TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse instituut

Triin Pilberg

KRÜPTOVALUUTA KARISTUSÕIGUSES

Magistritöö

Juhendaja
MA Andres Parmas

Tallinn
2021

Sisukord

Sissejuhatus

Lawrence Lessig tuli juba 2000 aastal oma essees välja mõttega „kood on seadus“ (*„code is law“*). Ta leidis, et igal ajastul on oma reguleeriv asutus ja meie ajastul on selleks küberruum. Ka sellel oma regulaator aga kuna inimesed on nii keskendunud vabanemisest riigi võimu alt, ei nähta, kuidas ka küberruum meie vabaduste jaoks oht on. Küberruumi kontrollib kood, mis seab reeglid ja tingimused, kuidas saab seda kasutada, millele ja kui vabalt juurde pääseb. Lessig leidis, et kood on ajas muutumas ja kui me ei suuda mõista, kuidas see hakkab mõjutama meie põhiseadusest tulenevaid õigusi, jääme nendest ilma ja seda hakkab asendama kood ise. Kes aga tegelikult koodi arhitektuuri taga on ja seda suunab, pole teada.[1] Tänapäeval tõlgendatakse seda mõtet pigem, et kui tarkvarakood mingi tegevuse kinnitab, siis see on lubatud. Plokiahelaga lähedalt seotud inimesed arvavad, et tulevikus hakkab koos asendama seadust. Õigusteadlased sellega ei nõustu ja leiavad, et seadus on alati koodist ülim.

Küberruum, tarkavarakoodid ja plokiahelad on meie tänapäeva maailmas üha suurema kaaluga ja igapäeva eluga aina tihedamalt seotud. See on olnud tehnoloogia arengu ja selle poolt suuremate ning globaalsemate võimaluste pakkumise tõttu loogiline areng. Üheks meie sajandi leiutiseks on olnud plokiahel oma võimekuse, sõltumatuse ja algoritmide keerukusega, mida loodetakse tulevikus üha laialdasemalt kasutada. Plokiahel lõi krüptovaluuta, ehk siis varalist väärtust omava koodide rea, mis on sama moodi tänaseks päevaks väga laialdaselt levinud ja mille väärtuse kõikumistel hoiab suur osa inimkonnast silmas peal, sest see on uudne ja põnev aga peamiselt seetõttu, et võimalus krüptovaluuta pealt rahaliselt teenida on väga suured.

Krüptovaluuta atraktiivsus ja samal ajal selle uudsus on tekitanud ka probleeme. Algoritmidel, millel krüptoraha põhineb, on küberruumis endas kokku lepitud nii öelda seadused, millest kõigil osalistel tuleb kinni pidada, et süsteem toimiks ja kõik see töötab vastastikusel usaldusel. Füüsilisesse maailma need kokkulepped aga üle ei kandu ja õiguslikult on krüptovaluuta suhteliselt reguleerimata. Kuna krüptoraha on oma olemuselt palju anonüümsem kui üldiselt tunnustatud valuutad, siis kasutatakse seda väga aktiivselt kuritegelikus maailmas illegaalsel teel saadud tulude varjamiseks ning oma tegevuseks vajalike teenuste ning vahendite eest tasumisel. Samal ajal rünnatakse ka krüptovaluutat ennast. Häkkimise või pahavara kasutamise teel saadakse juurdepääs arvutitesse ja seejärel isikute krüptoraha kaitsevahenditele, mis annavad ligipääsu krüptorahale ja võimaluse see endale kanda. Samuti rünnatakse rahakoti

[1] Lessig, E., *Code Is Law. On Liberty in Cyberspace*, Harvard Magazine, 01/2020.

teenusepakkujaid, kus krüptorahad asuvad ja tehakse tühjaks tuhandeid rahakotte. Selliste krüptovaluuta omastamise puhul on kannatanuteks isikud, kes sellega on kaotanud oma rahalist väärtust omavat vara.

