūšis, pavyzdžiui, sandorius tarp asmenų, taip pat virtualiojo turto paslaugų teikėjų veiklą ar operacijas, centralizuotų ir decentralizuotų virtualiųjų valiutų skirtumus ir į tai, ar jas kontroliuoja virtualaus turto paslaugų teikėjas.¹⁶⁴ Siekiant užtikrinti, kad politikos formuotojai, FŽP, teisėsaugos institucijos, priežiūros institucijos ir kiti subjektai veiksmingai koordinuotų kovos su pinigų plovimu, teroristų finansavimu veiklą šalies viduje, kaip nurodyta 2 rekomendacijoje, būtina koordinuoti veiksmus nacionaliniu lygmeniu.¹⁶⁵

Pinigų plovimo kriminalizavimas ir nusikalstamu būdu įgytų pajamų konfiskavimas: Šią sritį apima 3 ir 4 rekomendacijos. Siekiant, jog valstybės stiprintų savo baudžiamąją sistemą, reikalaujama, jog pinigų plovimas turėtų būti apibrėžiamas kaip bet koks turtas, nepriklausomai nuo jo vertės, kuris naudojamas nusikalstamu būdu gautoms pajamoms nuslėpti, įskaitant virtualiąsias valiutas. Šalys turėtų išplėsti savo kovos su pinigų plovimu įstatymų taikymo sritį, kad į ją būtų įtrauktos pajamos iš nusikalstamos veiklos naudojant virtualią valiutą (3 rekomendacija).¹⁶⁶ Tad konfiskavimas ir laikinosios priemonės, susijusios su išplautu turtu, pajamomis, turtu, kuris yra pajamos iš terorizmo, turėtų būti taikomas ir virtualiam turtui (4 rekomendacija).¹⁶⁷

¹⁶⁴ *Ibid.* 38 psl.

¹⁶⁵ *Ibid.* 41 psl.

¹⁶⁶ *Ibid.*

¹⁶⁷ *Ibid.* 42 psl.

Nurodoma, kad vyriausybės turi nustatyti bausmes fiziniams ir juridiniams asmenims. Šalys turėtų panašiai nustatyti sankcijas virtualaus turto paslaugų teikėjams, kurie pažeidžia jų kovos su pinigų plovimu ir kovos su terorizmo finansavimu reikalavimus, ir tokios sankcijos turėtų būti taikomos ne tik pačiam paslaugų teikėjui, bet ir jo direktoriams bei vyresniajai vadovybei (35 rekomendacija).¹⁶⁸

Terorizmo finansavimas ir ginklų platinimo finansavimas: Kalbant apie terorizmo finansavimą, S. Wang. su X. Zhu pažymi, jog teroristinėms organizacijoms naudojantis kriptovaliuta, tarptautinė bendruomenė patiria didesnę spaudimą kovoti su terorizmo finansavimu. Teroristines organizacijas naudoti kriptovaliutas labiausiai skatina jos anonimiškumas ir griežtos nacionalinės finansinės priežiūros nebuvimas. Ir nors teroristinės organizacijos kriptovaliutas dar naudoja ribotai, o virtualių valiutų naudojimas teroristų finansavimui dar tik pradedamas, nes tai nėra subrendęs teroristų finansavimo būdas. Tačiau nepaisant to, atsižvelgiant į sparčią technologijų raidą, Šalys ir tarptautinės organizacijos turi būti budrios, tobulinti savo kriptovaliutų reguliavimo sistemas ir užkirsti kelią įvairiems terorizmo finansavimo būdams įvairiais kanalais.¹⁶⁹

Atsižvelgiant į tai, FATF šiam klausimui skiria dėmesio nuo 5 iki 8 rekomendacijos. Visų pirma, nurodoma, jog šalys turėtų nedelsdamos įšaldyti asmenų ar subjektų, įtrauktų į asmenų ar subjektų, kuriems taikomos tikslinės finansinės sankcijos už terorizmą ir teroristų finansavimą, sąrašą, lėšas ar kitą turtą, įskaitant virtualiąsias valiutas, ir užtikrinti, jog jis būtų įšaldytas. Taip pat, turėtų nedelsdamos įšaldyti ir į sąrašą įtrauktų asmenų ar subjektų turtą, įskaitant virtualią valiutą, ir užtikrinti, kad jis nebūtų prieinamas šiems asmenims ar subjektams (7 rekomendacija). Šalys taip pat turėtų taikyti atitinkamas priemones, siekdamos apsaugoti pelno nesiekiančias organizacijas nuo piktnaudžiavimo terorizmo finansavimu, kaip nurodyta 8 rekomendacijoje, įskaitant atvejus, kai slaptas lėšų nukreipimas teroristinėms organizacijoms yra susijęs su virtualiu turtu.¹⁷⁰ Ši problema aptarta ir pirmoje darbo dalyje, išskiriant, jog terorizmo finansavimas prisidengiant ne pelno siekiančiomis, labdaros organizacijoms kelia vis daugiau susirūpinimo tarptautinei bendruomenei.

Prevenčinės priemonės: FAFT nuolatos pabrėžia poreikį sugriežtinti finansų sektoriaus priežiūrą, pateikiami konkretūs pasiūlymai dėl finansų sektoriaus reguliavimo ir priežiūros sistemos, įskaitant ir informacijos atskleidimo, registravimo ir pranešimo apie įtartinus sandorius reikalavimus.

¹⁶⁸ *Ibid.* 43 psl.

¹⁶⁹ Shacheng Wang, Xixi Zhu, Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing, *Policing: A Journal of Policy and Practice*, Volume 15, Issue 4, December 2021, Pages 2329–2340

¹⁷⁰ *Ibid.* 42 psl.

9 rekomendacijoje reikalaujama, kad bankų bei kitų finansų įstaigų slaptumo įstatymai būtų pavaldūs ir netrukdytų FATF rekomendacijų įgyvendinimui.

Labai svarbu pažymėti, kad 10 rekomendacijoje reikalaujama, jog vyriausybės ir įpareigosios organizacijos sukurtų deramo klientų tikrinimo procedūras. Deramo klientų patikrinimo procedūra turėtų padėti virtualaus turto paslaugų teikėjams ir kitiems įpareigotiems subjektams įvertinti pinigų plovimo ir terorizmo riziką. Pradinis deramas klientų patikrinimas turi apimti kliento ar tikrojo savininko tapatybės nustatymą, tapatybės patikrinimą.¹⁷¹ Atkreiptinas dėmesys, jog šiai rekomendacijai pagrindus suteikė Bazelio komitetas. Taip pat tikimasi, kad šalys užtikrins, jog paslaugų teikėjai bent penkerius metus saugotų visų sandorių ir deramo klientų tikrinimo procesų įrašus (11 rekomendacija).¹⁷² Pasak G. Soana, iš tiesų, nustatydama kliento pažinimo procedūras ir ataskaitų teikimo pareigas ir rinkos vidaus sandoriams, reguliavimo institucija pirmą kartą pripažįsta būtinybę įsikišti į rinką.¹⁷³

Be kita ko, šioje vietoje Malte Möser and Arvind Narayanan aiškina, jog bankai yra centralizuoti tradicinio finansų sektoriaus prieigos taškai, todėl jie yra patogus objektas siekiant užtikrinti pinigų plovimo prevencijos reglamentavimą. Bet virtualių valiutų veikimas iš esmės skiriasi nuo tradicinių finansų sistemų, nes leidžia kurti sąskaitas nepriklausomai nuo bet kurios finansų įstaigos ir be galimybės užtikrinti tapatybės tikrinimo reikalavimų. Užuoat tvarkant sąskaitas kaip įrašus centralizuotoje duomenų bazėje, kuri leidžia užtikrinti kliento pažinimo procesą, virtualių valiutų sąskaitas reprezentuoja kriptografiniai raktai, o sistema veikia be centrinės institucijos. Kadangi raktų kūrimas yra greitas ir pigus, daugelis virtualių valiutų skatina vienkartinį adresų naudojimą. Tokiu atveju, kai vartotojas gauna pinigų, jis gali sukurti naują raktų porą, taip padidindamas savo privatumą, nes jo sandoriai paskirstomi tarp daugelio skirtingų sąskaitų. Neturint specialių žinių, tam pačiam naudotojui priklausančių adresų, kurie nenaudojami vienu metu, neįmanoma lengvai identifikuoti.¹⁷⁴ Virtualių valiutų atveju, kaip teigia autoriai, tapatybes galima įgyti ir patikrinti tik tada, kai naudotojai peržengia tradicinės finansų sistemos ribą, bendraudami su reguliuojamais tarpininkais, pavyzdžiui, keityklomis ar mokėjimo paslaugų teikėjais. Bet net jei tapatybės gali identifikuojamos šiose sistemų sankirtose, reguliavimo institucijos negaus išsamaus vaizdo apie asmens sandorius, nes jie gali būti vykdomi naudojant daug skirtingų adresų, iš kurių tik nedidelė dalis tampa žinoma tarpininkui.¹⁷⁵ Dėl šios priežasties, autoriai teigia, jog toks tradicinis reguliavimo įgyvendinimas gali būti bevaisis.

¹⁷¹ *Ibid.* 49 psl.

¹⁷² *Ibid.* 52 psl.

¹⁷³ Soana, Giulio, *Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?*, Wiley, 2021

¹⁷⁴ Möser, Malte and Arvind Narayanan. "Effective Cryptocurrency Regulation Through Blacklisting." (2019).

¹⁷⁵ *Ibid.*

26 ir 27 rekomendacijose, pažymima, kad virtualiojo turto paslaugų teikėjų veiklą prižiūrėtų ar stebėtų kompetentinga institucija, bet ne savireguliacinio organas, kuris turėtų vykdyti riziką pagrįstą priežiūrą ar stebėseną.¹⁷⁶

Papildomos priemonės konkrečioms klientams ir veiklai: 12 rekomendacijoje kalbama apie politikoje dalyvaujančius asmenis ir jų šeimos narius ar artimus bendrininkus ir reikalaujama, kad įstaigos imtųsi papildomų priemonių, papildančių 10 rekomendacijoje nurodytas deramo klientų patikrinimo priemones, kad nustatytų, ar ir kada jie su jais vykdo verslo santykius, įskaitant lėšų šaltinio nustatymą, kai tai aktualu.¹⁷⁷

Atskirai turėtų būti atkreiptas didesnis dėmesys į 15 rekomendaciją, kuri dar vadinamoji *kelionių taisyklės* (angl. *travel rule*), pagal kurią reikalaujama, kad finansų subjektai, kai sandoriai viršija tam tikrą ribą, vykdytų informacijos registraciją apie klientus.¹⁷⁸ Minėtoji taisyklė yra svarbi priemonė sprendžiant pinigų plovimui būdingą informacijos asimetriją, nes leidžia nustatyti klientus ir taip lengviau atsekti įtartinus sandorius. Tačiau dėl virtualaus turto pobūdžio šios taisyklės taikymas tampa problemiškas. Remiantis FATF rekomenduojama *kelionių taisykle*, virtualaus turto paslaugų teikėjai privalo perduoti kliento duomenis, kai klientas, atlikdamas tarptautinį pervedimą tarp virtualaus turto paslaugų teikėjų, siunčia didesnę nei 1 000 USD/EUR ribą viršijančią vertę.¹⁷⁹ Nors, kaip minėta anksčiau, Europos Sąjungoje norima atsisakyti tokios *de minis* ribos, nes manoma, jog virtualių valiutų naudotojai galėtų apeiti taisykles sukurdami beveik neribotą pervedimų skaičių.

Pasak A. Schmidt norint veiksmingai įgyvendinti šią rekomendaciją, reikia nuoseklių standartų ir tarptautinio bendradarbiavimo reguliavimo lygmeniu. FATF rekomendacijos yra tik minimalūs reikalavimai, ir kiekviena jurisdikcija jas interpretuos skirtingai. Dėl to kyla problemų, kadangi vienoje šalyje vykdymas užtikrinamas, o kitoje šalyje - ne, pirmosios šalies virtualaus turto paslaugų teikėjai gali negalėti leisti sudaryti sandorio su antrosios šalies virtualaus turto paslaugų teikėjais, o tai stabdo pasaulinį likvidumą.¹⁸⁰

Be kita ko, 15 rekomendacijoje reikalaujama, kad šalys turėtų valdyti ir mažinti riziką, kylančią dėl virtualaus turto, ir užtikrinti, kad virtualaus turto paslaugų teikėjai būtų reguliuojamos pinigų plovimo ir teroristų finansavimo tikslais, licencijuojamos arba registruojamos ir kad joms būtų taikomos veiksmingos stebėsenos sistemos ir užtikrinama, kad būtų laikomasi atitinkamų

¹⁷⁶ FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, 47 psl., 2021 m.,

¹⁷⁷ *Ibid.* 52 psl.

¹⁷⁸ Velkes, Gabrielle Chasin, International Anti-Money Laundering Regulation Of Virtual Currencies And Assets, 897 psl., 2020 m.

¹⁷⁹ *Ibid.*, 898 psl.

¹⁸⁰ Schmidt, Alicia, Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model, *International Journal of Law and Information Technology*, Volume 29, Issue 4, Winter 2021, Pages 332–363

priemonių, kurių reikalaujama FATF rekomendacijose. Šios rekomendacijos aiškinamojoje pastaboje nustatytos kelios taisyklės, susijusios su jurisdikcijų, atsakingų už virtualaus turto paslaugų teikėjų reguliavimą. Pirma, jie turi būti licencijuojami arba registruojami jurisdikcijoje (-ose), kurioje (-iose) jie yra sukurti. Antra, jei virtualaus turto paslaugų teikėjas yra fizinis asmuo, turėtų būti reikalaujama, kad jis būtų licencijuotas arba registruotas toje jurisdikcijoje, kurioje yra jo verslo vieta. Taip pat nurodoma, kad šalys gali apsvarstyti galimybę sumažinti virtualaus turto paslaugų teikėjų keliamą riziką išplėsdamos savo licencijavimo ar registravimo režimą, kad virtualaus turto paslaugų teikėjai, siūlantys produktus ir (arba) paslaugas klientams jų jurisdikcijoje arba vykdančios operacijas iš jos, būtų licencijuojamos ar registruojamos toje jurisdikcijoje.

Tačiau dėl šios 15 rekomendacijos L. de Koker et al. išsako savo abejones, teigiant, jog su virtualaus turto paslaugų teikėjais susijusią reguliavimo jurisdikciją reglamentuojančių teisės aktų nuostatos yra plačios, tačiau FATF jurisdikcijos schema yra neaiški ir palieka spragų.¹⁸¹ Kaip vieną iš problemų šie autoriai įvardina fiziniams asmenims, esantiems virtualaus turto paslaugų teikėjais, taikomą verslo vietos testą. Šalys gali atsižvelgti į tai ar verslo įrašai laikomi jurisdikcijos teritorijoje. Tačiau toks reikalavimas debesijos paslaugų eroje yra ribotas. Vien faktas, kad pagrindiniai įrašai laikomi jurisdikcijos teritorijoje esančiame debesijos serveryje, labai menkai užtikrina šalies priežiūros institucijos priežiūrą. Tai gali leisti priežiūros institucijai gauti prieigą prie tam tikros informacijos, tačiau ji negali imtis jokių priežiūros ar vykdymo užtikrinimo veiksmų. Be kita ko, pažymima, jog tokius įrašus taip pat galima lengvai perkelti į kitos jurisdikcijos debesijos serverį, o pirminė jurisdikcija gali nesunkiai nustatyti tą naująjį paslaugų teikėją ar kitą jurisdikciją.¹⁸²

Dar viena L. de Koker et al. pastebima spraga, kalbant apie reguliavimą remiantis produktų siūlymu klientams šalies jurisdikcijoje, nes jurisdikcijoje gali nebūti jokio fizinio ar juridinio asmens, kurį būtų galima patraukti atsakomybėn, arba patalpų ar įrašų, su kuriais būtų galima susipažinti. Išplėtus jurisdikcijos reikalavimą tuo pagrindu, kad piliečiai gali naudotis paslauga ar produktu, globalizuotoje, skaitmeninėje ekonomikoje labai išplečiama taikymo sritis, ir tai gali būti ne pagal daugelio reguliavimo institucijų galimybes.¹⁸³

18 rekomendacijoje kalbama apie vidaus kontrolę ir užsienio filialius, reikalaujama, kad šalys reikalautų, jog įpareigotieji subjektai, kaip su virtualiu turtu susiję paslaugų teikėjai, turėtų vidaus kontrolės priemones, kad būtų galima nustatyti pinigų plovimo ir teroristų finansavimo

¹⁸¹ de Koker, L., Ocal, T., Casanovas, P. (2022). Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge. In: Goldbarsht, D., de Koker, L. (eds) *Financial Technology and the Law . Law, Governance and Technology Series*, vol 47. Springer, Cham.

¹⁸² *Ibid.*

¹⁸³ FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris

politikos ir procesų veiksmingumą bei rizikos valdymo kokybę visose operacijose, padaliniuose, filialuose tiek šalies viduje, tiek, užsienyje.

