TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Õiguse instituut

Aido Ojassalu

RAHAPESUVASTASE DIREKTIIVI NR.5 SOBIVUS RAHAPESU TÕKESTAMISEKS KRÜPTORAHA TEHINGUTES

Magistritöö
Õppekava HAJM08/15, peaeriala Õigusteadus, Eesti avalik ja eraõigus

Juhendaja: Janika Aben, MA eq

Tallinn 2019

Deklareerin, et olen koostanud töö iseseisvalt ja
olen viidanud kõikidele töö koostamisel kasutatud
teiste autorite töödele, olulistele seisukohtadele ja andmetele,
ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.
Töö pikkuseks on 16225 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Aido Ojassalu ……

(allkiri, kuupäev)

Üliõpilase kood: 178811HAJM

Üliõpilase e-posti aadress: Aido.Ojassalu@gmail.com

Juhendaja: Janika Aben

Töö vastab kehtivatele nõuetele

……

(allkiri, kuupäev)

Kaitsmiskomisjoni esimees: /lisatakse ainult lõputöö puhul/

Lubatud kaitsmisele

……

(nimi, allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Magistritöö eesmärk on välja selgitada, kas rahapesuvastane direktiiv nr.5[1] (edaspidi AMLD nr.5)[2] on sobiv vahend takistamaks rahapesu krüptoraha tehingutes. Kuna krüptoraha on uudne valdkond, siis sellega tekkivad võimalused rahapesuks on erinevad sellest, mis siiani kurjategijate käsutuses on olnud, seega on vaja ka uudset lähenemist regulatiivsel tasandil. 30.05.2018 vastu võetud AMLD-ga nr.5 tegi Euroopa Liit esimesed olulised regulatiivsed sammud rahapesu tõkestamiseks krüptoraha tehingutes. Põhilised muutused, mis nimetatud direktiiv kaasa tõi, olid loakohustuse ja hoolsuskohustuse nõuete laiendamine krüptoraha rahakoti teenuste pakkujatele ja kauplemisplatvormidele. Krüptoraha valdkond on uudne valdkond, kus edasiareng on kiire ning viimastel aastatel on turule tulnud mitmed uudsed võimalused – anonüümsust pakkuvad krüptorahad ja teenusepakkujad. Viimaste uuringute kohaselt kasutatakse just neid kõige enam krüptorahaga läbiviidavaks rahapeuks. Seega on oluline hinnata, kas uutel regulatsioonidel on mõju ka sellisel kujul tehtava rahapesu vastu võitlemisel või mitte. Töö käigus selgus, et loakohustuse taotlemise protsess vajab täiendamist, kuna see pole hetkel piisavalt põhjalik takistamaks probleemsetele ettevõtetele tegevuslubade väljastamist. Hoolsuskohustuse nõuded vajavad samuti täiendamist, kuna kõige suuremad probleemikohad, milleks on anonüümsete krüptorahadega tehtavad tehingud, vajaks täiendavat tähelepanu. Kindlasti peab aga rohkem tähelepanu pöörama sektoris tegutsevate ettevõtete monitoorimisele.

Võtmesõnad: Krüptoraha, AMLD nr.5, loakohustus, hoolsuskohustus

[1] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/843, 30. mai 2018, millega muudetakse direktiivi (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist, ning millega muudetakse direktiive 2009/138/EÜ ja 2013/36/EL (EMPs kohaldatav tekst), OJ L 156, 19.6.2018, lk. 43–74. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32018L0843, 01.04.2019

[2] Anti Money Laundering Directive

SISSEJUHATUS

Finantsmaailmas on viimastel aastatel toimunud palju muutusi. Meie raha liigutatakse, kaubeldakse, säilitatakse, valideeritakse ja verifitseeritakse mittemateriaalsete arvutivõrgustike poolt.[3] See tähendab, et enamik rahast ei ole enam paberkujul meie enda käes, vaid see on tohututes arvutisüsteemides. See on toonud inimestele palju täiendavaid mugavusi – näiteks ei pea sularaha kaasas kandma ning maksed on kiiremad kui kunagi varem. Kuid saadud mugavusel on ka omad ohukohad. Kiirus ja mugavus kõigile toob paratamatult kaasa ka kiiruse ja mugavuse neile kes ei tegutse heas usus - kurjategijatele. Kunagi ei ole olnud nii kerge liigutada suurtes kogustes raha nii kiirelt erinevate jurisdiktsioonide vahel kui täna. Kiiremad tehingud toovad kaasa ka selle, et aina lihtsam on teha mingi konkreetse rahaga palju tehinguid, mis toob kaasa kriminaalse raha päritolu tuvastamise muutumise aina keerulisemaks. Nende ja mitmete muude põhjuste tõttu on rahapesu täna saavutanud suur mastaabi. Ootamatult on ka Eesti muidu usaldusväärsena paistnud pangandussüsteemi tabanud mitmed rahapesu juhtumid, mille puhul nende mastaapsust on raske hoomata. Näiteks Danske Banki puhul võib aastate 2007 ja 2015 vahel pestud raha summa ulatuda ligikaudu 230 miljardi USA dollarini.[4] Võrdluseks - Eesti riigieelarve tulud 2017. aasta kohta olid ca 12,5 miljardit USA dollarit.[5] Hoolimata sellest, et summad on tohutud (mis peaks suurendama ka võimalust, et need satuvad õiguskaitseorganite tähelepanu alla) võis selline tegevus jätkuda aastaid. See näitab, et õiguskaitseorganitel on võitluses rahapesu vastu veel väga palju teha.

Läbi Suurbritannia pestakse igal aastal raha üle 115 miljardi dollari väärtuses.[6] Maailmas iga-aastaselt pestava raha suuruseks hinnatakse 2-5% globaalsest sisemajanduse koguproduktist, seega on selle suurusjärk 800 miljardi kuni 2 triljoni USA dollari vahel. Kuigi

---

[3] Gamble, C. (2017). The Legality and Regulatory Challenges of Decentralised Crypto-Currency: A Western Perspective, 20 International Trade & Business Law Review. 346-361, lk 347

[4] Schwartzkopff, F. (2019). Contagion From Danske Case Feeds a New Fear in Borderless EU. Kättesaadav: https://www.bloomberg.com/news/articles/2019-03-10/danske-laundering-contagion-feeds-a-new-fear-in-borderless-eu, 20.03.2019

[5] Eesti Statistikaamet. (2019). Riigieelarve tulud ja kulud, aasta. Kättesaadav: https://www.stat.ee/53713, 20.03.2019

[6] Counting the cost of money laundering. (2018). Kättesaadav: https://www.independent.co.uk/news/business/news/counting-the-cost-of-money-laundering-a8122916.html, 20.03.2019

marginaal nende numbrite vahel on tohutu, on isegi kõige madalam hinnanguline iga-aastane pestava raha suurus selline, mis peaks panema riikide valitsusi, regulaatoreid ja õiguskaitseorganeid probleemiga aina enam tegelema.[7] Rahapesu eesmärgiks on kurjategijatel ühtviisi varjata toimepandud kuritegusi ning samas ka takistada õiguskaitseorganitel raha ja muid varasid arestimast.[8]

Pestava raha hulk on viimastel aastatel toonud kaasa paljud erinevad täiendavaid regulatsioone eri tasemetel, millega valitsused, õiguskaitseorganid ja finantsjärelevalvega tegelevad organisatsioonid üritavad rahapesu takistada.

30.mail 2018 võtsid Euroopa Parlament ja Euroopa nõukogu vastu direktiivi 2018/843, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist. Avalikkusele on nimetatud direktiiv rohkem teada kui AMLD nr.5. Nimetatud direktiiviga prooviti tuua lahendusi probleemidele, mis olid jäänud reguleerimata 2015. aastal vastu võetud direktiiviga[9] 2015/849, mis on tuntud kui AMLD nr.4. Samuti oli see oluline sõnum, et Euroopa Liit peab rahapesuvastast võitlust üheks oma prioriteediks. AMLD nr.5 toob mitmed uuendused ja täiendused, mille liikmesriigid peavad oma seadustesse üle võtma hiljemalt 20. jaanuariks 2020. Muu hulgas olid AMLD nr.5 erilise fookuse all krüptoraha tehingud (direktiivis küll nimetati neid virtuaalvääringuteks), mida näiteks veel AMLD-s nr.4 eraldi välja ei olnud toodud.

Siinkohal ongi oluline selgitada, et kuna krüptorahade puhul on tegemist alles välja kujuneva valdkonnaga, siis tihti kasutatakse krüptoraha, virtuaalvaluuta, virtuaalvääringu jne mõisteid läbisegi, seda ka õiguskirjanduses. Tegelikult on tegemist erinevate mõistega, mille erinevust autor käesolevas magistritöös lühidalt ka selgitab. Kuna käesoleva töö kirjutamisel oli tihti ka viidatud tekstides nimetatud väljendeid kasutatud läbisegi, siis autor kasutab läbivalt terminit „krüptoraha“, kui just ei ole tegemist olukorraga kus tulebki erinevat terminoloogiat kasutada.

---

[7] Money-Laundering and Globalization. Kättesaadav: https://www.unodc.org/unodc/en/money-laundering/globalization.html, 20.03.2019

[8] The Money-Laundering Cycle. Kättesaadav: https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html, 20.03.2019

[9] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/849, 20. mai 2015, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ (EMPs kohaldatav tekst),OJ L 141, 5.6.2015, lk. 73–117. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32015L0849, 01.04.2019

Rääkimaks krüptorahast, tuleks kõigepealt anda põgus selgitus sellele, mis krüptoraha on. Lühidalt öeldes on krüptoraha selline digitaalne raha, mis toetub krüptograafiale.[10] Krüptograafia omakorda on andmete turvaomaduste tagamine matemaatika kaudu.[11] Täpsema definitsiooni annab autor krüptoraha kohta juba käesoleva töö sisuosas.

Krüptorahad on kujunenud välja viimase kümne aasta jooksul. On ilmselt sobiv küsida miks on krüptorahad populaarseks saanud? Üheks põhjuseks võib tuua selle, et inimeste usaldus traditsioonilise raha vastu on vähenenud.[12] Krüptorahade osas on tänasel hetkel veel palju küsimusi. Tihti peetakse neid „pettuseks", palju räägitakse sellest, et need on mööduv nähtus. On isegi öeldud, et krüptorahad võivad maksuparadiiside asemel saada maksude maksmisest eemalhoidvate isikute lemmikuks.[13] Kuna tegemist on uue viisiga raha vahetada, on regulaatorid väljendanud muret, et plokiahelaga seonduvatel rahadel on potentsiaal olla kasutatavad rahapesuks.[14] Tõenäoliselt kõige suurem kriitika, mida krüptorahade osas tehakse ongi see, et see võimaldab teha illegaalseid tehinguid nii internetis kui ka rahvusvaheliselt.[15] Ometigi on krüptorahadel tänaseks maailmas välja kujunenud juba oma kindel koht. 10.05.2019 seisuga[16] on maailmas olemas 2166 krüptoraha, mille koguväärtus on üle 192 miljardi dollari, kuid 2018. aasta jaanuaris kui tuntuim krüptoraha bitcoin oli oma hinna tipus, oli kõikide krüptorahade turuväärtus ligikaudu 825 miljardit dollarit. Tegemist on finantsiliselt märkimisväärse summaga.

Kuna krüptorahade puhul on tegemist uue valdkonnaga, siis on selge, et selles valdkonnas on palju seda mis on seadusandja tasemel reguleerimata (muidugi on juba eriküsimus kui palju seadusandja peab üldse reguleerima igat uut valdkonda) ja eri jurisdiktsioonides on selle kohta väga erinevaid käsitlusi. Alati on ka neid, kes uutes valdkondades tekkivaid võimalusi

---

[10] Frankenfield, J. Cryptocurrency. (2019). Kättesaadav: https://www.investopedia.com/terms/c/cryptocurrency.asp, 20.03.2019

[11] Virunurm, K. (2018). RIA krüptouuring – ID-kaart ja plokiahelad. Kättesaadav: https://blog.ria.ee/tag/kruptograafia/, 20.03.2019

[12] Cvetkova, I. (2018). Cryptocurrencies Legal Regulation, 5 BRICS Law Journal. 128-153, lk 132

[13] Marian, O. (2013-2014). Are Cryptocurrencies Super Tax Havens, 112 Michigan Law Review First Impressions. 38-48, lk 38

[14] Brookes, A. (2018). U.S. Regulation of Blockchain Currencies: A Policy Overview, 9 American University Intellectual Property Brief. 75-104, lk 83

[15] Gerkis, J. Krikunova, S. (2014). Bitcoin and Other Virtual Currencies: Approaching U.S. Regulatory Acceptance, 39 Administrative and Regulatory Law News. 4-8, lk 5

[16] Coinmarketcap. Kättesaadav: https://coinmarketcap.com/, 20.03.2019

kuritegelikel eesmärkidel ära tahavad hakata kasutama. Nii ka krüptorahade puhul. Krüptorahadega seonduva rahapesu osas on öeldud, et krüptorahad teevad selle tavapärasest kergemaks ja need on ideaalsed vahendid muu hulgas rahapesuks oma anonüümsuse tõttu.[17] Isegi kui krüptorahade võrgustikud võivad tulevikus areneda välja tugevamateks ja paremini kaitstud süsteemideks, on fakt see, et hetkel on probleem olemas.[18]

Näiteks, 2018. aastal võis krüptoraha tehingute puhul rääkida umbes 1,7 miljardist dollarist, mille osas oli kahtlus rahapesus.[19] Kuna nimetatud uuringus uuriti vaid osa krüptorahade tehingutest võib arvata, et tegemist on pigem tagasihoidliku hinnanguga. Euroopa Politseiameti (edaspidi Europol) üks juhtidest Rob Wainwright näiteks on toonud välja, et Europol on nägemas trendi, kus miljardites raha, mis on teenitud tänavatel narkootikumide müügist, konverteeritakse krüptorahadeks.[20] Seega on läbi krüptorahade toimuv rahapesu kindlasti oluline teema. Samuti on oluline õiguskaitseorganite ja seadusandjate koostöö vältimaks seda, et rahapesu krüptorahadega muutub veelgi suuremaks probleemiks.

Käesolevas töös üritab autor selgitada välja krüptorahade definitsiooni eri õigusruumides ja kohtupraktikat selle kohta, lisaks ka tehnoloogia eripärasi, mille abil krüptorahad toimivad. Nimetatu kohta antakse ülevaade töö esimeses osas. Töö teises osas keskendub autor rahapesule üldisemalt ning viisidele, mille abil toimub praegusel ajal krüptorahaga tehingutes rahapesu. Praeguste rahapesuvastaste regulatsioonide ja alles jõustuma hakkavate regulatsioonide valguses uurib autor hetkel levinumaid krüptoraha tehingutes kasutatavaid rahapesuskeeme. Lõppjäreldusteni jõudmiseks kasutab autor erinevate riikide õigusteadlaste kirjutatut, samuti eri riikide kohtupraktikat, muu hulgas nii *common law* riikide kui ka Mandri-Euroopa riikide oma. Kuna krüptoraha tehingutega seonduvaid rahapesu teemalisi kohtuvaidlusi Mandri-Euroopa olnud ei ole, siis toob autor kohtupraktikas välja Ameerika Ühendriikides ette tulnud kohtulahendid.

---

[17] Grinberg, R. (2012). Bitcoin: An Innovative Alternative Digital Currency, 4 Hastings Science & Technology Law Journal. 159-208, lk 161

[18] Sonderegger, D. (2015). A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation, 47 Washington University Journal of Law & Policy. 175-216, lk 207

[19] Cryptocurrency Anti-Money Laundering Report, 2018 Q4. (2019). Kättesaadav: https://ciphertrace.com/wp-content/uploads/2019/01/crypto_aml_report_2018q4.pdf, 20.03.2019

[20] Silva, S. (2018). Criminals hide 'billions' in crypto-cash - Europol. Kättesaadav: https://www.bbc.com/news/technology-43025787, 20.03.2019

Töö lõpus annab autor soovitusi millistele probleemidele tuleks täiendavalt tähelepanu pöörata ning mõtteid, millest loodetavasti ka praktikas kasu võib tulla. Töös kasutatakse kvalitatiivset uurimust ning täpsemalt võrdlevat analüüsi. Võrdlev analüüs põhineb erinevates seadustes toodud sätete võrdlemisel ning järeldused tehtakse deduktiivse meetodi abil. Peamisteks kasutatavateks seadusteks on rahapesu ja terrorismi rahastamise tõkestamise seadus[21] (edaspidi RahaPTS) ning makseasutuste ning makseasutuste ja e-raha asutuste seaduse (edaspidi MERAS).[22]

Kuna Eestit ja Euroopa üldiselt mõjutab rahapesuvastases võitluses kahtlemata kõige rohkem AMLD nr.5, siis töö hüpoteesiks ongi see, et AMLD nr.5 toodud muudatused ei ole sobivad vahendid krüptorahaga seonduvas rahapesuvastases võitluses. Hüpoteesi kinnitamiseks tuleb töö käigus leida vastused erinevatele uurimisküsimustele. Töö uurimisküsimused on:

1) Millised on kõige suuremad ohud mis kaasnevad krüptorahaga?
2) Milliseid preventiivseid meetmeid sisaldab AMLD nr.5 ja kas need katavad krüptorahast tulenevaid riske asjakohaselt?
3) Kas krüptorahadega tehtav rahapesu võib tänu oma eripäradele põhjustada selle, et AMLD-s nr.5 olevat rahapesu definitsiooni on vaja muuta või katab tänane regulatsioon ära ka erijuhud krüptorahaga tehtavas rahapesus?

.

[21] Rahapesu ja terrorismi rahastamise tõkestamise seadus. - RT I, 13.03.2019, 126
[22] Makseasutuste ja e-raha asutuste seadus - RT I, 13.03.2019, 23

1. KRÜPTORAHA

1.1. Krüptoraha olemus

1.1.1. Krüptoraha üldine selgitus Bitcoini näitel

Kuigi tavapäraselt peetakse krüptoraha alguseks 31.10.2008 Satoshi Nakamoto poolt avaldatud kirjutist "Bitcoin: A Peer-to-Peer Electronic Cash System"[23], siis tegelikkuses on sarnastel tööpõhimõtetel põhinevaid lahendusi mõeldud välja ennegi. Juba 1983. aastal pakkus Ameerika Ühendriikide krüptograaf David Chaum välja elektroonilise raha variandi, mis põhines krüptograafilistel tehingutel ning mille allkirjastab pank.[24] Sarnastel põhimõtetel rajas Chaum 1989. aastal ettevõtte DigiCash. Tema pakutud e-raha teenus seisnes selles, et kliendi pangast liikusid e-kirja teel krüpteeritud teated kaupmehe juurde nii, et algpunkti polnud võimalik tuvastada. Kuid nimetatud süsteemi edu ei saatnud. Ameerika Ühendriikides tundis pakutava teenuse vastu huvi vaid üks pank ning kolme aasta jooksul oli süsteemil kokku vaid 5000 kasutajat. Ühe põhjusena, miks ettevõtmist ei saatnud edu, võib tuua selle, et nii kaupmehed kui pangad ei tundnud teenuse vastu huvi, kuna nende huvides oli reklaaminduse eesmärgil koguda klientide kohta võimalikult palju infot. Juba 1998. aastal lõpetas ettevõte tegevuse ja läks pankrotti.[25]

Krüptograafial toimivat elektroonilist raha pakuti välja ka 1996. aastal NSA (National Security

---

[23] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Kättesaadav: https://bitcoin.org/bitcoin.pdf. 20.03.2019

[24] Chaum, D. (1982). Untraceable Electronic Cash. Kättesaadav: http://blog.koehntopp.de/uploads/chaum_fiat_naor_ecash.pdf, 20.03.2019

[25] Pitta, J. (1999). Requiem for a Bright Idea. Kättesaadav: https://www.forbes.com/forbes/1999/1101/6411390a.html#7a463e03715f, 20.03.2019

Agency ehk USA Riiklik Julgeolekuagentuur) töötajate poolt välja antud artiklis.[26] Nimetatud artikli olulisemad punktid olid kahevõtme süsteem, kus üks võti on avalik ja teine on privaatne, ning süsteemi anonüümsus. Mõlemad nimetatud põhimõtted on ka bitcoini ja muude krüptorahade oluliste tööpõhimõtete hulgas.

Krüptorahade sünd toimus siiski pärast juba eespool mainitud Satoshi Nakamoto kirjutist. Nimetatud kirjutises tõi ta välja, et internetikaubandus on peaaegu ainusõltuv finantsasutustest, kes kolmanda osapoolena elektroonilisi makseid vahendavad.[27] See omakorda toob aga lisakulusid kasutajatele. Samuti leidis Nakamoto, et puudub selline vahend, mis võimaldaks teha makseid ilma usaldusväärse kolmanda osapooleta. Nende probleemide lahenduseks pakkus ta välja elektrooniliste maksete süsteemi, mis põhineb mitte usaldusel vaid krüptograafilistel tõenditel. See omakorda võimaldaks aga kahel osapoolel otsejoones teineteisega suhelda. Seega puuduks vajadus usaldusväärse kolmanda osapoole (pank) olemasoluks. Samuti seletas ta selles kirjutises lahti krüptograafilistel tõenditel põhineva uue elektroonilise raha süsteemi tööpõhimõtted ja selle taga paikneva tehnoloogia.[28]

Tänaseni ei ole suudetud tuvastada kas selline isik nagu Satoshi Nakamoto ka tegelikkuses eksisteeris ning erinevates väljaannetes on palju spekuleeritud selle üle, kes selle isiku taga tegelikkuses oli. Muu hulgas on ka Ameerika Ühendriikide valitsus üritanud välja selgitada, kellega on tegu, kartuses, et tegelikkuses võib tegemist olla Venemaa või Hiina agendiga.[29]

Bitcoini võrgustikule pani Satoshi Nakamoto ametlikult aluse 03.01.2009, kui kaevandas esimesed viiskümmend bitcoini. Maailma esimene krüptoraha tehing tehti 12.01.2009 kui Satoshi Nakamoto saatis kümme bitcoini tuntud krüptograafia entusiast Hal Finney'le.[30] Esimese kaubandusliku tehingu bitcoinidega tegi aga Florida programmeerija Laszlo Hanyecz,

---

[26] Law, L. Sabett, S. Solinas, J. (1997). How to Make a Mint: The Cryptography of Anonymous Electronic Cash. American University Law Review 46, no.4. 1132-1162, lk 1132.
[27] Nakamoto (2008), *supra nota* 23
[28] *Ibid.*
[29] Who is the real Satoshi Nakamoto? (2018). Kättesaadav: https://medium.com/@cryptaldashcoin/who-is-the-real-satoshi-nakamoto-55bacbbee566, 20.03.2019
[30] Peterson, A. (2014). Hal Finney received the first Bitcoin transaction. Here's how he describes it. Kättesaadav: https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/?noredirect=on&utm_term=.9c565c311cff, 20.03.2019

kes 2010. aastal maksis 10 000 bitcoini kahe pizza eest.[31]

Bitcoini algusfaasis toimus ka selle ajaloos siiani ainuke edukas bitcoini võrgustiku häkkimine, kui 06.08.2010 suutis tundmatu häkker korraga teha juurde 184 miljardit bitcoini.[32] Tegelikult on bitcoinide teoreetiline limiit 21 miljonit bitcoini, pärast seda bitcoine juurde enam võimalik teha ei ole.[33] Plokiahela kopeerimisega lahendati probleem kiirelt, kuna sellel ajal ei olnud süsteemil veel palju kasutajaid. Seega intsident suuri probleeme ei põhjustanud.[34] Täna selline kopeerimine enam niivõrd kergelt ja edukalt teostatav ei oleks, kuna kopeeritavate tehingute hulk oleks äärmiselt suur - seisuga 10.05.2019[35] on bitcoini süsteemis tehtud üle 410 miljoni tehingu.