Teema aktuaalsus seisneb üha rohkem levinud plokiahela tehnoloogia kasutamises. Kõige tuntum krüptovaluuta on Bitcoin, kuid tegelikult on selle kõrval veel tuhandeid alternatiivseid plokiahela lahendusi kasutavaid valuutasid. Krüptovaluutad oma olemuselt on äärmiselt kõikuva väärtusega, hind võib muutuda mõne päevaga mitme tuhande euro võrra. Kogu turg meenutab mõnes mõttes börsi, kus hinnad on mõjutatud firmadega seotud muudatustest või majandusuudistest. Sama moodi on ka krüptovaluuta puhul, kui on kuulda, et keegi investeerib Bitcoini, viib see kiirelt hinnad lakke. Seda oli näha ka veel sel aastal, kui Elon Musk otsustas osta suures koguses bitcoine, uudise järgselt tõusis mõneks ajaks Bitcoini väärtus 20%. küll aga langeb hind, kui tuleb teave mõnest uuest häkist näiteks rahakotiteenuse pakkuja vastu. Suurte teenimisvõimaluste tõttu on see maailm inimeste jaoks ahvatlev, sinna suunatakse üha enam raha ja seda soovivad ka ära kasutada kurjategijad. Alles hiljuti tuli uudis, kus Türgis pani kauplemisplatvormi omanik toime 2 miljardi dollari suuruse pettuse.[2] Üha suureneva populaarsuse tõttu on krüptovaluutad ka suuremas ohus kurjategijate poolsetele rünnetele, kuid üldiselt on õiguskaitseorganite käed on lühikesed varade tagasi saamiseks ja kurjategijate kindlaks tegemiseks. Sellelaadsete rünnakute uurimiseks on vaja väga head krüptomaailmast arusaamist, aega ja ressursse. Samuti ei ole suudetud seadusandlikult kõiki aspekte reguleerida.

Uurimiseesmärgiks on magistritöös analüüsida krüptovaluuta sobituvust Eesti karistusõiguslikku süsteemi arvestades selle uudsust, kiiret arengut, selle mitte kvalifitseerumist tunnustatud raha tüübina ja rahvusvahelise üldise regulatsiooni puudumist aga samal ajal soovi selle poole liikuda. Käesoleva töö eesmärgiks on uurida ja leida vastus järgmistele probleemküsimustele:

- Kas arvestades krüptovaluuta eriomadusi on võimalike rünnete puhul omaniku õigused Eestis karistusõiguslikult kaitstud?
- Kas karistusõiguslik regulatsioon krüptovaluutadega seonduvalt on Eestis piisav, kui ei, siis millises valdkonnas oleks vaja õiguslikku arengut?

[2] *Türgis toimus kahe miljardi dollari suurune krüptorahapettus*, ERR, 23.04.2021. https://www.err.ee/1608188698/turgis-toimus-kahe-miljardi-dollari-suurune-kruptorahapettus

Tulenevalt autori teadmistest Eesti karistusõigusest ja krüptovaluutast on magistritöö hüpoteesiks, et Eesti karistusõigus ei hõlma kõiki krüptovaluutadega seonduvate kuritegude kvalifitseerimiseks vajalikke koosseise, et oleks tagatud kuritegudega kahjustatud isikute õiguste kaitse.

Töö esimeses peatükis avatakse krüptovaluutade olemus ja kuidas need tehniliselt toimivad, millega need tagatud on ning millised on süsteemiga seotud teenustepakkujad. Kuna krüptoraha süsteem riigipiire ei tunne ja on globaalselt kasutatav, annab autor ülevaate, kuidas erinevad finantssektori asutused ja pangad seni seda defineerinud ning käsitlenud on. Samuti, kuidas seda on teinud erinevad maailma riigid, kui rangelt või vastupidi liberaalselt, oma regulatsioonides kohaldanud. Seejärel tuuakse konkreetsemalt välja, mida arvab krüptovaluutast Eesti pangandus- ja finantssektor ning kuidas ja mis on seadustes peetud võimalikuks paika panna. Samuti seda, mida nähakse ette, et on probleemid, mida tulevikus adresseerima peaks.