19 rekomendacijoje išskiriamos didesnės rizikos šalys, kurių atžvilgiu reikalaujama, jog įpareigotieji subjektai, susistiprintas deramo kliento patikrinimo priemonės verslo santykiams ir sandoriams su fiziniiais ir juridiniais asmenimis iš didesnės rizikos šalių. Tai ypač aktualu virtualaus turto veiklai ir su juo susijusiems paslaugų teikėjams, atsižvelgiant į tarpvalstybinį jų veiklos pobūdį.¹⁸⁴

Tarptautinis bendradarbiavimas: Paskutinis ypač svarbus FATF rekomendacijų bruožas - jose pabrėžiamas tarptautinis bendradarbiavimas. Tai yra vyriausybių tarpusavio bendradarbiavimas, kuris ypač paplitęs savitarpio teisinės pagalbos ir ekstradicijos srityse, taip pat agentūrų tarpusavio bendradarbiavimas. Todėl 37-40 rekomendacijos apima reikalavimus, susijusių su tarptautiniu bendradarbiavimu, įskaitant savitarpio teisinę pagalbą, tarpvalstybinį turto įšaldymą ir konfiskavimą, ekstradiciją ir apskritai kuo platesnį tarptautinį bendradarbiavimą, be kita ko, pinigų plovimo, susijusių pirminių nusikaltimų ir teroristų finansavimo srityje. G. Pavlidis pažymi, jog finansinės žvalgybos padalinių ir kompetentingų teisėsaugos institucijų dalijimasis informacija gali padėti atlikti finansinius ir baudžiamuosius tyrimus ir užkirsti kelią pinigų plovėjui ir terorizmo finansuotojų jurisdikcijos pasirinkimui.¹⁸⁵ Šiai rekomendacijai pritaria ir A. S. M. Irwin su A. B. Turner, teigiant, jog sklandaus dalijimosi žvalgybos informacija praktikoje pabrėžiama teisėsaugos institucijų bendradarbiavimo svarba, bendras grėsmės suvokimas, pasitikėjimas, technologijų naudojimas, operatyvumas ir teikiamos informacijos kontekstas - visi šie veiksniai prisideda prie bendradarbiavimo žvalgybos srityje stiprinimo. Tačiau, pažymima, jog žvalgybinės informacijos apie su virtualiomis valiutomis susijusius kibernetinius nusikaltimus gavimas gali būti unikalus iššūkis dėl virtualių valiutų tapatybės ir sandorių anonimiškumo.¹⁸⁶

Aukščiau apibūdintos rekomendacijos yra dalis visų 2021 m. atnaujintų standartų. Akivaizdu, jog reguliavimas per 6 metus stipriai pasikeitė ir išsiplėtė, pasidarė griežtesnės bei tikslesnis. Pirmųjų rekomendacijų metu buvo plėtojama tik apie virtualių valiutų ir jų keityklų sąvoka, naujosios rekomendacijos pateikia terminą virtualus turtas bei virtualaus turto paslaugų teikėjai, kuris yra gerokai platesnis ir daugiau aprėpiantis negu tik virtualių valiutų keityklas. Taip pat, rekomenduojama reguliavimą klasifikuoti pagal sandorių pobūdį, virtualių valiutų tipus. Be kita ko, prie pinigų plovimo bei terorizmo finansavimo, išskiriama nauja aktuali sritis, tai - kovos su ginklų platinimu finansavimas. Tikriausiai vienas iš svarbiausių naujų aspektų, virtualaus turto

¹⁸⁴ *Ibid.* 66 psl.

¹⁸⁵ Pavlidis, G. (2020), "International regulation of virtual assets under FATF's new standards", *Journal of Investment Compliance*, Vol. 21 No. 1, pp. 1-8

¹⁸⁶ Angela S M Irwin, Adam B Turner, "Illicit Bitcoin transactions: challenges in getting to the who, what, when and where", *Journal of Money Laundering Control*, 2018

paslaugų teikėjai turėtų atlikti klientų patikrą bei kaupti ir saugoti su jų sandoriais susijusią informaciją atitinkamą laiko tarpą, kad tokie duomenys, esant reikalui būtų prieinami kontrolei atliekančioms institucijoms. Dar vienas aspektas, jog ir pačių šalių kompetentingi organai turėtų vykdyti statistinį stebėjimą, susijusį su įtartinais virtualaus turto sandoriais.

Iš esmės, pagrindinis FATF standartų komponentas yra tas, kad jie turėtų būti taikomi virtualiajam turtui atsižvelgiant į jo rizikos pobūdį, nepriklausomai nuo to, kaip virtualusis turtas įvardijamas nacionalinėje teisėje. FATF pažymi, kad virtualusis turtas gali būti susijęs su didesne pinigų plovimo ir teroristų finansavimo rizika ir kad gali prireikti tinkamų rizikos mažinimo priemonių tokiai neteisėtai veiklai nustatyti ir kovoti su ja. Kliento ir sandorio šalies tapatybės nustatymo nebuvimas yra ypač problemiškas virtualaus turto, kuris yra tarpvalstybinio pobūdžio, atveju. Nepakankamas neskaidrių sandorių rizikos valdymas nustatant ir tikrinant kliento tapatybę didina pinigų plovimo ir terorizmo finansavimo pavojų, taip pat apsunkina lėšų atsekamumą.¹⁸⁷

Šiuo metu pasaulinį FATF tinklą sudaro daugiau kaip 205 jurisdikcijos visame pasaulyje, todėl drąsiai galima teigti, jog tai yra tarptautinės kovos su pinigų plovimu ir teroristų finansavimu pagrindas. Siekiant kovoti su pasaulinėmis grėsmėmis ir užtikrinti, kad nusikaltėliams ir teroristams neliktų spragų, kuriomis jie galėtų pasinaudoti, būtina veiksmingai reaguoti nacionaliniu, regioniniu ir pasauliniu mastu.¹⁸⁸ Šiuo atveju, vienas iš išskirtiniausių FATF rekomendacijų aspektų yra dėmesys jų įgyvendinimui, kurį FATF atlieka vykdant vertinimus. Tad nors FATF rekomendacijos nėra teisiškai privalomos ar įpareigojančios net FATF nariams ir neturi įstatymo galios, tačiau dėl to, kad jų įgyvendinimui skiriama daug dėmesio, jos daro virš valstybinę įtaką arba bent jau suteikia postūmį prevencinių nacionalinių kovos su pinigų plovimu įstatymų ir praktikos rengimui visame pasaulyje. Dėl neprivalomo FATF rekomendacijų pobūdžio svarbu įvertinti negriežtosios teisės funkciją ir reikšmę šioje srityje.

Siekdama užtikrinti savo standartų perkėlimą į nacionalinę teisę, FATF reguliariai tikrina šalių narių įstatymus ir praktiką. Stebėsenos sistema grindžiama nuolat atliekamais kiekvienos FATF narės vertinimais, kur FATF ekspertai peržiūri, kaip įgyvendinami standartai, ir atlieka išsamią vidaus įstatymų ir praktikos analizę pinigų plovimo ir teroristų finansavimo srityje, galiausiai įvertindami vidaus pinigų plovimo ir teroristų finansavimo sistemos veiksmingumą.¹⁸⁹

Remiantis naujausiais pateikiamais vertinimais, pavyzdžiui, Italija, nors ir priklauso Europos Sąjungai, gali būti vienas iš pavyzdžių, kaip taikoma rizika pagrįstas požiūris į virtualųjį turtą ir virtualiojo turto paslaugų teikėjus remiantis FATF rekomendacijomis. Šioje valstybėje

¹⁸⁷ *Ibid.* 16 psl.

¹⁸⁸ FATF, Annual Report 2020-2021, 60 psl., <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/Annual-Report-2020-2021.pdf>

¹⁸⁹ Pavlidis, Georgio, "Financial action task force and the fight against money laundering and the financing of terrorism: Quo vadimus?", *Journal of Financial Crime*, Vol. 28 No. 3, pp. 765-773, 2021

virtualių valiutų paslaugų teikėjai, užsiimantys penkiomis funkcinėmis veiklomis, kaip apibrėžta FATF, priskiriami prie AML/CFT prievolių gavėjų ir laikomi įpareigotaisiais subjektais. Registracija, kaip apibūdinama 14 rekomendacijoje, yra būtina sąlyga, kad su virtualiu turtu susiję paslaugų teikėjai galėtų vykdyti savo veiklą Italijoje.

Atkreiptinas dėmesys, jog šios srities politikos formavime intensyviai veikia Italijos FŽP, kurių nuolatos atliekamos analizės, be kita to, FŽP, remiantis 2 rekomendacija, siekia sustiprinti bendradarbiavimą su privačiuoju sektoriumi – bankais, mokėjimo įstaigomis bei lošimų operatorius, nurodo jiems atkreipti dėmesį į galimas neįprastas operacijas, pavyzdžiui, bankinius pervedimus, grynųjų pinigų įnešimą ir išėmimą, naudojimąsi išankstinio mokėjimo kortelėmis, susijusias su kriptovaliutų pirkimu.¹⁹⁰ Toks bendradarbiavimas galėtų būti įvardinamas kaip viešojo ir privatačio sektoriaus partnerystės strategija ir yra plačiai paplitęs Europos Sąjungoje, leidžia subalansuoti rizikas ir leisti greičiau prisitaikyti prie kintančios aplinkos.

Tačiau Italijos įstatymas aiškiai apima tik virtualiųjų ir fiat valiutų mainus ir saugomų piniginių mainus, kas yra priešingai naujausioms FATF gairėms, Įstatymas nereguliuoja virtualiųjų valiutų mainų.

Kalbant apie Norvegiją, kuri kovos su pinigų plovimu taisyklės, virtualiosios valiutos keitimo ir saugojimo paslaugų teikėjams pradėtas taiko Norvegijos pinigų plovimo įstatymą, kuris taikomas keitimo paslaugų ir virtualiosios valiutos saugojimo paslaugų teikėjams. Pateikiama virtualios valiutos apibrėžtis labai panaši į FATF 2015 m. gairėse pateiktą apibrėžtį, vartojamas tas pats terminas (t. y. virtuali valiuta) ir tas pats apibrėžimas.¹⁹¹

Prieš kelis metus Suomijos finansų priežiūros institucija (FIN-FSA) paskelbė naujas taisykles ir gaires virtualiųjų valiutų teikėjams pagal naują įstatymą, tačiau, kitaip nei FATF rekomendacijose, ši valstybė nelaiko visų virtualiųjų valiutų turtu. Pažymėtina, kad FIN-FSA pripažįsta, kad jos terminologija skiriasi nuo FATF terminologijos, bet nepaisant to, mano, kad šis skirtumas yra minimalios reikšmės, nes, jos nuomone, virtualiosios valiutos yra palyginti nedidelis reiškinys.¹⁹²

Žvelgiant į Azijos regioną, viena iš progresyviausių savo požiūriu į virtualų turtą bei virtualaus turto paslaugų teikėjus yra Japonija. Dar 2016 m. Japonija reaguodama į 2015 m. išleistas FATF virtualaus turto gaires iš dalies pakeitė Mokėjimo paslaugų įstatymą ir Nusikalstamu būdu įgytų pajamų pervedimo prevencijos įstatymą, taip pagal 14 rekomendaciją įsteigė virtualaus turto paslaugų teikėjų stebėsenos grupę.

¹⁹⁰ FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, 89-90 psl., 2021 m.

¹⁹¹ Velkes, Gabrielle Chasin, International Anti-Money Laundering Regulation Of Virtual Currencies And Assets , 2020

¹⁹² *Ibid.*

Šalis, taip pat kaip ir Italija, vykdo registracijos procedūrą, kurios metu yra įvertinama pareiškėjų AML / CFT programos, daugiausia dėmesio skirdama pareiškėjų rizikos vertinimo ir jų verslo plano suderinamumui. Pažymėtina, nacionaliniu lygiu vykdoma ir FATF rekomenduojama statistikos analizė, kasmet iš įpareigotųjų subjektų surenkami AML/CFT statistiniai ir kokybiniai duomenys, siekiant įvertinti jų rizikos poveikį.

Šalyje dalinai vykdoma sektoriaus savireguliacija, įsteigta tam skirta organizacija su kuria yra koordinuojami veiksmai, siekiama įvesti kelionių taisyklę, kaip įtvirtintą 16 rekomendacijoje.¹⁹³

Galiausiai, Jungtinės Amerikos Valstijos, kaip finansų įstaigoms taikomos kovos su pinigų plovimu ir teroristų finansavimu reguliavimo ir priežiūros sistemos dalį, sukūrė plačią virtualaus turto pinigų plovimo ir teroristų finansavimo prevencijos ir kovos su juo sistemą, pagal kurią šios srities paslaugų teikėjams ir veiklai taikomas iš esmės toks pat reguliavimas kaip ir su neskaitmeniniu turtu susijusiai veiklai pagal finansų įstaigoms taikomą kovos su pinigų plovimu ir teroristų finansavimu reguliavimo sistemą.

Valstybė ypač susitelkusi į represinį modelį, Teisingumo departamentas ir kitos federalinės agentūros imasi agresyvių civilinių ir baudžiamųjų vykdymo užtikrinimo veiksmų prieš neteisėtą veiklą, susijusią su skaitmeniniu turtu, tiek administracinėse procedūrose, tiek federaliniame teisme, siekdamos kovoti su neteisėta veikla, susijusia su skaitmeniniu turtu. Įdomu, kad kitaip nei dauguma šalių, kurios net nereguliuoja šiuos srities, JAV yra iškėlusios bylų ir patraukusios atsakomybės ir pavienių tarpusavio mainų operatorius (*peer-to-peer*).

Tačiau svarbu pastebėti, kad remiantis ataskaita, nors 128 jurisdikcijos informavo apie savo pažangą įgyvendinant peržiūrėtus FATF standartus, t. y. pranešė, kad priėmė teisės aktus, būtinus persvarstytiems FATF standartams įgyvendinti, tačiau net 70 jurisdikcijų dar neįgyvendino peržiūrėtų standartų savo nacionalinėje teisėje.¹⁹⁴

Apibendrinant galima būtų padaryti išvadą, jog tokia švelnioji teisė, nors ir yra neformali, o susitarimai teisiškai neprivalomi pagal bendrąją tarptautinę teisę, suteikia valstybėms esminį lankstumą ir laisvę vystyti laikui bėgant, taip pat galimybę vidaus teisėje nustatytus įsipareigojimus pritaikyti prie iškilusių problemų. Skirtingai nuo tradicinių sutartinių įsipareigojimų, kuriuos pasirašiusios vyriausybės turi paversti vidaus teise, kad jie turėtų privalomą teisinę galią, prevencinės kovos su pinigų plovimu priemonės, kaip FATF rekomendacijos, įgyvendinamos taikant įvairius, neįpareigojančius mechanizmus. Išskirtinai svarbus FATF rekomendacijų bruožas - dėmesys jų įgyvendinimui, kuris pasiekiamas FATF

¹⁹³ FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, 91-93 psl., 2021 m.

¹⁹⁴ *Ibid.* 2 psl.

vertinant rekomendacijų vykdymą. Nepaisant to, kad FATF rekomendacijos nėra teisiškai privalomos, jos padarė didelę įtaką prevencinių nacionalinių kovos su pinigų plovimu teisės aktų ir politikos formavimui visame pasaulyje. Tačiau matome, jog šalys, nors remdamosis aprašytais standartais, tačiau juos pritaiko pagal savo poreikius, kartais didesnę dėmesį skirdamos vienoms rekomendacijoms negu kitoms. Toks harmonizuoto požiūrio trūkumas gali sąlygoti frakcionuotą pinigų plovimo prevencijos sistemą, blogiausiu atveju, sukuriant reguliacinius arbitražus, kuriais galėtų pasinaudoti potencialūs nusikaltėliai.

3.3.2 Pinigų plovimo ir teroristų finansavimo standartų minkštosios normatyvinės struktūros poveikis Europos Sąjungos teisei

Kaip matoma, FATF rekomendacijos kuria pasaulines normas, darančias įtaką AML/CTF teisės aktams visame pasaulyje, ypač Europos Sąjungoje. Nors yra neprivalomos formos, tačiau rekomendacijos įsitvirtino kaip tarptautinis standartų nustatinėtojas kovos su pinigų plovimu ir terorizmo finansavimu srityse, ir dabar tos pačios neprivalomos rekomendacijos įgijo beveik privalomą pobūdį dėl didelės FATF narių dalies ir su rekomendacijomis susijusio sankcijų mechanizmo. Be to, šios beveik privalomos normos dažnai buvo paverstos teisiškai privalomomis tarptautinių kietųjų priemonių dalimis. Kaip pažymi L. Borlini su F. Montanaro, todėl AML/CTF srityje egzistuoja gilus ir dinamiškas ryšys tarp švelniosios ir griežtosios teisės, nes viena teisė remiasi kita ir stiprina ją nuolatinėje partnerystėje.¹⁹⁵

ES, kaip ir FATF, parengė kovos su pinigų plovimu ir teroristų finansavimu strategiją, kuri grindžiama prevencija ir baudžiamuoju persekiojimu. Europos Sąjunga buvo pirmoji regioninė organizacija, sukūrusi išsamią kovos su pinigų plovimu ir teroristų finansavimu reguliavimo sistemą. Tačiau dėl didelės ES valstybių narių patirties baudžiamosiose bylose kriminalizavimas pasirodė esąs sunkiau įgyvendinamas nei prevencija. ES teisėje nebuvo nei bendros šio nusikalstamo pažeidimo apibrėžties, nei suderintos bausmių už jį sistemos.¹⁹⁶

Pirmoji Kovos su pinigų plovimu direktyva (AMLD1) buvo priimta dar 1990 m., siekiant užkirsti kelią piktnaudžiavimui finansų sistema pinigų plovimo tikslais. Joje buvo numatyta, kad įpareigotieji subjektai, užmegzdami verslo santykius, turi taikyti deramo klientų tikrinimo reikalavimus, tokio kaip - nustatyti ir patikrinti klientų tapatybę, stebėti sandorius ir pranešti apie įtartinus sandorius. Šie teisės aktai buvo nuolat peržiūrimi siekiant sumažinti su pinigų plovimu ir

¹⁹⁵ Borlini, Leonardo, Montanaro, Francesco, The Evolution of The Eu Law Against Criminal Finance: The “Hardening” Of FATF Standards Within The EU, 2017

¹⁹⁶ *Ibid.*

teroristų finansavimu susijusią riziką.¹⁹⁷ Diskutuoiant dėl Pirmosios kovos su pinigų plovimu direktyvos, Europos Komisija ir valstybės narės nusprendė, kad pinigų plovimas ES lygmeniu turėtų būti uždraustas, o ne kriminalizuotas. Tačiau šioje direktyvoje taip pat buvo pateikta deklaracija, kurioje valstybės narės raginamos kriminalizuoti pinigų plovimą. Vėlesnėse pinigų plovimo prevencijos direktyvose buvo laikomasi to paties požiūrio.¹⁹⁸

Po daugiau nei 10 metų buvo priimta antroji direktyva, iš dalies pakeitusi pirmąją.¹⁹⁹ Po to kai 1995 ir 1998 m. Europos Komisija pateikė ataskaitas apie AMLD1 įgyvendinimą ir 1996 m. FATF atnaujino savo rekomendacijas. Atsižvelgdama į šiuos pokyčius, Europos Komisija pasiūlė direktyvą, kuri iš esmės pakeitė AMLD1. 2001 m. buvo priimta Antroji kovos su pinigų plovimu direktyva (AMLD2). Į naująją direktyvą įtraukti tokie įpareigotieji subjektai kaip kazino, prekyautojai didelės vertės prekėmis, nekilnojamojo turto agentai ir teisininkai. Joje taip pat gerokai išplėsta, kas pagal kovos su pinigų plovimu teisinę sistemą laikoma nusikalstama veikla.²⁰⁰ Šios direktyvos buvo 2005 m. buvo apjungtos trečiosios direktyvos (AMLD3).²⁰¹ 2004 m. atnaujinus FATF rekomendacijas ir daugiau dėmesio skyrus terorizmo finansavimo problemai, pinigų plovimo situacija vėl pasikeitė. Todėl Europos Komisija pasiūlė visiškai naują direktyvą, kuri pakeitė esamą teisinę sistemą. Šiame pasiūlyme taip pat nustatytas rizika pagrįstas požiūris, pagal kurį mažesnės rizikos atvejais siūloma taikyti supaprastintą deramą patikrinimą, o didelės rizikos atvejais - sustiprintą deramą patikrinimą.²⁰² Trečiąją pakeitusi ketvirtoji (AMLD4) direktyva įsigaliojo 2015 m.²⁰³ Po jos netrukus sekė ir penktoji direktyva (AMLD5), įsigalėjusi 2020 metų sausio mėnesį ir iš dalies pakeitusi ketvirtąją.²⁰⁴ Nepraėjus nė pilniems metams, 2020 gruodžio mėn. įsigalėjo dar viena nauja direktyva, skirta kovoti su pinigų plovimu

¹⁹⁷ European Commission, Anti-money laundering and countering the financing of terrorism, https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en

¹⁹⁸ Borlini, Leonardo, Montanaro, Francesco, The Evolution of The Eu Law Against Criminal Finance: The “Hardening” Of FATF Standards Within The EU, 2017

¹⁹⁹ Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering - Commission Declaration

²⁰⁰ Vandezande, Niels, Virtual Currencies: A Legal Framework, 281 psl., 2018 m.