Samas võib bitcoini võrgustiku tugevust kiita, kuna see on jäänud siiani ainsaks edukaks rünnakuks bitcoini võrgustiku vastu. Süsteemi koodiridade kvaliteeti on kiitnud paljude muude hulgas ka tuntud USA infotehnoloogia turvalisuse ekspert Dan Kaminsky.[36] Ta kommenteeris, et pole varem midagi taolist näinud ning selgitas, et bitcoini võrgustiku toimiseks vajalike koodiridade kirjutamine eeldab maailma tipptasemel programmeerimisoskust ja suurt arusaama programmeerimiskeelest C++.

2011. aastal hakkasid tekkima juba järgnevad krüptorahad näiteks nagu Litecoin, Namecoin ja Swiftcoin.[37] Kuid ükski neist pole saanud ligilähedaselt sama populaarseks kui bitcoin. Seisuga 10.05.2019 on kogu bitcoini võrgustiku väärtus üle kuue korra suurem kui väärtuselt teise krüptoraha Etherumi oma ning suurem kui kõikide teiste krüptorahade väärtus kokku.[38]

---

[31] Castillo, M. (2018). The Founder Of Bitcoin Pizza Day Is Celebrating Today In The Perfect Way. Kättesaadav: https://www.forbes.com/sites/michaeldelcastillo/2018/05/22/the-founder-of-bitcoin-pizza-day-is-celebrating-today-in-the-perfect-way/#1da250bd5d9c, 20.03.2019

[32] Quenstion, A. (2016). The Biggest Bitcoin Hacks and Thefts of All Time. Kättesaadav: https://hacked.com/biggest-bitcoin-hacks-thefts-time/, 20.03.2019

[33] Piana, C. (2017). Bitcoin: An Open Source Currency and More, 9 International Free and Open Source Software Law Review. 35-44, lk 39

[34] Who or What Can Put an End to Bitcoin? (2018). Kättesaadav: https://www.ccn.com/guest-spot-who-or-what-can-put-an-end-to-bitcoin, 20.03.2019

[35] Total Number of Transactions. (2019). Kättesaadav: https://www.blockchain.com/charts/n-transactions-total, 20.04.2019

[36] Davis, J. (2011). The Crypto-Currency. Kättesaadav: https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency, 20.03.2019

[37] Bigmore, R. (2018). A decade of cryptocurrency: from bitcoin to mining chips. Kättesaadav: https://www.telegraph.co.uk/technology/digital-money/the-history-of-cryptocurrency/, 20.03.2019

[38] Coinmarketcap, *supra nota* 16

1.1.2. Krüptoraha tehnoloogia ja selle seos detsentraliseeritud plokiahelaga

Geenius krüptoraha taga on plokiahel. Plokiahel on digitaliseeritud ja detsentraliseeritud kõikidest krüptograafilistest tehingutest. See on protsess, mille käigus loetav andmestik muudetakse raskesti murtavaks koodiks, mille abil on võimalik jälgida krüptorahade oste ja müüke.[39]

Plokiahel on nagu avalik pearaamat (*public ledger*), mis hoiab kõiki avalikke võtmed iga tehingu kohta. Avalikud võtmed, mida tuntakse ka bitcoini aadressidena jäävad kõik plokiahelasse, kuid nad ei ole seotavad kellegi reaalse identiteediga. Seega on plokiahel pseudonüümne,[40] mitte anonüümne. Kõik plokiahelas toimunud tehingud on tegelikkuses nähtavad kõikidele, kes tahavad avaliku pearaamatu *(public ledger)* alla laadida. Siin tekib küsimus, et kuna tegemist on detsentraliseeritud süsteemiga, millel puudub keskne süsteemi haldaja, siis kellel oleks võimalik kõikide pseudonüümsete kasutajate andmeid näha ja vajadusel tuvastada. Siin tekibki koht, kus autori hinnagul peitub nii krüptorahade võlu privaatuse näol kui ka risk kuritegevuse kergemaks muutmisel. See on kahtlemata ka täiendav risk just rahapesu puhul, kuna puudub keskne jõud, mis omaks täpset infot tehingute sisu osas – see muudab ka ametivõimude töö oluliselt keerulisemaks.

Kuigi plokiahelat kirjeldatakse tihti kui midagi, mida on võimatu muuta, on tähtis meeles pidada, et see on niimoodi ainult niikaua, kuni selle loojad sellesse sekkuda ei otsusta. Plokiahel saab oma nime faktist, et ta koosneb kõikide tehingute väljavõtetest mis on grupeeritud plokkideks, mis omavahel seotuna moodustavad ahela. Ahela loomine plokkidest toimub läbi algoritmide konsensuse, mis erinevad vastavalt sellele, mis plokiahelaga on tegu. Usaldusväärsuse säilitab kõikide osavõtjate vaheline konsensus.[41]

Samas esineb võimalus, et juhul kui üks kaevandaja või kaevandajate kollektiiv saab oma kontrolli alla vähemalt 51% kogu võimsusest võrgustikus, on olemas oht, et plokiahelat ähvardab „konsensuse rünnak“ (seda tuntakse ka kui 51% rünnakut). Siis muutub plokiahel

[39] Pirani, A. (2018). Cryptocurrency: A Magical Bubble or the Future of Currency, 5 Court Uncourt. 29-31, lk 29
[40] Rodrigues, U. (2018). Law and the Blockchain, 104 Iowa Law Review. 679-730, lk.710
[41] Finck, M. (2018). Blockchains: Regulating the Unknown. German Law Journal. 665-691, lk 668

manipuleeritavaks, kuna võrgustiku ausatel sõlmedel on võimatu plokiahelat kinnitada. Seega on plokiahela avalik pearaamat (*public ledger*) nende käes, kellel on enamik võrgustiku võimekusest. See tähendab muu hulgas seda, et ausate tehingute tegemisest võidakse keelduda või jäetakse need ootele ning teatud aadressidel võidakse blokeerida müntide (krüptoraha) kasutamine.[42] Kuigi tuntumate krüptorahade puhul pole sellise rünnaku läbiviimine ilmselt võimalik nende suuruse tõttu, siis väiksemate krüptorahade puhul on selline haavatavus kindlasti probleem.[43] Muu hulgas võib selliste rünnakute tagajärjel tekkida võimalus (ja ka vajadus) rahapesuks, kuna kurjategijad saavad enda käsutusse teatud hulga krüptoraha, mis nende käsutuses on illegaane. Seega tuleb see krüptoraha muuta legaalseks. Seega on krüptorahade tehnoloogiasse kirjutatud sisse probleem, mis võib oluliselt soodustada rahapesu toimepanekut. Kuna sellised rünnakud on muutumas aina sagedasemaks,[44] mis omakorda toob kahtlemata kurjategijatele kaasa aina suureneva vajaduse rahapesuks, siis on regulatiivsel tasandil vaja astuda samme just rahapesu vastaseks võitlemiseks, kuna piirates kurjategijate võimalust konkreetse krüptoraha ülevõtmisel 51% rünnakuga sealt varastatud krüptoraha legaalseks teha, kaob suuresti ka kurjategijate motivatsioon sellist rünnakut läbi viia, kuna nende võimalus sellelt tulu teenida on raskendatud.

Kuigi plokiahel on tehnoloogia, mis on teinud krüptoraha võimalikuks, siis on see tehnoloogia võimaldanud innovaatoritel mõelda välja ka suure hulga teisi lahendusi. Seega on väga oluline teha vahet plokiahelal ja krüptorahadel.[45] Välja mõeldud lahendused põhinevad plokiahela tehnoloogia kesksel lahendusel, milleks on võimekus pakkuda „levitatud, kuid tõendatult õigeid andmeid“. Seega detsentraliseerivad plokiahelad andmete säilitamise ja informatsiooni juhtimise. Seetõttu võib plokiahel olla väga kaugele ulatuv innovatsioon. Eelnevalt ei olnud võimalik koordineerida tegevust internetis ilma vahemehe või kolmanda osapooleta. Selle tõttu liigub ka enamik inimeste interneti ja interneti välisest tegevusest läbi vahemeeste, mitte ei tehta seda läbi partnervõrgu (*peer to peer*) teineteisega otse suheldes. Plokiahel võimaldab krüptorahasid vahetada erinevate osapoolte vahel ilma kellegi teise osaluseta.[46] Seega

---

[42] Alcantara, C. Dick, C. (2017). Decolonization in a Digital Age: Cryptocurrencies and Indigenous Self-Determination in Canada, 32 Canadian Journal of Law & Society. 19-35, lk 32

[43] Copeland, T. (2019). Barbarians at the altcoin gates. Kättesaadav: https://decryptmedia.com/4408/cryptocurrencies-protect-51-attacks, 05.05.2019

[44] Hertig, A. (2018). Blockchain's Once-Feared 51% Attack Is Now Becoming Regular. Kättesaadav: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular, 05.05.2019

[45] Finck (2018), *supra nota* 41, lk 668.

[46] *Ibid.,* lk.668

võimaldab plokiahel isikutel ka sellist omavahelist suhtlemist ja tehingute tegemist, mis eelnevalt on sõltunud kolmanda osapoole olemasolust.

Õiguskirjanduses on ka öeldud, et plokiahela läbipaistvus vähendab korruptsiooniohtu. Sellest tulenevalt on olemas ka riike, kes kaaluvad plokiahela avalikus sektoris kasutusele võtmist.[47] Seega võib öelda, et isegi kui krüptorahad lõpuks läbi kukuvad, siis on plokiahela tehnoloogial siiski tänu oma mitmekülgsusele lootustandev tulevik.[48]

Krüptorahade puhul räägitakse tihti nende kaevandamisest. Kaevandamiseks nimetatakse plokiahela viimase kümne minuti tehingute kinnitamise protsessi, mis paneb need nimekirja ja loob kõige viimase ploki, mis kinnitamist vajab. See põhineb konsensusel ja hoiab plokiahela terve ja puutumatuna. Põhimõtteliselt toimub krüptorahade kaevandamine arvutite poolt, mis ülemaailmselt võistlevad üksteisega viimase loodud ploki kinnitamise eest. Iga uue ploki loomisega loovad kaevandajad "räsi", mis võtab informatsiooni kõige viimasest plokist ja muudab selle unikaalseks tähtede ja numbrite kombinatsiooniks. Iga uus räsi võtab oma koha sisse ploki lõpus. Iga uus räsi sisaldab räsi eelnevast plokist. Seega, kui keegi sooviks muuta plokki, mis juba aina pikenevas ahelas olemas on, muutuks see räsi ja muutuks ka iga sellele eelnev räsi. See teavitaks kogu võrgustikku, et kuskil on probleem. Iga uue räsi loomisega saab kaevandaja krüptoraha.[49]

Krüptoraha kaevandamine tähendab lühidalt öeldes matemaatiliste probleemide lahendamist, mille abil on võimalik liita kokku plokiahela plokke.[50] Samuti võib öelda, et krüptorahade kaevandamiseks nimetatakse tehingute vahendamise ja kinnitamise loogikat.[51] Bitcoinide puhul lõi Satoshi Nakamoto kaevandamise reeglid selliseks, et mida rohkem kaevandamise jõudu võrgustikus on, seda keerulisem on lahendada kaevandamise matemaatilisi probleeme. Seega on kaevandamise protsess iseeneslikult muutuv sõltuvalt võrgustiku võimekusest. Mida rohkem kaevandajaid liitub, seda raskemaks muutub lahendatav matemaatiline probleem. Kui

---

[47] Pirani (2018), *supra nota* 39, lk 30
[48] McLeod, S. (2017). Bitcoin: The Utopia or Nightmare of Regulation, 9 Elon Law Review. 553-578, lk 554
[49] Detwiler, P. /2016). Mining Bitcoins Is A Surprisingly Energy-Intensive Endeavor. Kättesaadav: https://www.forbes.com/sites/peterdetwiler/2016/07/21/mining-bitcoins-is-a-surprisingly-energy-intensive-endeavor/#708da0ff5bbf, 20.03.2019
[50] Bitcoin's Mathematical Problem. (2017). Kättesaadav: https://blog.programster.org/bitcoins-mathematical-problem, 20.03.2019
[51] Mis on kaevandamine? Kättesaadav: http://www.kryptoraha.ee/kaevandamine/, 20.03.2019

kaevandajaid jääb vähemaks, muutub lahendatav matemaatiline probleem jälle kergemaks. Seda teatakse ka kui kaevandamise raskust (*mining difficulty*).[52] Sellise reegli lõi Nakamoto põhjusel, et soovis hoida bitcoini võrgustikku tulevate uute bitcoinide arvu pidevalt stabiilsena. Seega tegi ta seda selleks, et hoida ära inflatsiooni.[53]

Üks täiendav asjaolu, mille jaoks on veel krüptoraha kaevandamist vaja, on vältida topelt-kulutamise (*double spending*) probleemi.[54] Selleks asjaoluks, mis teeb bitcoini (ja teisedki krüptorahad) eriliseks, ongi Nakamoto innovaatiline lahendus eespool mainitud topeltkulutamise (*double spending*) probleemile.[55] Topeltkulutamise probleem (*double spending)* oli ka üheks põhjuseks, miks eelnevad katsed luua digitaalne raha läbi kukkusid. Topeltkulutamine tähendab sama raha kahekordset kasutamist. Füüsiliselt eksisteeriva rahaga ei ole see võimalik ning see ei ole probleemiks, kuna sularaha ära andes ei saa isik seda enam teistkordselt kasutada.[56] Mis puudutab aga arvutivõrgus eksisteerivat raha, siis krüptorahaga tehingut tehes saadetakse info kõikidesse võrgustikku sõlmedesse (*nodes*), mis on arvutid, mis juhivad tarkvara, mille peal konkreetne krüptoraha toimib. Need sõlmed saavad info tehingu kohta ja kinnitavad selle, see aga võtab aega. Seega tekib aga probleem. Mis takistab kellelgi tehingut kopeerimast ja seda uuesti välja saatmast, enne kui võrgustik on tehingu ära kinnitanud? Kuidas saaks võrgustik teada, milline tehing „õige“ on?[57] Tõendamaks, et topeltkulutamist pole juhtunud, pakub plokiahel variandi kuidas kõik võrgustiku sõlmed *(nodes)* on kõikidest tehingutest teadlikud - seega teavitatakse bitcoini puhul kõiki sõlmi *(nodes)* kõikidest tehingutest. Sõlmed *(nodes)* võimaldavad jõuda konsensuseni milline on ainuke õige ajalooline tehingute järjekord. Seega on bitcoini lahendus topeltkulutamise probleemile see, et kui enamik sõlmi *(nodes)* nõustuvad milline tehing toimus esimesena, ei lähe hilisemad katsed teha topeltkulutamine arvesse.[58]

---

[52] What is Bitcoin Mining and is it Profitable? (2019). Kättesaadav: https://99bitcoins.com/bitcoin-mining/, 20.03.2019
[53] *Ibid.*
[54] Bitcoin's Mathematical Problem (2017), *supra nota* 50
[55] Tu, K. Meredith, M. (2015). Rethinking Virtual Currency Regulation in the Bitcoin Age, 90 Washington Law Review 271-347, lk 280.
[56] How Does a Blockchain Prevent Double-Spending of Bitcoins? (2018). Kättesaadav: https://medium.com/innerquest-online/how-does-a-blockchain-prevent-double-spending-of-bitcoins-fa0ecf9849f7, 20.03.2019
[57] *Ibid.*
[58] *Ibid.*

Seega võib kokkuvõtlikult öelda, et kuigi tehnoloogial, millel krüptorahad põhinevad, on olemas nõrkuseid, mis võivad soodustada või kaasa tuua rahapesu (lisaks ka muid kriminaalseid tegevusi), on tehnoloogia siiski uuenduslik ja suure potentsiaaliga ning lahendanud mitmed probleemid, mida eelnevalt pole lahendada suudetud. Kuigi eespool mainitud 51% rünnaku tehnoloogilise poole osas ei suuda rahapesuvastased regulatsioonid efektiivsed olla (rünnakute ärahoidmiseks vajaks muutmist tegelikkuses kogu plokiahela tehnoloogia toimimise loogika), on see siiski koht, kus mõju saaks olla just sobivatel rahapesuvastastel regulatsioonidel. Sobivad rahapesuvastased meetmed omaksid kahtlemata mõju 51% rünnakute ärahoidmisel, kuna kui kurjategijatel on keeruline enda kontrolli all olevast võrgustikust krüptoraha „puhtaks pesta" ja sellelt tulu teenida, on seda väiksem ka nende motivatsioon selliseid rünnakuid toime panna.

1.1.3. Krüptoraha hoidmise ja tehingutega seotud ohud

Krüptorahade kohta on tehtud palju kriitikat finantsekspertide poolt.[59]Ameerika suurima panga JP Morgan juht Jamie Dimon nimetas krüptorahasid pettuseks,[60] mis ühel hetkel õhku lendavad ning lisas, et krüptorahad sobivad ainult narkodiileritele, mõrvaritele ja inimestele kes elavad kohtades nagu Põhja-Korea. Samuti lisas ta, et vallandaks koheselt töötaja kes tema investeerimispangas bitcoinidesse investeeriks, kuna esiteks on see pangareeglite vastu ning teiseks on selliste investeeringute tegijad rumalad.

Ameerika finantsõiguse advokaat Jay Adkisson on öelnud, et hoolimata sellest mida võib öelda krüptorahaga seonduva kohta, on see olnud üks suurimaid rikkuse hävitajaid inimkonna ajaloos.[61] Samuti lisas ta, et krüptorahad on muutumas majanduslikult halvast ideest pettuseks.

Õiguskirjanduses on ka öeldud, et krüptorahad on oht nii kodumaisele ja kui ka rahvusvahelisele turvalisusele. Samuti on need ohuks ka investorite säästudele ja

---

[59] Top 10 expert's criticisms on Bitcoin and other cryptocurrencies. (2017). Kättesaadav: https://coinpedia.org/information/experts-criticisms-bitcoin-cryptocurrencies/, 20.03.2019

[60] Monaghan, A. (2017). Bitcoin is a fraud that will blow up, says JP Morgan boss. (2017). Kättesaadav: https://www.theguardian.com/technology/2017/sep/13/bitcoin-fraud-jp-morgan-cryptocurrency-drug-dealers, 20.03.2019

[61] Adkisson, J. (2018). The Great Cryptocurrency Scam. Kättesaadav: https://www.forbes.com/sites/jayadkisson/2018/11/20/the-great-cryptocurrency-scam/#66ba11fa359f, 20.03.2019

finantsturgudele, kuna vähendavad investorite turvatunnet.[62]

Kuna bitcoinidel ja krüptorahadel üldiselt puudub keskne võim, jääb nende väärtus ilmselt alati teatud määral volatiilseks. Näitena võib tuua selle, et bitcoinide väärtus langes dramaatiliselt pärast seda, kui Hiina regulaatorid keelasid pankadel ja makseid teostavatel ettevõtetel bitconidega tegelemise, kui nad klassifitseerid bitcoini kaubaks, mitte rahaks. Kuigi Hiina regulaatorid ei keelanud isikutel täielikult bitcoinidega tehinguid teha, saatis see siiski olulise teate investoritele.[63] Siit nähtub, et krüptorahad on rohkem tundlikud välistele faktoritele regulatsioonide muutumisel kui tavapärane raha – kindlasti mõjutab seda ka fakt, et tavapärane raha on eksisteerinud palju kauem ning ootamatuid muutusi selle regulatsioonides toimub vähem. See on kahtlemata ka üks olulistest hinna volatiilsuse põhjustest.

Kuigi eespool mainitud näidete puhul ei ole tegemist olukordadega, mida AMLD nr.5 või võimalikud muud rahapesuvastased regulatsioonid lahendada saaks, annavad need siiski ettekujutluse sellest, et krüptorahad kätkevad endas mitmeid riske. Autori hinnangul on siiski võimalik järjepideva regulatsioonide (sealhulgas ka rahapesuvastaste regulatsioonide) täiendamisega krüptoraha valdkonna üldist usaldusväärsust märgatavalt suurendada ning stabiliseerida. Usaldusväärsuse kasv tooks endaga kaasa ka kuritegevuse vähenemise krüptoraha tehingutes.

Eespool mainitud probleemid ja krüptorahade populaarsus ongi tänaseks päevaks sundinud seadusandjaid ja regulaatoreid (nii riigisiseseid kui ka rahvusvahelisi) hindama potentsiaalseid riske, mida aina enam leviv detsentraliseeritud raha endas kätkeb. Kuigi krüptorahade kasutegurid on toonud juurde uusi kasutajaid, kaupmehi, investoreid ja ärisid, siis kätkeb krüptoraha innovaatilisuses ka oht. Regulaatorid on aga olnud raskustes otsustamisega, kuidas ja kas peaks reguleerima krüptorahasid.[64]

Krüptoraha nõrkuste puhul on oluline mainida ka selle kulukust. Nimelt on krüptoraha kaevandada suutvate arvutite ostmine ja tööshoidmine on kulukas. Kuna sellega on hakatud

---

[62] Engle, E. (2016). Is Bitcoin Rat Poison: Cryptocurrency, Crime, and Counterfeiting (CCC). 16 Journal of High Technology Law. 340-393, lk 393.
[63] Gerkis, Krikunova (2014), *supra nota* 15, lk 4
[64] Tu, Meredith (2015), *supra nota* 55, lk 296

aina rohkem tegelema, on ka matemaatilised probleemid muutunud aina keerulisemaks, mistõttu nende lahendamine nõuab arvutitelt aina rohkem võimsust. Arvatakse, et 2019. aastal kasutab ainuüksi bitcoini võrgustik sama palju energiat kui terve Iirimaa.[65] Teise uuringuga on välja selgitatud, et ainuüksi bitcoinide kaevandamine võtab aastas 73,2 terawatt tundi energiat. See on 0,24 % kogu maailma aasta energiatarbimisest. Tõenäoliselt on see esmakordne juhus maailma ajaloos kui üks maksesüsteem on loodusele kahjulik ning vajab juba seetõttu reguleerimist.[66] Võib ka öelda, et krüptorahade saamist nii-öelda peavoolu rahaks takistab kindlasti ka see, et nende kaevandamiseks, saamiseks ja hoiustamiseks läheb väga palju arvutijõudlust.[67]

Sellest tulenevalt tekib paratamatult küsimus, kas süsteem, mis iseenesest väärtust ei oma (ning mille väärtus turul on paljuski spekulatiivne), millega seonduvad mitmed olulised finantsriskid ning mille töös hoidmine on tohutult kulukas ja kahjulik keskkonnale, on süsteem mille levik peaks olema lubatud? Autor leiab, et kuigi eespool mainitud probleemid on tõsised murekohad, tuleks krüptoraha puhul arvestada, et tegemist on siiski lahendusega, mis tänaseks ajaks on eksisteerinud vaid natuke kauem kui kümme aastat ning mis võimaldab lahendusi, mis eelnevalt olid võimatud. Seega peaks seadusandjate ja regulaatorite eesmärk olema järk-järguline probleemkohtade likvideerimine läbi mõtestatud õigusloome ja järelevalve, mis samas annaks siiski piisava võimaluse uuenduslikel tehnoloogilistel lahendustel täiendavalt areneda. Kahtlemata toob järjepidev areng kaasa ka selle, et regulatsioonides saavutatakse teatud stabiilsus, mis kogu valdkonna volatiilsust vähendab.