Töö teises peatükis tuuakse välja kõik krüptovaluutaga seonduvad riskid, millega selle kasutajad võivad silmitsi seista. Riskide puhul tuuakse konkreetseid elulisi näiteid, kus on tihtilugu olnud suured varalised kahjud, ning millised on selliste juhtumite puhul süsteemi kitsaskohad. Analüüsitakse rahapesu ja erinevate pettustega, ka ICOdega, seotud riske ning seda, millist rolli mängivad skeemides krüptovaluutad ja miks kurjategijad on vahendina valinud just krüptoraha. Rünnete sihtmärgiks on tihtipeale ka vahendusplatvormid, milliseid ründeid on toime pandud nii rahvusvahelisel tasandil kui Eestis. Avatakse ka krüptovaluutade pseudo-anonüümsusega seotud probleeme, mis on üks omadustest, miks need üldse loodi aga samal ajal on uurimisasutuse jaoks suureks probleemiks, kui proovitakse kahjustatud isikute õigusi kaitsta.

Kolmandas jaos uuritakse, milline on Eesti karistusseaduslikult krüptovaluuta puhul kaitstav õigushüve ja kuidas see eelpool analüüsitud iseloomulikke tunnuseid arvestades õigussüsteemi koosseisutunnuste järgi erinevate kvalifikatsioonide alla käib. Analüüsitakse erinevaid võimalikke käsitlusi ning millised Samuti tuuakse välja senised Eesti õigussüsteemi kokkupuuted küberkuritegevusega, mis on mingil moel krüptovaluutaga seotud. Eraldi peatutakse omandil ja selle vastu toime pandavatel tegudel ning kuidas peaks näiteks privaatvõtit ja krüptovaluutat ennast välja toodud koosseisude puhul käsitlema. Samamoodi

avatakse arvutisüsteemidega seotud koosseisud ning seda, kas ja millisel moel plokiahelat saab pidada arvutisüsteemiks või arvutiandmeteks.

Allikatena on kasutatud rahvusvaheliste ja Eesti finantsorganisatsioonide välja andud hinnanguid, hoiatusi ja arvamusi (sh ESMA, FAFT, EBA, Rahandusministeerium), Europoli riskianalüüse ja kokkuvõtteid küberkuritegevusega seotult, Eesti ja Euroopa Liidu õigusakte ja õigusalast kirjandust ja teadusartikleid. Samuti on kasutatud nii Eesti kui välisriikide uudiste artikleid ning krüptovaluutaga tegelevate interneti lehekülgedel avaldatud teavet või statistikat. Viimast on kasutatud just põhjusel, et kõik kasutatav info oleks võimalikult päevakajaline. Krüptovaluutasse puutuv on nii uudne ning igapäevaselt muutuv ning sellega seotult pole veel ka liiga palju teaduslikke artikleid ning uurimusi avaldatud.

Varasemalt on Tartu Ülikoolis krüptovaluutadega seotud teemasid magistritöödes uuritud kahel korral. Töös „Krüptorahade käibemaksu regulatsioon“ (Kuusemäe, K., 2015), kus leitakse, et bitcoini puhul on tegemist maksevahendiga finantsturu mõttes ja sellega kauplemisel tekkiv käive on maksuvaba käive, kuid käibemaksu objektiks võivad olla tehingu sooritamiseks vajalikud teenused ning kauplemisel tekkiv käive. Samuti on kirjutatud töö teemal „Krüptoraha platvormi kasutaja õiguste kaitse tagamine“ (Viikoja, S., 2019), milles jõuti järeldusele, et kuna platvormipidaja ja platvormi kasutaja vahelisele suhtele kohaldusid sellel hetkel vaid eraõiguslikud sätted, ei paku need teenuse omapära arvestades kasutajale piisavalt õiguslikku kaitset. Samuti kinnitati püstitatud väidet, et investorikaitse meetmeid ei saa laiendada krüptoraha platvormi kasutajale, kuna seal osutatavad teenused ei allu finantsturgude normidele.