²⁰¹ Komisijos Direktyva 2006/70/EB, 2006 m. rugpjūčio 1 d., nustatanti Europos Parlamento ir Tarybos direktyvos 2005/60/EB įgyvendinimo priemones, susijusias su „politikoje dalyvaujančių asmenų“ apibrėžimu, ir supaprastinto deramo klientų tikrinimo procedūroms taikomus techninius kriterijus bei išimtis, suteikiamas dėl to, kad finansinė veikla verčiamasi retai arba labai ribotai

²⁰² Vandezande, Niels, Virtual Currencies: A Legal Framework, 281 psl., 2018 m.

²⁰³ Europos Parlamento ir Tarybos Direktyva (ES) 2015/849, 2015 m. gegužės 20 d., dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos, kuria iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 ir panaikinama Europos Parlamento ir Tarybos direktyva 2005/60/EB bei Komisijos direktyva 2006/70/EB

²⁰⁴ Europos Parlamento ir Tarybos Direktyva (ES) 2018/843, 2018 m. gegužės 30 d, kuria iš dalies keičiama Direktyva (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos ir iš dalies keičiamos direktyvos 2009/138/EB ir 2013/36/ES

baudžiamosiomis teisės priemonėmis.²⁰⁵ Tokia direktyvų kaita per sąlyginai trumpą laiko tarpą, galima teigti, akivaizdžiai parodo, jog pinigų plovimo problematika yra ypač aktuali ir greitai evoliucionuojanti bei kelianti vis naujų iššūkių.

2012 m. Europos Komisija pripažinus, kad reikia periodiškai peržiūrėti teisinę sistemą, kad būtų atsižvelgta į naujai kylančias grėsmes, Komisija atkreipė dėmesį į keletą nedidelių pakeitimų, kuriuos reikėjo atlikti, kad teisinė sistema atitiktų naujai iš dalies pakeistas FATF rekomendacijas.²⁰⁶

Kaip teigiama ALMD4 preambulėje, ši Direktyva skirta kovoti su pinigų plovimo grėsme bei matomas jau minėtas siekis suderinti Europos Sąjungos reguliavimą su FATF rekomendacijomis. Direktyvoje pateikiama gana plati pinigų plovimo samprata, kuri skamba taip:

- „Turto konversija arba perdavimas, žinant, kad šis turtas yra gautas iš nusikalstamos veiklos arba dalyvaujant tokioje veikloje, siekiant nuslėpti arba užmaskuoti neteisėtą turto kilmę arba siekiant padėti kokiam nors asmeniui, kuris dalyvauja tokioje veikloje, išvengti teisinių to asmens veiksmų pasekmių;
- Turto tikrojo pobūdžio, šaltinio, vietos, disponavimo, judėjimo, teisių ar nuosavybės teisių į turtą slėpimas arba užmaskavimas, žinant, kad toks turtas yra gautas iš nusikalstamos veiklos arba dalyvaujant tokioje veikloje;
- Turto įsigijimas, turėjimas arba naudojimas, jo gavimo metu žinant, kad šis turtas gautas iš nusikalstamos veiklos arba dalyvaujant tokioje veikloje;
- Dalyvavimas, bendrininkavimas, pasikėsinimas įvykdyti ir pagalba, kurstymas, palankesnių sąlygų sudarymas ir patarimai vykdant bet kurį iš a, b ir c punktuose nurodytų veiksmų.“²⁰⁷

Sąvoka turtas, pagal 3 str. 3 d. yra suprantama, kaip: „<...> bet koks fizinis arba ne fizinis, kilnojamasis arba nekilnojamasis, materialus arba nematerialus turtas ir bet kokios formos, įskaitant elektroninę ar skaitmeninę, teisiniai dokumentai arba priemonės, įrodantys nuosavybės teisę į šį turtą arba su juo susijusias teises“. O veikla yra pripažįstama pinigų plovimu net tada, kai veiksmai, dėl kurių atsirado turtas, skirtas pinigų plovimui, buvo vykdomi kitos valstybės narės teritorijoje ar trečiosios valstybės teritorijoje (1 str. 4d).

Pagal 2 straipsnio 1 dalį prie privalomų subjektų priskiriamos kredito įstaigos, finansų įstaigos, fiziniai ar juridiniai asmenys, vykdantys profesinę veiklą, pavyzdžiui, auditoriai, mokesčių konsultantai, taip pat notarai ir kiti nepriklausomi teisininkai, dalyvaujantys sudarant finansinius ar nekilnojamojo turto sandorius ar įmonių paslaugų teikėjai, nekilnojamojo turto agentai ir

²⁰⁵ Europos Parlamento ir Tarybos Direktyva (ES) 2018/1673, 2018 m. spalio 23 d., dėl kovos su pinigų plovimu baudžiamosios teisės priemonėmis

²⁰⁶ Vandezande Niels, Virtual Currencies: A Legal Framework, 282 psl., 2018 m.

²⁰⁷ *Ibid.* 1 str. 3 d.

azartinių lošimų paslaugų teikėjai. Pažymėtina, kad 4 straipsnio 1 dalyje reikalaujama, kad valstybės narės išplėstų direktyvos taikymo sritį, įtraukiant kitas profesijas ir kitų kategorijų įmones, kurios užsiima veikla, kuri ypač gali būti naudojama pinigų plovimui ar teroristų finansavimui, tačiau nepatenka į 2 straipsnyje išvardytų įpareigotųjų subjektų sąrašą. Galima daryti išvadą, kad tokia pareiga įpareigoja valstybes vykdyti nuolatinę pinigų plovimo nusikaltimų priežiūrą ir rizikos vertinimą.

Atkreiptinas dėmesys, kad įpareigotieji subjektai privalėjo atlikti deramą klientų patikrinimą, kuris taip pat minimas FATF rekomendacijose, ir apima kliento identifikavimą, kliento tapatybės nustatymą. Kadangi direktyva grindžiama rizikos nustatymu, valstybės narės gali pasirinkti mažesnės rizikos sektorius ir leisti įpareigotoms įmonėms atlikti paprastesnį deramą klientų patikrinimą (15 straipsnio 1 dalis).

Galiausiai kiekviena šalis narė, turi įsipareigoti įsteigti finansinės žvalgybos padalinį, kuris veiksmingai kovotų su pinigų plovimu ir terorizmo finansavimu. Įpareigotieji subjektai privalo bendradarbiauti su FŽP ir, jei turi pagrindo manyti, savo iniciatyva pranešti apie lėšas, gaunamas iš neteisėtos ar nusikalstamos veiklos.²⁰⁸ Atsižvelgiant į tai, kad pinigų plovimas yra tarptautinio pobūdžio, reikalaujama bendradarbiauti tiek šalies viduje, tiek tarptautiniu mastu.²⁰⁹ Galima matyti, jog šios taisyklės tiesiogiai siejasi su FATF ypač skatinamu politikos formavimu, kuris pagrįstas bendradarbiavimu tiek nacionaliniu, tiek tarptautiniu lygmeniu.

Šio darbo apimtyje, nors virtualiosios valiutos tiesiogiai nepateko į AMLD4 taikymo sritį, platus turto sąvokos aiškinimas rodo, kad kovos su pinigų plovimu teisinė sistema neapsiriboja įprastais, fiziniais banknotais ar monetomis, bet apima ir materialų bei nematerialųjį turtą.²¹⁰ Šiuo atveju galima teigti, kad virtualiosios valiutos gali būti laikomos nematerialiuoju turtu ir, kad kovos su pinigų plovimu taisyklės gali būti taikomos virtualiosioms valiutoms, gautoms vykdant neteisėtą veiklą arba naudojamoms teroristų finansavimui.²¹¹

Tačiau N. Vandezande teigimu, kiti suabejojo ar virtualiosios valiutos paslaugas teikiantys subjektai, tokie kaip virtualių valiutų keityklos, galėtų būti laikomi įpareigotaisiais subjektais, kuriems taikoma kovos su pinigų plovimu teisinė sistema. Remiantis direktyva, įpareigotieji subjektai turėjo pranešti apie veiklą, kuri gali būti susijusi su pinigų plovimu arba teroristų finansavimo veikla. Todėl tokiu atveju, jeigu virtualiųjų valiutų paslaugų teikėjai nėra įtraukiami į kovos su pinigų plovimu teisinės sistemos taikymo sritį, manomai, apie pinigų plovimo veiklą

²⁰⁸ *Ibid.* 33 1 d. a p.

²⁰⁹ *Ibid.* 3 skirsnis. Bendradarbiavimas

²¹⁰ Vandezande, Niels, *Virtual Currencies: A Legal Framework*, 295 psl., 2018 m.

²¹¹ *Ibid.*

naudojant virtualiąsias valiutas nebūtų pranešama. Todėl visa laiką buvo išlikęs klausimas, ar kiti virtualiosios valiutos paslaugų teikėjai gali patekti į kitų įpareigotųjų subjektų taikymo sritį.²¹²

Taigi, AMLD4 kaip ir prieš tai buvusiose direktyvose virtualios valiutos nėra minimos, tačiau kiek vėliau buvo iniciuoti teisėkūros veiksmai, kad su virtualiomis valiutomis susiję subjektai būtų įtraukti į direktyvų prieš pinigų plovimą taikymo sritį. Dėl šios priežasties svarbu atsižvelgti kokių veiksmų buvo imamasi bei koks buvo atliekamas virtualių valiutų vertinimas iki įsigaliojant AMLD5.

Praėjus vos vieneriems metams po AMLD4 priėmimo, Europos Komisija pateikė Europos Parlamentui ir Tarybai komunikatą su veiksmų planu, kuriuo siekiama sustiprinti kovą su terorizmo finansavimu, kurį paskatino tuo metu ES ir kitose šalyse įvykdyti teroro aktai. Kadangi Europos Sąjungos pinigų plovimo politika neatsiejama nuo teroristų finansavimo, todėl direktyvos peržiūra kovos su terorizmo finansavimu klausimais taikoma ir pinigų plovimo nusikaltimams, taip pat identifikuota, jog virtualiosios valiutos šiais klausimais sukuria naujų iššūkių.²¹³ Komisija pasiūlė iš dalies keisti Kovos su pinigų plovimu nuostatas, įtraukiant virtualios valiutos konvertavimo platformas. Įvertinta reali rizika, jog siekdamos nuslėpti sandorius, teroristų organizacijos gali pasinaudoti virtualiomis valiutomis, nes tokie sandoriai, nors ir fiksuojami, tačiau nėra jokio įtartinai veiklai nustatyti skirto pranešimų teikimo mechanizmo, kuris prilygtų tam, kuris yra tradicinėje bankininkystėje. Kadangi buvusiu laiku virtualios valiutos nebuvo reglamentuojamos, Komisija pasiūlė anoniminį valiutos konvertavimą pavesti kompetentingų institucijų kontrolei, išplėsdama Kovos su pinigų plovimu direktyvos taikymo sritį taip, kad ji aprėptų virtualiosios valiutos konvertavimo platformas, siekiant užtikrinti, kad jos būtų prižiūrimos pagal kovos su pinigų plovimu ir teroristų finansavimu teisės aktus nacionaliniu lygmeniu. Taip pat buvo svarstoma, kaip reguliavimo perimetras galėtų pasiekti ir prie interneto prijungtu virtualių valiutų piniginių paslaugų teikėjus.²¹⁴

Tais pačiais metais Komisija teigė, kad valdžios institucijos nekontroliuoja virtualiųjų valiutų sandorių Europos Sąjungoje ir kad nėra konkrečių teisės aktų, kuriuose būtų nustatyti stebėsenos reikalavimai. Todėl virtualiųjų valiutų keityklos ir piniginių saugojimo paslaugų teikėjai turėtų būti paskirti įpareigotiems subjektams pagal ketvirtąją Kovos su pinigų plovimu direktyvą ir įpareigoti įgyvendinti prevencines priemones bei pranešti apie įtartiną veiklą. Komisijos teigimu, naujosios rekomendacijos padėtų sumažinti su virtualiosiomis valiutomis

²¹² *Ibid.* 298 psl.

²¹³ Europos Komisija, Komisijos komunikatas Europos Parlamentui ir Tarybai, Kovos su teroristų finansavimu stiprinimo veiksmų planas, 3 psl., 2016 m., https://eur-lex.europa.eu/resource.html?uri=cellar:c6e0de37-ca7c-11e5-a4b5-01aa75ed71a1.0010.02/DOC_1&format=PDF

²¹⁴ *Ibid.* 5 psl.

susijusį anonimiškumą, todėl padidėtų kovos su pinigų plovimu ir teroristų finansavimu veiksmingumas.²¹⁵

2017 m., Europos Komisijos ataskaitoje Europos Parlamentui ir Tarybai dėl pinigų plovimo ir teroristų finansavimo rizikos, turinčios įtakos vidaus rinkai ir tarpvalstybinei veiklai, iš naujo įvertinama, jog virtualiosios valiutos kelia didelę pinigų plovimo ir teroristų finansavimo riziką. Teigiama, kad nors kai kurios valstybės narės nusprendė šiuos finansinius produktus reglamentuoti pagal nacionalinius teisės aktus, visa ES teisėkūros sistema šiuo atžvilgiu nebėra tinkama. Taigi, nors ir stengiamasi siūlyti naujus techninius sprendimus, kad būtų padidintas finansinių paslaugų greitis, saugumas ir veiksmingumas, tai sukuria daugiau naujų galimybių nusikaltėliams.²¹⁶ Komisijos pasiūlyme dėl AMLD4 pakeitimo buvo teigiama, kad tiek virtualiųjų valiutų mainų platformos, tiek piniginių paslaugų teikėjai būtų įpareigoti iki minimumo sumažinti sandorių duomenų anonimiškumą. Be to, griežtesni atsakingų institucijų, įskaitant priežiūros institucijas, bendradarbiavimo reikalavimai padės veiksmingai perduoti informaciją tarp šalių. Kai kurie iš sprendimų klausimų apimtų padidinto deramo klientų tikrinimo procesų pobūdį didelės rizikos trečiosiose šalyse, o tai leistų sukurti vieningesnę strategiją šioje srityje. Be to, būtų galima išplėsti taikymo sritį ir padaryti lengviau prieinamą tikrųjų savininkų registruose esančią informaciją.²¹⁷

3.3.3 AMLD5 veikimo sritis

Kaip jau minėta skyriuje apie AMLD4 taikymo sritį, nuo pat direktyvos taikymo pradžios ji buvo pagrindinė teisėkūros priemonė, skirta užkirsti kelią Europos Sąjungos finansų sistemos naudojimui pinigų plovimui ir terorizmo finansavimui. Siekiant spręsti su pinigų plovimu ir teroristų finansavimu susijusias problemas, direktyvoje buvo nustatyta teisinė sistema, pagal kurią buvo reikalaujama, kad valstybės narės nustatytų riziką, ją išanalizuotų ir imtųsi priemonių jai sumažinti.

Atkreiptinas dėmesys, jog FATF rekomendacijas, AMLD4 bei AMLD5 direktyvas jungia bendras bruožas - rizikas paremtas požiūris, kuriuo siekiama palengvinti rinkos dalyviams tenkančią naštą ir palengvinti reguliavimo priemonių įgyvendinimą. Laikantis šio požiūrio daroma prielaida, kad kovos su pinigų plovimu ir teroristų finansavimu sistemos sudedamosios dalys -

²¹⁵ Europos Komisija, Pasiūlymas Europos Parlamento Ir Tarybos Direktyva iš dalies keičianti Direktyvą (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos ir iš dalies keičianti Direktyvą 2009/101/EB, 12 psl., 2016 m.