Oluline on ka teada, kuidas toimub krüptorahade "hoiustamine“, kuna nimetatud teemaga seonduvad mitmed probleemid. Krüptoraha hoitakse digitaalsetes rahakottides, mida saab käsutada kasutaja kelle käes on nii-öelda privaatne võti. See digitaalne rahakott on nagu pangakonto, mida kasutatakse krüptoraha hoiustamiseks, ülekannete tegemiseks ning ostlemiseks. Vastavat digitaalset rahakotti on vaja nii krüptorahadega kauplemiseks kui ka

---

[65] It now costs more to make bitcoin than the cryptocurrency is worth. (2019). Kättesaadav: https://www.newscientist.com/article/mg24132162-900-it-now-costs-more-to-make-bitcoin-than-the-cryptocurrency-is-worth/?fbclid=IwAR09n-d1ub6z5LxoWViFRzLeN1pzCsFGABsFDJgtQ_Y4R2bYyCj-K7TEM08, 20.03.2019

[66] Maume, P. Fromberger, M. (2019). Regulations of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws, 19 Chicago Journal of International Law. 548-585, lk 550

[67] Sonderegger (2015), *supra nota* 18, lk 187

nende varadena omamiseks.[68] Siin esineb risk, et väga kerge on kaotada ligipääs oma privaatsele võtmele, mis tähendab, et konkreetne krüptoraha on igaveseks kadunud ning sellele ligipääsu taastamine sisuliselt enam võimalik ei ole, eriti arvestades, et krüptoraha süsteem on üldiselt detsentraliseeritud ja ilma keskse omanikuta.[69]

On olemas erinevaid variante krüptoraha hoiustamiseks.[70] Üheks variandiks ongi erinevate krüptoraha kauplemisplatvormide kasutamine. Siin tuleb arvestada riskiga, et hoiustades krüptoraha vastaval kauplemisplatvormil, sõltub hoiustaja krüptoraha säilimine kauplemisplatvormi usaldusväärsest. Teatud krüptorahade kauplemisplatvormid nagu Mt.Gox, Tradehill ja Bitcoinica ongi sattunud häkkerite ja petturite rünnakute alla ning seeläbi on sinna investeerinud isikud kandnud suuri rahalisi kaotusi.[71] Teiseks variandiks on veebipõhise rahakoti kasutamine. Ka sellisel variandil on see risk, et tegelikult on isik usaldanud oma krüptoraha kolmanda isiku kätesse.[72] Kolmanda variandina võib tuua riistvara rahakoti.[73] Sellise rahakoti puhul on privaatvõti salvestatud mälupulgale. Sellist rahakotti peetakse üldiselt turvaliseks. Neljandaks võib tuua paberrahakoti. Sellise rahakoti puhul prinditakse vastav privaatvõti välja ning seda võib hoiustada ükskõik millises kohas. Kuigi see on kõige turvalisem selles osas, et seda pole võimalik häkkida, on selle oluline miinus see, et igapäevase kauplemistegevuse puhul ei ole see sobilik variant.[74]

Nagu eespool kirjutatust tuleneb, võib krüptoraha osta erinevatel kauplemisplatvormidel. Need võimaldavad kasutajatel konverteerida tavapärast raha krüptorahaks ja vastupidi. Vahetuse võimalus on nii kasutajalt kasutajale *(peer to peer)* baasil kui ka kauplemisplatvormi endaga.[75] See tõstatab aga oma probleemid, kuna erinevad teenusepakkujad, kes pakuvad kauplemisplatvorme, kus krüptoraha võib kas hoiustada või sellega kaubelda, ei pruugi olla

---

[68] Ahmeddirar. (2019). Top 6 Best Cryptocurrency Wallets 2019, Everything You Need To know. Kättesaadav: https://ripplecoinnews.com/top-5-best-cryptocurrency-wallets, 01.05.2019
[69] Dickson, B. (2018). Everything you need to know about bitcoin wallets. Kättesaadav: https://www.dailydot.com/debug/bitcoin-wallets-cryptocurrency-hardware, 20.03.2019
[70] Arroyo, C. (2017). Holding Cryptocurrency—The Real Risks. Kättesaadav: https://hackernoon.com/holding-cryptocurrency-the-real-risks-3c54ca8d73b6, 01.05.2019
[71] Engle (2016), *supra nota* 62, lk 353
[72] LetKnowNews. (2018). 5 Types of Cryptocurrency Wallets and Their Pros & Cons. Kättesaadav: https://medium.com/letknownews/5-types-of-cryptocurrency-wallets-and-their-pros-cons-4215fdf59324, 01.05.2019
[73] *Ibid.*
[74] *Ibid.*
[75] Jeans, E. (2015). Funny Money or the Fall of Fiat: Bitcoin and Forward-Facing Virtual Currency Regulation , 13 Colorado Technology Law Journal 99-127, lk 106

turvalised ning võivad tuua kaasa potentsiaalsed riskid krüptorahade investoritele.[76] Just kauplemisplatvormide ja krüptoraha rahakoti teenuse pakkujate puhul on oluline tagada, et nad jälgiksid olulisi rahapesuvastaseid ja tunne oma klienti protseduure, samuti peab olema tagatud nende tehnoloogiline tugevus häkkimiste vastu – sellised meetmed vähendavad oluliselt kurjategijate võimalusi nende süsteeme ära kasutada. Just nimetatud teenusepakkujate võimekus kaitsta ennast häkkimiste vastu on oluline asjaolu, millele järelevalveorganid peaksid tähelepanu pöörama. Samuti leiab autor, et kauplemisplatvormide ja krüptoraha rahakotiteenust pakkuvate isikute majandusliku toimetuleku osas peaks olema täiendav järelevalve, kuna tegelikkuses omavad nimetatud isikud enda käes paljude isikute vara. Seega tuleks autori hinnangul siinkohal seadusandjatel hinnata teatud finantstagatiste süsteemi loomise vajalikkust.

Kõik eespool toodu aga näitab vajadust, et vastavaid teenuseid saaks pakkuda vaid konkreetseid tegevuslube omavad ettevõtted, mis on tõestanud riigile, et nad vastavad seadustest toodud nõuetele.

Krüptoraha teemal on Eestis olnud siiani üks kohtuvaidlus. Nimetatud vaidluses oli tegemist krüptoraha vahendamisega tegeleva leheküljega. Riigikohtu 11.04.2016 lahendis 3-3-1-75-15[77] oli tegemist olukorraga kus Otto Albert de Voogd registreeris veebiaadressi www.btc.ee, millel pakuti 2014. märtsis isikutele võimalust soetada või müüa krüptoraha bitcoin. Teenusepakkuja kontor oli registreeritud Tallinnas ning tehingute eest võimaldati tasuda nii sularahas kui ka ülekandega. Enne ettekirjutuse tegemist pöördus Politsei- ja Piirivalveameti alla kuuluv rahapesu andmebüroo (edaspidi RAB) O. A. de Voogdi poole ning selgitas, et soovib teenust pakkuva isiku suhtes läbi viia järelevalvet rahapesu ja terrorismi rahastamise tõkestamise seaduses (edaspidi RahaPTS) sätestatud nõuete täitmise üle. RAB kohustas ettekirjutusega de Voogdi esitama kirjalikku teavet oma tegevuse kohta ning talle esitati kuus küsimust bitcoin'ide ostmise ja müümise teenuse osutamise kohta ning paluti esitada klientide andmed. Otto Albert de Voogd vaidlustas selle halduskohus. Menetlus jõudis välja Riigikohtusse, mis jättis jõusse ringkonnakohtu otsuse 3-14-50581.

Kohus leidis, et asjaolu, et seaduseelnõu väljatöötamise ja vastuvõtmise ajal ei olnud krüptoraha

[76] Goforth, C. (2019). The Lawyer's Cryptionary: A Resource for Talking to Clients about Crypto-transactions, 41 Campbell Law Review. 47-120, lk 60
[77] RKHKo 3-3-1-75-15

bitcoin veel loodud, ei tähenda, et alternatiivsete maksevahendite teenuse pakkuja mõiste ei saa hõlmata ka nimetatud krüptoraha vahetusteenuse pakkujaid. Alternatiivsete maksevahendite teenuse pakkuja mõiste sätestati 28. jaanuaril 2008 jõustunud rahapesu ja terrorikuritegude rahastamise tõkestamise seaduses. Eelnõu (SE 137) seletuskirjast nähtub seadusandja tahe kehtestada regulatsioon, mis võimaldab rahapesuvastasele regulatsioonile allutada ka ebatraditsioonilisi rahalist väärtust omavate vahendite ülekande ja edastamise viise (e-kuld, e-hõbe, elektroonilised rahakotid), samuti alternatiivseid maksevahendeid, mida võidakse kasutada rahapesu ja terrorikuritegude rahastamise skeemides ning mille olulisemaks jooneks on see, et need süsteemid võimaldavad tehinguosalistel rahalist väärtust üle kanda kohe, mugavalt, turvaliselt ja anonüümselt.

Samuti leidis kohus, et krüptoraha, sealhulgas bitcoin'id, on suhteliselt piiratud levialaga ning avaldavad hetkel üsna marginaalset mõju rahandussüsteemi toimimisele, vastab bitcoin'idega majandustegevusena kauplemine alternatiivsete maksevahendite teenuse pakkumise mõistele. bitcoin'il on seega rahaline väärtus ja sellega on võimalik täita kohustusi. Teatud määral sarnasele järeldusele on jõudnud ka Euroopa Kohus lahendis *Skatteverket vs David Hedqvist*,[78] kus rõhutati, et krüptorahal bitcoin ei ole muud mõtet, kui olla kasutatav maksevahendina.

Riigikohus leidis, et seadusandja tahteks oli allutada ebatraditsioonilised maksevahendid rahapesuvastasele regulatsioonile. Krüptoraha bitcoin omab selgelt väärtust ja võib olla rahapesu objektiks. Majandustegevusena bitcoin'idega kaupleja tegevuse allutamine rahapesuvastasele regulatsioonile ja riiklikule järelevalvele on seetõttu mõistlik.

Seega leidsid Eesti kohtud juba krüptorahade varajases staadiumis, et hoolimata krüptorahade selle konkreetse ajahetke marginaalsusest, on see siiski teema, mille osas rahapesuvastase võitlusega tegelevad järelevalve organisatsioonid on õigustatud järelevalvet tegema ning selle hetkel kehtinud regulatsioonid seda ka võimaldasid. Kuigi eespool mainitud Riigikohtu poolt tehtud kohtulahendis ei tuvastatud (ning see polnud ka küsimuse all) kas antud kauplemisplatvorm oli probleemne selle kasutajate jaoks või mitte, siis Ameerika Ühendriikide kohtupraktikast võib leida ka juhtumeid, kus kauplemisplatvorm on üritanud oma kasutajaid

[78] EKo 22.10.2015, C-264/14 Skatteverket versus David Hedqvist

petta. Kohtulahendis Commodities Futures Trading Commission[79] (edaspidi CFTC) vs Patrick K. McDonnell & Coin Drop Markets (edaspidi CDM)[80] tuvastati, et McDonnell ja CDM tegelesid krüptoraha petuskeemidega. McDonnell kutsus kliente saatma raha ja krüptoraha CDM-ile, pakkudes vastu krüptoraha kauplemise nõustamise teenust. Samuti pakkus McDonnell võimalust CDM-i nimel osta ja kaubelda krüptorahadega. Tegelikkuses nõustamise teenust seda ostnud klientidele ei pakutud ning CDM-ile raha saatnud kliendid ei saanud selle eest midagi. Kohtumenetluse käigus oli McDonnelli ja CDM ainuke vastuargument see, et CFTC-l puudus jurisdiktsioon nimetatud küsimusega tegeleda, kuna tegemist oli krüptorahaga.

Kohus leidis, et süüdistatav tegeles osariikide ja riikide vahelise pettusega, mis oli seotud kaupade müügitehingutega. Süüdistatava pettus oli seotud valeinfo andmisega ning klientide raha ja krüptoraha väärkasutamisega, mis oli seotud krüptorahade nagu bitcoinide ja litecoin'ide müügitehingutega.

Mainitud näidete valguses on selge, et krüptoraha valdkonna puhul on tegemist valdkonnaga, mille puhul väga oluline on tagada, et krüptoraha rahakotiteenuse pakkujad ja kauplemisplatvormid vastaksid rangetele tingimustele ning nende tegevuse üle eksisteeriks efektiivne kontroll. Kuna vastavate teenuste pakkujate käes on isikute vara, siis on järelevalve teostajate ülesanne tagada, et vastavate teenusepakkujate tegevus toimuks heas usus ja klientide varade säilimiseks on tehtud kõik võimalik. Seega on ka vältimatu tegevuslubade nõue selliste teenuste pakkujatelt.

1.2. Krüptoraha definitsioon

Täpsustada tuleb ka krüptorahade definitsiooni ning selgitada nende paiknemist eri õigusruumides, kuna erinevad käsitlused krüptoraha olemuse kohta võivad viia ka erinevate lähenemisteni kuritegevuse ja eriti rahapesu teemadel. Samas on ka väga vajalik selgitada, miks

[79] Ameerika Ühendriikide kaupade ja futuuride kauplemise komisjon
[80] UNITED STATES DISTRICT COURT EASTERN DISTRICT OF NEW YORK, 18-CV-361, *CFTC vs Patrick K. McDonnell & Coin Drop Markets*

üldse krüptorahad vajaksid täiendavat regulatsiooni. Selle osas võib välja tuua järgnevad neli peamist põhjendust:[81]

1) tarbijate kaitse
2) võitlus rahapesuga
3) finantssüsteemi turvalisuse ja selguse tagamine
4) võitlus maksude tasumisest eemale hoidmisega

Õiguskirjanduses on öeldud, et krüptorahade puhul võib rääkida digitaalinstrumentidest, mis ei ole välja antud suveräänse institutsiooni või kommertspanga poolt ning millel nii-öelda „füüsiline keha“ puudub.[82] Isegi nimetatud digitaalinstrumentide täpsem defineerimine on osutunud keeruliseks, kuna nii erialakirjanduses kui ka tavakasutuses kasututakse tihti läbisegi väga erinevaid väljendeid. Kuna neid instrumente võib kasutada rahana nimetatakse neid tihti „elektrooniliseks rahaks“, digitaalseks valuutaks“, „virtuaalrahaks“ või „krüptorahaks“.[83]

Kuigi krüptorahasid ühendab see, et need põhinevad sarnasel detsentraliseeritud plokiahela tehnoloogial, siis eri jurisdiktsioonides nende kohta kasutatav terminoloogia on väga erinev. Mõnede näidetena kuidas erinevates riikides krüptoraha defineeritakse võib tuua järgnevad - digitaalne valuuta (Argentiina, Tai ja Austraalia), virtuaalne kaup (Kanada, Hiina ja Taiwan), krüpto-token (Saksamaa), makse token (Šveits), kübervaluuta (Itaalia ja Liibanon), elektrooniline valuuta (Kolumbia, Liibanon) ja virtuaalne vara (Honduuras ja Mehhiko).[84]

Kirjanduses on öeldud, et krüptoraha on innovaatiline ja virtuaalne raha, mis kasutab krüptograafiat turvalisuse tagamiseks - selle tõttu on seda ka raske võltsida. Krüptoraha oluline omadus on tema orgaanilisus, see ei ole välja antud ühegi valitsusasutuse poolt, mille tõttu peaks see hüpoteetiliselt olema kindel valitsuste takistustegevuse või kontrolli osas.[85]

Kuna krüptorahade populaarsus on aina tõusmas, siis on oluline, et seadusandjad leiaksid õige viisi kuidas neid reguleerida, arvestades, et krüptorahade populaarsuse tõustes suurenevad ka

---

[81] Gatto, J. Broeker, E. (2015). Bitcoin and beyond: Current and Future Regulation of Virtual Currencies, 9 Ohio State Entrepreneurial Business Law Journal. 429-470, lk 430
[82] Cvetkova (2018), *supra nota* 12, lk 129
[83] *Ibid., lk* 129
[84] Library of Congress. (2018). Regulation of Cryptocurrency Around the World. Kättesaadav: https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf, 20.03.2019
[85] Pirani (2018), *supra nota* 39, lk 29

võimalikud probleemid. Korrektse regulatsiooni puudus riiklikult toetamata krüptorahade puhul võib kiiresti muutuda õiguslikuks probleemiks.[86]

Kui kategoriseerida rahvusvahelised (riikide põhiselt) regulatsioonid, mis seonduvad krüptorahadega siis võib need jagada kolmeks:[87]

1) Vastuvõtlikud krüptorahadele
2) Keelanud krüptorahad
3) Nende kahe vahepeal või ignoneerivad krüptorahasid

Krüptoraha entusiast Ofir Beigel'i poolt administeeritava lehekülje 99Bitcoins andmetel[88] on kõige sõbralikumad riigid krüptoraha osas järgnevad riigid (järjestuses): Malta, Bermuuda, Šveits, Gibraltar, Sloveenia, Singapur, Eesti, Georgia, Valgevene, Hong Kong, Jaapan ja Saksamaa. Samas on ka mitmeid riike, mis on tänaseks krüptorahad keelustanud – nendeks on näiteks Alžeeria, Boliivia, Egiptus, Maroko, Nepaal, Pakistan, Araabia Ühendemiraadid ja Vietnam.[89] Lisaks on mitmed Lähis-Ida ja Kagu-Aasia riigid, kes küll otseselt oma regulatsioonides krüptoraha ei ole ära keelanud, kuid siiski võib aru saada, et eelduslikult on krüptoraha seal keelatud. Lisaks kuulub nende hulka ka Leedu.[90]

Teada tuntud mõte sellest, et tehnoloogia on seadustest ees, oli väga hästi nähtav just algsetes katsetes defineerida krüptoraha.[91] Sama probleem oli muu hulgas ka 90ndate keskpaigas seadusandjatel, regulaatoritel ja kohtutel interneti osas õige regulatsiooni leidmisega.[92]

---

[86] Lovell, A. (2018). Avoiding Liability: Changing the Regulatory Structure of Cryptocurrencies to Better Ensure Legal USe, 104 Iowa Law Review. 926-957, lk 934
[87] Jeans (2015), *supra nota* 75, lk 108
[88] A Complete List of Bitcoin Friendly Countries. (2019). Kättesaadav: https://99bitcoins.com/bitcoin-friendly-countries/, 20.04.2019
[89] Library of Congress. (2019). Legal Status of Cryptocurrencies. Kättesaadav: https://www.loc.gov/law/help/cryptocurrency/map1.pdf, 20.04.2019
[90] *Ibid.*
[91] Zaytoun, H. (2019). Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft, 97 North Carolina Law Review. 395-431, lk 408
[92] Salbu, S. (1998). Who Should Govern the Internet: Monitoring and Supporting a New Frontier , 11 Harvard Journal of Law & Technology. & Tech. 429-480, lk 431. Viidatud Goldman, T. (1996). How Microsoft Gets Its Way in Washington. Legal Times.

Enamike finantsorganisatsioonide, finantsjärelevalve organisatsioonide ning muude krüptorahaga erineval viisil seotud organisatsioonide antud definitsioonidest krüptorahale saab lugeda välja sarnasusi. Üks suuremaid sarnasusi on see, et mitmed organisatsioonid peavad krüptoraha virtuaalraha üheks alamhulgaks.

Euroopa Keskpank selgitas oma väljaandes krüptoraha olemust järgnevalt - virtuaalraha on selline raha tüüp mis on reguleerimata, välja antud ja tavaliselt kontrollitud oma arendajate poolt ning mida kasutatakse ja aktsepteeritakse spetsiifilise virtuaalkommuuni liikmete poolt.[93]

Täiendavalt jagas[94] Euroopa Keskpank virtuaalrahad veel kolmeks:

1) Virtuaalrahad, mida saab kasutada ainult suletud virtuaalsüsteemis, tavapäraselt erinevates online mängudes (näiteks kuld arvutimängus World of Warcraft).
2) Virtuaalrahad, mis on ühepoolselt seotud reaalse majandusega - eksisteerib vahetuskurss raha ostuks (traditsioonilise rahaga) ja ostetud raha saab kasutada ostmaks virtuaalseid kaupu ja teenuseid (erijuhtudel ka reaalseid kaupu ja teenuseid).
3) Kahesuunalise vooluga virtuaalsete maksevahendite süsteemid, mille puhul on virtuaalsed maksevahendid nagu iga teine konverteeritav valuuta, mis omab kahte vahetuskurssi (müügikurss ja ostukurss) ning mida saab kasutada nii virtuaalsete kui ka tavapäraste kaupade ja teenuste ostmiseks.

Krüptorahad nagu näiteks bitcoin kuuluvad Euroopa Keskpanga hinnangul viimase tüübi hulka. Neid võib nii osta kui müüa traditsioonilise raha eest ning neid võib kasutada ostmaks nii virtuaalseid kui ka reaalseid kaupu ja teenuseid.

Sarnaselt Euroopa Keskpangale kategoriseeris ka Rahvusvaheline Valuutafond (edaspidi IMF[95]) krüptorahasid virtuaalrahade alamhulgana, mida defineeritakse väärtuse digitaalse esindusena, mille on välja andnud erasektori arendajad ning mis on nimetatud nende enda arvestusühikus. IMF-i kohaselt katab virtuaalraha mõiste suure hulga erinevaid valuutasid

---

[93] European Central Bank. (2012). Virtual currency schemes. Kättesaadav: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, 20.03.2019
[94] *Ibid.,* lk 13
[95] International Monetary Fund

alustades tavalistest IOU-dest (nii-öelda „I owe you's", millised on näiteks interneti ja mobiilide kupongid ning lennumiilid) kuni virtuaalrahadeni, mida tagavad sellised varad nagu kuld ja krüptorahad nagu bitcoin.[96]

Samas on ka finantsjärelevalve organisatsioone, kelle definitsioon krüptorahast on põimunud virtuaalraha definitsiooniga niivõrd, et krüptoraha pole virtuaalraha alamhulk, vaid neid käsitletakse ühena. Näitena võib sellest tuua Financial Action Task Force[97] (edaspidi FATF) ehk rahapesuvastase töökonna, mis defineerib krüptoraha järgnevalt:[98]

Virtuaalraha on digitaalne representatsioon väärtusest, millega saab digitaalselt kaubelda ja mis funktsioneerib kas/või

1) Maksevahendina;
2) Väärtuse ühikuna;
3) Midagi, mis võimaldab säilitada väärtust, kuid mis ei ole ametlik maksevahend.

Samuti tõi FATF oma krüptoraha definitsiooni andmisel välja, et krüptoraha ei anna välja ega garanteeri ükski jurisdiktsioon ja see täidab ülaltoodud kriteeriume vaid virtuaalraha kommuuni kasutajate omavahelise kokkuleppe tõttu. Virtuaalraha võib eristada fiat rahast, milleks on nii mündid kui ka paberraha riigis, kus see on ametlik maksevahend.

Autorile üllatavalt ei kasuta eespool mainitud organisatsioonid krüptoraha defineerimisel autori hinnangul ilmselt kõige olulisemat aspekti – nimelt seda, et see põhineb krüptograafilistel tõenditel ja plokiahelal, mis autori hinnangul ongi need asjaolud, mis konkreetselt krüptoraha teistest erinevatel elektroonilistel viisidel esinevatest rahadest oluliselt eristab.

Kui otsida definitsioone krüptoraha kohta, kus oleks toodud sisse see, et see põhineb krüptograafial, siis Eesti Krüptoraha Liit (edaspidi EKL) defineerib krüptoraha järgnevalt: „Krüptoraha on üks alaliik digitaalrahast. Digitaalraha on alternatiiv füüsilisele rahale nagu

---

[96] Habermeier, K. (2016). Virtual Currencies and Beyond: Initial Considerations. Kättesaadav: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 20.03.2019

[97] FATF on riikide valitsuste vaheline organ, mis töötab välja rahapesu ja terrorismi rahastamise vastase võitluse standardeid ning meetodeid ja edendab sellealast poliitikat.