Magistritöös on kasutatud teoreetilist meetodit, mille puhul on kasutatud induktiivset ja kvalitatiivset uurimismeetodit, et allikates toodud seisukohti läbi töötada ning nendest tulenevalt oma järeldusteni jõuda. Antud töö puhul on sisu-ja vorminõudeid järgitud vastavalt Tartu Ülikooli Õigusteaduskonna professorite J. Sootak ja H. Siimets-Gross koostatud üliõpilastööde kirjutamise ja vormistamise juhendit järgides (Juura, Tallinn 2020).

Käesoleva töö puhul on kõige iseloomustavamad märksõnad Eesti märksõnastikust: krüptoraha, karistusõigus, kuritegevus, küberkuriteod.

1. Krüptovaluuta olemus

Krüptovaluuta (*cryptocurrency*) loodi eesmärgil, et riik ei saaks inimese rahakasutust jälgida. Krüpto tuleneb kreeka keelsest sõnast *kruptós*, mis tähendab peidetud või salajane. Pärast 2008 aastal aset leidnud majanduskrahhi oli inimeste usaldus riigi ja pankade vastu suurel määral vähenenud ja oldi vastuvõtlikud uutele alternatiivsetele võimalustele oma raha hoida ja kasutada. 2009. aastal lõi tundmatu inimene või ühendus, kes kannab pseudonüümi Satoshi Nakamoto, esimese krüptoraha Bitcoini, mis oma olemuselt pidi olema sama anonüümne ja vabalt kasutatav kui sularaha. Võttes arvesse maailmas valitsevat olukorda oli Bitcoinil suur populaarsus ja selle väärtus hakkas kiirelt kasvama. Satoshi Nakamoto lahendas oma leiutatud plokiahelaga (*blockchain*) arvutiteaduses tuntud nn Bütsantsi väejuhi probleemi. Allegooriliselt seisnes probleem selles, et kui mitu eraldiseisvat väeüksust varitsevad ühte linna, saavad väejuhid omavahel suhelda võimalikust taktikast või ründehetkest vaid käskjalgade kaudu. See tekitab aga probleemi, et kas informatsioon üldse kohale jõuab, milles ei saa kunagi kindel olla, ega ei ole reetureid, kes vahepeal informatsiooniga manipuleeriks ja kas teine väejuht väljakäidud taktikaga üldse kaasa tuleb. Plokiahelaga aga loodi süsteem, mis iseennast kontrollib ja valeinformatsiooni võimaluse välistab.[3]

Plokiahel on kokkuvõtvalt andmestruktuuri eriliik muudatuste tõkestamiseks, mida kasutatakse mõningates hajusraamatute tehnoloogiates (*distributed ledger technology* ehk DLT). Hajusraamat on viis, kuidas salvestada ja jagada andmeid üle mitmete arvestusraamatute (*ledgers*). Seega on tehingud hajutatud üle andmebaasi, ilma kindlat asukohta omamata, hoides koopiaid paljusid arvuteid ühendavas võrgus. Igal arvestusraamatul on täpselt samad andmed, mida koos ülal peetakse ja kontrollitakse arvutiserverite võrgu poolt, mida kutsutakse halduriteks (*nodes*). Plokiahelad hoiavad ja edastavad andmeid plokkides ja on üksteisega seotud digitaalse ahelana.[4]

Hajusraamatud jagunevad omakorda loalisteks ja loatuteks. Loaliste hajusraamatute puhul on teenusepakkujad fikseeritud ja tegutsetakse lepingu või õigusakti alusel. Loatute puhul aga ei ole teenusepakkujad fikseeritud ja igaüks võib hakata teenuse halduriks. Viimast hajusraamatu liiki kasutavad ka enamik krüptoraha süsteemid.[5]

---

[3] Redman, J., *Triple-Entry Bookkeeping: How Satoshi Nakamoto Solved the Byzantine Generals' Problem*, Bitcoin.com, 2.02.2020. https://news.bitcoin.com/triple-entry-bookkeeping-how-satoshi-nakamoto-solved-the-byzantine-generals-problem/

[4] World Bank Group. Distributed Ledger Technology (DLT) and Blockchain, lk 1.