²¹⁶ European Commission, Report From The Commission To The European Parliament And The Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 2017

²¹⁷ *Ibid.* 12 psl.

ypač reguliavimas, reikalavimų laikymasis ir kontrolė - turėtų būti apibrėžtos atsižvelgiant į pavojus, kuriems sumažinti jos skirtos. Todėl ji grindžiama tikslais, kurių reikia siekti taikant tam tikrus elgesio standartus, kuriuos turi apibrėžti pačios įpareigosios šalys, atsižvelgdamos į unikalias aplinkybes ir daugeliui situacijų būdingus pavojus.²¹⁸

Kaip rodo ES kovos su pinigų plovimu politika, rizika grindžiamas požiūris paprastai yra veiksmingesnis už taisyklėmis grindžiamą požiūrį, t. y. kovos su pinigų plovimu taisyklių rinkinį, kuriame neatsižvelgiama į skirtingą organizacijų pobūdį ir rizikos pobūdį. Pirmiausia, jis suteikia įpareigotiesiems subjektams paprastą ir nebrangų metodą mažmeninei bankininkystei ir atvejams, apskritai neturintiems išskirtinių rizikos ypatybių. Tuo tarpu kai rizikos dydis didėja, įpareigosios organizacijos privalo rinkti daugiau informacijos apie savo klientus.²¹⁹

Kalbant apie pinigų plovimą pasitelkiant virtualias valiutas, penktosios direktyvos preambulėje teigiama, jog dabartinės vis labiau populiarėjančios finansinės technologijos, nepaisant didėjančios jų sklaidos, nebuvo reguliuojamos Europos Sąjungos teisės aktais. Todėl siekiant neatsilikti nuo technologinės pažangos ir besiformuojančių tendencijų, buvo ypač svarbu imtis papildomų priemonių.²²⁰ Tai paskatino daugiau dėmesio skirti virtualiosios valiutos konvertavimo paslaugų teikėjams ir depozitinių piniginių paslaugų teikėjams, kuriems netaikomas Europos Sąjungos reguliavimas. Tad atsirado būtinybė išplėsti AMLD4 taikymą, įtraukiant virtualios valiutos konvertavimo ir depozitinių piniginių paslaugų teikėjus.²²¹

AMLD5 direktyvoje pirmą kartą reikalaujama, kad du virtualiųjų valiutų rinkos dalyviai - keityklos ir depozitinių piniginių paslaugų teikėjai - laikytųsi kovos su pinigų plovimu pareigų. Šioje naujoje direktyvoje abu įpareigotieji subjektai yra laikomi rinkos prižiūrėtojais, todėl privalo nustatyti ir stebėti savo naudotojus, siekiant sumažinti virtualių valiutų suteikiamą anonimiškumą, kuris kelia iššūkių veiksmingam baudžiamajam persekiojimui.²²² Tokiu būdu užtikrinamas taip reikalingas skaidrumas Europos Sąjungos virtualių valiutų sektoriuje. ALMD5 reguliavimo perimetru siekiama užtikrinti, kad virtualiųjų valiutų konvertavimo į *fiat* valiutas paslaugų teikėjai, taip pat depozitinių piniginių paslaugų teikėjai, prieš teikdami savo produktus ar paslaugas, atliktų deramą klientų patikrinimą.

Prisimenant virtualių valiutų sąvoką, šioje direktyvoje jos apibrėžiamos kaip: „virtualioji valiuta – skaitmeninė vertės forma, kuri nėra išleista arba užtikrinta centrinio banko ar viešosios valdžios institucijos, nebūtinai susieta su teisės aktais nustatyta valiuta ir neturinti teisinio valiutos

²¹⁸ Borlini, Leonardo, Montanaro, Francesco, The Evolution of The Eu Law Against Criminal Finance: The “Hardening” Of FATF Standards Within The EU, 2017

²¹⁹ *Ibid.*

²²⁰ Europos Parlamento Ir Tarybos Direktyva (ES) 2018/843, 2018 m. gegužės 30 d, kuria iš dalies keičiama Direktyva (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos ir iš dalies keičiamos direktyvos 2009/138/EB ir 2013/36/ES

²²¹ *Ibid.*

²²² Soana, Giulio, Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?, Wiley, 2021

ar pinigų statuso, tačiau pripažįstama fizinių arba juridinių asmenų kaip atsiskaitymo priemonė ir galinti būti perduodama, laikoma arba parduodama elektroniniu būdu“²²³, galima išskirti požymius, jog į AMLD5 taikymo sritį patenka tos valiutos, kurios gali būti perduotos, laikomos ar parduodamos elektroniniu būdu, nėra atsižvelgiama į tai ar tai dvikryptės ar vienkryptės virtualios valiutos, t. y. ar jos įsigyjamos už realius pinigus ir vėliau panaudojamos tik virtualiuose pasaulyuose, įsigyjant prekes ar paslaugas, ar jos gali būti pervedamos į kitas virtualias valiutas ir jomis prekiaujama virtualių valiutų rinkose.

Autorė norėtų atkreipti dėmesį, jog direktyvoje lietuvių kalba vartojama sąvoka „atsiskaitymo priemonė“, tačiau anglų kalba ta pati sąvoka įvardinama kaip „*means of exchange*“, kas galėtų būti suprantama kaip „mainų priemonė“. Būtent dėl pastarojo supratimo kai kurie mokslininkai analizuoja šią sąvokos dalį. Šiuo atveju galima būtų pažymėti L. Haffke *et al.* nuomonę, jog kiekvienas virtualios valiutos naudojimas apima jos mainus - arba į kitą virtualią valiutą arba į *fiat* valiutą, arba į kitą prekę ar paslaugą. Tačiau šių autorių nuomone, toks platus aiškinimas yra klaidingas, nes taip plačiai aiškinama sąvoka neturėtų beveik jokios ribojamosios funkcijos. Tokiu atveju, beveik viskas (net ir pvz., akmenys) gali būti tokiu būdu naudojama kaip mainų priemonė. Todėl kovos su pinigų plovimu teisės aktai galėtų būti išplėsti iki sistemos, kuria siekiama stebėti visus privačių prekių sandorius.²²⁴

Atsižvelgiant į papildytą įpareigotųjų subjektų sąrašą galima atrasti spragų. Pagal AMLD5 reguliavimą, į įpareigotųjų subjektų sąrašą patenkančios virtualiųjų valiutų keityklos, rodo, kad virtualiųjų valiutų kovos su pinigų plovimu reguliavimo taikymo sritis apsiriboja tik tam tikromis dvikrypčių schemų virtualiosiomis valiutomis, t. y. tada kai už *fiat* valiutas yra įsigyjamos virtualios valiutos ir atvirkščiai. Į taikymo sritį nepatenka kitos virtualiųjų valiutų schemas, įskaitant virtualiųjų valiutų mainus į kitas virtualias valiutas. Taip pat nepatenka ir virtualios valiutos, naudojamos prekėms ir paslaugoms gauti, nereikalaujant jų keisti į teisėtą mokėjimo priemonę ar panašias priemones, arba naudojantis piniginės paslaugų teikėjo paslaugomis.²²⁵ Todėl šioje vietoje sudaroma galimybė virtualių valiutų keitykloms išvengti prievolių pagal AMLD5. Galima daryti prielaidą, jog ES teisės aktų leidėjai pasirinko nereguliuoti virtualių valiutų keityklų į virtualias valiutas dėl fakto, jog jos neturi tiesioginio ryšio su *fiat* valiutų sistema. L. Haffke *et al.* nuomone, toks argumentas yra ypač klaidingas. Visų pirma, pačioje direktyvoje pripažįstama, kad nusikaltėliai gali pervesti pinigus į Sąjungos finansų sistemą. Be kita ko, *fiat*

²²³ Europos Parlamento Ir Tarybos Direktyva (ES) 2018/843, 2018 m. gegužės 30 d, kuria iš dalies keičiama Direktyva (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos ir iš dalies keičiamos direktyvos 2009/138/EB ir 2013/36/ES

²²⁴ Haffke, Lars, et al. Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them, 2020

²²⁵ Cancelli, Lorenzo, The Growing Crypto-assets Threat to Anti-money Laundering: How Institutions Are Coping with This Phenomenon, 15 psl., 2020 m., https://www.unive.it/pag/fileadmin/user_upload/dipartimenti/economia/doc-eng/eudifin/wp/WP12.pdf

valiutos sistemoje klasikinės *fiat* valiutos keityklos jau yra įpareigotieji subjektai pagal AMLD4. Įtraukdami virtualių valiutų keityklas, kaip įpareigotuosius subjektus, įstatymų leidėjai AML reguliavimo požiūriu sinchronizuotų virtualiųjų valiutų sistemas su *fiat* valiutų sistema. Tai yra svarbu, nes virtualių mainai kelia panašią pinigų plovimo ir terorizmo finansavimo riziką, nes keičiama viena valiuta į kitą. Todėl logiška, kad virtualių valiutų mainams būtų taikomi kovos su pinigų plovimu reikalavimai.²²⁶ Šio darbo autorė pritaria L. Haffke *et al.* teiginiui, jog tai būtų lengviausia padaryti pakeitus paslaugų teikėjų, teikiančių virtualiųjų valiutų ir *fiat* valiutų mainų paslaugas, apibrėžtį. Tad būtų rekomenduojama valstybėms narėms iš dalies pakeisti įpareigotojo subjekto apibrėžtį, jog būtų įtraukiami paslaugų teikėjai, teikiantys mainų paslaugas tarp virtualiųjų valiutų ir *fiat* valiutų arba tarp virtualiųjų valiutų.

Pereinant prie depozitinių piniginių paslaugų teikėjų, remiantis AMLD5 1 str. d. 19 p. tokių paslaugų teikėjas apibūdinamas kaip: „subjektas, kuris teikia paslaugas, skirtas privatiems šifravimo raktams savo klientų vardu apsaugoti ir virtualiosioms valiutoms laikyti, saugoti ir perduoti“, tai galima suprasti, kaip subjektus, kurie teikia saugojimo paslaugas klientų vardu. Be to, kaip nurodyta anksčiau, yra programinės įrangos piniginių paslaugų teikėjų, kurie teikia paslaugas, skirtas prisijungti prie virtualiųjų valiutų tinklų. Kadangi jie nelaiko raktų savo klientų vardu, o tik suteikia galimybę klientams saugoti savo virtualiąsias valiutas, galima daryti pagrįstą išvadą, kad tokie programinės įrangos piniginių paslaugų teikėjai nėra saugotojai piniginių paslaugų teikėjų atžvilgiu. Todėl AMLD5 reguliavimo perimetras neapima visų galimų piniginių paslaugų teikėjų.²²⁷ G. Soana teigimu, asmuo, norintis naudoti virtualią valiutą, neteisėtais tikslais, gali tiesiog laikyti savo raktus šaltosiose piniginėse ir taip išvengti bet kokios priežiūros.²²⁸ Be kita ko, sąsajų, leidžiančių sąveikauti su blokų grandine rankiniu būdu įvedant privatųjį raktą, teikėjai taip pat nepatenka į AMLD5 taikymo sritį.

Šiuo klausimu pasisakantys L. Haffke *et al.*, teigia, kad AMLD5 gali būti netaikoma visiems piniginių paslaugų teikėjams saugotojams, nes jie užuot saugoję privačius raktus, gali reikalauti, kad naudotojai įvestų privačius raktus rankiniu būdu. Jei piniginių paslaugų teikėjai taip pritaikytų savo verslo modelį, jie nebebūtų įpareigotieji subjektai pagal AMLD5. Šie mokslininkai kelia klausimą ar AMLD5 taikymo sritis turėtų būti išplėsta, įtraukiant ne saugotojų piniginių paslaugų teikėjus ir sąsajos teikėjus. Autorių nuomone, tai nėra pagrįsta, nes jei AML reguliuotų visų trijų tipų paslaugų teikėjus, nebebūtų įmanoma pervesti virtualiųjų valiutų blokų grandinėje be pirmojo identifikavimo, kas reiškia, jog joks sandoris nebebūtų įmanomas įvykdyti prisidengiant pseudonimu ar anonimiškai. L. Haffke *et al.* teigimu, palyginti su gryniaisiais pinigais

²²⁶ Haffke, Lars, et al. Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them, 2020

²²⁷ Soana, Giulio, Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?, Wiley, 2021

²²⁸ *Ibid.*

virtualiosios valiutos būtų pernelyg reguliuojamos, nes bet koks sandoris grynaisiais pinigais tarp dviejų žmonių gali būti visiškai anonimiškas. Todėl svarbu pažymėti, jog blokų grandinės sandorio vertinimas pagal kovos su pinigų plovimu įstatymą neturėtų priklausyti nuo naudojamos piniginės ar piniginių paslaugų teikėjo tipo. Kadangi privačiam sandoriui grynaisiais pinigais AML įstatymas netaikomas, tai neturėtų būti taikomas ir privačiam sandoriui virtualiomis valiutomis. Jei visos virtualių valiutų keityklos taps įpareigotaisiais subjektais, nėra reikalo piniginių paslaugų teikėjams taikyti AML įstatymą.²²⁹

Kadangi AMLD5 daugiausia dėmesio skiriama virtualiųjų valiutų konvertavimo į *fiat* valiutas pinigus ir atvirkščiai paslaugų teikėjams, taip pat piniginių paslaugų teikėjams, galima sakyti, kad kitiems virtualiųjų valiutų rinkos dalyviams skiriama mažai reguliavimo dėmesio arba jo visai neskiriama. Pavyzdžiui, kasėjų pramonė nėra įtraukta į AMLD5 teisės aktų, kuriais reglamentuojamos ES pastangos kovoti su pinigų plovimu ir terorizmo finansavimu, reguliavimo perimetrą. Tačiau šioje vietoje nuomonės išsiskiria, štai D. S. Ramalho ir N. I. Matos teigia, jog šie subjektai nepatenka į direktyvos taikymo sritį, nes nesaugo piniginių lėšų, tačiau tokia išimtis gali būti prieštaringa. Šiuo atveju, neįmanoma atmesti galimybės naudoti kasybos centrus pinigų plovimo tikslais, tai galėtų būti suprantama, kad prevencinės priemonės yra aktualios ir šioje veikloje. Taip atsitiks, pavyzdžiui, jei kasybos grupės valdytojas, gavęs kasybos veiklos metu gautą pirmąją bitkoinų partiją, pasiliks juos sau, o neteisėtos kilmės bitkoinus išplatins kitiems kasėjams.²³⁰ Su tokia nuomone nesutinka L. Haffke *et al.*, teigdami, iš pirmo žvilgsnio gali atrodyti, kad būtų nuoseklu visiems kasėjams taikyti AML reikalavimus. Tačiau, autorių nuomone, tai būtų nepagrįsta: kasėjai neturėtų tapti įpareigotaisiais subjektais. Naudojimas kasybos paslaugomis pinigams plauti nėra ypatingas bruožas lyginant su kitomis pinigų plovimo veiklomis, atsižvelgiant į bendrą ekonominį ciklą. Pavyzdžiui, galima įsteigti netikrą parduotuvę, kurioje būtų galima plauti neteisėtai įgytus pinigus - arba įsteigti virtualių valiutų kasybos grupę. L. Haffke *et al.* nuomone abi veiklos susijusios su vienodomis pinigų plovimo rizikomis, todėl turėtų būti traktuojamos reguliavimo požiūriu - vienodai.²³¹

Į direktyvos taikymo sritį taip pat nepatenka maišymo paslaugų teikėjai. Šiuo atveju, D. S. Ramalho, N. I. Matos bei L. Haffke *et al.* nuomonės sutampa ir autoriai sutinka, jog ši sritis bene problemiškesnė reguliavimo atžvilgiu, nes maišymo operacijos, nors dažnai atliekamos teisėtais tikslais, siekiant apsaugoti asmeninį turtą ar naudotojo privatumą, taip pat jos suteikia anonimiškumą sistemoje kuri dažnai naudojama neteisėtai veiklai. Atsižvelgiant į tai, kad

²²⁹ Haffke, Lars, et al. Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them, 2020

²³⁰ Silva Ramalho, D., Igreja Matos, N. What we do in the (digital) shadows: anti-money laundering regulation and a bitcoin-mixing criminal problem. *ERA Forum* 22, 487–506

²³¹ Haffke, Lars, et al. Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them, 2020

maišymo operacijos atlieka svarbų vaidmenį ir teisėtai apsaugant virtualias valiutas, ir neteisėtai slepiant jų galimą nusikalstamą kilmę, būtų ypač svarbu, kad tokio pobūdžio paslaugų teikėjams būtų aiškiai taikoma direktyva. Nepaisant to, kad šios paslaugos dažniausiai yra susijusios su piniginių paslaugų teikėjais, ypač piniginių, per kurias maišomi bitkoinai - saugotojais, - todėl tokiais atvejais jiems taikomos direktyvoje numatytos prevencinės pareigos, tiesioginis jų įtraukimas į subjektyviąją šių pareigų taikymo sritį, neatsižvelgiant į piniginių saugojimo paslaugas, sustiprintų sistemos veiksmingumą ir padėtų išvengti galimų reguliavimo spragų.²³²

Svarbu atkreipti dėmesį, jog nors virtualių valiutų keityklų reguliavimas yra neabejotinai svarbus mažinant atotrūkį tarp kriptovaliutų ir įprastų rinkų ir nusikaltėliai nuolat naudojami šiomis paslaugomis kaip priemone patekti į virtualių valiutų rinką, tačiau pakankamai motyvuoti asmenys visada galės gauti prieigą prie virtualiosios valiutos rinkos per tikrą bendravimą su kitais asmenimis, kurie taip pat pasirenkę prekiauti virtualia valiuta. G. Soana teigimu, *peer-to-peer* santykiai, nors užima daugiau laiko nei naudojimasis keityklų paslaugomis, ypač įgyjant virtualių valiutų už dideles suma, bet jie neturėtų atmetami, kaip pasirinkimas plauti neteisėtas lėšas. Tačiau, jie taip pat nėra įtraukti į direktyvos taikymo sritį.²³³