[98] Financial Action Task Force. (2014). Virtual Currencies Key Definitions and Potential AML/CFT Risk. Kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 20.03.2019

paberraha või mündid. Digitaalrahaks nimetatakse digitaalses vormis ühikut, mis esindab mingisugust vääringut. Digitaalraha jaguneb omakorda virtuaalrahadeks ning krüptorahadeks. Virtuaalraha on kasutusel näiteks erinevates arvutimängudes, esindatuna tokenite või krediidina. Krüptorahaks nimetatakse rahasüsteemi, mida traditsiooniliselt iseloomustab krüptograafilistel (matemaatilistel) alustel üles ehitatud turvalisus, detsentraliseeritud isereguleeruv maksetesüsteem ning võrgu ja tarkvara läbipaistvus.“[99]

Autor ei nõustu EKL-i arvamusega krüptoraha definitsiooni selle osas, et krüptoraha iseloomustab võrgu läbipaistvus (läbipaistvus on krüptorahade puhul mõneski osas näilik, kuna kuigi tehingute hulk ja konkreetse tehingu maht on küll tavapäraselt nähtav, siis selle tehingu tegelik sisu on võrgustiku pseudonüümsuse tõttu lõpuni siiski teadmata).

Seega vastupidiselt eelnevatele organisatsioonidele eristab EKL selgelt virtuaalraha ja krüptoraha mõisteid, pidades krüptoraha hoopis digitaalraha alaliigiks, virtuaalraha samas aga rohkem arvutimängudega seonduvaks. Teatud määral sarnase käsitluseni on jõudnud ka Maailmapank. Maailmapank on defineerinud[100] krüptoraha kui digitaalsete valuutade alamhulka, mida ta defineerib väärtuse digitaalse esindusena, mis on nimetatud nende enda arvestusühikus, mis on erinevad e-rahast, mis omakorda on tavapärane digitaalne makseviis, mis esindab ja on nimiväärtusega fiat rahas. Fiat raha on konkreetse valitsuse poolt välja antud raha, mis ei ole tagatud ühegi kauba, nagu näiteks kulla või hõbedaga. Fiat raha väärtus tuleneb nõudluse-pakkumise vahelisest suhtes ja selle välja andnud valitsuse stabiilsusest, mitte seda tagava kauba väärtusest.[101] Siit tuleb välja ka peamine vahe fiat raha ja krüptorahade vahel – kui fiat rahade stabiilsust tagab selle välja andnud valitsus, siis krüptorahadel nende detsentraliseerituse tõttu sellist stabiliseerimismehhanismi ei ole.

Kuna käesoleva töö jaoks on äärmiselt oluline AMLD nr.5, siis peab autor vajalikuks tuua välja ka selle definitsiooni krüptorahade kohta. AMLD-s nr.5 defineeritakse krüptoraha kui „virtuaalvääringut“ – digitaalsel kujul esitatud väärtus, mida ei ole välja andnud ega taganud keskpank ega avaliku sektori asutus, mis ei pruugi olla seotud ametliku vääringuga ja millel ei

[99] Mis on krüptoraha? Kättesaadav: http://www.kryptoraha.ee/tehnoloogia/, 20.03.2019
[100] Natarjan, H. Krause, S. Gradstein, H. (2017). Distributed Ledger Technology (DLT) and Blockchain. Kättesaadav: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 20.03.2019
[101] Chen, J. (2019). Fiat Money. Kättesaadav: https://www.investopedia.com/terms/f/fiatmoney.asp, 20.03.2019

ole vääringu või raha õiguslikku staatust, kuid mida füüsilised või juriidilised isikud aktsepteerivad vahetusvahendina ning mida on võimalik elektrooniliselt üle kanda ja säilitada ning millega on võimalik elektrooniliselt kaubelda.[102]

Seega võrreldes toodud organisatsioonide käsitlustega on AMLD nr.5 umbmäärasem, jättes võtmata seisukoha kas tegemist on digitaalraha või virtuaalrahaga, mis on aga ka mõistetav kuna nimetatud direktiivi kasutus ja mõju on laiem kui vaid tehingud krüptorahaga. Autori hinnangul on selline lähenemine ka mõistlik, kuna lisaks kõikidele turul olevatele krüptorahadele peab see ära katma ka võimalikud lähedased alternatiivid, mis juba turul on või mis sinna alles tulemas on.

Kohtupraktikas on krüptoraha definitsiooni peamiseks probleemiks olnud see, kas seda defineerida rahana või mitte. Siinkohal on selliseid küsimusi tekkinud praktikas just Ameerika Ühendriikide kohtupraktikas. Mainitavad kohtulahendid on kõik seotud ka töös käsiteldava rahapesu teemaga. Üks esimesi kohtulahendeid, mis krüptoraha osas üldse ning täpsemalt rahapesu osas tehti oli U.S. Securities and Exchange Commission[103] (edaspidi SEC) vs Trendon Shavers.[104] Nimetatud 2014. aasta lahendis meelitas Trendon Shavers inimesi investeerima oma investeerimisega tegelevasse ettevõttesse BTCST, lubades maksta intressi 1% päevas. Tegelikkuses oli tegemist tüüpilise Ponzi skeemiga, kus varem investeerinutele maksti raha hiljem investeerinud inimeste arvelt. Kogu arveldamine toimus bitcoinide kaudu, nii investorite kui ka Shaversi poolt. Paljud investorid kandsid rahalisi kaotusi, kokku 263 104 bitcoini ulatuses, mille väärtus praeguse hetke (10.05.2019) kursi kohaselt oleks umbes 1,65 miljardit USA dollarit.

SEC leidis, et Shavers pettis investoreid ning BTCST-sse tehtud investeeringuid tuleks käsitleda väärtpaberitena nagu defineerib seda föderaalne väärtpaberiseadus. Shavers omakorda leidis, et BTCST tehtud investeeringud ei ole väärtpaberid, kuna bitcoini ei saa käsitleda rahana ning see ei ole kuidagi reguleeritud USA-s kehtivate regulatsioonide poolt.

---

[102] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/843, 30. mai 2018, millega muudetakse direktiivi (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist, ning millega muudetakse direktiive 2009/138/EÜ ja 2013/36/EL (EMPs kohaldatav tekst), OJ L 156, 19.6.2018, lk. 43–74. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32018L0843, 01.04.2019
[103] Ameerika Ühendriikide Finantsinspektsioon
[104] Eastern District of Texas, 4:13-CV-416, *SEC vs Trendon Shavers*

Kohus aga leidis oma otsuses, et bitcoin siiski on raha või üks raha vorme ning investorid, kes tegid investeeringuid BTCST-sse, tegid siiski rahalise investeeringu. Sellest tulenevalt leidis kohus, et Shavers'i juhtum kuulus SEC-i jurisdiktsiooni alla.

Krüptoraha võimalik defineerimine rahana või mitterahana tõusetus ka kaasuses *US vs Faiella*, kus Robert Faiella ja kaassüüdistatav Charlie Shrem juhtisid bitcoinidega tegelevat turgu veebilehel "Silk Road" ehk siis Siiditeel. [105] Siiditee oli esimene nii-öelda pimeda veebi turg, kust oli võimalik soetada erinevaid kaupu/teenuseid, kõige rohkem oli nimetatud lehekülg tuntud narkootikumide vahendamise poolest. Lehekülg suleti 2013. aastal FBI[106] poolt.

Süüdistatavad müüsid Siiditee leheküljel bitcone ning võimaldades USA dollarite vahetamist bitcoinide vastu, tegelesid nad raha ülekannetega. Robert Faiella sai raha ülekandeid oma klientidelt ja olles need vahetanud bitcoinide vastu, kandis ta need üle klientide kontodele Siiditee leheküljel. Ka siin oli süüdistava põhiline argument enda kaitseks see, et krüptoraha ei saa käsitleda rahana.

Kohus lükkas süüdistatava argumendid tagasi ning leidis, et vastavalt Ameerika Ühendriikide seadustele on bitcoin käsitletav rahana, süüdistatav tegeles rahaülekannete tegemisega ning ta oli raha ülekandja. Oma argumentatsioonis toetus kohus muu hulgas Merriam Webster sõnaraamatu definitsioonile raha kohta, kus muu hulgas on öeldud, et raha võib olla midagi mis funktsioneerib raha ühikuna (*unit of account*) kui raha füüsiliselt ei eksisteeri. See teeb bitcoinist kohtu hinnangul raha, kuna sellega on võimalik osta kaupu ja teenuseid. Seega kinnitas kohus *SEC vs Shavers* lahendis toodut.

Kohtuvaidluses *US vs Ross William Ulbricht*[107] süüdistati juba mainitud Siiditee asutajat Ross Ulbrichti rahapesus, häkkimises, narkootikumide vahendamises ning kuue inimese tapmiskatses läbi palgamõrvarite palkamise. Rahapesu osas on oluline välja tuua, et palju kauplemist nimetatud platvormil toimus just läbi bitcoinide. Lehel võimaldati teha makseid läbi

---

[105] United States District Court, S.D. New York, No. 14-cr-243 (JSR). *USA v Robert M. FAIELLA, a/k/a "BTCKing," and Charlie Shrem*
[106] Federal Bureau of Investigation ehk Föderaalne Juurdlusbüroo
[107] United States District Court, S.D. New York, No. 14–cr–68 KBF, *United States v. Ulbricht*

bitcoinil baseeruva süsteemi, mille eesmärk oli võimaldada illegaalseid tehinguid, kus muu hulgas peideti kasutajate tegelikud andmed ja asukohad.

Nimetatud vaidluses kaitses Ulbricht ennast rahapesu süüdistuste vastu sellega, et ütles, et bitcoinid ei ole rahalised instrumendid, seega ei saa tehingud mis on seotud bitcoinidega olla aluseks rahapesusüüdistusele. Samuti kaitses ta ennast ka Ameerika Ühendriikide Maksuameti hinnanguga,[108] mis ütles, et krüptorahasid tuleb käsitleda varana, mitte rahana. Samuti lisas Ulbricht, et krüptorahadel on mõned, kuid mitte kõik, ametlike rahade omandused ning need ei ole kuskil kasutatavad seadusliku maksevahendina. Veel lisas ta, et bitcoinide kasutamine anonüümseteks tehinguteks ei tähenda ipso facto, et nimetatud tehingud on seotud ebaseaduslike asjaoludega. Anonüümsus iseenesest ei ole kuritegu.

Kohus lükkas tagasi argumendi, et bitcoin ei ole raha, öeldes: Bitcoinid hõlmavad endas väärtust – see on nende eesmärk ja funktsioon – ning nad on maksevahendiks (*medium of exchange*). Rahapesu käsitlevad seadused defineerivad rahalisi tehinguid kui inter alia "raha liikumist erinevatel viisil“ või [ ] mis sisaldab ühte või rohkemat rahalist instrumenti. Rahalist instrumenti defineeritakse kui münti või valuutat, isiklikku tšekki, pangatšekki jne.

Kohus leidis, et bitcoine võib kasutada asjade eest maksmiseks või vahetuse vahendina ja seda saab vahetada rahasse, millega võib asjade eest maksta. Bitcoini ainuke väärtus ongi selles, et sellega saab asjade eest maksta - see on digitaalne ja sellel puudub katsutav vorm; seda ei saa panna riiulile või kollektsioneerida. Selle vorm on digitaalseid bitid ja baidid, mis kokku annavad midagi millel on väärtus. Neid saab osta ja müüa seaduslike maksevahendite eest. Veel täiendas kohus, et kui narkootikumidega seotud tehingus maksti rahas, mis vahetati hiljem kullaks ning siis tagasi rahaks, siis puudub kahtlus selles, et tegemist on rahapesuga. Kohus leidis, et bitcoine kasutades on võimalik raha pesta.

Eespool toodud kohtulahendite kohaselt tuli Ameerika Ühendriikides bitcoine (ja seda laiendades võib tõlgendada, et krüptoraha üldiselt) käsitleda rahana.

Teatud määral kattub selle loogikaga ka Ameerika Ühendriikide Ülemkohtu lahendi Wisconsin

---

[108] Notice 2014-21. Kättesaadav: https://www.irs.gov/pub/irs-drop/n-14-21.pdf, 20.03.2019

Central Ltd. v. United States[109] kohta kirjutatud eriarvamus. Nimetatud kohtulahend ei puuduta küll otseselt krüptoraha, kuid on oluline seetõttu, et nimetatud lahendis mainis Ameerika Ühendriikide Ülemkohus esmakordselt krüptoraha. Nimetatud juhtumis oli tegemist küsimusega, kas töötajale antud aktsiaoptsioonid on maksustatav kompensatsioon. Ameerika Ühendriikide Ülemkohtu kohtunik Stephen Breyer kirjutas oma eriarvamuses (mida toetasid lisaks veel kolm ülemkohtunikku), et tema hinnangul peaks kohtud laiendama oma definitsiooni raha kohta. "Mida me oleme pidanud rahaks, on aja jooksul oluliselt muutunud. Võib-olla ühel päeval makstakse töötajatele palka bitcoinides või mingis muus krüptorahas.“

Kuigi kohtunik Stephen Breyeri näol on tegemist pigem konservatiivsete vaadete poolest tuntud kohtunikuna, võib tema eriarvamusest lugeda välja suhteliselt liberaalset tõlgendust krüptorahade kohta, millega nõustusid ka mõned teised ülemkohtunikud. See võib anda ka märku potentsiaalsest Ameerika Ühendriikide Ülemkohtu tõlgendusest krüptorahade kohta.

Kuigi eespool mainitud lahendid ei ole üks-ühelt võrreldavad Euroopas kehtivate regulatsioonidega, annavad nad samas siiski olulise info sellest, kuidas kohtupraktika rahapesusse krüptoraha tehingutes on suhtunud. Ameerika Ühendriikide kohtupraktika näidete toomine on oluline ka sellepärast, et Euroopas vastav kohtupraktika puudub.

Õiguskirjanduses leidub ka seisukohti selle osas, et tegelikkuses ei erine krüptoraha eriti palju tavapärasest rahast. Sisuliselt on vaid väike osa majandusest sularahas. Enamik rahast on elektroonilises vormis, mis tähendab, et tegelikult on need vaid andmed arvutis. Enam ei ole kogu raha riigi poolt kullaga tagatud. Praegune süsteem töötab inimeste ning rahaliste institutsioonide ja valitsuse vahelise usalduse põhjal, kes kõik usuvad, et seaduslikul maksevahendil on ka tulevikus ikka veel olemas väärtus. Ka krüptorahad põhinevad kasutajate usul, et tulevikus on neil veel väärtus.[110]

Eespool toodud organisatsioonide käsitluste kohaselt on üheks suurimaks erinevuseks, mis käsitlustes on, see kas krüptoraha puhul on tegemist virtuaalraha alamhulgana või digitaalraha

[109] Breyer, J. (2017). Dissenting. Kättesaadav: https://www.supremecourt.gov/opinions/17pdf/17-530_6537.pdf, 20.03.2019
[110] Cvetkova, I. (2018). Cryptocurrencies Legal Regulation, 5 BRICS Law Journal. 128-153 lk 130. viidatud Guttmann, B. (2013). The Bitcoin Bible:All You Need to Know About Bitcoins 123-124 (Germany: BoD)

alamhulgana. Autori hinnangul see siiski suurt praktilist olulisust ei oma. Paljuski sõltub antav definitsioon selle andnud organisatsiooni tegevusvaldkonnast. Kõige olulisem on pigem see, et organisatsioonidel oleks ühine arusaam sellest, et krüptoraha stabiilse arengu tagamiseks on vaja jõuda konsensuseni krüptoraha seadustes paiknemise osas. Ühise definitsiooni ja arusaama leidmine krüptoraha valdkonnast on oluline ka kuna krüptorahad on oma olemuselt geograafilisi piire ületavad.

Autor ise aga pakuks välja alternatiivse definitsiooni krüptorahale – „krüptoraha on virtuaalselt esinev krüptograafial põhinev detsentraliseeritud raha, mida võib käsitleda maksevahendina." Nimetatud definitsioon on autori hinnangul sobilik, kuna toob välja krüptoraha kõige olulisemad põhimõtted. Detsentraliseeritus on äärmiselt oluline osas krüptoraha tööpõhimõttest ning kahtlemata ka suur osa sellest, mis teeb selle inimeste jaoks atraktiivseks. Samuti on krüptoraha jaoks tähtsal kohal see, et selle tööpõhimõtted seisnevad krüptograafial – see eristab seda teistest virtuaalsel kujul esinevatest rahadest. Oluline on välja tuua ka see, et tegemist on maksevahendina, mida paljud aktsepteerivad, kuid siiski ei ole tegemist ametliku maksevahendina.

Kindlasti tuleb nõustuda õiguskirjanduses toodud seisukohtadega, et krüptoraha paiknemine seadustes on täna veel ebaselge. Seega oleks vaja leida täpne strateegia krüptoraha regulatsioonides, saavutamaks parim tasakaal krüptoraha omanike ja regulaatorite vahel.[111]

[111] Nahorniak, I. Leonova, K. Skorokhod, V. (2016). Cryptocurrency in the Context of Development of Digital Single Market in European Union, 3 InterEULawEast: Journal for International and European Law, Economics and Market Integrations. 107-123, lk 116

2. RAHAPESU KRÜPTORAHA TEHINGUTES

2.1. Rahapesu definitsioon

Terminit rahapesu hakati esimest korda kasutama 1920ndatel kui teatud kriminaalsed grupeeringud Ameerika Ühendriikides (näiteks nagu Al Capone ja Bugsy Moran) avasid autopesulaid ja riietepesulaid, mille eesmärgiks oli „musta raha“ pesemine.[112]

AMLD nr.5 sätestab, et rahapesuna käsitletakse järgnevaid tahtlikke tegevusi:

1) Vara muundamine või üleandmine, kui on teada, et selline vara on saadud kuritegelikust tegevusest või selles osalemisest, eesmärgiga varjata vara ebaseaduslikku päritolu või abistada kuritegelikus tegevuses osalevat isikut, et see isik saaks hoiduda oma tegude õiguslikest tagajärgedest.
2) Vara tõelise olemuse, päritolu, asukoha, käsutamisviisi, ümberpaigutamise, omandiõiguse või muude varaga seotud õiguste varjamine, kui on teada, et selline vara on saadud kuritegelikust tegevusest või selles osalemisest.
3) Vara omandamine, valdamine või kasutamine, kui selle saamisel on teada, et selline vara on saadud kuritegelikust tegevusest või selles osalemisest.
4) Punktides 1, 2 ja 3 osutatud tegudes osalemine, seotus nendega, nende toimepanemise katsed ning nendele kaasaaitamine ja kihutamine või nende soodustamine või nendeks nõuandmine.

Eestis kehtiv RahaPTS §4 lg 1 sätestab, et rahapesu on kuritegelikust tegevusest saadud vara või selle asemel saadud vara:

[112] Urziceanu, R. (2008). Money Laundering,.AGORA International Journal of Juridical Sciences. 305-311, lk 306

1) Muundamine või üleandmine, kui on teada, et selline vara on saadud kuritegelikust tegevusest või selles osalemisest, eesmärgiga varjata vara ebaseaduslikku päritolu või abistada kuritegelikus tegevuses osalenud isikut, et ta saaks hoiduda oma tegude õiguslikest tagajärgedest.
2) Omandamine, valdamine või kasutamine, kui selle saamisel on teada, et see on saadud kuritegelikust tegevusest või selles osalemisest.
3) Tõelise olemuse, päritolu, asukoha, käsutamisviisi, ümberpaigutamise või omandiõiguse varjamine või varaga seotud muude õiguste varjamine või kui on teada, et selline vara on saadud kuritegelikust tegevusest või selles osalemisest.

Seega võib öelda, et rahapesu on kriminaalne tegevus, mille käigus läbi mitmete tehingute muudetakse illegaalne raha selliseks nagu oleks tegemist legaalse rahaga.[113] Seega on rahapesu juures väga oluline see, et toime on pandud nii-öelda eelkuritegu.

Kuigi rahapesu on mitmekülgne ja kompleksne protsess,[114] võib tavapäraselt selle protsessi jagada kolmeks erinevaks osaks:[115]

1) Paigutamine: Rahapesu toimepanija paigutab kriminaalselt teenitud raha legaalsesse ettevõtmisesse. See on ka kurjategija poolt vaadates kõige ohtlikum osa rahapesust. Siin peab raha deposiite jagama sellistes summades, et vältida erinevate finantsasutuste raporteerimisekohustuse alla sattumist või jagama raha deposiite nii, et need koosneks nii legaalsest kui illegaalsest rahast.[116] Finantsinspektsioon on nimetanud seda faasi ka süsteemi asetamiseks.[117]
2) Ladestamine: Rahapesu toimepanija eesmärk on distantseerida teenitud raha oma kriminaalsest taustast.[118] Tihti on tehingute jada väga keeruline.[119]

---

[113] Bank Secrecy Act/ Anti-Money Laundering Examination Manual, (2010). kättesaadav: https://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2010.pdf,
[114] *Ibid.*
[115] Levi, M. Reuter, P. (2006). Money Laundering, 34 Crime & Justice. 289-375, lk 311
[116] Bank Secrecy Act/ Anti-Money Laundering Examination Manual (2010), *Supra nota* 113
[117] Finantsinspektsioon. (2018). Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks.“ Kättesaadav: https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf, 20.03.2019
[118] Levi, M. Reuter, P. (2006), *supra nota* 115, lk 311
[119] Bank Secrecy Act/ Anti-Money Laundering Examination Manual (2010), *supra nota* 113

3) Integreerimine: Kui raha on juba finantssüsteemis, kasutatakse integreerimise protsessi tekitamaks näiline legaalsus täiendavate tehingutega. Need annavad rahapesijatele mõistliku põhjenduse raha päritolu kohta. Näitena võib tuua kinnisvara, väärtpaberite, võlakirjade jne ostu ja müüki.[120]

Rahapesuvastased seadused keskendusid algselt organiseeritud kuritegevusele, täpsemalt sellele, et selgitada välja teenitud tulu päritolu võimaldamaks organiseeritud kuritegevust takistada läbi nende rahavoogude peatamise.[121] Viimasel ajal on rahapesuvastaseid seadusi hakatud kasutama ka võitluses terrorismi vastu.[122] Praeguse aja suund on aga keskenduda rahapesuvastases võitluses mitte enam nendele kes üritavad raha pesta vaid eelkõige finantsinstitutsioonidele kelle juurest „must raha“ läbi käib.[123] Autor nõustub ja leiab, et see on ka kõige sobivam viis rahapesuga võitlemiseks, kuna pangad ja muud finantsasutused kust käib läbi suurel hulgal raha peavad olema maksimaalselt motiveeritud tegelema probleemsete isikutega. Järelevalvega tegelevad organisatsioonid saavad probleemiga tegeleda alles pärast vastava info nendeni jõudmist, kuid nii-öelda pettuse toimumise staadiumis ei ole neil tavapäraselt olemas teavet pettuse kohta, eriti arvestades, et rahapesu on rahvusvaheline ning geograafilisi piire ei tunne. Kuna pangad tegelevad probleemsete isikutega aga esmajärjekorras ning näevad tehinguid esimesena, siis ilma nendepoolse tähelepanuta rahapesule ja edukalt toimivate kontrolliprotsessideta (AML ja KYC)[124] pole ka võimalik mõjusalt rahapesu vastu võidelda. Traditsiooniliselt on sanktsioonide oht ja halb maine avalikkuse ees just see mida finantsasutused kindlasti vältida soovivad, kuna mainekahju on suur. Seega on oht, et regulaatorid määravad trahve või sanktsioone ning oht, et avalikkuse ees saab vastava finantsasutuse maine läbi halva kajastuse kahjustada, midagi mis kindlasti motiveerib finantsasutusi enda kontrollimehhanismidesse ressursse paigutama ja ka sisemiselt tulemusi nõudma. Fakt on, et järelevalveasutusteni jõuab tavapäraselt info pettusest alles siis kui pettus on juba toimunud. Tagantjärgi on rahapesuteemaliste pettuste vastu võitlemine ning vajadusel kriminaalmenetluste läbiviimine kindlasti kallim ja ebatõhusam meetod. Palju efektiivsem on aga pankadel ja muudel finantsasutusel takistada pettusi enne kui need üldse juhtuda saavad või

[120] *Ibid.*
[121] Christopher, C.M. (2014). Whack-A-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Money Laundering, 18 Lewis & Clark Law Review. 1-36, lk 3
[122] *Ibid.,* lk 36
[123] *Ibid.,* lk 36
[124] Anti Money Laundering (rahapesuvastane) ja Know Your Customer (tunne oma klienti) printsiibid

võimalikult varajases staadiumis. Sama põhimõte peaks kindlasti kehtima ka krüptoraha tehingutega seotud olevatele finantsasutusele.

Näitena võib siin tuua Jaapanis juhtunu. Krüptoraha vahetamise teenust pakkuvad operaatorid teavitasid 2017. aprillist detsembrini Jaapani politseid 669 juhul võimalikust rahapesuriskist. Siis muudeti sellistele operaatoritele kohustuslikuks politsei teavitamine tehingutest, kus on olemas rahapesu risk ning 2018. aasta jooksul teavitati politseid juba rohkem kui 7000 juhul.[125] See näitab vajadust läheneda asjale efektiivsete meetoditega. Antud juhul ongi see näide sellest, kuidas finantsasutuste motiveerimine sanktsioonide ähvardusel krüptorahaga toimuva rahapesu algstaadiumis probleemiga tegelemisel omab positiivset mõju. Kahtlemata on sellisel infovahetuse tohutul suurenemisel edukad tagajärjed rahapesu vastu võitlemises, kasvõi juba preventiivsest küljest, kuna pikas perspektiivis vähendab see kurjategijate „julgust“ pettusi proovida.

2.2. Rahapesu protsess krüptoraha vahendusel

Alates bitcoini loomisest 2009. aastal on krüptorahasid kasutatud kriminaalsete tegevuste läbiviimiseks. Neid on kasutatud alates rahapesust kuni narkootikumide ja illegaalsete relvade ostmiseni. Võib öelda, et alates juba loomisest on krüptorahad olnud seotud kriminaalse tegevusega.[126] Autor leiab, et paljuski võib selle põhjuseks olla just see, et krüptorahad on pikka aega olnud mõnes mõttes "metsiku lääne" rollis ehk siis regulaatorid, järelevalveorganid ja seadusandjad ei ole teadnud kuidas neile efektiivselt läheneda. Samuti on nii mõnelgi pool seadusandjad ja regulaatorid olnud probleemiga tegelemisel pigem passiivsed ning aeglased (siin võib tuua ka Euroopa näite).

Siiani on finantsregulatsioonide üks põhimõtteid olnud see, et regulaatoril on võimalus panna

[125] Cases of money laundering linked to cryptocurrency in Japan up tenfold in 2018. (2019). Kättesaadav: https://www.japantimes.co.jp/news/2019/02/28/national/crime-legal/cases-money-laundering-linked-cryptocurrency-japan-tenfold-2018/#.XIZS7fZuJPY, 20.03.2019

[126] Essaghoolian, N. (2019). Initial Coin Offerings: Emerging Technology's Fundraising Innovation, 66 UCLA Law Review. 294-343, lk 314.

vastavuskontrolli nõudeid tsentraliseeritud üksusele ning samuti kontrollida, kas neid nõudeid täidetakse.[127] Krüptorahade detsentraliseeritus tekitab aga unikaalse probleemi regulaatoritele, kuna puudub see tsentraalne jõud, kes saaks tavapäraseid rahapesuvastaseid meetmeid kasutusele võtta.[128] Seega ongi siin probleemi tuum selles, et vastupidiselt traditsioonilise rahaga tehtavatele tehingutele, ei ole krüptoraha tehingute puhul võimalik sanktsioneerida kedagi kui vastavaid rahapesuvastaseid meetmeid korrektselt kasutusele ei võeta.

Õiguskaitseorganitele täiendavaks takistuseks on ka see, et tänu viisile kuidas krüptorahasid tehakse, ei ole võimalik ühtegi krüptorahaga tegelevat äriühingut kas läbi otsida, alustada tema suhtes kohtumenetlust või äriühingut kinni panna.[129]

Krüptorahadega tehtava rahapesu mastaapi ja probleeme selgitas üks Europoli direktoritest Rob Wainwright, kes selgitas, et Europoli hinnangul pestakse Euroopas iga-aastaselt krüptorahade kaudu 3-4 miljardit naelsterlingit ning see number on kasvamas.[130] Ta lisas, et probleemiks on see, et krüptorahade puhul ei ole tegemist pankadega ning neil puudub tsentraaljuhtumine, seega ei saa õiguskaitseorganid neid tehinguid jälgida. Samuti on murekohaks see, et isegi kui kriminaalid suudetakse identifitseerida, ei ole võimalik nende varasid arestida, vastupidiselt tavalisele pangandussüsteemile.[131] Seega, isegi kui krüptorahad on muutunud aina rohkem reguleeritumaks, on läbi krüptorahade ja läbi nendega tegelevate kauplemisplatvormide liigutatud raha jälitamine õiguskaitseorganitele ikka veel väga keeruline.[132]

Kuigi on neid, kes ütlevad, et krüptoraha avalik register *(public ledger)* teeb sellest vähem atraktiivse vahendi rahapesu toimepanemiseks kui tavapärane raha ning rahapesu läbi plokiahelaga seonduva krüptoraha võib olla riskantsem kui teiste süsteemi kasutamine,[133] siis sellega autor ei nõustu kuna maha jääv jälg on alati selgem tavaliste pangatehingute puhul.

---

[127] Tu, Meredith (2015), *supra nota* 55, lk 297
[128] *Ibid.*, lk 297
[129] Twomey, P. (2013). Halting a Shifi in the Paradigm: The Need for Bitcoin Regulation, 16 Trinity College Law Review. 67-90, lk 75. Viidatud Brito, J. (2011). Online Cash Bitcoin Could Challenge Governments, Banks. Kättesaadav: http://techland.time.com/2011/04/16/online-cash-bitcoin-could-challenge-governments/2/, 20.03.2019
[130] Silva (2018), *Supra nota* 20
[131] *Ibid.*
[132] Hett, W. (2008). Digital Currencies and the Financing of Terrorism, 15 Richmond Journal of Law & Technology. 1-43, lk 12
[133] Brookes, A. (2018). *Supra nota* 14, lk 83

Samuti on tänaseks tekkinud juba krüptorahasid, mille puhul plokiahelal põhinev avalik register *(public ledger)* ei olegi avalik, nagu näiteks Monero. Monero ei avalda plokiahela registris liikunud krüptoraha tehingute andmeid. Seega ei ole õiguskaitseorganitel sisuliselt võimalik selle abil tehtud tehinguid jälgida.

Kuna krüptorahade puhul on mitmed võimalikud skeemid kuidas raha pesta, siis sellest tulenevalt tulebki välja selgitada millised rahapesu meetodid on praegusel hetkel kõige levinumad ning kõige problemaatilisemad. Samuti tuleks hinnata kehtivate ja kehtima hakkavate regulatsioonide sobivust rahapesu erinevate protsesside takistamise osas.

CipherTrace on ülemaailmselt tegutsev ettevõte, mis tegeleb plokiahela tehnoloogia arendamise ja rahapesuvastase vastavuskontrolliga, eesmärgiga teha krüptorahad, krüptotokenid ja plokiahel võimalikult turvaliseks. Nad on turul tuntud kui asjatundjad, kes krüptorahaga seonduvate kuritegude osas (sealhulgas rahapesu kohta) igas kvartalis põhjalikke raporteid koostavaid. Nende kogutud info ja raportite põhjal ongi hea analüüsida hetkel kõige levinumaid pettuse viise, mida krüptoraha tehingutes raha pesemiseks kasutatakse.

Viimases nende avaldatud raportis tuuakse välja, et suurimaks probleemiks hetkel on *„mixers“* (tihti tuntud kui *„tumblers“)* ja *„foggers“*.[134] Kuna nende tööpõhimõte ja eesmärgid on sarnased, siis kasutatakse käesolevas töös edaspidi läbivalt väljendit *„mixers“*. Nende teenuste pakkujate eesmärk on pakkuda teenust millega tehakse krüptoraha päritolu ja liikumine varjatuks, mis tahtmatult või tahtlikult on väga heaks abimeheks ka kurjategijatele, seal hulgas rahapesijatele. Kuna autorile teadaolevalt neid termineid otseselt Eesti keelde pole tõlgitud ja otsetõlge konteksti mõistes sobilik ei ole, kasutatakse magistritöö siseselt ingliskeelseid originaaltermineid.

"Mixers" tööpõhimõte seisneb selles, et kui isik teeb krüptoraha ülekandeid, siis saadetakse makse läbi vastava *"mixers'i,"* kus see seguneb kolmandate isikute tehtud maksetega ning alles siis saadetakse makse lõplikule saajale. Seega jõuab sihtkohta mitte konkreetse isiku (ehk siis rahapesija) saadetud krüptoraha, vaid võibolla näiteks kümne muu isiku poolt saadetud krüptoraha. See teeb aga sisuliselt võimatuks tuvastamise kes kuhu, millal ja kui palju

[134] Cryptocurrency Anti-Money Laundering Report, 2018 Q4, *supra nota* 19

krüptoraha saatis. Tehnoloogiliselt on nendega võimalik saata krüptoraha makseid ka ajalise viivitusega, mis tähendab, et jäljed on veelgi paremini segatud.[135] Traditsioonilisi pangandustermineid kasutades võiks tuua võrdluse, et see on samaväärne kui saata raha *off-shore* pankadesse mis asuvad näiteks Kaimanisaartel, Bahamal või Panamas.[136]

Teise probleemina võib tuua juba mainitud probleemi, et on olemas mitmed krüptorahad, mis on täiesti anonüümsed (mitte pseudonüümsed) nagu Monero, Zcash ja Dash.[137] Neist just esimese puhul on selle kasutamine rahapesus hästi teada.[138] Nende erinevus tavapärastest krüptorahadest seisneb selles, et nende plokiahela pearaamat ei ole avalik. Neist kõige tuntum ongi ilmselt Monero, mis asutati 2014. aastal.[139] Krüptorahade turuväärtuste suure kasvu ajal 2016. aastal oli ootamatult just Monero see krüptoraha, mille turuväärtus kasvas kõige enim kordi.[140] Põhiliseks põhjuseks miks selle krüptoraha turuväärtus nii palju tõusis peitubki ilmselt selles, et tegemist on täiesti anonüümse krüptorahaga, millega tehtud tehinguid on peaaegu võimatu jälitada. Need omadused ongi Monero'st teinud tumeda veebi kasutajate lemmiku. On tuvastatud, et selle kasutajate hulgas on nii krediitkaardi pettureid, narkodiilereid kui ka ebaseadusliku relvamüügiga tegelevaid isikuid.[141]

Tihti on rahapesuks kasutatavad ka krüptoraha hasartmänguleheküljed.[142] Internetis on sellised krüptorahale keskenduvaid kasiinosid hetkel üle saja.[143] Kurjategijad saavad nendel lehekülgedel teha kontosid ja kanda sinna vahendeid rahapesu toimepanemiseks. Nad teevad tavalisi panuseid ja tavapäraselt lihtsalt võtavad vahendid välja uuele aadressile. See teeb tehingute rea jälgimise keerulisemaks ja töötab mõnes mõttes kui *"mixers"*.

---

[135] How to use a Bitcoin mixer or tumbler. Kättesaadav: http://cryptorials.io/use-bitcoin-mixer-tumbler/, 20.03.2019
[136] Mixers, Tumblers, Foggers. Kättesaadav: https://ciphertrace.com/glossary/mixer-tumbler-fogger/, 20.03.2019
[137] O'Driscoll, A. (2018). Monero vs zcash vs dash: which is the most anonymous cryptocurrency? Kättesaadav: https://www.comparitech.com/crypto/anonymous-cryptocurrency-monerto-zcash/, 20.04.2019
[138] Dumont, M. (2018). Bitcoin And Monero Used To Launder $89M: Investigation. Kättesaadav: https://cryptodaily.co.uk/2018/09/bitcoin-monero-money-laundering/, 20.04.2019
[139] About Monero. A Brief History. (2019). Kättesaadav: https://www.getmonero.org/resources/about/, 20.04.2019
[140] Greenberg, A. (2017). Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire. Kättesaadav: https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/, 20.04.2019
[141] *Ibid.*
[142] Canellis, D. (2019). 76% of laundered cryptocurrency was washed with an exchange service. Kättesaadav: https://thenextweb.com/hardfork/2019/01/29/cryptocurrency-laundering-chainalysis/, 20.04.2019
[143] Bitcoin & Crypto Casinos. (2019). Kättesaadav: https://coinclarity.com/casinos/, 20.04.2019

Siinkohal tuleb hinnata vastavalt magistritöö sissejuhatuses püstitatud uurimisküsimusele, kas rahapesu mõiste vajaks muutmist või täpsustamist uute tehnoloogiliste arengute valguses krüptoraha tehingutes. Seega oleks vaja tuvastada, kas rahapesu käsitlevad sätted kehtivad ka uuemate krüptorahaga seonduvate pettuste nagu *„mixers“* ja Monero puhul.

Autori hinnangul eespool mainitud uute tehnoloogiliste arengute valguses AMLD nr.5 või RahaPTS toodud rahapesu definitsioon muutusi ega täiendusi ei vaja. *„Mixers'i“,* krüptokasiinode ja Monero suguste teenuste kasutamise puhul on autori hinnangul tegemist kehtiva regulatsiooni järgi vara tõelise olemuse ja päritolu varjamisega. Seega kuuluvad need autori hinnangul seaduses toodud rahapesu definitsiooni alla ning rahapesu definitsioon täiendamist ei vaja.

Krüptoraha puhul võib rahapesust rääkides täiendavalt välja tuua mõned eripärad, mis sellel võrreldes „tavalise“ rahapesuga on. Krüptorahade puhul võib rahapesu toimimise protsessi kirjeldada järgnevalt:

1) Paigutamine – sularaha eest ostetakse krüptoraha näiteks vahetusteenuse pakkujatelt või vahetatakse kuritegelikul teel saadud krüptoraha traditsioonilise raha vastu.[144] Isik võib avada mitmeid kontosid mitmete vahetusteenuse pakkujate juures. Vahetusteenuse pakkuja juures võib olla võimalik avada konto ka anonüümselt, mis tähendab, et ei peeta arvestust kes kui palju krüptoraha vahetab.[145]
2) Ladestamine – selles faasis toimub krüptoraha ülekandmine ühelt krüptoraha aadressilt teistele krüptoraha aadressidele. Tehingute tegemiseks kasutatakse ka kolmandate isikute krüptoraha aadresse. Samuti kasutatakse jälgede segamiseks erinevaid rakendusi. Ka võib krüptorahade eest osta teisi virtuaalseid või digitaalseid maksevahendeid.[146]

[144] Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies. (2014). Kättesaadav: https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf, 20.03.2019
[145] Morel, T. (2016). Rahapesu Bitcoin'idega. (Magistritöö). TÜ Õigusteaduskond. Tallinn.
[146] *Ibid., lk 33*

3) Integreerimine - kurjategija saab krüptoraha legaalsesse käibesse tuua, kui ostab krüptoraha eest kaupu ja teenuseid, kuna krüptorahasid aktsepteeritakse järjest rohkemate kaupmeeste poolt. Kurjategija võib krüptoraha eest osta auto või maja ning selle siis maha müüa ja vastu saada nii-öelda puhta raha. Samuti võib krüptoraha vahetada tagasi traditsioonilise raha vastu kauplemisplatvormi juures.[147]

Rääkides rahapesu regulatsioonide arengust, siis hetkel Euroopas kehtiv AMDL nr.4 võeti vastu 20.05.2015. Nimetatud direktiiviga toodi mitmeid muutusi Euroopas rahapesu ja finantskuritegevuse vastasesse võitlusesse. Näiteks olulisemad muutused, mille nimetatud direktiiv kaasa tõi, olid tegeliku kasusaaja regulatsioon, riikliku taustaga isikud (PEP ehk politically-exposed persons) ja riskipõhine lähenemime rahapesu takistamisele igal tasemel. Samuti pani see kohustuse ettevõtetele, kellel on enamusosalusega tütarettevõtted sellistes jurisdiktsioonides, mille rahapesuvastased reeglid ei ole nii põhjalikud kui Euroopa Liidu omad, et nad peavad järgima oma tütarettevõtetes samu rahapesuvastaseid reegleid mis emaettevõttes.[148]

Kuna AMLD nr.4 valmimise ajal ei olnud krüptoraha niivõrd olulise tähtsusega, siis konkreetselt krüptorahadele nimetatud direktiivis tähelepanu ei pööratud. Kuigi regulatsioonid kehtisid loomulikult kõigile, oli selge, et niivõrd spetsiifilise valdkonna kui krüptoraha reguleerimiseks on vaja direktiivi täiendada. Seega sai Euroopa Komisjon kiiresti aru, et krüptoraha vajaks täiendavat tähelepanu.

Euroopa Komisjon tuli 05.07.2016 välja Euroopa Parlamendi ja nõukogu neljanda rahapesu direktiivi nr 2015/849 (AMLD 4) muutmise eelnõuga, milles muu hulgas tehi ettepanek lisada rahapesuvastase direktiivi kohaldamisalasse virtuaalvääringute vahetamisega tegelevad platvormid ja nn digitaalse rahakoti pakkujad (*custodian wallet providers*), kes peaksid tegutsemiseks taotlema tegevusloa või vastava registreeringu.[149] Sellest sündis ka AMDL nr.5

---

[147] Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies. (2014), *supra nota* 144

[148] 4th Money Laundering Directive – What you need to know. (2017). Kättesaadav: https://vinciworks.com/blog/4th-money-laundering-directive-what-you-need-to-know/, 20.04.2019

[149] Rahandusministeerium. Analüüs virtuaalvääringute võimaliku tunnustamise ja kasutamise poliitika väljatöötamiseks. (2016). Kättesaadav: https://www.rahandusministeerium.ee/et/system/files_force/document_files/2016-vv_virtuaalvaaringute_analuus-22-07.pdf, 20.04.2019

AMLD nr.5 viib Euroopa Liidu umbes samasse punkti regulatsioonidega, mille Ameerika Ühendriigid võtsid vastu juba 2013. aastal. Euroopa regulaatorid olid eelnevalt võtnud hoiaku „ootame ja vaatame mis juhtub“ ajal kui krüptorahadega seonduvatest riskidest ei saadud veel hästi aru.[150] Seega võib öelda, et samal ajal kui Ameerika Ühendriikide valitsus tegutses, oldi Euroopas passiivsed.

AMLD nr.5 võeti vastu direktiiviga 2018/843. Nagu juba eelnevalt mainitud andis nimetatud direktiiv konkreetse definitsiooni krüptorahadele (direktiivis kasutati küll väljendit "virutaalvääringud").

Samuti sätestas AMLD nr.5 direktiivi mõttes kohustatud isikuteks teenuseosutajad, kes vahetavad virtuaalvääringut ametlikuks maksevahendiks ja vastupidi ning rahakotiteenuse pakkujad (isik, kes osutab oma klientide nimel krüptograafiliste privaatvõtmete kaitse teenuseid, et virtuaalvääringuid hoida, säilitada ja üle kanda). Seega hakkasid nimetatud teenuste osutajatele kehtima samad rahapesu takistamise nõuded, mis kehtivad näiteks krediidiasutustele.

Tuleb märkida, et Eesti viis muutused, mida AMLD nr.5 nõudis, oma seadustesse juba enne AMLD nr.5 vastuvõtmist Euroopa Liidu tasemel. Peamiselt saab välja tuua järgnevad kaks kohustust krüptorahaga tegelevate ettevõtetele, millised Eesti tõi oma seadustesse 7.11.2017 jõustunud RahaPTS’ga, kui tõi mõiste "virtuaalvääring". Sellele eelnevalt kehtis seaduses termin "alternatiivne maksevahend". Need kaks peamist kohustust on:

1) Loakohustus (RahaPTS §70 jj)
2) Hoolsuskohustus (RahaPTS § 20 jj)

Loakohustuse ja hoolsuskohustuse sisunõuete täpsem analüüs toimub punktides 2.3.1 ja 2.3.2.

[150] Robinson, T. (2018). 5th AML Directive: EU Regulation of Cryptocurrency Businesses. Kättesaadav: https://www.elliptic.co/our-thinking/5th-aml-directive-eu-regulation-cryptocurrency, 20.03.2019

2.3. AMLD nr 5-st tulenevad rahapesuvastased preventiivsed meetmed krüptoraha tehingutes

2.3.1. Krüptoraha vahendaja või hoidja tegevusloa nõue

Kõigepealt tuleb välja tuua tegevusloa hankimise kohustus. Selle järgi peab krüptoraha raha vastu vahetamise teenust ja rahakotiteenust pakkuval ettevõtjal olema vastav tegevusluba.[151] Eesti oli esimene riik Euroopa Liidus, kes selle nõude vastavalt AMLD nr.5 oma seadustesse tõi, mis omakorda tõi kaasa selle, et paljud rahvusvahelised krüptorahaga tegelevad ettevõtted soovisid Eestis tegevuslube taotleda.[152] Eestis väljastab nimetatud lubasid RAB. Seisuga 10.05.2019 näitab päring Majandus- ja Kommunikatsiooniministeeriumi hallatavasse majandustegevuse registrisse,[153] et Eestis on välja antud 710 kehtivat krüptoraha rahakotiteenuse luba ja 808 krüptoraha raha vastu vahetamise teenuse luba.

Kas tegevusloa hankimise nõue on sobiv meede krüptoraha tehingutes rahapesu takistamiseks? Selle sobivuse hindamiseks tuleb analüüsida kogu tegevusloa taotluse protsessi, põhjalikkust ja võimalikke kitsaskohti.

Tegevusloa saamiseks peab juriidiline isik esitama RAB-ile taotluse, kus on toodud RahaPTS § 70 toodud teave, taotlus peab vastama ka majandustegevuse seadustiku üldosa seaduse (edaspidi MSÜS)[154] § 19 toodud tingimustele (kuid nimetatud nõudmised on pigem üldisemat laadi). Nõutud teave sisaldab RahaPTS kohaselt kokkuvõtvalt järgnevat:

1) Teenuse pakkumise koha aadress;
2) Teenuse pakkumise eest vastutava isiku nimi ja kontaktandmed;
3) Välismaise juriidilise isiku puhul ettevõtte omaniku ja tegeliku kasusaaja andmed;
4) Juriidilise isiku puhul teenusepakkuja juhtorgani liikme andmed;

[151] RahaPTS, *supra nota* 21
[152] Ullman, K. Demchuk, N. (2018). Virtuaalvääringu tegevusload Eestis. Kättesaadav: https://www.rmp.ee/uudised/juhile/virtuaalvaaringu-tegevusload-eestis, 20.03.2019
[153] Majandustegevuse register. Kättesaadav: https://mtr.mkm.ee./tegevusluba?m=97, 20.03.2019
[154] Majandustegevuse seadustiku üldosa seadus - RT I, 13.03.2019, 22

5) Protseduurireeglid ja sisekontrolli eeskirjad ning nende kontrollimise kord vastavalt rahvusvahelise sanktsiooni seaduse (edaspidi RsanS)[155] § 12 lõikele 6;
6) Vastutava juhatuse liikme või kontaktisiku andmed vastavalt RahaPTS § 17, mis muu hulgas sätestab kohustuse, et nimetatud isikul on laitmatu maine;
7) Finantssanktsioonide rakendamise eest vastutava isiku andmed ja kontaktandmed vastavalt RsanS § 12 lõikele 6;
8) Kui ettevõtte juhtorgani liige, tegelik kasusaaja või omanik on välismaalane, siis tema koduriigi karistusregistri tõend, mis tõendab karistuse puudumist riigivõimuvastase või rahapesualase süüteo või muu tahtlikult toimepandud kuriteo eest.