Tačiau, be galimų trūkumų, Europos teisės aktų leidėjo sprendimas sukurti šią sistemą yra ypač svarbus, nes pirmą kartą apibrėžiamos virtualiosios valiutos ir šioje rinkoje dalyvaujantys subjektai. Aiškos ir nuoseklios terminologijos nebuvimas yra pagrindinė šios srities problema, trukdanti komunikacijai ir pažangai. Kalbant apie reguliavimo ginčus, patikima apibrėžtis Europos teisėje yra veiksmingumo ir aiškumo aspektas. Jis taip pat siunčia aiškią žinią tiek valstybėms narėms, tiek tradicinės ir virtualiosios rinkos dalyviams, jog virtualiosios valiutos yra aktuali tema Europos lygmeniu, todėl būtinas reguliavimas. Tai ypač svarbu, nes virtualiosios valiutos yra ir pavojus, ir potencialus ekonominės pažangos šaltinis. Todėl labai svarbu išsaugoti ir užtikrinti jų reguliuojamą vystymąsi, nes visiškai panaikinus reguliavimą kyla pavojus, kad šia rinka pasinaudos nusikaltėliai, įbaugins investuotojus ir naudotojus ir galiausiai nuslopins jų augimą.²³⁴

Galiosiausiai, remiantis praėjusių metų EBI ataskaita, teigiama, kad su virtualiomis valiutomis susijusi rizika su laiku tik išaugo. Kompetentingos institucijos tai aiškino nuolatine virtualių valiutų rinkos plėtra tiek sandorių apimties, tiek klientų bazės požiūriu. Su virtualiosiomis valiutomis susijusi rizika Europos finansų sektoriui pirmiausia kyla tada, kai reguliuojamų kredito ir finansų įstaigų klientai dalyvauja virtualiųjų valiutų sandoriuose arba veikia kaip virtualiojo turto paslaugų teikėjai. Pagrindinė priežastis, dėl kurios didėja pinigų plovimo ir terorizmo rizikos poveikis, yra skaidrumo trūkumas, susijęs su virtualiojo turto sandoriais ir šiuose sandoriuose

²³² Silva Ramalho, D., Igreja Matos, N. What we do in the (digital) shadows: anti-money laundering regulation and a bitcoin-mixing criminal problem. *ERA Forum* 22, 487–506

²³³ *Ibid.*

²³⁴ Soana, Giulio, *Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?*, Wiley, 2021

dalyvaujančių asmenų tapatybe.²³⁵ EBI pastebi, kad kompetentingoms institucijoms ir toliau kyla didelių sunkumų siekiant neatsilikti nuo rinkos pokyčių ir veiksmingai užtikrinti dabartinės reguliavimo sistemos vykdymą. Padėtį dar labiau apsunkina tai, kad dauguma ir tam tikros rūšies virtualių valiutų operacijų dabar nepatenka į AMLD5 taikymo sritį.²³⁶

3.3.4 Kova su pinigų plovimu baudžiamosios teisės priemonėmis

Skyrelio apie pinigų plovimo ir teroristų finansavimo standartų minkštosios normatyvinės struktūros poveikį Europos Sąjungos teisei pradžioje buvo paminėta, kad dėl didelės ES valstybių narių patirties baudžiamosiose bylose kriminalizavimas pasirodė esąs sunkiau įgyvendinamas ir ilgą laiką nebuvo nei bendros šio nusikalstamo pažeidimo apibrėžties, nei suderintos bausmių už jį sistemos. Šį faktą galima buvo laikyti dideliu trūkumu, atsižvelgiant į tai, jog direktyvomis buvo siekiama harmonizuoti pinigų plovimą Europos Sąjungos lygmeniu.

Harmonizavimo bandymų būtų ir anksčiau. Sutarties dėl Europos Sąjungos veikimo (SESV) 83 straipsnyje numatytas konkretus teisinis pagrindas priimti ES antrinės teisės aktus, kuriais siekiama kovoti su ypač sunkiais nusikaltimais, turinčiais tarpvalstybinį mastą dėl tokių nusikaltimų pobūdžio ar poveikio arba dėl ypatingo poreikio kovoti su jais bendrai.²³⁷ Tačiau užuot taikiusi SESV 83 straipsnį, 2015 m. gegužės mėn. priimdama griežtesnės kovos su pinigų plovimu ir teroristų finansavimu taisyklės, ES taikė SESV 114 straipsnį, kuris yra teisės aktų derinimo teisinis pagrindas. Kaip aiškina L. Borlini bei F. Montanaro, jais buvo siekiama kovoti su padidėjusia pinigų plovimo nusikaltimų rizika, standartizuoti pinigų plovimo sąvoka ES lygmeniu, ypač tiksliau apibrėžiant su ja susijusias pagrindines nusikalstamas veikas, siekiant formuoti vienodą šios nusikalstamos veikos supratimą. Tai būtų buvęs pagrindas lengviau atlikti tarptautinius tyrimus, sustiprėtų valstybių narių policijos, teismų ir FŽP bendradarbiavimas.²³⁸ Tačiau ES valstybių narių baudžiamieji įstatymai tebuvo labai skirtingi, nepaisant taip siekiamos harmonizacijos. Dėl nuolatinių nacionalinių teisės aktų skirtumų Europos Komisija, reaguodama į šias problemas, pateikė pasiūlymą dėl teisės akto, dėl pinigų plovimo ir nusikalstamu būdu įgytų pajamų konfiskavimo. 2012 m. Komisija pateikė teisėkūros procedūra priimamo akto pasiūlymo planą, kuris būtų priimtas remiantis Europos Bendrijų sutarties 83 straipsniu. Juo buvo siekiama

²³⁵ EBA, Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector, 2 psl., 2021, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

²³⁶ *Ibid.*

²³⁷ Europos Sąjungos ir Sutarties dėl Europos Sąjungos veikimo suvestinės redakcijos 2012/C 326/01 2012/C 326/01, 2012

²³⁸ Borlini, Leonardo, Montanaro, Francesco, The Evolution of The Eu Law Against Criminal Finance: The "Hardening" Of FATF Standards Within The EU, 2017

suderinti pinigų plovimo sąvoką visose ES valstybių narių teisinėse sistemose. Šis teisės akto pasiūlymas būtų sėkmingai užbaigęs ES pastangas kovoti su pinigų plovimu, tačiau siūlymas nebuvo priimtas.²³⁹ Taip galėjo būti dėl to, kad valstybės nenorėjo suteikti ES daugiau įgaliojimų baudžiamosios teisės srityje, ypač derinant tam tikrų nusikaltimų apibrėžtis ir sankcijas.

Po pirminių harmonizavimo bandymų, Direktyva Kovos su pinigų plovimu baudžiamosios teisės priemonėmis buvo priimta tik 2020 m. ir yra naujausia kovos su pinigų plovimu teisės aktų paketo dalis, kurios, kaip ir pirminių bandymų pagrindinis tikslas - suderinti pinigų plovimo apibrėžtį, taikymo sritį ir sankcijas už pinigų plovimo taisyklių pažeidimus nacionalinėje teisėje, siekiant optimizuoti valstybių narių bendradarbiavimą. Naujoji teisinė sistema palengvina teismų ir teisėsaugos pareigūnų bendradarbiavimą kovojant su pinigų plovimu ir teroristų finansavimu.

Atkreiptinas dėmesys, jog Direktyvos siekis taip pat suderinti esamą reglamentavimą su kitais tarptautiniais įsipareigojimais, pavyzdžiui, tokiais kaip kylančiais iš 2005 m. Europos Tarybos konvencijos dėl pinigų plovimo, nusikalstamu būdu įgytų pajamų slėpimo, paieškos, arešto ir konfiskavimo bei terorizmo finansavimo, taip pat siekiant suderinti su FATF atnaujintomis rekomendacijomis. Naujoji direktyva parodo, jog pinigų plovimas bei su juo susijęs terorizmo finansavimas yra ypač opios problemos Europos Sąjungos lygmeniu, nes kelia iššūkius finansų sektoriaus vientisumui, stabilumui, reputacijai, taip pat ir visai Europos Sąjungos vidaus rinkai bei jos saugumui, pažymint, jog virtualiosios valiutos ir jų naudojimas vieni iš rizikos veiksnių.²⁴⁰

Visų pirma, remiantis Direktyvos 2018/1673 3 str. 1 d., apibrėžiamas pinigų plovimo nusikaltimas ir juo laikoma: „*turto konversija arba perdavimas, žinant, kad šis turtas yra gautas iš nusikalstamos veiklos, siekiant nuslėpti arba užmaskuoti neteisėtą turto kilmę arba siekiant padėti kokiam nors asmeniui, kuris dalyvauja tokioje veikloje, išvengti teisinių to asmens veiksmų pasekmių, turto tikrojo pobūdžio, šaltinio, vietos, disponavimo, judėjimo, teisių ar nuosavybės teisių į turtą nuslėpimas arba užmaskavimas, žinant, kad toks turtas yra gautas iš nusikalstamos veiklos, turto įsigijimas, turėjimas arba naudojimas, jo gavimo metu žinant, kad šis turtas gautas iš nusikalstamos veiklos*“.

Direktyvos tikslas kriminalizuoti pinigų plovimą, kai jis padaromas tyčia ir žinant, kad buvo gautos pajamos iš nusikalstamos veikos, todėl šiame kontekste neturėtų būti jokio skirtumo tarp to, ar pajamos iš nusikalstamos veikos buvo gautos tiesiogiai, ar netiesiogiai, ir to, ar iš

²³⁹ *Ibid.*

²⁴⁰ Europos Parlamento ir Tarybos Direktyva (ES) 2018/1673, 2018 m. spalio 23 d., dėl kovos su pinigų plovimu baudžiamosios teisės priemonėmis

objektyvių faktinių aplinkybių galima daryti išvadą apie ketinimą ar žinojimą, kad pajamos iš nusikalstamos veikos buvo gautos.²⁴¹

Reikėtų paminėti, kad nusikalstama veika apibrėžiama kaip elgesys, už kurį pagal nacionalinę teisę numatyta daugiau kaip vienerių metų laisvės atėmimo bausmė, arba bet koks nusikaltimas, už kurį numatyta minimali daugiau kaip šešių mėnesių laisvės atėmimo ar įkalinimo bausmė. Direktyvoje tai apima net 22 veikas, kurios yra tokios, kaip: dalyvavimas organizuotos nusikalstamos grupės ir reketo veikloje, terorizmas, neteisėta prekyba narkotikais ir psichotropinėmis medžiagomis. Apimama ir korupcija, sukčiavimas ir pan. Išskiriami nusikaltimai aplinkai, nužudymas, sunkus sveikatos sutrikdymas. Galiausiai tai yra ir mokestiniai nusikaltimai, susiję su tiesioginiais ir netiesioginiais mokesčiais, kaip nustatyta nacionalinėje teisėje, turto prievartavimas, klastojimas, manipuliavimas rinka, bei kibernetiniai nusikaltimai, bei daugelis kitų veikų.²⁴²

Atsižvelgiant į tai, esminiai naujosios direktyvos aspektai - tai visų pirma suvienodintas neteisėtų veiksmų, kurie laikomi pinigų plovimo nusikaltimais, apibūdinimas, kuris yra pagrindinė naujosios direktyvos sudedamoji dalis. Kitas svarbus požymis tai, kad valstybės narės privalo virtualiąsias valiutas priskirti turtui, kuris gali būti naudojamas pinigams plauti. Akivaizdu, kad nusikalstamų veikų sąrašas yra labai išsamus ir kad daugelį iš išvardytų nusikalstamų veikų galima tiesiogiai susieti su virtualiųjų valiutų naudojimu, kaip priemone atlikti mokėjimams, vietoj realių pinigų darant nusikalstamą veiką, o tai kelia dar didesnių iššūkių.²⁴³ Siekiant, kad baudžiamųjų priemonių taikymas būtų lengvesnis, siūloma, kad apkaltinamąjį nuosprendį būtų galima priimti nekeliant reikalavimo ankstesniam apkaltinamajam nuosprendžiui dėl tos nusikalstamos veiklos. Taip pat neturėtų būti reikalaujama tiksliai nustatyti su ta nusikalstama veika susijusių faktinių elementų ar aplinkybių, be kita ko, turėtų būti atsižvelgiama į tai, kad nusikalstama veika buvo padaryta kitoje valstybėje narėje arba trečiojoje valstybėje.²⁴⁴

Kitas direktyvos tikslas - kovoti su pinigų plovimu, todėl valstybės narės privalo užtikrinti, kad už pinigų plovimo nusikaltimus būtų baudžiama mažiausiai ketverių metų laisvės atėmimo bausme. Nusikaltimus padariusiems fiziniams asmenims turėtų būti numatytos papildomos sankcijos ar priemonės, pavyzdžiui, baudos.²⁴⁵ Valstybės narės taip pat turi teisę nustatyti sunkinančias aplinkybes, kurios gali apimti tokius veiksmus, kaip, pavyzdžiui, išplautų lėšų suma

²⁴¹ Eucrium, Wahl, Thomas, New Directive on Criminalisation of Money Laundering, 2019, <https://eucrium.eu/news/new-directive-criminalisation-money-laundering/>

²⁴² *Ibid.* 2 str. 1 p.

²⁴³ Eucrium, Wahl, Thomas, New Directive on Criminalisation of Money Laundering, 2019, <https://eucrium.eu/news/new-directive-criminalisation-money-laundering/>

²⁴⁴ Europos Parlamento ir Tarybos Direktyva (ES) 2018/1673, 2018 m. spalio 23 d., dėl kovos su pinigų plovimu baudžiamosios teisės priemonėmis (12)

²⁴⁵ *Ibid.* (14)

arba nusikaltimo pobūdis, pavyzdžiui, korupcija, seksualinis išnaudojimas, prekyba narkotikais ar terorizmas.²⁴⁶

Paskutinis punktas - aiškiau reglamentuojama, kuri valstybė narė turi jurisdikciją ir kaip sprendžiami jurisdikcijos klausimai, pavyzdžiui, ar veika visiškai ar iš dalies buvo padaryta jos teritorijoje, ar nusikaltėlis yra tos šalies pilietis. Tam gali prireikti, kad valstybė išplėstų savo jurisdikciją nusikaltimams, padarytiems už jos ribų. Dėl to gali būti reikalaujama, kad nusikaltėlis būtų nuolatinis tos valstybės gyventojas arba kad nusikaltimas, be kita ko, būtų padarytas toje valstybėje įsteigto juridinio asmens naudai.²⁴⁷

Apibendrinant galima teigti, jog ši direktyva pagaliau leido pasiekti Europos Sąjungos norą harmonizuoti pinigų plovimo apibrėžtį, taikymo sritį ir sankcijas už pinigų plovimo taisyklių pažeidimus nacionalinėje teisėje, taip optimizuojant valstybių narių bendradarbiavimą, kuris yra kertinė ne tik Europos Sąjungos kovos su pinigų plovimu sistemos dalis, tačiau ir svarbus FATF rekomendacijų elementas, svarbiausiai, į šios Direktyvos perimetrą įtraukiant į virtualių valiutų sąvoką.

3.3.5 Reglamentas dėl informacijos, teikiamos pervedant lėšas

Apžvelgus direktyvas, taip pat reiktų atkreipti dėmesį į reglamentą dėl informacijos, teikiamos pervedant lėšas, kuris yra vienas iš Europos Sąjungos teisės aktų paketo, kuriuo siekiama kovoti bei užkirsti kelią pinigų plovimui ir terorizmo finansavimu. Reglamento preambulėje teigiama, jog pinigų plovimas, teroristų finansavimas bei organizuotas nusikalstamumas yra aktualios problemos, kurios reikalauja sprendimo visos Europos Sąjungos lygiu. Kol nebus įgyvendintos konkrečios ES lygmens derinimo priemonės, pinigų plovėjai ir teroristų finansuotojai galės laisvai naudotis laisvu kapitalo judėjimu integruotame Sąjungos finansų sektoriuje, kad padėtų vykdyti savo neteisėtas operacijas.²⁴⁸ Todėl, vadovaujantis FATF 15 rekomendacija, jau minėta *kelionių taisykle*, šiuo reglamentu nustatomos taisyklės, pagal kurias, siekiant užkirsti kelią pinigų plovimui ir teroristų finansavimui, juos aptikti ir tirti, lėšų pervedimo metu turi būti teikiama informacija apie mokėtoją ir gavėją, kai bent vienas iš lėšų pervedime dalyvaujančių mokėjimo paslaugų teikėjų yra įsisteigęs Sąjungoje.²⁴⁹ Mokėjimo paslaugų teikėjas privalo prie lėšų pervedimų pridėti informaciją apie mokėtoją, pavyzdžiui, mokėtojo vardą ir pavardę, mokėjimo sąskaitos numerį ir mokėtojo adresą, taip pat oficialaus asmens tapatybės dokumento numerį, kliento identifikavimo numerį arba kliento gimimo datą ir

²⁴⁶ *Ibid* (15)

²⁴⁷ *Ibid*. 10 str.

²⁴⁸ Europos Parlamento Ir Tarybos Reglamentas (ES) 2015/847, dėl informacijos, teikiamos pervedant lėšas, ir kuriuo panaikinamas Reglamentas (EB) Nr. 1781/2006

²⁴⁹ *Ibid*. 1 str.

vieta. Norint apdoroti mokėjimus, taip pat būtina pateikti informaciją apie gavėjus, pavyzdžiui, jų vardą, pavardę ir mokėjimo sąskaitos numerį. Matoma, jog yra reikalaujama panašios informacijos, kaip ir kliento pažinimo metu.²⁵⁰ Jei mokėjimo paslaugų teikėjas operacijos vykdymo metu sužino apie trūkstamą informaciją, jis privalo pareikalauti, kad informacija būtų pateikta, kitu atveju, operacija bus laikoma netinkama vykdyti.²⁵¹ Tokio lygio operacijų atsekamumas laikomas svarbia pinigų plovimo ir kitų finansinių nusikaltimų prevencijos, nustatymo ir tyrimo priemone.²⁵²

Reglamentas tiesiogiai taikomas lėšų pervedimams bet kokia valiuta, o lėšos suprantamos kaip banknotai ir monetos, pinigai sąskaitoje arba elektroniniai pinigai, kaip apibrėžta Direktyvos 2009/110/EB 2 straipsnio 2 punkte.²⁵³

Taigi, virtualiosios valiutos akivaizdžiai nepatenka į reglamento taikymo sritį, nes neatitinka lėšų apibrėžties, kuri yra sąlyginai siaurai nustatyta. Todėl atitinkamai galima teigti, kad šis reglamentas nėra sukurtas specialiai kovai su pinigų plovimu naudojant virtualiąsias valiutas.²⁵⁴ Kita vertus, pažvelgę į naujausias FATF gaires dėl rizikos vertinimu pagrįsto požiūrio į virtualųjį turtą ir virtualiojo turto paslaugų teikėjus, matome, kad šios taisyklės turėtų būti pakeistos, ir adaptuotos ir virtualiosios valiutos paslaugų teikėjams.