Siinkohal lisab autor, et punktis 7 viidatud RsanS-i sätet § 12 lg 6 tegelikkuses olemas ei ole, seega on kehtivas RahaPTS'i redaktsioonis hetkel viga. Ilmselt on seadusandja tegelikkuses mõelnud RsanS § 13 lg 6 ning sellest ka autor töös lähtub. Nimetatud viga seaduses kaotatakse 01.01.2020 jõustuvate uute RahaPTS ja RsanS redaktsioonidega.

Tegevusluba antakse kui tegevusluba taotlev ettevõte vastab RahaPTS § 72 toodud nõuetele:

1) Ettevõttel, tema juhtorgani liikmel, tegelikul kasusaajal ja omanikul puudub muu hulgas rahapesualane süütegu või muu tahtlik kuritegu;
2) RahaPTS § 17 sätestatud kontaktisik vastab toodud nõuetele.

Tegevusloa võib kehtetuks tunnistada vastavalt RahaPTS § 75 muu hulgas kui ettevõtja korduvalt ei täida järelevalve asutuse ettekirjutusi või kui ettevõtja ei ole taotletud tegevusalal asunud tegutsema kuue kuu jooksul loa väljastamisest alates. Samuti võib tegevusloa tunnistada kehtetuks vastavalt MsÜS § 37 lg 1 toodud alustele (muu hulgas tegevusloa taotlusel tahtlikult valeandmete esitamisel või majandustegevusest loobumisel).

Kui hinnata toodud nõudeid, siis tegelikult ei ole need ebamõistlikult koormavad ettevõtjate suhtes, eriti arvestades, et tegemist on teiste isikute finantsvarasid kontrollida võivate juriidiliste isikutega. Pigem on tegemist täiesti elementaarse teabe küsimisega ettevõtetelt veendumaks, et seaduses nõutud sisekontrolli reeglid ja protseduurireeglid oleksid olemas. Kuna Eesti suguse

[155] Rahvusvahelise sanktsiooni seadus - RT I, 29.06.2018, 69

riigi ettevõtluse edukaks toimimiseks ja kiireks arenguks ongi vajalik, et oldaks uuenduslikud ning valmis võtma kalkuleeritud riske ettevõtluse soosimisel, siis on mõistetav, et regulatsioonide, piirangute ja kontrollidega ei tohi kunagi liiga kaugele minna. Seega ei tohiks teha loataotluse protsessi ettevõtete jaoks liialt koormavaks.

Samas on aga ettevõtluse soodustamine ainult teema üks külg. Ükskõik millise sektori kuritegevuse takistamiseks tuleb siiski kasutusele võtta mõistlikud vahendid ja võimalused. Lisaks on sektori edukaks toimimiseks just ausate ettevõtjate jaoks samuti vaja probleemsete ettevõtjate turult kõrvaldamist ning nende tegevuse igakülgset takistamist. Eriti tähelepanelik tuleb aga olla just finantssektoris, kus kaalul on inimeste finantsvarad.

Autor leiab, et oluline on ka hinnata võimalikke potentsiaalseid sanktsioone, mis reegleid rikkuvaid isikud võivad tabada.

Kui juriidiline isik tegutseb tegevusloata, siis võimaldavad karistusseadustiku[156] § 372 lg 1 ja lg 3 määrata vastavale isikule tegevusloata tegutsemise eest rahalise trahvi kuni 32 000 eurot. Tegevusloa menetluse protsessis majandushaldusasutusele (antud juhul RAB) valeandmete esitamise eest võimaldavad MSÜS § 75 lg 1 ja lg 2 teha trahvi vastavalt füüsilise isikule kuni 300 trahviühikut ja juriidilisele isikule kuni 3000 eurot. Autori hinnangul on ebamõistlik, et võimalik trahv valeandmete esitamise eest on oluliselt väiksem kui loata tegutsemine. Pigem võib just esimese puhul eeldada rohkem „teadlikkust“. Seega võiks siin olla koht, kus seadusandjad võiksid kaaluda võimalike sanktsioonide karmistamist just valeandmete esitamise osas.

Analüüsides nõudeid, mida RahaPTS tegevusloa taotlejatele paneb, nähtub, et tegevusluba taotleva juriidilise isikuga seotud olulistelt isikutelt nõutakse muu hulgas karistusregistri tõendi esitamist, mis on üheks aspektiks laitmatu maine kontrollimisel. Autori hinnangul ei tee selle esitamine veel isikut „laitmatu mainega“ olevaks. Näiteks võiks siin paralleelina tuua nii-öelda „tankistid“, kes pannakse maksuvõlgadega mahajäetavate ettevõtete juhatuse liikmeteks. Kuigi enamjaolt ei ole nad kohtulikult karistatud, ei ole nad kindlasti laitmatu mainega. Autor leiab, et tõenäoliselt ei tohiks tänapäeval, kus enamik teavet inimeste kohta on internetist kättesaadav

[156] Karistusseadustik - RT I, 13.03.2019, 77

ning RAB-il on kindlasti olemas edukalt toimiv koostöö teiste Euroopa Liidu riikide sarnaste asutustega (ka AMLD-s nr.5 on toodud, et erinevate riikide RAB-id peavad tegema koostööd, muu hulgas ka liidu liikmesriikide RAB-id kolmandate riikide RAB-idega), laitmatu maine tuvastamine siiski keeruline olla.

Samas on Rahandusministeerium ja RAB saanud aru,[157] et vastavate tegevuslubade saamine on hetkel pigem liiga lihtne ning kasutusele tuleks võtta täiendavaid meetmeid. Mainitud artiklis räägiti soovist, et firmade registrijärgne asukoht ja peakontor peavad olema Eestis ja välisriigis registreeritud ettevõtja puhul tuleb siin asutada filiaal. Autori hinnangul on tegemist heade muudatustega, kuna see tekitab personaalsema vastutuse konkreetse ettevõttega seotud isikutele. Näiteks filiaali puhul vastutab filiaali juhataja isiklikult kahju eest, mida ta juhatajana põhjustas (nagu äriühingu juhatuse liige) vastavalt äriseadustiku[158] § 315 ja § 385 lg 5. Kuid autori hinnangul ei ole nimetatud muudatused piisavad, kuna probleemkohti jääb. Pigem tuleks tegevuslubade menetluse protsessis näha laiemat potentsiaalset probleemi, mis tegelikult ei piirdu ainult välisriikidest pärit isikutega, vaid on laiem, hõlmates sealhulgas ka Eesti kodanikke, kes vastavaid tegevuslube taotlevad. Nimelt võib väga tihti nii-öelda ausa ja laitmatu mainega juhatuse liikme või omaniku taga olla tegelik juht, kes aga kuskilt välja ei paista. Samas on selline probleem kestev ning sellele lahendust leida on väga raske, kuna ilma ebamõistlikult ettevõtet kontrollimata pole sellise tegeliku juhi tuvastamine ilmselt võimalik. Samuti eeldaks see ebamõistlikult suurte ressursside investeerimist loataotluse menetlemise protsessi, mis tõenäoliselt mõju omamiseks peaks oma põhjalikkuselt olema võrdne tavapärase kriminaalmenetluse läbiviimisega. See ei oleks aga mõistlik arvestades RAB-i käsutuses olevat ressurssi ning oleks ka vastuolus haldusmenetluse seaduse[159] § 5 lg 2 toodud haldusmenetluse ühe oluliseima põhimõttega, milleks on haldusmenetluse läbiviimine eesmärgipäraselt ja efektiivselt, samuti võimalikult lihtsalt ja kiirelt, vältides üleliigseid kulutusi ja ebameeldivusi isikutele. Sellest aspektist vaadates ei oleks menetluse muutmine sisuliselt jälitustegevuseks kindlasti põhjendatud.

Samas tuleb siiski rõhutada, et tavapäraselt on probleemiks hoopis see, kuidas nimetatud

[157] Vogelberg, J. (2018). Krüpto-rahapesu tõkestavad peagi karmimad seadused. Kättesaadav: https://www.aripaev.ee/uudised/2018/11/27/krupto-rahapesu-tokestavad-peagi-karmimad-seadused, 20.04.2019
[158] Äriseadustik - RT I, 28.02.2019, 10
[159] Haldusmenetluse seadus - RT I, 13.03.2019, 55

ettevõtted oma tegevuse ajal käituvad. Loataotluse protsess on kindlasti oluline, kuid nimetatud protsess seab siiski vaid raamistiku mingi tegevuse lubatavuse võimaldamiseks. Kuritegevus toimub üldiselt aga juba pärast vastavate tegevuslubade väljastamist – seda kas hooletusest või tahtlusest. Siinkohal leiab autor, et on oluline teatud määral ka hinnata tegevusloa saanud ettevõtete reaalset osalemist majanduses. Kuna Maksu- ja Tolliamet teeb kvartaalselt[160] väljavõtte kõikide ettevõtete maksulaekumistest, siis avalikke andmeid võrreldes selgus, et 800-st[161] erinevast ettevõttest kes nimetatud tegevuslube omavad on 2019. aasta esimeses kvartalis reaalselt makse tasunud vaid 45 ettevõtet kogusummas 186 914,93 eurot. See tähendab, et enamik nendest ettevõtetest vähemalt maksude tasumise mõistes tegevad ei ole, mis tekitab küsimuse nende üldises tegevuses. Samuti on oluline välja tuua, et mainitud ettevõtetest vaid 18-l oli töötajate registri kohaselt rohkem kui üks töötaja. Kuigi maksulaekumiste andmete pinnalt järelduste tegemine võib olla ennatlik ning autor nõustub, et see kindlasti ei anna täielikku pilti olukorrast, tekib siiski selle kohaselt küsimus nende ettevõtete tegevuse osas. Samuti kinnitab see seda, et tegelikkuses tegevusloa taotluse menetlusest märksa olulisem on tagada efektiivne järelevalve nimetatud tegevusloa saanud ettevõtjate üle. See on aga pigem küsimus mida AMLD nr.5 puudutas vähe.[162] Kahtlemata tekib selliseid andmeid vaadates küsimus mainitud ettevõtete reaalse tegevussuutlikuse osas – ilma töötajateta ettevõte puhul on kaheldav, kas KYC ja AML protseduure suudetakse läbi viia tasemel, mida on vaja efektiivse kontrolli teostamiseks. Probleemiks on kindlasti see, et tegevusloa taotlemine toimub üldjuhul enne vastava tegevuse algust ja hoolimata sellest millised protseduurireeglid ja sisekontrolli reeglid paigas on, ei pruugi need reaalse tegevuse ajal töötada mitmetel erinevatel põhjustel.

Autori hinnangul võiksid seadusandjad ja järelevalve teostajad kaaluda protsessi põhjalikumaks muutmiseks mõningate täienduste tegemisst tegevusloa menetlusprotsessi. Nende kaudu oleks võimalik koguda olulist taustainfot, mis suurendaks tegevusloa menetlusprotsessi tulemuslikkust. Ühe võimalusena näeb autor tegevusluba taotleva ettevõtja oluliste seotud

---

[160] Eesti Maksu- ja Tolliamet. (2019). Tasutud maksud, käive ja töötajate arv. Kättesaadav: https://www.emta.ee/et/kontaktid-ja-ametist/maksulaekumine-statistika/tasutud-maksud, 20.04.2019.

[161] See number ei lähe kokku rahakoti teenuse pakkujate krüptoraha raha vastu vahetamist võimaldavate ettevõtete hulgaga, kuna paljudel ettevõtetel tegevusload kattuvad

[162] AMLDs nr.5 küll öeldi, et liikmesriigid peavad tagama, et pädevatel asutustel on piisavad volitused, seal hulgas õigus nõuda igasugust teavet, mis on oluline kohustuste täitmise jälgimiseks ja kontrolli teostamiseks, ning piisavad rahalised ja tehnilised vahendid ning inimressursid oma ülesannete täitmiseks, kuid konkreetseid täpsemaid lahendusi ei toonud

isikute (tegelik kasusaaja, omanik, juhatuse liige, prokurist) arvelduskontode esitamise kohustuslikuks tegemist. Väga tihti on isikute arvelduskontod väga olulised indikaatorid isikute majandusliku käitumise, igapäevaste tegevuste, usaldusväärsuse ning potentsiaalsete riskide ja seoste osas. Samuti tekitaks see kogu protsessile ka suurema „sisumenetluse" tunnetuse. Lisaks ei oleks see haldusmenetluse seaduse mõistes ebamõistlikult isikuid koormav vahend, kuna tavapäraselt ei nõua isikult enda arvelduskonto hankimine ebamõistlikult palju pingutust. Samuti ei oleks vastavate arvelduskontode analüüs oluline ressursikulu ka menetlust läbiviiva asutuse jaoks. Kuigi siinkohal võib tekkida küsimus, kas tegemist on proportsionaalse meetmega, siis autori hinnangul on tegemist proportsionaalse meetmega, kuna see on vajalik kuritegevuse (rahapesu) takistamiseks.

Paralleeli võib siin tuua krediidiandjate ja -vahendajate seaduses[163] (edaspidi KAVS) toodud nõuetele olulise osa omajate kohta. KAVS § 28 jj sätestavad erinevad olulised nõuded krediidiandjates ja krediidivahendajates olulist osalust omavate isikute tausta kohta ning Finantsinspektsiooni poolt nende suhtes läbi viidava menetluse reeglid. Nimetatud menetlus eeldab põhjaliku teabe esitamist Finantsinspektisoonile, kuna krediidiandjate ja krediidivahendajate puhul on väga oluline tagada, et isikud, kes valdkonnas tegutsevad, oleksid laitmatu reputatsiooniga ning mitte ainult ei näiks korrektse taustaga, vaid seda ka reaalselt oleks. See õigustab ka Finantsinspektsiooni poolt läbi viidavat põhjalikumat kontrolli. Muu hulgas tuleb välja tuua KAVS § 31 lg 13 toodud säte, mille kohaselt olulise osa omandaja peab esitama Finantsinspektsioonile andmed ja dokumendid rahaliste ja mitterahaliste vahendite päritolu kohta, mille abil ta soetab olulise osa. Autori hinnangul on sarnaste meetmete kasutamine ka krüptorahade tegevuslubade menetlustes mõistlik lahendus, kuna ka krüptoraha valdkonnas tegutsevad tegevuslubade omajad omavad kontrolli paljude isikute vara üle. Seega peab isikute taust olema täiesti puhas.

Lisaks on autor juba eelnevas peatükis avaldanud arvamust, et kaalumise alla võiks võtta teatud finantstagatiste määramise tegevuslubade menetluses. Paralleele võiks tuua krediidiasutustele kehtivatest kapitalipuhvri nõuetest, kuid autori hinnangul ei saaks neid üks-ühele kohaldada, kuna krüptoraha sektoris on ettevõtte põhised riskid pigem suuremad (kuigi kindlasti mitte mahult), kuid samas on tegutsevad ettevõtted jälle oluliselt väiksemad võrreldes

[163] Krediidiandjate ja -vahendajate seadus - RT I, 13.03.2019, 97

krediidiasutustega. Seega võiks krediidiasutuste seaduses (edaspidi KAS)[164] toodud kapitalipuhvri nõuded väikse omakapitaliga krüptorahaga tegelevates ettevõtetes pigem oma eesmärki mitte täita. Seega võiks finantstagatis olla pigem kohustusliku vastutuskindlustuse laadne, mis peaks katma ära võimalikud kahjunõuded, mille kahju saanud kliendid esitada võivad. Autor hinnangul võiks see olla mõjus ja sobiv vahend tagamaks, et tegevuslube taotlevad juriidilised isikud on ka reaalselt motiveeritud nimetatud valdkonnaga tegelema ning neil on olemas ka finantsiline tugevus vajalikke turvameetmeid kasutusele võtta – seda nii tehnoloogilisel tasemel arvutirünnakute vältimiseks kui ka rahapesu takistamisel. See garanteeriks ka selle, et turule tuleks vähem isikuid kelle tegevuse eesmärk on problemaatiline – see lihtsustaks oluliselt järelevalveorganite tööd.

Lisaks võiks kaaluda täiendavalt finantsilise jätkusuutlikkuse kontrolli teostamist tegevuslubade taotlejatele. Selle eesmärgiks võiks olla tagada see, et ettevõtted, kes vastavaid krüptorahaga seotud teenuseid pakkuma hakkavad, on ka reaalselt valmis selliseid teenuseid edukalt pakkuma ning neil on piisavad ressursid tagamaks parimate tehnoloogiliste vahendite kasutuse ja kompetentse tööjõu – see aga omakorda oleks oluline viis kindlustamaks isikute vara kaitse ning ka selle, et turule tuldakse eesmärgiga seal reaalselt osaleda, mitte eesmärgiga olla rahapesu vahendaja. Samuti näitaks majanduslik jätkusuutlikus ka suuremat võimekust rahapesu vastu võidelda.

Alternatiivina autori ettepanekutele võib võrdlusmomendina veel välja tuua MERAS-es toodud nõuded makseteenuste ja e-raha teenuste osutajatele. Autori hinnangul võib paralleeli tuua, kuna mõlemad seadused reguleerivad tegevusloa menetlusi juriidiliste isikute osas, kelle käsutusse annavad isikud oma rahalised vahendid (lihtsalt vahendid on erinevad). Seega sõltub paljuski just tegevusloa menetlusest, et sellised load väljastataks vaid neile isikutele, kes tegutsevad heas usus ning kes ei ole probleemsed. Võrreldes kahes seaduses toodud tegevuslubade menetlemise protsessi võib öelda, et MERAS-es toodud nõuded tegevusloa saamiseks on oluliselt põhjalikumad kui seda on nõuded RahaPTS-is toodud nõuded krüptorahaga seotud tegevuslubade osas. See ei ole autori hinnangul mõistlik, kuna isikute vara on kaalul mõlemal juhul ning mõlema puhul on imperatiivne, et tegevusloa menetlemise protsessis tuvastataks kõik riskid, mis konkreetse ettevõttega seonduvad.

[164] Krediidiasutuste seadus - RT I, 13.03.2019, 98

Kui võrrelda tegevusloa saamise protsesse, siis kui RahaPTS-is toodud tegevusloa protsess on pigem formaalsete nõuete täitmine, siis MERAS-es toodud tegevusloa protsessis nõutakse tegevusloa taotlejalt muu hulgas tegevuskava, bilanssi ja kasumiaruannet, andmeid teenuste osutamiseks vajalike infotehnoloogiliste vahendite kohta, olulist osalust omavate isikute andmed (MERAS § 40 lg 12 sätestab, et füüsilisest isikust omandaja varanduslikku seisu tõendavad dokumendid tuleb esitada viimase kolme aasta kohta) ning äriühingu omavahendite suurust tõendavaid dokumente koos vandeaudiitori aruandega. Lisaks on vajalik äriplaani esitamine. Seega on autori hinnangul tegemist väga põhjaliku menetlusega, mille nõuete ülevõtmisel saaks krüptoraha tegevuslubade menetlusprotsess kindlasti oluliselt põhjalikumaks. Eriti on rõhku pandud just äriühingu finantsilise jätkusuutlikkuse ja majandusliku seisu uurimisele – see krüptorahadega seonduvate tegevuslubade menetluses tähelepanu all ei ole. Samuti toob MERAS sisse nõuded infotehnoloogiliste vahendite kohta, mis on olulised garanteerimaks kasutajate rahaliste vahendite turvalisuse. Hetkel krüptoraha tegevuslubade taotluses selliseid nõudeid ei ole, mille toomine oleks aga vajalik, kuna ebakvaliteetsete infotehnoloogilise vahendite kasutamine võib suurendada ohtu sattuda häkkerite rünnakute alla – see on aga üks algpõhjustest sellele, et toimub rahapesu.

Kuna tegelikkuses on ka Eesti Riigikohus juba mainitud otsuses 3-3-1-75-15 liigitanud krüptoraha alternatiivsete maksevahendite hulka, siis võib tegelikult tuua välja võimaluse, et Eesti võiks kaaluda lühiajaliselt krüptorahade tegevuslubade protsessi nõuete muutmist ning allutamist hoopis MERAS-ile. Selle kasuks räägib ka fakt, et MERAS toob välja mitmed muud nõuded, mis eelduslikult garanteeriks, et krüptoraha tegevuslube omaks vaid korrektse taustaga ettevõtjad/ettevõtted (näiteks nagu aktsiakapitali ja osakapitali miinimumnõuded).

Pikemas perspektiivis, nagu juba mainitud, on rahapesu näol tegemist valdkonnaga, mis ületab geograafilisi piire. Seega on rahapesuvastases võitluses edu saavutamiseks vajalik, et Euroopas oleksid harmoniseeritud reeglid ning see eeldab vastavate täiendavate nõuete väljatoomist ka direktiivis.

Kokkuvõtlikult leiab autor, et tänane tegevuslubade menetluse protsess ei ole piisavalt põhjalik ning tekitab riski, et probleemse taustaga ettevõtted saavad liiga lihtsalt sektoris tegutsemise load. Probleemse taustaga ettevõtted toovas kaasa selle, et sektoris hakkab vohama kuritegevus ning rahapesu toimepanek muutub kergeks. Seega tuleks muuta protsessi põhjalikumaks ning

selleks oli autoril kaks ettepanekut – täiendada praegust tegevusloa protsessi järgmiste nõuetega:

1) Oluliste seotud isikute arvelduskontode kontroll;
2) Finantstagatise nõue;
3) Majandusliku jätkusuutlikuse kontroll

Alternatiivina võiks aga kaaluda MERAS-es toodud tegevusloa nõuete ülevõtmist, kuna seal toodud nõuded kattuvad paljuski autori hinnanguga sellest kuidas tegevusloa protsessi peaks täiendama tagamaks, et sektor oleks kaitstud rahapesu vastu.

2.3.2. AMLD nr.5 sobivus rahapesu takistamisse hoolsuskohustuse mõistes

Teisena tuleb välja tuua hoolsuskohustus. Tegemist on sisuliselt KYC ja AML põhimõtetega. Kuigi töö keskendub rahapesu takistamisse Euroopa põhiselt, siis antud juhul toob autor välja Eesti RahaPTS-is kehtivad sätted. Seda põhjusel, et juba mainitud AMLD nr.4 tõi Euroopa Liidu liikmesriikidele ühise raamistiku finantsüsteemi rahapesuks kasutamise takistamise kohta,[165] seega on olulisemad põhimõtted harmoniseeritud. RahaPTS §19 kohaselt peab kohustatud isik kohaldama hoolsusmeetmeid järgnevatel juhtudel:[166]

1) ärisuhte loomisel;
2) ärisuhte väliselt tehingute tegemisel või vahendamisel, kui need ületavad üheaastase perioodi jooksul 15 000 eurot;
3) hoolsusmeetmete kohaldamisel kogutud teabe või dokumentide ebapiisavuse või tõelevastavuse kahtluste korral;
4) rahapesu kahtluste korral hoolimata piirsummast.

RahaPTS § 20 sätestab hoolsusmeetmed, mida tuleb kohustatud isikul kasutada.[167]

---

[165] Heckman, H. Vansimpsen, D. Dubois, T. (2017). KYC in Europe - What You Need to Know. Kättesaadav: https://b-hive.eu/news-full/2017/6/8/kyc-in-europe-what-you-need-to-know, 20.03.2019
[166] RahaPTS, *supra nota* 21
[167] *Ibid.*

1) Kliendi isikusamasuse tuvastamine ning esitatud teabe kontrollimine usaldusväärsest allikast;
2) Kliendi esindaja isikusamasuse ja esindusõiguse tuvastamine ja kontrollimine;
3) Tegeliku kasusaaja tuvastamine.

Autori hinnangul tuleks meetmete mõju tuleb hinnata erinevate rahapesu faaside kaupa.

Esimeseks takistuseks rahapesus krüptorahade kaudu ongi krüptoraha hankimine illegaalselt teenitud raha eest. See eeldab krüptoraha rahakoti olemasolu ja võimekust kanda raha tehingu eest krüptoraha müüjale.

Siinkohal hindab autor, et nimetatud hoolsuskohustuse nõuded on isegi sobivad, kuna nad kindlasti teevad rahapesu protsessi ebamugavamaks ja kulukamaks.[168] Siinkohal saab eristada kahte probleemi. Esimene neist on võimekus kanda raha krüptoraha müüjale, mis eeldab sobiva pangakonto või sarnase variandi olemasolu. Nimetatu osas ei muuda ALMD nr.5 midagi, kuna pankadele ja muudele finantsasutustele kehtisid vastavad hoolsuskohustuse nõuded juba eelnevalt. Ilmselt on viimaste aegade skandaalide valguses pangad ja muud finantsasutused hakanud nimetatud nõuete reaalsele täitmisele ka aina enam tähelepanu pöörama. Lisaks on tänasel hetkel olemas mitmeid variante kuidas osta krüptoraha ilma pangakontot üldse omamata, paljud neist variantidest ei vaja muud kui näiteks mobiiltelefoni numbrit, mille hankimine on tänapäeval imelihtne.[169] Mobiiltelefoninumbri hankimine on ka kurjategija poolt turvaline, kuna kõnekaardi kasutamisel on tema isiku tuvastamine sisuliselt võimatu.

Mis puutub krüptoraha rahakoti tegemisse kauplemisplatvormides, siis siin toimub mõnes mõttes vastupidine tavapärasele, ehk siis kui tavapäraselt on eesmärgiks teha illegaalsest rahast legaalne krüptoraha, siis kauplemisplatvormid tulevad esimeses faasis mängu pigem juhul kui tegemist on vajadusega saada lahti illegaalsest krüptorahast (näiteks võib olla toimunud häkkimine) nii-öelda legaalse raha vastu. Sellisel juhul on krüptoraha kauplemisplatvormidel

---

[168] Siinkohal peab autor vajalikus lisada, et efektiivne kuritegevuse takistamine majanduskuritegude puhul ei saa tihti olla nende täielik takistamine mis pahatihti on võimatu, vaid selle tegemine niivõrd kalliks ja ebamugavaks, et kurjategijatel ei tasu selle tegemine enam ära.

[169] How to Buy Bitcoin without a Bank Account. (2019). Kättesaadav: https://www.buybitcoinworldwide.com/buy-bitcoin-without-bank-account/, 20.03.2019

olevast hoolsusmeetmete kohustusest kindlasti kasu. Samas jääb selgusetuks, kui põhjalikku kontrolli sellised kauplemisplatvormid üldse suudavad teostada. Eespool toodud statistika selle kohta, et enamik sellistest kauplemisplatvormidest on ilma töötajateta, tähendab tõenäoliselt seda, et on raske oodata, et hoolimata näiliku sisekontrolli ja AML riskikontrolli siseeeskirjade olemasolust, neid reaalselt efektiivselt täita suudetakse, arvestades just kvaliteetse tööjõu puudust. Kindlasti eeldab efektiivne hoolsuskohustuse täitmine siinkohal ka oskust saada infot plokiahelas nähtavatest tehingutest (juhul kui tegemist on pseudonüümse krüptorahaga), mis aga omakorda eeldab teatud tehnoloogilist võimekust. On ettevõtteid nagu Chainalysis Inc, kes pakuvad küll vajalikku rahapesu tuvastamise tarkvara, kuid siiski on kaheldav, et enamik väiksemaid kauplemisplatvorme suudaksid selliseid lahendusi efektiivselt kasutusele võtta.

Teise faasi osas saab rääkida ladestamisest. Nagu mainitud toimub siin pidev raha liigutamine ühelt aadressilt teise. Siin osas tulebki kõige rohkem mängu eespool mainitud *mixers,* samamoodi ka anonüümsed krüptorahad nagu Monero. Tavapäraselt liigutatakse raha läbi nimetatud platvormide korduvalt tehes nende abil krüptoraha algne päritolu ning selle tehingute ajalugu mittetuvastatavaks või liigutatakse raha pseudonüümsest krüptorahast anonüümsesse krüptorahasse. Kuna antud tehingute jadas AMLD-s nr.5 toodud muudatused midagi ei muuda, siis siin regulatsioon rahapesu ei takista. Isik võib vabalt endale teha krüptoraha rahakoti ilma, et ta peaks ennast üheski portaalis registreerima (näiteks rahakott mis asub isiku enda arvutis) ning sinna kantakse üle juba selleks hetkeks tundmatu päritoluga krüptorahad. Samuti on isikul lähtuvalt regulatsioonist võimalik teha endale piiramatu hulk rahakotte, mille kõikide väärtus tuleks hoida alla 15 000 euro. Aga just siin jääb autori hinnangul puudu regulatsioonist mis aitaks võidelda rahapesu vastu. Võib küll rääkida sellest, et hoolsuskohustust järgiv kauplemisplatvorm peaks pöörama kohest tähelepanu kui toimub raha ülekandmine anonüümsetele kauplemisplatvormidele, kuid juba eespool toodud põhjustel on kaheldav milline on kauplemisplatvormide reaalne võimekus probleemiga tegeleda. On selge, et juhul kui krüptoraha on juba saadetud edukalt *mixers-isse* või anonüümsesse krüptorahasse, on nii kuriteo takistamine kui ka näiteks hilisem isikute süüdimõistmine väga komplitseeritud.

Kolmanda faasi osas saab rääkida integeerimisest. Nimetatud osas on pettuse ära hoidmine juba sisuliselt võimatu kuna selleks hetkeks on raha läbi erinevate anonüümsete „*mixers'ite*“ või Monero taoliste krüptorahade ära pestud. See tähendab, et krüptoraha võib hakata liigutama läbi erinevate pseudonüümsete kauplemisplatvormide või üldse vahetada krüptoraha tavaliseks rahaks ning raha algse päritolu tuvastamine on juba võimatu. Siinkohal leiab autor, et

AMLD-s nr.5 toodud regulatsioon siin kuidagi kaasa ei aita ja on kaheldav, et miski regulatsioon seda selles faasis üldse enam teha suudaks. Rahapesu takistamiseks on vaja takistada selle toimepanekut juba eelnevates faasides.

Nagu juba eelnevalt kirjeldatud, tuleb krüptoraha tehingutes rahapesu takistada faasides I ja II, kusjuures autori hinnangul on kõige kriitilisem just faas II, kuna siin on võimalik veel tehinguid takistada. Siin tekibki küsimus, kuidas efektiivselt seadusandlikul tasemel probleemile läheneda. Kuigi krüptorahaga tegelevatel ettevõtjatel on olemas hoolsuskohustus alati teavitamaks rahapesu kahtlusega tehingutest, siis autori hinnangul nimetatust ei piisa, kuna kauplemisplatvormide võimekus selliseid tehinguid tuvastada ei ole selge. Siin tuleb mängu aga eelmises peatükis kirjeldatud tegevuslubade menetlusprotsess, mis vajaks täiendamist – see peaks olema just see etapp, kus tagatakse, et sektoris tegelevad ettevõtted omaksid seda võimekust.

Potentsiaalselt kõige lihtsam variant võiks alati olla üritada midagi ära keelata – antud juhul siis eespool mainitud anonüümsed krüptorahad nagu Monero, Zcash ja Dash ning erinevad süsteemid nagu *mixers*. Autoril puudub teadmine millised oleks tehnilised võimalused selliste krüptorahade ja süsteemide keelustamiseks ning kas internetti pakkuvatel ettevõtetel oleks võimalik tehnoloogiliste vahenditega vastavatesse keskkondadesse ligipääsu takistada konkreetses piirkonnas. Ilmselt võiks lahenduseks olla see, et üks rahapesuvastase hoolsuskohustuse täitmise nõue olekski see, et vastavat tegevusluba omav kauplemisplatvorm ei tohi võimaldada tehinguid anonüümsete krüptorahadega või võimaldada oma platvormidelt *mixers'i* taolistesse süsteemidesse krüptoraha ülekandmist. Selline keeld võiks küll nii-öelda tavakasutajale (isikule kelle soov ei mitte tegeleda rahapesuga, vaid täiesti ausalt teenitud raha liikumise või päritolu mis iganes põhjusel varjamine) mõjuda pärssivalt (ning tekitada pahameelt isikute privaatsusse tungimise osas), kuid avaldaks kahtlemata mõju ka rahapesuga tegelevatele kurjategijatele. Pikas perspektiivis tooks see kaasa ka krüptoraha usaldusväärsuse kasvu, mis krüptoraha tuleviku perspektiive vaadates kahtlemata ülimalt oluline on.

Kindlasti on kogu eduka hoolsuskohustuse protsessi toimise järgimiseks tagada, et järelevalveasutused tegeleks aktiivselt ka vastavad tegevusload saanud juriidiliste isikute tegevuse monitoorimisega. Aktiivne järelevalve aitab tagada selle, et tegevusloa saanud ettevõtted oma tegevuses võimalikult hoolsad on ning kõiki seadustes toodud nõudeid täidavad.

Aktiivse monitoorimise vajadust toetab ka FATF.[170]

Samas on autoril raske vastu vaielda ka õiguskirjanduses öeldud arvamusele, et kuigi krüptorahade puhul on tegemist anonüümsuse ja detsentraliseeritusega, siis selle vastu peaks võitlema ainult niipalju, kui on vaja võitlemaks kuritegevuse vastu.[171] Ehk siis, kindlasti ei tohi lämmatada innovatsiooni ja minna regulatsiooniga liiga kaugele.

Autori hinnangul võiks hoolsuskohustuse vajalikkuse osas tuua ka järgneva näite. 06.12.2013 loodi krüptoraha dogecoin.[172] Nimetatud krüptoraha loodi naljana ning see sai oma nime tuntud interneti meemi järgi.[173] Hoolimata sellest sai dogecoin kiiresti väga populaarseks ning selle turuväärtus oli juba 2014. aasta jaanuariks tõusnud 60 miljoni dollarini. Oma väärtuse tipphetkel 2017. aasta detsembris oli kõikide dogecoinide turuväärtuseks koguni 1,956 miljardit dollarit.[174]

Autori hinnangul võiks siin olla täiendavalt koht, kus lähtuvalt kliendi kaitse eesmärgist, peaks kauplemisplatvorm kliente potentsiaalselt riskantsete tehingute tegemisel teavitama võimalikest riskidest. Ka siin võib paralleeli tuua KAS-iga, mille § 89 ja § 89[1] sätestavad kliendi kaitse põhimõtted, seal hulgas kliendi teavitamise erinevatest riskidest teatud tehingute tegemisel. Autori hinnangul oleks krüptoraha valdkonnas mõistlik see AMLD-s nr.5 välja tuua. See pakuks klientidele täiendava kaitse ning aitaks viia uuele tasemele ka kogu valdkonna usaldusväärsuse ja stabiilsuse. Kliendi kaitse, rahapesu takistamise ja kogu krüptoraha pikaajalise usaldusväärsuse saavutamise nimel peaks autori hinnangul nimetatud suutlikus kõigil kauplemisplatvormidel kohustuslik olema. Kliendi kaitse ja rahapesu takistamise kindel osa peaks olema ka see, et teatud krüptorahad tuleks kanda nii-öelda musta nimekirja ning selliseid tehinguid ei tohiks tegevuslubasid omavad ettevõtjad võimaldada.

---

[170] Financial Action Task Force. (2018). International standards on combating money laundering and the financing of terrorism & proliferation. The FATF recommendations. Kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, 10.05.2019

[171] Marian, O. (2015-2016). A Conceptual Framework for the Regulation of Cryptocurrencies, 82 University of Chicago Law Review. Dialogue. 53-68, lk.59

[172] McGuire, P. (2013). Such Weird: (The Founders of Dogecoin See the Meme Currency's Tipping Point. Kättesaadav: https://motherboard.vice.com/en_us/article/jp5x3d/dogecoins-founders-believe-in-the-power-of-meme-currencies, 19.04.2019

[173] Hutcheon, S. (2014). The rise and rise of dogecoin, the internet's hottest cryptocurrency. Kättesaadav: https://www.smh.com.au/technology/the-rise-and-rise-of-dogecoin-the-internets-hottest-cryptocurrency-20140124-31d24.html, 20.03.2019

[174] Coinmarketcap, *supra nota* 16

Kokkuvõtlikult võib öelda, et hoolsuskohustuse nõuded on sobivad vahendid rahapesu takistamiseks, kuid pigem on suurem küsimus nende järgimises – see eeldab, et sektoris tegelevad ettevõtjad omaksid ka reaalselt võimekust nõudeid järgida. Selle osas on väga olulised nii tegevuslubade menetlus, mis garanteerib tegevusluba omavate ettevõtjate kõrge taseme ning järelevalveasutuste poolt läbi viidava aktiivse sektoris tegelevate ettevõtjate monitoorimise. Aktiivne monitoorimine järelvalveasutuste poolt on seda efektiivsem ja mõjusam, mida väiksem on ettevõtete hulk, mida tuleb monitoorida. Selle osas leiab autor, et täna on Eestis erinevaid krüptoraha tegevuslubasid omavate ettevõtete hulk ebamõistlikult suur, mis teeb tulemusliku monitoorimise keeruliseks.

KOKKUVÕTE

Krüptoraha valdkond on uudne valdkond mitmete eriliste nüanssidega. Samas kaasnevad uute valdkondade toodud uuenduslikkusega tihti ka mitmed probleemid, kuna need pakuvad uusi võimalusi ka kurjategijatele. Krüptoraha valdkonnana on vaid kümneaastane, kuid tänaseks päevaks on krüptorahaga toimuv rahapesu saanud õiguskaitseorganitele juba suureks probleemiks. Kuna krüptoraha poolt pakutavad võimalused on finantsmaailmas uudsed, on see tõsiseks väljakutseks seadusandjatele ja õiguskaitseorganitele – kuidas takistada valdkonnas rahapesu, milles osas kehtivad regulatsioonid on alles väljakujunemas?

Kuigi Euroopa oli aeglasem kui Ameerika Ühendriigid krüptorahaga tehtava rahapesu vastases võitluses, võeti Euroopa tasemel 30.mail 2018 vastu AMLD nr.5. Nimetatud direktiiviga loodeti takistada krüptorahaga tehtavat rahapesu. Ometi võib niivõrd kiiresti arenevas valdkonnas probleemkohaks tihti olla see, et seadusandja poolt vastuvõetud lahendused on oma jõustumise ajaks juba ajast maha jäänud ning reaalselt kuritegevust ei takista. Sellest tulenevalt püstitaski autor töö hüpoteesiks - „AMLD nr.5 ei ole sobiv vahend tõkestamaks rahapesu krüptorahaga.“ Hüpoteesile vastuse andmise kergendamiseks püstitas autor ka kolm abistavat uurimisküsimust.

1) Millised on kõige suuremad ohud, mis kaasnevad krüptorahaga?
2) Milliseid preventiivseid meetmeid sisaldab AMLD nr.5?
3) Kas rahapesu definitsioon vajab täiendamist arvestades krüptoraha eripärasi?

Töö esimene pool keskendus krüptoraha definitsiooni selgitamisele, kus autor tuvastas, et käsitlused üle maailma eri jurisdiktsioonides on vägagi erinevad, samuti annavad krüptorahale erinevaid definitsioone erinevad organisatsioonid. Samuti tõi autor töö esimeses pooles välja olulisemad tehnoloogilised uuendused, mille krüptoraha kaasa on toonud (plokiahel ja topelt-kulutamise probleemi lahendamine). Nimetatud lahenduste võimalused võivad ulatuda kaugemale kui vaid krüptoraha. Kõige olulisema osana keskendus töö esimene osa uurimisküsimusele krüptorahaga kaasnevatest suurimatest ohtudest vastuse leidmisele. Tänasel hetkel on suurimateks ohtudeks, mis krüptorahaga seonduvad, selle volatiilsus, kasutamine kuritegevuses (eelkõige rahapesu), rünnakud krüptoraha vastu (51% rünnak näiteks) ning kauplemisplatvormide/rahakotiteenust pakkuvate ettevõtetega seonduvad ohud. Kuigi kõiki

neist ei ole võimalik regulatsioonidega täielikult ära hoida, on mõjusate regulatsioonidega võimalik neid probleeme oluliselt vähendada. Seda on ka vaja valdkonna stabiilseks ja jätkusuutlikus edasiarenguks.

Töö teises pooles uuris autor hetkel enim levinud viise krüptorahaga rahapesemisel ning hindas AMLD-s nr.5 toodud muudatuste sobivust selliste rahapesujuhtumite takistamiseks.

Autor tuvastas, et enim levinud meetodid krüptorahaga rahapesemiseks on praegusel ajal järgnevad:

1) *Mixers* - selliste teenuste abil muudetakse krüptoraha anonüümseks, kuna erinevate isikute krüptorahad segatakse kokku.
2) Anonüümsed krüptorahad nagu Monero - nende vahe tavapärase krüptorahaga on see, et detsentraliseeritud plokiahel on anonüümne, mitte pseudonüümne. Seega ei ole andmed tehingute sisu kohta kellelegi nähtavad ega kättesaadavad.
3) Krüptoraha hasartmänguleheküljed – neid kasutatakse tehingute jälgede segamiseks.

Kuna Eesti on AMLD nr.5 põhimõtted RahaPTS-i juba üle võtnud, siis sai Eesti näite põhjal paljuski anda hinnangu direktiivi mõjule ning kuna väga paljuski on raamistik Euroopas harmoniseeritud, siis võib öelda, et antud hinnang ei piirdu ainult Eestile, vaid on laiendatav kogu Euroopale. Siinkohal on ka oluline võtta arvesse, et krüptoraha kui detsentraliseeritud süsteem, omab suurepärast võimet levida üle geograafiliste piiride väga kiiresti ning odavamalt kui seda võimaldab hetke finantssüsteem tavalisel rahal. Seega eeldab sellises võitluses igasugune regulatsioonide poolt saavutatav edu seda, et need oleks võimalikult harmoniseeritud ning kurjategijatel oleks võimalikult vähe nii-öelda süsteemi nõrku kohti mida ära kasutada.

Oluline oli tuvastada, kas krüptoraha eripära võib tähendada, et rahapesu definitsioon vajab täiendamist või muutmist. Autor leidis, et AMLD-s nr.5 sätestatud rahapesu definitsiooni alla kuuluvad ka praegusel hetkel kõige levinumd rahapesu viisid. Sellest tulenevalt rahapesu definitsioon täiendamist ei vaja ning praegune regulatsioon on piisav.

Hindamaks kas eespool toodud näitete osas oleks AMLD nr.5 sobiv vahend rahapesu takistamiseks, tuli hinnata vastava direktiiviga toodud preventiivseid meetmeid, mis sellega seonduvalt krüptorahaga tegelevatele ettevõtetele laienevad. Nendeks preventiivseteks

meetmeteks on tegevusloakohustus ning hoolsuskohustus.

Tegevusloakohustus tähendab, et krüptoraha raha vastu vahetamise teenust või rahakotiteenust pakkuval ettevõtjal peab olema vastav tegevusluba RAB-ilt. Nimetatud protsessi hinnates jõudis autor seisukohale, et kuigi tegevusloa hankimise protsess on toimiv, on seal siiski puudujääke, mille likvideerimisel muutuks protsess efektiivsemaks ning tagaks, et vastavaid tegevuslube omaks sobivama taustaga ettevõtjad.

Autor pakkus välja kolm täiendust, millega võiks regulatsioone täiendada, tagamaks, et tegevusloa saanud ettevõtjate taust on kontrollitud, neid tulevikus kasutada soovivate isikute finantsvarad oleks võimalikult hästi tagatud ning rahapesuoht oleks võimalikult minimaalne. Autori hinnangul oleksid sobivateks täiendusteks:

1) Ettevõttega seotud oluliste isikute pangakontode esitamise kohustuslikuks tegemine;
2) Finantstagatise esitamine;
3) Majandusliku jätkusuutlikuse kontroll.

Alternatiivina pakkus autor välja ka selle, et võiks kaaluda tegevusloa menetluse läbiviimist MERAS-es toodud nõuetele vastavalt – seal toodud nõuded kattuvad paljuski autori täiendustega ning tänu oma põhjalikkusele suudaks samuti tagada selle, et vaid usaldusväärsed ettevõtted saavad tegevusloa. .

Nimetatud meetmed garanteeriks kehtivast regulatsioonist oluliselt paremini selle, et vastavaid teenuseid pakkuvad ettevõtjad on suutelised klientide vara kasutama, neil oleks majanduslik suutlikkus tegutseda ning hoiaks turult eemal kahtlase taustaga isikud – kõik need oleksid olulised sammud rahapesu takistamisel. Kuigi on tähtis tagada uuenduslike ideede kasutamise võimalus ettevõtjatele, siis ei tohi unustada, et vastav sektor saab areneda ja tegutseda kõige paremini siis, kui turg on puhas probleemsetest isikutest. Seega võib kokkuvõttes öelda, et tänane loataotluse protsess vajab kindlasti täiendamist. Rahapesu takistamiseks on vajalik tagada, et vastavad tegevusload oleks ainult äärmiselt usaldusväärsetel ettevõtetel, kuid tänase regulatsiooni kohaselt on tegevuslubade saamine pigem liialt kerge, mis tähendab, et tegevuslube võivad kergelt saada ka sellised ettevõtted, kelle osas eksisteerib risk rahapesu toimepanekuks.

Teiseks oluliseks muutuseks, mille AMLD nr.5 tõi, on hoolsuskohustuse normide määramine.

Nimetatud muudatusega hakkavad krüptorahaga tegelevatele ettevõtetele kehtima samasuguseid hoolsuskohustuse nõuded oma klientidega tegelemisel nagu pankadele. Siinkohal jõudis autor arusaamale, et kuigi see on õige suund kuhu liikuda ning antud lähenemise puhul on tegemist sobiva meetmega, tuleks hoolsuskohustuse nõudeid natuke siiski täiendada. Kindlasti tuleks eraldi suurt rõhku pöörata just probleemsete krüptorahadega (nagu Monero) tehtavatele tehingutele ning ka erinevatele teistele anonüümsust võimaldavate lahenduste kasutamisele. Kuna nimetatud variandid on muutunud väga problemaatilisteks rahapesu võimaldajateks krüptoraha tehingutes, tuleks kaaluda tegevusluba omavatelt krüptoraha kauplemisportaalidelt selliste tehingute tegemise mittevõimaldamist – see tuleks seada osaks hoolsuskohustusest.

Samuti leidis autor, et tänasest märksa enam tuleb keskenduda sektoris tegelevate ettevõtete aktiivsele monitoorimisele tagamaks, et AMLD-s nr.5 toodud nõudeid ka reaalselt täietakse.

Kokkuvõtlikult leidis autor, et hüpotees sai kinnituse selle osas, et AMLD nr.5 ei suuda pakutavate nõuetega täielikult katta olemasolevaid probleemkohti ning vajaks nii tegevuslubade kui ka hoolsuskohustuse osas täiendusi, kuigi problemaatilisem on kindlasti tegevuslubade menetlus. Samas on sellega tehtud esimesed olulised sammud, mis on vajalikud krüptorahaga toimuva rahapesu teatud kontrolli alla saamiseks. Seega võib öelda, et nimetatud regulatsiooni täiendamisel ja parandamisel on võimalik täna esinevaid suuremaid probleemkohti juba edukalt reguleerida. Samuti andis autor töö käigus soovitusi, milliseid lahendusi ja täiendusi võiks tegevusloamenetluses või hoolsuskohustuses juurde tuua, tagamaks, et rahapesuvastane võitlus krüptoraha tehingutes oleks võimalikult edukas.