3.3.6 Tarptautinis bendradarbiavimas

Tarptautinės pastangos kontroliuoti pinigų plovimą prevencinėmis kovos su pinigų plovimu priemonėmis visada skatina didinti tarptautinį bendradarbiavimą AML teisės srityje. Atsižvelgiant į nusikaltimo tarp nacionalinį pobūdį, tarptautinis bendradarbiavimas yra ypač svarbus, nes pinigų plovimo nusikaltimui būdingas tarptautinis elementas suteikia nusikaltėliams pranašumą patalpinti išplautą turtą už valstybės, kurioje buvo įvykdytas nusikaltimas jurisdikcijos ribų. Tai suvokdama ir FATF tarptautinio bendradarbiavimo stiprinimo klausimui, kaip minėta, skyrė 37-40 rekomendacijas.

Pasak E. Ebikake, tarptautinis bendradarbiavimas yra būtinas ir dėl valstybės suvereniteto koncepcijos, kuri apriboja valstybės galimybes atlikti tyrimo ir vykdymo užtikrinimo veiksmus tik savo teritorijoje. Pagal tarptautinę teisę vykdymo jurisdikcija yra išimtinai teritorinio pobūdžio. Valstybė, prašanti pagalbos iš kitos valstybės, gali tai daryti oficialiomis priemonėmis - savitarpio

²⁵⁰ *Ibid.* 4 str. 1-2 d.

²⁵¹ *Ibid.* 8 str.

²⁵² *Ibid.* Direktybos preambulė

²⁵³ *Ibid.* 3 str. 8 p.

²⁵⁴ European Parliament, Prof. Dr. Houben, Robby, Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion, 24 psl., 2018, <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>

teisine pagalba arba neoficialiomis priemonėmis - savitarpio pagalba. Tarpvyriausybiniis bendradarbiavimas teikiant savitarpio teisinę pagalbą yra tarptautinio bendradarbiavimo sudedamoji dalis, pagal kurią prašančiajai valstybei leidžiama taikyti privalomas priemones, kad būtų surinkti įrodymai, kurių reikia prašančiojoje valstybėje. Kita vertus, sąvoka - savitarpio pagalba - reiškia neformalios paramos teikimą tarp valstybių. Dažnai tai įgyvendinama bendradarbiaujant policijos pareigūnams arba agentūroms.²⁵⁵

Konceptualių požiūriu tarptautinis bendradarbiavimas baudžiamosiose bylose visų pirma skirtas spręsti prašančiosios valstybės vykdymo įgaliojimų trūkumo baudžiamosiose bylose klausimą. Vykdymo įgaliojimų neturėjimas tarptautinio AML kontekste gali pasireikšti dviem būdais. Visų pirma, informacija, reikalinga įrodyti, kad buvo padarytas pinigų plovimo nusikaltimas. Antra, neteisėtai gautos lėšos gali būti kitoje jurisdikcijoje nei ta, kurioje ketinama vykdyti baudžiamąjį persekiojimą už pinigų plovimo nusikaltimą.²⁵⁶

Galima teigti, jog tarptautinį bendradarbiavimą Europos Sąjungos lygmeniu tarp šalių įtvirtina ir palengvina Europolas, kuris yra Europos Sąjungos teisės agentūra, padedanti ES valstybėms narėms kovoti su sunkiais tarptautiniais nusikaltimais, taip pat bendradarbiaujantis su tarptautinėmis organizacijomis ir kitomis ES nepriklausančiomis šalimis.²⁵⁷ Geras šios organizacijos veikimo pavyzdys galėtų būti Europolo veiksmai ir dalyvavimas išaiškinant prekybos schemą, kurios metu organizuotas nusikalstamas tinklas iš aukų visoje Europoje išviliojo apie 30 mln. eurų. Nusikalstamas tinklas valdė kelias atskiras internetines prekybos platformas, kurių kiekvienoje buvo skelbiamas didelis atlygis už investicijas į didelės rizikos pasirinkimo sandorius ir kriptovaliutas. Nusikalstamai grupei priklausė kelios profesionaliai atrodančios prekybos platformos, apie kurias buvo skelbiama socialinėje erdvėje ir paieškos sistemose, viliojant aukas užsiregistruoti jų paslaugoms.²⁵⁸ Šios organizacijos nariai apsimesdavo brokeriais, kai skambindavo aukoms telefonu iš savo įkurto skambučių centro. Įtariamieji naudojo fiktyvią programinę įrangą, kad parodytų investavimo rezultatus ir paskatintų aukas investuoti daugiau. Europolo teigimu, sukčiavimo schema, kurią daugiausia organizavo Izraelio piliečiai, buvo platinama per skambučių centrus, įsikūrusius Bulgarijoje ir Šiaurės Makedonijoje. Vienas iš būdų, kuriais Europolas padėjo vykdyti operaciją, tai palengvino keitimąsi informacija tarp šalių, teikė analitinę pagalbą ir koordinavo operatyvinius veiksmus. Siekdami suteikti informacijos tyrėjams

²⁵⁵ Ebikake, Emmanuel E., *Money Laundering: An Assessment of Soft Law as a Technique for Repressive and Preventive Anti-Money Laundering Control*, 2021

²⁵⁶ *Ibid.*

²⁵⁷ Europol, *Apie Europolą*, <https://www.europol.europa.eu/about-europol:lt>

²⁵⁸ Europol, *Trading scheme resulting in €30 million in losses uncovered*, 2021 m., <https://www.europol.europa.eu/media-press/newsroom/news/trading-scheme-resulting-in-€30-million-in-losses-uncovered>

vietoje, Europolo specialistai operacijos dieną realiuoju laiku vertino operatyvinę informaciją pagal Europolo duomenų bazes.²⁵⁹

Apibendrinant galima teigti, jog tarptautinis bendradarbiavimas yra iš svarbiausių kovos su pinigų plovimu sistemos sudedamųjų dalių. Tokio pobūdžio nusikaltimai, kaip matoma iš pateikto pavyzdžio, dažniausiai apjungia ne vieną jurisdikciją, todėl tiek savitarpio pagalba, tiek teisinė savitarpio pagalba arba tokių organų, kaip Europolas, tarpininkavimas yra ypatingai reikalingi vykdyti efektyvią represinę kovą su pinigų plovimu.

3.4 Tarptautinių atsiskaitymų banko pozicija ir centrinių bankų skaitmeninės valiutos

Tarptautinių atsiskaitymų bankas (TAB) (angl. *The Bank for International Settlements, BIS*) - tai dar viena tarptautinė organizacija, kurios svarbos negalima atmesti kalbant apie pinigų plovimo reguliacinę raidą. TAB veikia kaip dialogo ir plataus tarptautinio bendradarbiavimo forumas, taip pat sudaroma platforma dalijimuisi žiniomis bei atsakingam naujovių diegimui.²⁶⁰ Atsižvelgiant į TAB veiklos pobūdį, natūralu, jog virtualios valiutos taip pat vienas iš TAB interesų.

Galima būtų teigti, jog Tarptautinių atsiskaitymų banko pozicija yra viena iš griežčiausių virtualiųjų valiutų atžvilgiu. 2021 m. Bazelio komiteto konsultaciniame dokumente dėl kriptoturto pozicijos pažymima, jog nors kriptovaliutų rinka tebėra maža lyginant su pasaulinės finansų sistemos dydžiu, o bankų pozicijos kriptovaliutų rinkoje šiuo metu yra ribotos, jos absoliutus dydis yra reikšmingas, atsižvelgiant į spartų rinkos vystymąsi. Komiteto teigimu, virtualios valiutos kelia įvairius rūpesčius, įskaitant, bet neapsiribojant vartotojų apsauga, pinigų plovimu ir terorizmo finansavimu. Be kita ko, su virtualiu turtu susijusių paslaugų augimas gali didinti rizikas bankams ir bendram finansų rinkos stabilumui.²⁶¹

Komitetas taiko skirtingą požiūrį nei FATF ar Europos Sąjunga. Siekdamas nustatyti mažiausią įmanomą riziką, siūlo virtualiąsias valiutas suskirstyti į dvi grupes: pirmąją grupę, kuri atitinka visus standartus, ir antrąją grupę, kuri neatitinka visų reikalavimų, todėl jai priskiriama didesnė rizika. Visų pirma, reikalaujama, jog virtualusis turtas turi turėti stabilizavimo mechanizmą, t. y. palaikyti nuolatinį ir veiksmingą ryšį tarp jo vertės ir pagrindinio tradicinio turto, kas padėtų sumažintų virtualių valiutų vertės svyravimus.²⁶² Kitas reikalavimas - virtualiosios valiutos, turinčios stabilizavimo mechanizmus, turi užtikrinti visišką išperkamumą, suprantamą

²⁵⁹ *Ibid.*

²⁶⁰ The Bank for International Settlements, The BIS Promoting global monetary and financial stability through international cooperation, https://www.bis.org/about/profile_en.pdf

²⁶¹ The Bank for International Settlements, Basel Committee on Banking Supervision, Consultative Document, Prudential treatment of cryptoasset exposures, 1 psl., 2021 m., <https://www.bis.org/bcbs/publ/d519.pdf>

²⁶² *Ibid.* 4 psl.

kaip galimybę visada iškeisti virtualias valiutas į grynuosius pinigus, obligacijas, akcijas ar kitą tradicinį turtą.²⁶³ Trečioji sąlyga, kad virtualios ir tinklo funkcijos, kuriomis jos remiasi, įskaitant paskirstytųjų duomenų technologiją, būtų sukurtos ir vykdomos taip, kad bet kokia didelė rizika būtų tinkamai sumažinta ir valdoma. Tai reiškia, kad su šiomis funkcijomis susijusią veiklą vykdančys subjektai turi laikytis griežtos rizikos valdymo ir rizikos kontrolės politikos ir praktikos, apimančios rinkos ir likvidumo rizikas, operacines rizikas ir duomenų praradimo rizikos stebėseną, taip pat įvairią nefinansinę riziką, kaip trečiųjų šalių rizikos valdymą ir kovą su pinigų plovimu ir teroristų finansavimu.²⁶⁴ Taigi, visas minėtas sąlygas atitinkančios virtualios valiutos bus laikomos TAB atžvilgiu saugiomis.

Nagrinėdamas, kaip gali būti formuojamas virtualiųjų valiutų rizikos ribojimu pagrįstas reguliavimas, Komitetas vadovaujasi trimis pagrindiniais principais: panašios operacijos, paprastumas ir minimalūs kriterijai. Visų pirma, apie panašią veiklą, kuri grindžiama nuostata, kad virtualusis ir tradicinis turtas, kurie yra panašūs pagal savo ekonomines funkcijas ir keliamą riziką, pasakytina, jog neturėtų būti skirtingai tvarkomi rizikos ribojimo tikslais, todėl turėtų būti atsižvelgiama į bet kokią papildomą riziką, kuri gali kilti dėl unikalių kriptovaliutų savybių ir kitų veiksnių, palyginti su tradiciniu turtu. Kita teorija, vadinama, paprastumo, susijusi su nuostata, kad kai kurių rūšių virtualiojo turto svarba gali didėti dėl to, kad laikui bėgant didėja jo sisteminė reikšmė. Todėl būtina supaprastinti ir pritaikyti riziką ribojantį virtualiųjų valiutų reguliavimą, todėl šiame kontekste gali būti reikšmingas virtualiojo turto skirstymas į kategorijas pagal jo keliamą riziką. Galiausiai, minimalaus standarto sąvoka reiškia, kad bet kokia Komiteto nustatyta rizikos ribojimo tvarka, taikoma kriptografiniam turtui, pirmiausia būtų laikoma minimaliu standartu.²⁶⁵

Apibendrinant, tarptautinių atsiskaitymų banko teigimu, virtualiosios valiutos gali tapti ilgalaikiu iššūkiu centrinių bankų gebėjimui reguliuoti pinigų politiką. Todėl labai svarbu, kad reguliavimo institucijos sudarytų sąžiningas konkurencijos sąlygas didžiosioms technologijų įmonėms ir kitiems bankams, atsižvelgdamos į klientų bazę, lengvą prieigą prie informacijos ir skirtingus didelių technologijų įmonių verslo modelius.²⁶⁶ Dėl šios priežasties būtent TAB ypač stipriai pasisako už centrinių bankų skaitmenines valiutas.

Tarptautinio atsiskaitymų banko teigimu centrinių bankų susidomėjimas centrinio banko leidžiamomis skaitmeninėmis valiutomis (angl. *central bank digital currencies, CBDC*), kaip alternatyva virtualioms valiutomis, pasireiškia kritiniu metu, nes vis daugiau dėmesio sulaukia

²⁶³ *Ibid.* 5 psl.

²⁶⁴ *Ibid.* 5 psl.

²⁶⁵ The Bank for International Settlements, Basel Committee on Banking Supervision, Discussion paper, Designing a prudential treatment for crypto- assets, 8 psl., 2019 m., <https://www.bis.org/bcbs/publ/d490.pdf>

²⁶⁶ Haynes, Andrew, Yeoh, Peter, Cryptocurrencies and cryptoassets: regulatory and legal issues, 123 psl., 2020

bitkoinas ir kitos virtualios valiutos. TAB nuomone, kad kriptovaliutos yra greičiau spekuliacinis turtas nei pinigai, o daugeliu atvejų jos naudojamos pinigų plovimui, išpirkos reikalaujančių programų atakoms ir kitiems finansiniams nusikaltimams palengvinti.²⁶⁷

Nors terminas CBDC nėra tiksliai apibrėžtas, pasak N. Bilotta, paprastai manoma, kad jis reiškia centrinio banko įsipareigojimą, kuris dažnai apibūdinamas kaip skaitmeninė šalies suverenios valiutos reprezentacija, išleista centrinio banko ir užtikrinta centrinės vyriausybės kreditu. Vietoje popierinių pinigų spausdinimo, centriniai bankai kuria virtualius pinigus, kurie yra monetų ir banknotų skaitmeninė versija.²⁶⁸

CBDC gali būti laikomas priemone pinigų plovimo ir (arba) teroristų finansavimo pavojui sumažinti, nes visi susiję sandoriai turėtų vykti per reguliuojamą finansų tarpininką, kuriam taikomi kovos su pinigų plovimu ir teroristų finansavimu teisės aktai. Tai leidžia manyti, kad tokios naujos kartos centralizuotos virtualios valiutos bus mažesnio anonimiškumo.²⁶⁹ Šiuo atžvilgiu verta paminėti, kad TAB pažymi, kad CBDC išleidimas gali būti naudingas ne tik veiksmingesnėms ir saugesnėms mokėjimo ir atsiskaitymo sistemoms, bet ir kovai su pinigų plovimu ir terorizmo finansavimu. Tiek, kiek CBDC užtikrina skaitmeninius įrašus ir atsekamumą, jie gali padėti geriau įgyvendinti kovos su pinigų plovimu ir terorizmo finansavimu teisės aktus ir kartu sumažinti atitikties užtikrinimo išlaidas. Dėl tokios nacionalinės valiutos architektūros ji taptų atspari pinigų plovimo ir (arba) finansavimo problemoms ir atgrasytų nuo reikalavimų neatitinkančio naudojimo.²⁷⁰

Tačiau kai kurių ekspertų manymu, tokiose valiutose galėtų būti daugiau nacionalizmo, negu planavimo ir išankstinio apgalvojimo ir tai labai galėtų apriboti jų naudingumą ir augimo potencialą.²⁷¹ E. L. Sidorenko et al. išskiria kelias potencialias CBDC problemas. Visų pirma, kyla pavojus, kad jei visą CBDC sistemą kontroliuos centrinis bankas, tada asmuo, net jei per klaidą jam bus atimta teisė atsidaryti sąskaitą skirtą CBDC, bus atskirtas nuo finansų sistemos. Taip pat pažymima, jog spartus CBDC diegimas ir galimas spartus grynųjų pinigų apyvartos atsisakymas gali neigiamai paveikti vyresnio amžiaus žmones ir gyventojus, neturinčius sąskaitų bankuose. Trečioji problema į kurią atkreipia dėmesį E. L. Sidorenko et al., jog CBDC skverbimasis į šalis, kuriose silpnos finansų institucijos ir didelė infliacija, gali sukelti situaciją, kai asmenys ir įmonės

²⁶⁷ BIS, BIS Annual Economic Report, 2021, 67 psl., <https://www.bis.org/publ/arpdf/ar2021e3.pdf>

²⁶⁸ Bilotta, Nicola, CBDCs for Dummies: Everything You Need to Know about Central Bank Digital Currency (And Why You Shouldn't Be Afraid of It), 2021.

²⁶⁹ Global Legal Insights, Blockchain & Cryptocurrency Regulation 2022, Cryptocurrency compliance and risks: A European KYC/AML perspective Fedor Poskriakov & Christophe Cavin Lenz & Staehelin, 142 psl., 2022 m.

²⁷⁰ *Ibid.*

²⁷¹ Chuen, David Lee Kuo, Handbook OF DIGITAL CURRENCY Bitcoin, Innovation, Financial Instruments, and Big Data, 67 psl., 2015

nuspręs ne keisti CBDC į vietinę valiutą, o kaupti ją namuose ir atsiskaityti ja, todėl valstybei kyla rizika prarasti pinigų politikos kontrolę šalyje.²⁷²

Apibendrinant, autorės nuomone kyla klausimas ar centrinių bankų leidžiamos virtualios valiutos atitinka virtualių valiutų pradininko S. Nakamoto pirminę idėją, kuri suteikė pagrindą tokiam virtualių valiutų rinkos vystymuisi kaip matoma dabar. Nes, visų pirma, tai buvo kuriama kaip įrankis, kuriuo būtų galima pinigus siųsti internetu tiesiogiai iš vienos šalies kitai šaliai, nepereinant per finansų įstaigą. Be kita ko svarbu pabrėžti ir tai, kad kriptovaliutos egzistuoja tik skaitmeniniu pavidalu, nes tai prieštarauja *fiat* pinigams, kurie gali egzistuoti ir skaitmeniniu, ir fiziniu pavidalu. Galima daryti prielaidą, jog CBDC būtų kitokio tipo centralizuota skaitmeninių pinigų rūšis, kuri dar kartais vadinama elektroniniais pinigais,

²⁷² Sidorenko, E. L., Legal and Economic Implications of Central Bank Digital Currencies (CBDC), Economic Systems in the New Era: Stable Systems in an Unstable World, 2021

IŠVADOS

1. Tarptautiniuose teisės aktuose nėra pateikiama vieninga ir suderinta virtualiųjų valiutų sąvoka. Bendro sutarimo nėra ir lyginant reguliavimą nacionaliniu lygmeniu, literatūroje pateikiamos sąvokos yra apibrėžiamos remiantis pirminiuose teisės šaltiniuose naudojamais terminais. Tokie nesutarimai dėl terminologijos gali būti viena iš kliūčių, trukdančių sukurti gerą reguliavimo sistemą bei užkirsti kelią ateityje suderinti reguliavimą tarp šalių. Dėl virtualiųjų valiutų sandoriams būdingo tarptautinio pobūdžio skirtingas institucijų terminų aiškinimas gali skatinti rinkos dalyvius siekti pradėti veiklą palankesnio reguliavimo šalyse.
2. Atsižvelgiant į tai, kad pinigų plovimas yra tarpvalstybinis reiškiny, todėl tradicinis požiūris į tarptautinę teisėkūrą buvo ribotas ir ne toks veiksmingas kaip būdas sukurti tarptautinį pinigų plovimo problemos sprendimą. Šiuo atveju, kovos su pinigų plovimu internacionalizavimas buvo vienas iš dinamiškų kovos su pinigų plovimu komponentų, nes jis atitiko pasaulinį pinigų plovimo metodų pobūdį. Dėl šio aspekto kova su pinigų plovimu pasireiškė tarptautiniais standartais, kurie apima privalomas ir neprivalomas normas. Viena iš svarbiausių ir tolimesnius pagrindus sukūrusi pinigų plovimo prevencijos tarptautinių santykių reglamentavimui yra Vienos konvencija. Iš kitos pusės, pagrindą neprivalomoms taisyklėms sukūrė Bazelio bankininkystės komitetas.
3. FATF sukurti principai, kurie gali būti įvardinami kaip švelnioji teisė, padarė didelę įtaką tiek nacionaliniu, tiek tarptautiniu kovos su pinigų plovimu ir teroristų finansavimu reglamentavimui. Šiai dienai FATF galima laikyti įtakingiausia tarptautine institucija, formuojančia kovos su pinigų plovimu politiką ir telkiančia visuotinį supratimą kaip kovoti su tokio pobūdžio nusikalstama veikla. Tai galima pagrįsti, jog standartams būdingas lankstumas yra ypač svarbūs tokioje sparčiai besikeičiančioje ir evoliucionuojančioje srityje. Tai taip pat suteikia galimybę valstybėms iš karto neprisiimti pernelyg griežtų įsipareigojimų.
4. Galima teigti, jog ES buvo pirmoji regioninė organizacija, aktyviai dalyvavusi kuriant pasaulines normas, ir ji dėjo daug pastangų, kad neatsiliktų nuo pasaulinės švelniosios teisės kovos su pinigų plovimu ir terorizmo finansavimu srityse. FATF standartai turėjo daug įtakos šios teisės srities politikos formavime Europos Sąjungos kontekste.
5. Nepaisant svarbaus minštosios teisės vaidmens ir įtakos, dabartinės pasaulinės pastangos kovoti su pinigų plovimu yra fragmentiškos, ne homogeniškos, tai ypač akivaizdu

išanalizavus šalių virtualių valiutų ir su jomis susijusio pinigų plovimo reglamentavimą nacionaliniu lygmeniu. Dėl tarpvalstybinio virtualių valiutų rinkų pobūdžio, kai vienos jurisdikcijos subjektai gali būti veikiami virtualių valiutų ir su jomis susijusios veiklos, kurios iš esmės nepriklauso tos jurisdikcijos reguliavimo kontrolei, virtualios valiutos gali didinti riziką finansų rinkos stabilumui. Todėl būtent dėl unikalių virtualių valiutų savybių, kaip decentralizuotas pobūdis, kuris leidžia vykdyti sandorius savitarpio lygmeniu, tarpvalstybiniu mastu, be tarpininkų, virtualias valiutas yra ypač sunku reglamentuoti.

6. FATF ir Europos Sąjunga vadovauja tarptautiniam požiūriui į virtualių valiutų reguliavimą, tačiau jų gairėse daugiausia dėmesio skiriama virtualių valiutų ir *fiat* valiutų sąveikai, dėl šios priežasties daliai virtualių valiutų dalyvių reguliavimo sistemos iki šiol skyrė mažai dėmesio, dėl šios priežasties galima teigti, jog esantis reglamentavimas nėra pakankamas. AMLD5 lygmeniu, reguliavimas taikomas siaurai, atsižvelgiant, jog reguliuojami tik virtualių valiutų mainai į *fiat* valiutas ir atvirkščiai, o Europos Sąjunga nėra numačiusi priemonių virtualiosios valiutos mainų į virtualiąją valiutą reguliavimui.
7. Tarptautinis bendradarbiavimas yra ypač svarbus atsižvelgiant į tarptautinį pinigų plovimo panaudojant virtualias valiutas nusikaltimo pobūdį, nes pinigų plovimui būdingas tarptautinis aspektas suteikia nusikaltėliams pranašumą valdyti nelegalų turtą už valstybės, kurioje buvo padarytas nusikaltimas, jurisdikcijos ribų. Todėl tarptautinis bendradarbiavimas reguliavimo srityje, sukuriant nuoseklesnę, labiau suderintą ir koordinuotą reguliavimo sistemą ir taikant vykdymo užtikrinimo priemones įvairiose jurisdikcijose galėtų sumažinti tikimybę, jog rinkos dalyviai galėtų pasinaudoti reguliacinėmis spragomis. Be kita ko, tai ypač palengvintų valstybėms vykdyti baudžiamąjį persekiojimą, taip pat leistų greičiau bei paprasčiau surinkti įrodymus.

REKOMENDACIJOS

1. Atsižvelgiant į faktą, jog tarptautiniuose teisės aktuose nėra pateikiama vieninga ir suderinta virtualiųjų valiutų sąvoka, įstatymų leidėjai, siekiant padėti harmonizuoti reguliavimo sistemą, turėtų imtis priemonių, kad, rinkdamos empirinius duomenis ir bendradarbiaudamos su svarbiomis suinteresuotosiomis šalimis, įskaitant kitas reguliavimo institucijas, būtų sukurta tinkamesnė apibrėžtis. Remiantis tuo, nacionaliniai politikos formuotojai turėtų, atsižvelgdami į virtualių valiutų požymius, turėtų įtraukti šią sąvoką į nacionalinius teisės aktus.
2. Didesnis reguliacinis aiškumas gali turėti didelę įtaką virtualiųjų valiutų rinkoms, nes skatintų pasitikėjimą ir pritrauktų į virtualiųjų valiutų rinką naujų rūšių klientų, taip pat paskatintų techninę pažangą, kurią gali stabdyti teisinio aiškumo trūkumas. Nacionalinis pinigų plovimo reguliavimas iš esmės yra nepakankamas, todėl būtina apibrėžti ir perduoti nacionalinių reguliavimo institucijų ribas ir atsakomybę tarptautiniu lygmeniu, kad tiek sektoriaus dalyviams, tiek naudotojams būtų aiški reguliavimo priežiūra, kuria vėliau būtų galima dalintis tarp šalių. Be kita ko, Europos Sąjungos lygmeniu ypač rekomenduojama į reguliacijos perimetrą įtraukti virtualių valiutų keityklas, kurios vykdo keitimus iš virtualių valiutų į virtualias valiutas.
3. Atsižvelgiant į faktą, jog virtualių valiutų technologijos yra ypač sparčiai kintančios ir neteisėtą veiklą vykdančios subjektai gali prisitaikyti prie šių technologijų greičiau nei teisėsauga, svarbu, jog valstybės dėtų visas pastangas, kad teisėsaugos institucijos turėtų pakankamą kompetencijos lygį, galėtų tirti ir nutraukti neteisėtą virtualiųjų valiutų technologijų naudojimą. Turėtų būti rengiamos koordinuotos strateginės mokymo programos, kurios galėtų pareigūnams suteikti techninį supratimą. Tarptautiniu ar regioniniu lygmeniu galėtų būti kuriamos atvirojo kodo priemonėmis pareigūnams. Taip pat esama galimybių plėtoti dirbtinį intelektą, o mašininis mokymasis galėtų padėti nustatyti pinigų plovimo būdus ir elgseną, siekiant automatizuoti pranešimus apie įtartina veiklą.
4. Bendradarbiavimas su virtualiųjų valiutų rinkos dalyviais galėtų padėti įgyvendinti tinkamą reguliavimą ir plėtoti institucijų kompetenciją. Valstybės galėtų sukurti specialias platformas, kuriose virtualiųjų valiutų rinkos dalyviai galėtų keistis informacija su viešuoju sektoriumi ir atvirkščiai. Tokia informacija galėtų būti naudojama įvairiems tikslams, įskaitant mokymo, žvalgybos informacijos rinkimo ir operatyvinius tikslus.

LITERATŪROS SĄRAŠAS

Teisės aktai:

1. “EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2015/ 849 - 2015 m. gegužės 20 d. - dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos, kuria iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/ 2012 ir panaikinama Europos Parlamento ir Tarybos direktyva 2005/ 60/ EB bei Komisijos direktyva 2006/ 70/ EB,” 2015, 45.
2. “EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES) 2015/ 847 - 2015 m. gegužės 20 d. - dėl informacijos, teikiamos pervedant lėšas, ir kuriuo panaikinamas Reglamentas (EB) Nr. 1781/ 2006,” 2015, 18.
3. “UNITED NATIONS CONVENTION AGAINST ILLICIT TRAFFIC IN NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES, 1988,” n.d., 31.
4. Europos Parlamento ir Tarybos Direktyva (ES) 2018/1673, 2018 m. spalio 23 d., dėl kovos su pinigų plovimu baudžiamosios teisės priemonėmis
5. Europos Parlamento ir Tarybos Direktyva (ES) 2018/843, 2018 m. gegužės 30 d, kuria iš dalies keičiama Direktyva (ES) 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos ir iš dalies keičiamos direktyvos 2009/138/EB ir 2013/36/ES
6. Europos Parlamento ir Tarybos Direktyva 2009/110/EB, dėl elektroninių pinigų įstaigų steigimosi, veiklos ir riziką ribojančios priežiūros, iš dalies keičianti Direktyvas 2005/60/EB ir 2006/48/EB ir panaikinanti Direktyvą 2000/46/EB, 2009 m. rugsėjo 16 d.
7. TARYBOS DIREKTYVA 1991 m. birželio 10 d. dėl finansų sistemos apsaugos nuo jos panaudojimo pinigų plovimui
8. Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering
9. EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA 2005/60/EB 2005 m. spalio 26 d. dėl finansų sistemos apsaugos nuo jos panaudojimo pinigų plovimui ir teroristų finansavimui
10. Europos Sąjungos ir Sutarties dėl Europos Sąjungos veikimo suvestinės redakcijos 2012/C 326/01 2012/C 326/01, 2012
11. 2006 m. rugpjūčio 1 d. Komisijos direktyva 2006/70/EB, nustatanti Europos Parlamento ir Tarybos direktyvos 2005/60/EB įgyvendinimo priemones, susijusias su politikoje dalyvaujančių asmenų apibrėžimu, ir supaprastinto deramo klientų tikrinimo procedūroms taikomus techninius kriterijus bei išimtis, suteikiamas dėl to, kad finansinė veikla vėrčiamasi retai arba labai ribotai

Internetiniai tinklapiai:

1. “About Us | United Nations.” Accessed April 29, 2022. <https://www.un.org/en/about-us>.
2. Europol. “Apie Europolą.” Accessed April 29, 2022. <https://www.europol.europa.eu/about-europol:lt>.
3. “Corda | Leading DLT Platform for Regulated Industries.” Accessed April 29, 2022. <https://www.corda.net/>.

4. "Crypto Assets: New Rules to Stop Illicit Flows in the EU | News | European Parliament," March 31, 2022. <https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu>.
5. "Cryptocurrency Prices, Charts and Market Capitalizations | CoinMarketCap." Accessed April 29, 2022. <https://coinmarketcap.com/>.
6. "El Salvador Becomes First Country to Adopt Bitcoin as National Currency - WSJ." Accessed April 29, 2022. <https://www.wsj.com/articles/bitcoin-comes-to-el-salvador-first-country-to-adopt-crypto-as-national-currency-11631005200>.
7. IMF. "IMF Executive Board Concludes 2021 Article IV Consultation with El Salvador." Accessed April 29, 2022. <https://www.imf.org/en/News/Articles/2022/01/25/pr2213-el-salvador-imf-executive-board-concludes-2021-article-iv-consultation>.
8. "Know Your Customer (KYC) Verification Guide for Cryptocurrency Trading," December 31, 2018. <https://bitgap.com/blog/know-your-customer-kyc-verification-guide-for-cryptocurrency-trading>.
9. Investopedia. "Monero (XMR) Cryptocurrency." Accessed April 29, 2022. <https://www.investopedia.com/tech/introduction-monero-xmr/>.
10. "New Directive on Criminalisation of Money Laundering." Accessed April 29, 2022. <https://eucrim.eu/news/new-directive-criminalisation-money-laundering/>.
11. Scribd. "Scribd." Accessed April 29, 2022. https://www.scribd.com/embeds/403354285/content?start_page=1&view_mode=scroll&access_key=key-PO7nONsRTuwcFDEcY5f&show_recommendations=true.
12. Smith, Ian. "IMF Urges El Salvador to Drop Bitcoin as Legal Tender." euronews, January 26, 2022. <https://www.euronews.com/next/2022/01/26/the-imf-warns-el-salvador-to-drop-bitcoin-as-a-legal-currency>.
13. "Tax Treatment of Cryptocurrencies | Australian Taxation Office." Accessed April 29, 2022. <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/>.
14. "The Virtual Currency Regulation Review - The Law Reviews." Accessed April 29, 2022. <https://thelawreviews.co.uk/title/the-virtual-currency-regulation-review/usa>.
15. Europol. "Trading Scheme Resulting in €30 Million in Losses Uncovered." Accessed April 29, 2022. <https://www.europol.europa.eu/media-press/newsroom/news/trading-scheme-resulting-in-€30-million-in-losses-uncovered>.
16. "Who We Are - Financial Action Task Force (FATF)." Accessed April 29, 2022. <https://www.fatf-gafi.org/about/whowear/>.

Specialioji literatūra:

1. Ajello, Nicholas J. "Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination." *BROOKLYN LAW REVIEW* 80 (n.d.): 28.
2. Al-Zaqibh, Ahmad Aqeil Mohamad. "International Laws on Money Laundering." *International Journal of Social Science and Humanity*, 2013, 43–47. <https://doi.org/10.7763/IJSSH.2013.V3.191>.
3. European Commission - European Commission. "Anti-Money Laundering and Countering the Financing of Terrorism." Text. Accessed April 29, 2022. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en.
4. Badmus, Gbolahan. "A Global Guide to a Crypto Exchange Regulatory Framework." *Journal of Law, Policy and Globalization* 90 (2019): 9.

5. Bains, Parma. "Blockchain Consensus Mechanisms." IMF. Accessed April 29, 2022. <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/01/25/Blockchain-Consensus-Mechanisms-511769>.
6. Bakos, Yannis, and Hanna Halaburda. "Tradeoffs in Permissioned vs Permissionless Blockchains: Trust and Performance." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, February 1, 2021. <https://doi.org/10.2139/ssrn.3789425>.
7. Bank, European Central. "Electronic Money." European Central Bank, November 16, 2016. https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html.
8. Bank for International Settlements, Committee on Payments and Market Infrastructures. *Digital Currencies*, 2015.
9. Beekarry, Navin. "The International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law." *International Law*, 2011, 58.
10. Bilotta, Nicola. "CBDCs for Dummies: Everything You Need to Know about Central Bank Digital Currency (And Why You Shouldn't Be Afraid of It)," 2021, 18.
11. Biryukov, Alex, Dmitry Khovratovich, and Sergei Tikhomirov. "Privacy-Preserving KYC on Ethereum," n.d., 8.
12. "Bitcoin (\$BTC USD) News: China PBOC Says Crypto-Related Transactions Illegal - Bloomberg." Accessed April 29, 2022. <https://www.bloomberg.com/news/articles/2021-09-24/china-deems-all-crypto-related-transactions-illegal-in-crackdown>.
13. Blandin, Apolline, Ann Sofie Cloots, Hatim Hussain, Michel Rauchs, Rasheed Saleuddin, Jason G Allen, Bryan Zheng Zhang, and Katherine Cloud. "Global Cryptoasset Regulatory Landscape Study." *SSRN Electronic Journal*, 2019. <https://doi.org/10.2139/ssrn.3379219>.
14. StuDocu. "BlockChain Technology Beyond Bitcoin Abstract - BlockChain Technology Beyond Bitcoin Abstract A." Accessed April 29, 2022. <https://www.studocu.com/co/document/universidad-eia/calculo-integral/blockchain-technology-beyond-bitcoin-abstract/14736276>.
15. Borlini, Leonardo S., and Francesco Montanaro. "The Evolution of the EU Law Against Criminal Finance: The 'Hardening' of FATF Standards within the EU." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 28, 2017. <https://doi.org/10.2139/ssrn.3010099>.
16. Campbell-Verduyn, Malcolm. "Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance." *Crime, Law and Social Change* 69, no. 2 (March 1, 2018): 283–305. <https://doi.org/10.1007/s10611-017-9756-5>.
17. Cancelli, Lorenzo. "The Growing Crypto-Assets Threat to Anti-Money Laundering: How Institutions Are Coping with This Phenomenon," n.d., 21.
18. "Consultative Document - Prudential Treatment of Crypto-Asset Exposures," n.d., 25.
19. Dibrova, Alina. "Virtual Currency: New Step in Monetary Development." *Procedia - Social and Behavioral Sciences* 229 (August 2016): 42–49. <https://doi.org/10.1016/j.sbspro.2016.07.112>.
20. Ebikake, Emmanuel. "Money Laundering: An Assessment of Soft Law as a Technique for Repressive and Preventive Anti-Money Laundering Control." *Journal of Money Laundering Control* 19, no. 4 (January 1, 2016): 346–75. <https://doi.org/10.1108/JMLC-07-2015-0029>.
21. European Central Bank. *Virtual Currency Schemes*. Frankfurt am Main: European Central Bank, 2012.
22. European Central Bank. *Virtual Currency Schemes: A Further Analysis*. LU: Publications Office, 2015. <https://data.europa.eu/doi/10.2866/662172>.