SUMMARY

The suitability of Anti Money Laundering Directive nr.5 in combatting money laundering in cryptocurrency transactions.

Aido Ojassalu

Cryptocurrency is a field that is new and filled with various nuances. But as often is the case with new fields, though innovative, they also give new options and advantages to criminals, who can profit from them before regulations are at high enough level to stop them. Cryptocurrency is just ten years old, but money laundering using cryptocurrency has by now become a serious issue for law enforcement in various places of the world. Because the options that cryptocurrency enables are new, law makers and law enforcement are in trouble on how to best navigate the field and how to best tackle the problems in an area where regulations are still an ongoing development.

Even though Europe was slower in tackling money laundering in cryptocurrency transactions with regulations than the United States was, finally on the 30th may of 2018 AMLD nr.5 was ratified by European Parliament and Council. The aim was to stop money laundering activities from taking place using cryptocurrencies. But in a fast developing field, the issue is that often by the time a certain law can be enforced, already new methods of fraud have been developed. Due to that, the hypothesis of the masters thesis was that AMLD nr.5 is not the suitable tool to fight money laundering in cryptocurrency transactions.

To help find the answer to the hypothesis, the author put forward three research questions

1) What are the biggest dangers related to cryptocurrency?
2) What are the preventive measures put forth in AMLD nr.5?
3) Is there a need to change the definition of money laundering to suit the needs of cryptocurrency transactions?

The first part of the thesis concentrated on researching the definition of cryptocurrency, where the author discovered that in different jurisdictions, the definitions differ greatly. Also, in the first part, the author laid out the most important new technical innovations that cryptocurrency

has brought (block-chain and solution to double-spending problem). The most important part of the first part of the thesis was to discover the main dangers related to cryptocurrencies. The author discovered that those are mainly volatility of cryptocurrencies, money laundering, 51% attacks which enable hackers to take over certain cryptocurrencies (which in turn lead to criminals need to launder that those cryptocurrencies) and dangers related to storage and exchange services. Although it is not possible to completely eliminate all the dangers mentioned by developing better suited regulations (especially when it comes to voliatility), it is still possible to greatly decrease all the risks through that. Because many of those problems involve money laundering as the end result, the need for efficient and well-organized anti money laundering regulation is of essence.

In the 2nd part of the thesis, the author concentrated on finding what are the most common ways to launder money using cryptocurrencies. The discovery was that those are at the moment the use of mixers, anonymous cryptocurrencies like Monero and also cryptocurrency gambling sites. They all have the similarities of being able to hide the true path of cryptocurrency transactions, which makes it almost impossible for law enforcement to detect the people culpable.

To answer the hypothesis laid out in the introduction, the author first analysed the first preventive measure brought on by AMLD nr.5, with that being the authorisation obligation, which means that companies which provide services of exchanging a virtual currency against a fiat currency and companies which provide virtual currency wallet services, must first get an authorisation by authorities. Whilst the process works, there are, in the opinion of the author, certain improvements that could be made to make the process more detailed. Those improvements are:

1) Mandatory bank account statements from most important people involved with the company;
2) Providing a financial guarantee;
3) Economic analysis on whether the company is financially viable.

Such changes would improve the process and would mean that only the most trustworthy companies can provide services in cryptocurrency, thus decreasing the chances of money laundering greatly. Those measures would, in the opinion of the author, greatly decrease the chance that problematic companies would attempt to get such licenses or that they would

actually get such licenses. Less crime would also decrease other risks that are common with cryptocurrencies and would provide it with the stability it clearly needs to succeed long-term. Alternatively, the author proposed, that regulations from payment institutions and E-money institutions act (MERAS) could possibly be taken over to govern the authorisation process of companies asking for cryptocurrency licenses. MERAS provides quite similar demands on the authorisation process that the author proposed as improvements to current authorisation process, for example, the requirements for the companies to show economic viability. These would be effective in guaranteeing that only the serious and respectable companies get authorisation licenses.

The second important part is customer due diligence. In that regard, the author found that even though these regulations are on the right track, they still somewhat lack the decisiveness required to effectively combat money laundering. Probably the most important part to consider is that money laundering needs to be stopped in its early phases to be successful and for that to happen, the companies involved in the cryptocurrency sector, must have very exact guidelines. The biggest issue is how to handle anonymous cryptocurrencies and such service providers. In the view of the author, it should be mandatory that to fulfill customer due diligence measures, no exchange service provider should allow transactions with anonymous cryptocurrencies or cryptocurrency services such as Monero or *mixers*.

Author also found that the definition of money laundering does not need an update based on the special characteristics of a cryptocurrencies and the regulation in AMLD nr.5 covers it well.

As a result of the master's thesis, the author is of the opinion that the hypothesis is confirmed. Even though AMLD nr.5 is a good starting point for regulations, there is still a way to go to improve those regulations to a level neccesary enough to combat money-laundering effectively.

KASUTATUD ALLIKATE LOETELU

TEADUSARTIKLID

1) Alcantara, C. Dick, C. (2017) Decolonization in a Digital Age: Cryptocurrencies and Indigenous Self-Determination in Canada, 32 Canadian Journal of Law & Society. 19.

2) Brookes, A. (2018). U.S. Regulation of Blockchain Currencies: A Policy Overview, 9 American University Intellectual Property Brief 75.

3) Christopher, C.M. (2014). Whack-A-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Money Laundering, 18 Lewis & Clark Law Review. 1, 2.

4) Cvetkova, I. (2018). Cryptocurrencies Legal Regulation, 5 BRICS Law Journal. 128.

5) Engle, E. (2016). Is Bitcoin Rat Poison: Cryptocurrency, Crime, and Counterfeiting (CCC) 16 Journal of High Technology Law. 340.

6) Essaghoolian, N. (2019). Initial Coin Offerings: Emerging Technology's Fundraising Innovation, 66 UCLA Law Review. 294.

7) Finck, M. (2018). Blockchains: Regulating the Unknown. German Law Journal. 665.

8) Gamble, C. (2017). The Legality and Regulatory Challenges of Decentralised Crypto-Currency: A Western Perspective, 20 International Trade & Business Law Review.

9) Gatto, J. Broeker, E. (2015). Bitcoin and beyond: Current and Future Regulation of Virtual Currencies, 9 Ohio State Entrepreneurial Business Law Journal. 429.

10) Gerkis, J. Krikunova, S. (2014). Bitcoin and Other Virtual Currencies: Approaching U.S. Regulatory Acceptance, 39 Administrative and Regulatory Law News. 4.

11) Goforth, C. (2019). The Lawyer's Cryptionary: A Resource for Talking to Clients about Crypto-transactions, 41 Campbell Law Review. 47.

12) Grinberg, R. (2012). Bitcoin: An Innovative Alternative Digital Currency, 4 Hastings Science & Technology Law Journal. 159.

13) Hett, W. (2008). Digital Currencies and the Financing of Terrorism, 15 Richmond Journal of Law & Technology. 4.

14) Jeans, E. (2015). Funny Money or the Fall of Fiat: Bitcoin and Forward-Facing Virtual Currency Regulation, 13 Colorado Technology Law Journal. 99

15) Law, L. Sabett, S. Solinas, J. (1997). How to Make a Mint: The Cryptography of Anonymous Electronic Cash. American University Law Review 46, no.4.

16) Levi, M. Reuter, P. (2006). Money Laundering, 34 Crime & Justice. 289.

17) Lovell, A. (2018). Avoiding Liability: Changing the Regulatory Structure of Cryptocurrencies to Better Ensure Legal Use, 104 Iowa Law Review. 927.

18) Marian, O. (2013-2014). Are Cryptocurrencies Super Tax Havens, 112 Michigan Law Review First Impressions 38.

19) Marian, O. (2015-2016). A Conceptual Framework for the Regulation of Cryptocurrencies, 82 University of Chicago Law Review Dialogue 53.

20) Maume, P. Fromberger, M. (2019). Regulations of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws, 19 Chicago Journal of International Law 548.

21) McLeod, S. (2017). Bitcoin: The Utopia or Nightmare of Regulation, 9 Elon Law Review. 553

22) Nahorniak, I. Leonova, K. Skorokhod, V. (2016). Cryptocurrency in the Context of Development of Digital Single Market in European Union, 3 InterEULawEast: Journal for International and European Law, Economics and Market Integrations.

23) Piana, C. (2017). Bitcoin: An Open Source Currency and More, 9 International Free and Open Source Software Law Review. 35.

24) Pirani, A. (2018). Cryptocurrency: A Magical Bubble or the Future of Currency, 5 Court Uncourt 29.

25) Rodrigues, U. (2018). Law and the Blockchain, 104 Iowa Law Review. 679

26) Salbu, S. (1998). Who Should Govern the Internet: Monitoring and Supporting a New Frontier, 11 Harvard Journal of Law & Technology. 429

27) Sonderegger, D. (2015). A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation, 47 Washington University Journal of Law & Policy 175.

28) Tu, K. Meredith, M. (2015). Rethinking Virtual Currency Regulation in the Bitcoin Age, 90 Washington Law Review.

29) Twomey, P. (2013). Halting a Shifi in the Paradigm: The Need for Bitcoin Regulation, 16 Trinity College Law Review. 67, 75 Viidatud Brito, J. (2011). Online Cash Bitcoin Could Challenge Governments, Banks. Kättesaadav: http://techland.time.com/2011/04/16/online-cash-bitcoin-could-challenge-governments/2/

30) Urziceanu, R. (2008). Money Laundering, AGORA International Journal of Juridical Sciences. 305

31) Zaytoun, H. (2019). Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft, 97 North Carolina Law Review. 395

EESTI ÕIGUSAKTID

32) Haldusmenetluse seadus - RT I, 13.03.2019, 55

33) Karistusseadustik - RT I, 13.03.2019, 77

34) Krediidiandjate ja -vahendajate seadus - RT I, 13.03.2019, 97

35) Krediidiasutuste seadus - RT I, 13.03.2019, 98

36) Majandustegevuse seadustiku üldosa seadus - RT I, 13.03.2019, 22

37) Makseasutuste ja e-raha asutuste seadus - RT I, 13.03.2019, 23

38) Rahapesu ja terrorismi rahastamise tõkestamise seadus - RT I, 13.03.2019, 126

39) Rahvusvahelise sanktsiooni seadus - RT I, 29.06.2018, 69

40) Äriseadustik - RT I, 28.02.2019, 10

EL-I JA RAHVUSVAHELISED ÕIGUSAKTID

41) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/849, 20. mai 2015, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ (EMPs kohaldatav tekst),OJ L 141, 5.6.2015, lk. 73–117. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32015L0849

42) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/843, 30. mai 2018, millega muudetakse direktiivi (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist, ning millega muudetakse direktiive 2009/138/EÜ ja 2013/36/EL (EMPs kohaldatav tekst), OJ L 156, 19.6.2018, lk. 43–74. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32018L0843

EESTI KOHTULAHENDID

43) RKHKo 3-3-1-75-15

MUUD KOHTULAHENDID

44) Eastern District of Texas, 4:13-CV-416, SEC vs Trendon Shavers

45) United States District Court, S.D. New York, No. 14-cr-243 (JSR). USA v Robert M. FAIELLA, a/k/a "BTCKing," and Charlie Shrem

46) United States District Court, S.D. New York, No. 14–cr–68 KBF, United States v. Ulbricht

47) EKo 22.10.2015, C-264/14 Skatteverket versus David Hedqvist

48) UNITED STATES DISTRICT COURT EASTERN DISTRICT OF NEW YORK, 18-CV-361, CFTC vs Patrick K. McDonnell & Coin Drop Markets

MUUD ALLIKAD

49) 4th Money Laundering Directive – What you need to know. (2017). Kättesaadav: https://vinciworks.com/blog/4th-money-laundering-directive-what-you-need-to-know/

50) A Complete List of Bitcoin Friendly Countries. (2019). Kättesaadav: https://99bitcoins.com/bitcoin-friendly-countries/

51) About Monero. A Brief History. (2019). Kättesaadav: https://www.getmonero.org/resources/about/

52) Adkisson, J. (2018). The Great Cryptocurrency Scam. Kättesaadav: https://www.forbes.com/sites/jayadkisson/2018/11/20/the-great-cryptocurrency-scam/#66ba11fa359f

53) Ahmeddirar. (2019). Top 6 Best Cryptocurrency Wallets 2019, Everything You Need To know. Kättesaadav: https://ripplecoinnews.com/top-5-best-cryptocurrency-wallets

54) Arroyo, C. (2017). Holding Cryptocurrency—The Real Risks. Kättesaadav: https://hackernoon.com/holding-cryptocurrency-the-real-risks-3c54ca8d73b6

55) Bank Secrecy Act/ Anti-Money Laundering Examination Manual. (2010). kättesaadav: https://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2010.pdf

56) Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies. (2014). Kättesaadav: https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf

57) Bigmore, R. (2018). A decade of cryptocurrency: from bitcoin to mining chips. Kättesaadav: https://www.telegraph.co.uk/technology/digital-money/the-history-of-cryptocurrency/

58) Bitcoin & Crypto Casinos. (2019). Kättesaadav: https://coinclarity.com/casinos/

59) Bitcoin's Mathematical Problem. Kättesaadav: https://blog.programster.org/bitcoins-mathematical-problem

60) Breyer, J. (2017). Dissenting. Kättesaadav: https://www.supremecourt.gov/opinions/17pdf/17-530_6537.pdf

61) Canellis, D. (2019). 76% of laundered cryptocurrency was washed with an exchange service. Kättesaadav: https://thenextweb.com/hardfork/2019/01/29/cryptocurrency-laundering-chainalysis/

62) Cases of money laundering linked to cryptocurrency in Japan up tenfold in 2018. (2019). Kättesaadav: https://www.japantimes.co.jp/news/2019/02/28/national/crime-legal/cases-money-laundering-linked-cryptocurrency-japan-tenfold-2018/#.XIZS7fZuJPY

63) Castillo, M. (2018). The Founder Of Bitcoin Pizza Day Is Celebrating Today In The Perfect Way. Kättesaadav: https://www.forbes.com/sites/michaeldelcastillo/2018/05/22/the-founder-of-bitcoin-pizza-day-is-celebrating-today-in-the-perfect-way/#1da250bd5d9c

64) Chaum, D. (1982). Untraceable Electronic Cash. Kättesaadav: http://blog.koehntopp.de/uploads/chaum_fiat_naor_ecash.pdf

65) Chen, J. (2019). Fiat Money. Kättesaadav: https://www.investopedia.com/terms/f/fiatmoney.asp

66) Coinmarketcap. Kättesaadav: https://coinmarketcap.com/

67) Counting the cost of money laundering. (2018). Kättesaadav: https://www.independent.co.uk/news/business/news/counting-the-cost-of-money-laundering-a8122916.html

68) Copeland, T. (2019). Barbarians at the altcoin gates. Kättesaadav: https://decryptmedia.com/4408/cryptocurrencies-protect-51-attacks

69) Cryptocurrency Anti-Money Laundering Report, 2018 Q4. (2019). Kättesaadav: https://ciphertrace.com/wp-content/uploads/2019/01/crypto_aml_report_2018q4.pdf

70) Davis, J. (2011). The Crypto-Currency. Kättesaadav: https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

71) Detwiler, P. (2016). Mining Bitcoins Is A Surprisingly Energy-Intensive Endeavor. Kättesaadav: https://www.forbes.com/sites/peterdetwiler/2016/07/21/mining-bitcoins-is-a-surprisingly-energy-intensive-endeavor/#708da0ff5bbf

72) Dickson, B. (2018). Everything you need to know about bitcoin wallets. Kättesaadav: https://www.dailydot.com/debug/bitcoin-wallets-cryptocurrency-hardware/

73) Dumont, M. (2018). Bitcoin And Monero Used To Launder $89M: Investigation. Kättesaadav: https://cryptodaily.co.uk/2018/09/bitcoin-monero-money-laundering/

74) Eesti Maksu- ja Tolliamet. Tasutud maksud, käive ja töötajate arv. (2019). Kättesaadav: https://www.emta.ee/et/kontaktid-ja-ametist/maksulaekumine-statistika/tasutud-maksud

75) Eesti Statistikaamet. (2019). Riigieelarve tulud ja kulud, aasta. Kättesaadav: https://www.stat.ee/53713

76) European Central Bank. (2012). Virtual currency schemes. Kättesaadav: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

77) Financial Action Task Force. (2014). Virtual Currencies Key Definitions and Potential AML/CFT Risk. Kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

78) Finantsinspektsioon. (2018). Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks.“ Kättesaadav: https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf

79) Frankenfield, J. (2019). Cryptocurrency. Kättesaadav: https://www.investopedia.com/terms/c/cryptocurrency.asp

80) Greenberg, A. (2017). Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire. Kättesaadav: https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/

81) Habermeier, K. (2016). Virtual Currencies and Beyond: Initial Considerations. Kättesaadav: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

82) Heckman, H. Vansimpsen, D. Dubois, T. (2017). KYC in Europe - What You Need to Know. Kättesaadav: https://b-hive.eu/news-full/2017/6/8/kyc-in-europe-what-you-need-to-know,

83) Hertig, A. (2018). Blockchain's Once-Feared 51% Attack Is Now Becoming Regular. Kättesaadav: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular

84) How Does a Blockchain Prevent Double-Spending of Bitcoins? (2018). Kättesaadav: https://medium.com/innerquest-online/how-does-a-blockchain-prevent-double-spending-of-bitcoins-fa0ecf9849f7

85) How to Buy Bitcoin without a Bank Account. (2019). Kättesaadav: https://www.buybitcoinworldwide.com/buy-bitcoin-without-bank-account,

86) How to use a Bitcoin mixer or tumbler. Kättesaadav: http://cryptorials.io/use-bitcoin-mixer-tumbler

87) Hutcheon, S. (2014). The rise and rise of dogecoin, the internet's hottest cryptocurrency. Kättesaadav: https://www.smh.com.au/technology/the-rise-and-rise-of-dogecoin-the-internets-hottest-cryptocurrency-20140124-31d24.html

88) Financial Action Task Force. (2018). International standards on combating money laundering and the financing of terrorism & proliferation. The FATF recommendations. Kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

89) It now costs more to make bitcoin than the cryptocurrency is worth. (2019). Kättesaadav: https://www.newscientist.com/article/mg24132162-900-it-now-costs-more-to-make-bitcoin-than-the-cryptocurrency-is-worth/?fbclid=IwAR09n-d1ub6z5LxoWViFRzLeN1pzCsFGABsFDJgtQ_Y4R2bYyCj-K7TEM08

90) LetKnowNews. (2018). 5 Types of Cryptocurrency Wallets and Their Pros & Cons. Kättesaadav: https://medium.com/letknownews/5-types-of-cryptocurrency-wallets-and-their-pros-cons-4215fdf59324

91) Library of Congress. (2018). Regulation of Cryptocurrency Around the World. Kättesaadav: https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

92) Library of Congress. (2019). Legal Status of Cryptocurrencies. Kättesaadav: https://www.loc.gov/law/help/cryptocurrency/map1.pdf

93) Majandustegevuse register, kättesaadav: https://mtr.mkm.ee./tegevusluba?m=97

94) McGuire, P. (2013). Such Weird: The Founders of Dogecoin See the Meme Currency's Tipping Point. Kättesaadav: https://motherboard.vice.com/en_us/article/jp5x3d/dogecoins-founders-believe-in-the-power-of-meme-currencies

95) Mis on kaevandamine? Kättesaadav: http://www.kryptoraha.ee/kaevandamine/

96) Mis on krüptoraha. Kättesaadav: http://www.kryptoraha.ee/tehnoloogia/

97) Mixers, Tumblers, Foggers. Kättesaadav: https://ciphertrace.com/glossary/mixer-tumbler-fogger

98) Monaghan, A. (2017). Bitcoin is a fraud that will blow up, says JP Morgan boss. Kättesaadav: https://www.theguardian.com/technology/2017/sep/13/bitcoin-fraud-jp-morgan-cryptocurrency-drug-dealers

99) Money-Laundering and Globalization. Kättesaadav: https://www.unodc.org/unodc/en/money-laundering/globalization.html

100) Morel, T. (2016). Rahapesu Bitcoin'idega. (Magistritöö). TÜ Õigusteaduskond. Tallinn.

101) Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Kättesaadav: https://bitcoin.org/bitcoin.pdf

102) Natarjan, H. Krause, S. Gradstein, H. (2017). Distributed Ledger Technology (DLT) and Blockchain. Kättesaadav: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

103) Notice 2014-21. Kättesaadav: https://www.irs.gov/pub/irs-drop/n-14-21.pdf

104) O'Driscoll, A. (2018). Monero vs zcash vs dash: which is the most anonymous cryptocurrency? Kättesaadav: https://www.comparitech.com/crypto/anonymous-cryptocurrency-monerto-zcash/, 20.04.2019

105) Peterson, A. (2014). Hal Finney received the first Bitcoin transaction. Here's how he describes it. Kättesaadav: https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/?noredirect=on&utm_term=.9c565c311cff

106) Pitta, J. (1999). Requiem for a Bright Idea. Kättesaadav: https://www.forbes.com/forbes/1999/1101/6411390a.html#7a463e03715f

107) Quenstion, A. (2016). The Biggest Bitcoin Hacks and Thefts of All Time. Kättesaadav: https://hacked.com/biggest-bitcoin-hacks-thefts-time/

108) Rahandusministeerium. (2016). Analüüs virtuaalvääringute võimaliku tunnustamise ja kasutamise poliitika väljatöötamiseks. Kättesaadav: https://www.rahandusministeerium.ee/et/system/files_force/document_files/2016-vv_virtuaalvaaringute_analuus-22-07.pdf

109) Robinson, T. (2018). 5th AML Directive: EU Regulation of Cryptocurrency Businesses. Kättesaadav: https://www.elliptic.co/our-thinking/5th-aml-directive-eu-regulation-cryptocurrency

110) Schwartzkopff, F. (2019). Contagion From Danske Case Feeds a New Fear in Borderless EU. Kättesaadav: https://www.bloomberg.com/news/articles/2019-03-10/danske-laundering-contagion-feeds-a-new-fear-in-borderless-eu

111) Silva, S. (2018). Criminals hide 'billions' in crypto-cash - Europol. Kättesaadav: https://www.bbc.com/news/technology-43025787

112) The Money-Laundering Cycle. Kättesaadav: https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html

113) Top 10 expert's criticisms on Bitcoin and other cryptocurrencies. (2017). Kättesaadav: https://coinpedia.org/information/experts-criticisms-bitcoin-cryptocurrencies/

114) Total Number of Transactions. (2019). Kättesaadav: https://www.blockchain.com/charts/n-transactions-total

115) Ullman, K. Demchuk, N. (2018). Virtuaalvääringu tegevusload Eestis Kättesaadav: https://www.rmp.ee/uudised/juhile/virtuaalvaaringu-tegevusload-eestis

116) Virunurm, K. (2018). RIA krüptouuring – ID-kaart ja plokiahelad. Kättesaadav: https://blog.ria.ee/tag/kruptograafia

117) Vogelberg, J. (2018). Krüpto-rahapesu tõkestavad peagi karmimad seadused. Kättesaadav: https://www.aripaev.ee/uudised/2018/11/27/krupto-rahapesu-tokestavad-peagi-karmimad-seadused

118) What is Bitcoin Mining and is it Profitable? Kättesaadav: https://99bitcoins.com/bitcoin-mining/

119) Who is the real Satoshi Nakamoto? (2018). Kättesaadav: https://medium.com/@cryptaldashcoin/who-is-the-real-satoshi-nakamoto-55bacbbee566

120) Who or What Can Put an End to Bitcoin? (2018). Kättesaadav: https://www.ccn.com/guest- spot-who-or-what-can-put-an-end-to-bitcoin