23. European Police Office. *Why Is Cash Still King?: A Strategic Report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering*. LU: Publications Office, 2015. <https://data.europa.eu/doi/10.2813/698364>.
24. "Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing | Policing: A Journal of Policy and Practice | Oxford Academic." Accessed April 29, 2022. <https://academic.oup.com/policing/article/15/4/2329/6365869>.
25. "FATF Annual Report 2020-2021," n.d., 80.
26. Fletcher, Emily, Charles Larkin, and Shaen Corbet. "Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation." *Research in International Business and Finance* 56, no. 101387 (April 2021). <https://doi.org/10.1016/j.ribaf.2021.101387>.
27. Goodhart, Charles A. E. "The Two Concepts of Money: Implications for the Analysis of Optimal Currency Areas." *European Journal of Political Economy* 14, no. 3 (August 1, 1998): 407–32. [https://doi.org/10.1016/S0176-2680\(98\)00015-9](https://doi.org/10.1016/S0176-2680(98)00015-9).
28. Grigaitis, Denas. "TAIKYTINOS TEISĖS NUSTATYMAS KRIPTOVALIUTŲ SISTEMŲ DALYVIŲ SANTYKIAMS." *Jurisprudencija* 28, no. 1 (August 10, 2021): 158–78. <https://doi.org/10.13165/JUR-21-28-1-08>.
29. Haffke, Lars, Mathias Fromberger, and Patrick Zimmermann. "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, February 3, 2019. <https://doi.org/10.2139/ssrn.3328064>.
30. Hanafi, Author: "The Internationalization Of Anti-Money Laundering and The Compliance Of States." *Jurnal Hukum IUS QUIA IUSTUM* 20, no. 3 (2013): 343–61. <https://doi.org/10.20885/iustum.vol20.iss3.art1>.
31. Haynes, Andrew, and Peter Yeoh. *Cryptocurrencies and Cryptoassets: Regulatory and Legal Issues*. London: Informa Law from Routledge, 2020. <https://doi.org/10.4324/9781003034599>.
32. He, Dong, DHe@imf.org, Karl Habermeier, KHabermeier@imf.org, Ross Leckow, RLeckow@imf.org, Vikram Haksar, et al. "Virtual Currencies and Beyond: Initial Considerations." *Staff Discussion Notes* 16, no. 03 (2016): 1. <https://doi.org/10.5089/9781498363273.006>.
33. Helliär, Christine V., Louise Crawford, Laura Rocca, Claudio Teodori, and Monica Veneziani. "Permissionless and Permissioned Blockchain Diffusion." *International Journal of Information Management* 54 (October 1, 2020): 102136. <https://doi.org/10.1016/j.ijinfomgt.2020.102136>.
34. Hileman, Garrick, and Michel Rauchs. "2017 Global Cryptocurrency Benchmarking Study." *SSRN Electronic Journal*, 2017. <https://doi.org/10.2139/ssrn.2965436>.
35. Hofert, Eduard. "Regulating Virtual Currencies," n.d., 31.
36. Houben, Dr Robby, and Alexander Snyers. "Cryptocurrencies and Blockchain," n.d., 103.
37. "III. CBDCs: An Opportunity for the Monetary System," 2021, 31.
38. Irwin, Angela S. M., and Adam B. Turner. "Illicit Bitcoin Transactions: Challenges in Getting to the Who, What, When and Where." *Journal of Money Laundering Control* 21, no. 3 (July 2, 2018): 297–313. <https://doi.org/10.1108/JMLC-07-2017-0031>.
39. Lee, David. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, 2015.
40. "Legal and Economic Implications of Central Bank Digital Currencies (CBDC) | Springerprofessional.De." Accessed April 29, 2022. <https://www.springerprofessional.de/en/legal-and-economic-implications-of-central-bank-digital-currency/18470466>.
41. Markevych, Nadine Schwarz, Ke Chen, Kristel Poh, Grace Jackson, Kathleen Kao, Francisca Fernando, Maksym. "Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1)." IMF. Accessed April 29, 2022.

- <https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/14/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-463654>.
42. Mbiyavanga, Stefan. "CRYPTOLAUNDERING: ANTI-MONEY LAUNDERING REGULATION OF VIRTUAL CURRENCY EXCHANGES," 2019, 15.
 43. Monaco, Sofia Del. "Money Mules and Tumblers: Money Laundering during the Cryptocurrency Era.," n.d., 19.
 44. Möser, Malte, and Arvind Narayanan. "Effective Cryptocurrency Regulation Through Blacklisting," n.d., 24.
 45. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System," n.d., 9.
 46. Palley, Thomas. "The Evolution of Money Debate: Functionalism versus Chartalism, Schumpeterian Dynamics, Gresham's Fallacy, and How History Constrains Public Finance," no. 34 (2018): 29.
 47. Pavlidis, Georgios. "Financial Action Task Force and the Fight against Money Laundering and the Financing of Terrorism: Quo Vadimus?" *Journal of Financial Crime* 28, no. 3 (January 1, 2020): 765–73. <https://doi.org/10.1108/JFC-09-2019-0124>.
 48. ———. "International Regulation of Virtual Assets under FATF's New Standards." *Journal of Investment Compliance* 21, no. 1 (January 1, 2020): 1–8. <https://doi.org/10.1108/JOIC-08-2019-0051>.
 49. "Regulating Cryptocurrencies Checkpoints: Fighting a Trench War with Cavalry? - Soana - 2022 - Economic Notes - Wiley Online Library." Accessed April 29, 2022. <https://onlinelibrary.wiley.com/doi/full/10.1111/ecno.12195>.
 50. "Report on a Digital Euro," n.d., 55.
 51. Reuter, Peter. *Chasing Dirty Money: The Fight Against Money Laundering*. Peterson Institute, 2005.
 52. Rodrigues, Gustavo, Lahis Kurtz, and André Oliveira. "Cryptocurrencies and Anti-Money Laundering Regulation in the G20," n.d., 61.
 53. Sanz-Bas, David, Carlos del Rosal, Sergio Luis Nañez Alonso, and Miguel Angel Echarte Fernandez. "Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain." *Laws | An Open Access Journal from MDPI* 10, no. 3 (2021). <https://www.canlii.org/en/commentary/doc/2021CanLIIDocs1698#!fragment/undefined/BQCwhgziBcwMYgK4DsDWsBGB7LqC2YATqgJIAM0A5JQJQA0yWALgKYQCKiLhAnlZXQgsiCTtz7VBwwggDKWQkwBCfAEoBRADLqAagEEAcgGF1dJmAzQmWO DRpA>.
 54. Scharfman, Jason. "Cryptocurrency Compliance and Operations." Springer Books. Springer, 2022. <https://econpapers.repec.org/bookchap/sprsprbok/978-3-030-88000-2.htm>.
 55. Schmidt, Alicia. "Virtual Assets: Compelling a New Anti-Money Laundering and Counter-Terrorism Financing Regulatory Model." *International Journal of Law and Information Technology* 29, no. 4 (December 1, 2021): 332–63. <https://doi.org/10.1093/ijlit/eaac001>.
 56. Silva Ramalho, David, and Nuno Igreja Matos. "What We Do in the (Digital) Shadows: Anti-Money Laundering Regulation and a Bitcoin-Mixing Criminal Problem." *ERA Forum* 22, no. 3 (September 1, 2021): 487–506. <https://doi.org/10.1007/s12027-021-00676-4>.
 57. Singh, Kavid. "The New Wild West: Preventing Money Laundering in the Bitcoin Network," n.d., 30.
 58. Singh, Sunil Kumar, and Sumit Kumar. "Blockchain Technology: Introduction, Integration and Security Issues with IoT." *ArXiv:2101.10921 [Cs]*, January 26, 2021. <https://arxiv.org/abs/2101.10921>.
 59. Smith, Rhona. "Directive 2008/94/EC of the European Parliament and of the Council of 22 October 2008." In *Core EU Legislation*, by Rhona Smith, 423–26. London: Macmillan Education UK, 2015. https://doi.org/10.1007/978-1-137-54482-7_44.

60. Sprenger, Pascal, and Franziska Balsiger. "Anti-Money Laundering in Times of Cryptocurrencies," 2018, 4.
61. Subačius, Augustas, and Rasa Subačienė. "Cryptocurrency: Advantages and Disadvantages." *Buhalterinės Apskaitos Teorija Ir Praktika* 0, no. 19 (May 14, 2019): 1. <https://doi.org/10.15388/Batp.2019.1>.
62. Sullivan, Kevin. *Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business*. Berkeley, CA: Apress, 2015. <https://doi.org/10.1007/978-1-4302-6161-2>.
63. Swartz, Lana. "What Was Bitcoin, What Will It Be? The Techno-Economic Imaginaries of a New Money Technology." *Cultural Studies* 32, no. 4 (July 4, 2018): 623–50. <https://doi.org/10.1080/09502386.2017.1416420>.
64. "Taking Blockchain Seriously | SpringerLink." Accessed April 29, 2022. <https://link.springer.com/article/10.1007/s10978-018-9226-y>.
65. Teichmann, F. "Twelve Methods of Money Laundering," 2017. <https://doi.org/10.1108/JMLC-05-2016-0018>.
66. Torre, Dominique, and Sothearith Seang. "Proof of Work and Proof of Stake Consensus Protocols: A Blockchain Application for Local Complementary Currencies," August 23, 2019. <https://halshs.archives-ouvertes.fr/halshs-02268391>.
67. Utkina, Maryna, Roman Samsin, and Maksym Pochtovyi. "Financial Intelligence (Monitoring) of the Transactions with Virtual Assets: New Legislation and Best Practices of Foreign Countries." *Journal of Money Laundering Control* ahead-of-print, no. ahead-of-print (January 1, 2022). <https://doi.org/10.1108/JMLC-12-2021-0136>.
68. Vandezande, Niels. "Virtual Currencies under EU Anti-Money Laundering Law." *Computer Law & Security Review* 33, no. 3 (June 1, 2017): 341–53. <https://doi.org/10.1016/j.clsr.2017.03.011>.
69. Velkes, Gabrielle Chasin. "INTERNATIONAL ANTI-MONEY LAUNDERING REGULATION OF VIRTUAL CURRENCIES AND ASSETS." *MONEY LAUNDERING* 52 (n.d.): 32.
70. "Virtual Currencies – Key Definitions and Potential AML/CFT Risks," 2014, 17.
71. Intersentia NV. "Virtual Currencies: A Legal Framework." Accessed April 29, 2022. <https://intersentia.com/en/virtual-currencies-a-legal-framework.html>.
72. "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them by Lars Haffke, Mathias Fromberger, Patrick Zimmermann :: SSRN." Accessed April 29, 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328064.
73. springerprofessional.de. "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge." Accessed April 29, 2022. <https://www.springerprofessional.de/en/where-s-wally-fatf-virtual-asset-service-providers-and-the-regul/20101922>.
74. Wray, L Randall. "From the State Theory of Money to Modern Money Theory: An Alternative to Economic Orthodoxy," n.d., 35.

ANOTACIJA

Atsižvelgiant į virtualių valiutų technologinį naujumą bei sparčią pažangą, teisinio reglamentavimo nebuvimas sukėlė nemažai iššūkių pinigų plovimo prevencijos atžvilgiu. Dėl virtualių valiutų savybių, tokių kaip visiško ar dalinio anonimiškumo, tarpvalstybinio pobūdžio, ne visos tarptautinės pastangos užkirsti kelią virtualių valiutų panaudojimui pinigų plovimo nusikaltimo vykdymui iki šiol buvo sėkmingos.

Šiame magistro baigiamajame darbe siekiama išanalizuoti virtualių valiutų naudojimo keliamus iššūkius pinigų plovimo prevencijos teisiniam reglamentavimui tarptautinės teisės atžvilgiu. Visų pirma išnagrinėjant virtualias valutas, kaip reiškinių, vėliau įvertinant jų galimą panaudojimą pinigų plovimo nusikaltimo vykdymui. Darbe apibrėžiama kokios prevencinės priemonės taikomos nacionaliniu, regioniniu ir tarptautiniu lygmeniu, siekiant apriboti virtualių valiutų naudojimą pinigų plovimo tikslais.

Raktiniai žodžiai: virtualios valiutos, pinigų plovimas, pinigų plovimo ir terorizmo finansavimo prevencija, Bitcoin, AMLD5

ABSTRACT

Given the technological novelty and rapid progress of virtual currencies, the absence of a legal framework has created a number of challenges for AML. Due to the cross-border nature of virtual currencies, such as full or partial anonymity, not all international efforts to prevent the use of virtual currencies for money laundering offences have been successful to date.

This Master's thesis aims to analyse the challenges posed by the use of virtual currencies to the legal framework for the prevention of money laundering from an international law perspective. Firstly, by examining virtual currencies as a phenomenon, and then by assessing their potential use in the commission of money laundering offences. The work outlines what preventive measures are in place at national, regional and international level to limit the use of virtual currencies for money laundering purposes.

Keywords: virtual currencies, money laundering, AML/CFT, Bitcoin, FATF standards, AMLD5

SANTRAUKA

Šiame magistro baigiamajame darbe siekiama išanalizuoti virtualių valiutų reiškinių bei virtualių valiutų keliamus iššūkius pinigų plovimo prevencijos teisiniam reguliavimui tarptautinės teisės požiūriu, įvertinant teisinio reglamentavimo raidą laike.

Baigiamąjį darbą sudaro bendroji bei specialioji dalys. Pirmajame skyriuje pristatoma virtualių valiutų sąvoka, išskiriamos virtualių valiutų rūšys, paaiškinami jų skirtumai, virtualios valiutos, be kita ko, atskiriamos nuo realių valiutų bei elektroninių pinigų. Pateikiami apibendrinti virtualių valiutų požymiai. Taip pat šiame skyriuje aiškinamas virtualių valiutų technologinis mechanizmas, blokų grandinės samprata bei veikimo pagrindai. Norint efektyviai išaiškinti virtualių valiutų reglamentavimo probleminius klausimus, išskiriami virtualių valiutų rinkos dalyviai, apibrėžiamas jų vaidmuo.

Antrajame skyriuje atsakoma į klausimą, kas yra pinigų plovimas. Siekiant atskleisti virtualių valiutų pritaikymą pinigų plovimo nusikaltimo vykdymui, visų pirma, apibūdinami pinigų plovimo etapai, išskiriami tradiciniai pinigų plovimo metodai. Galiau apibūdinama su kokiais iššūkiais susiduriama panaudojant virtualias valiutas pinigų plovimo tikslais.

Specialiojoje darbo dalyje analizuojamos virtualių valiutų teisinio reglamentavimo problemos. Ši dalis turi kelis kertinius taškus. Pirmiausia, įvertinamas šalių nacionalinis požiūris į virtualių valiutų naudojimą pinigų plovimo atžvilgiu bei valstybių taikomi reglamentavimo metodai. Didelis dėmesys paskiriamas FATF standartų raidai bei šių rekomendacijų analizei, įvertinama pinigų plovimo prevencijos internacionalizacija, minkštųjų teisės normų įtaka. Antra, vertinama Europos Sąjungos teisės aktų raida bei šiuo metu galiojantis reglamentavimas skirtas užkirsti kelią virtualių valiutų naudojimui pinigų plovimo nusikaltimo vykdymui, įvertinamos naujovės bei išskiriamos paliktos galimos spragos, be kita ko, pažymima. Atkreipiamas dėmesys į tarptautinio bendradarbiavimo poreikį. Galiausiai įvertinama Tarptautinio atsiskaitymų banko nuomonė dėl virtualių valiutų keliamų grėsmių bei apžvelgiamas centrinių bankų skaitmeninių valiutų pobūdis ir pritaikymo galimybės.

SUMMARY

This Master's thesis aims to analyse the phenomenon of virtual currencies and the challenges posed by virtual currencies to the legal framework for the prevention of money laundering from the perspective of international law, assessing the evolution of the legal framework over time.

The thesis consists of a general and a specific part. The first chapter introduces the concept of virtual currencies, distinguishes the types of virtual currencies, explains their differences, and distinguishes virtual currencies from real currencies and electronic money, among other things. It provides a summary of the characteristics of virtual currencies. It also explains the technological mechanism of virtual currencies, the concept of the blockchain and the basics of its operation. In order to effectively clarify the regulatory issues surrounding virtual currencies, it identifies the players in the virtual currency market and defines their role.

The second chapter answers the question of what constitutes money laundering. In order to shed light on the application of virtual currencies to the crime of money laundering, it first describes the stages of money laundering and identifies the traditional money laundering methods. Finally, it describes the challenges faced when using virtual currencies for money laundering purposes.

The specific part of the thesis analyses the problems of legal regulation of virtual currencies. This part has several focal points. Firstly, it assesses the national approaches to the use of virtual currencies in relation to money laundering and the regulatory approaches taken by countries. The development of the FATF standards and the analysis of these recommendations are given considerable attention, as well as the internationalisation of anti-money laundering and the impact of soft law. Secondly, it assesses the evolution of European Union legislation and the current regulatory framework to prevent the use of virtual currencies for money laundering offences, evaluates innovations and identifies possible gaps left, including. The need for international cooperation is highlighted. Finally, it assesses the views of the Bank for International Settlements on the threats posed by virtual currencies and reviews the nature and applicability of central banks digital currencies.