[5] Krüptograafiliste algoritmide elutsükli uuring 2017, versioon 2.0, 09.02.2018, lk 16.

Plokiahela esmaseid eesmärke oli ära kaotada keskne osapool, näiteks pank või riik, et kindlustada omand konto ja seal oleva summa üle. Hajusraamat annabki krüptoraha mõttes selleks krüptograafilise võimaluse, luues süsteemi detsentraliseeritud arvestusraamatutest, mida haldab anonüümsete osalejate võrgustik, ilma, et peaks ühtegi institutsiooni usaldama.[6] Keegi konkreetset kontrolli teostada ei saa, süsteemil pole reegleid ega seaduseid, vaid kontrollib iseennast vastavalt kokkulepitule. Sellist keskse serverita süsteemi nimetatakse detsentraliseerituks.

Plokiahel ise kasutab krüptograafiat ja matemaatilisi algoritme, et muuta informatsioon kolmandate osapoolte jaoks loetamatuks ning luua ja kontrollida pidevalt kasvavat andmestruktuuri. Haldurites luuakse uus andmeplokk, mille informatsioon muutub krüpteeritud andmetena avalikuks ja seejärel kontrollivad haldurid plokki vastavalt eelmistele algoritmidele. Kui kõik haldurid on uue ploki kinnitanud, lisatakse see arvestusraamatusse, nö plokiahelasse.[7] Juba plokiahelas olevaid andmeid niisama lihtsalt muuta ega kustutada ei saa. Muudatuste või kustutamise korral on reegleid rikkunud haldur või häire tuvastatav. Seetõttu on plokiahelasse keeruline sisse häkkida, kuid see ei ole kindlasti võimatu. Haldur ise on tegelikult serveri või plokiahela hoiustamise seade, mis hoiab töös klientide tarkvara, uurib iga tehingu informatsiooni ja kogu plokiahelat, tagamaks protokolli järgimise. Kõik tehingud, mis protokolli ei järgi, lükatakse tagasi.

Uusi valuutaühikuid kaevandatakse (*mining*) ja emiteeritakse pidevalt juurde, see on protsess, mille käigus ülekanded kinnitatakse, kasutades selleks spetsiaalseid protsessoreid. Inimesed, kes sellega tegelevad on kaevurid (*miners*), kellel peab olema pidevalt ligipääs kõigile haldurites olevatele andmetele, et oma ülesannet täita. Nad võivad omakorda üles seada ka enda haldurid ja enamik seda ka teeb. Läbi kaevandamise teenitakse krüptoraha, millega saavad iga valideeritud tehingu eest tasustatud ka kaevurid ise. Krüptoraha ennast luuakse samuti kaevandamise kaudu, mis seisneb selles, et võimsad arvutid üle maailma lahendavad keerulisi matemaatilisi probleeme. Plokiahela süsteem tugineb konsensuse mehhanismil, millega on kõik haldurid nõustunud ja mis tähendab teatud valideerimise metoodikat, mis kindlustab tehingute korrektse järjestuse. Krüptoraha puhul aitab see ära hoida nö topelt-kulutamist, et ühte vahendit ei kantaks üle mitmeid kordi, kuna ülekanded ei ole registreeritud ja keskselt kontrollitud. Krüptoraha puhul kasutatakse üldiselt töötõenduse (*Proof of Work*) süsteemi, mis on ka ülalpool

[6] World Bank Group. Distributed Ledger Technology (DLT) and Blockchain, lk 3.
[7] *Ibidem*, lk 1.

kirjeldatud, ehk süsteemi, kus kaevurid peavad lahendama krüptograafilisi valemeid, et saaks moodustada uue lüli plokiahelasse. Kuna iga uus nö mõistatus on seotud eelneva plokiahelaga, muutub see aina pikemaks ning keerulisemaks ja selleks on vaja suurt hulka andmetöötlusressursse. Näiteks Bitcoini puhul tekib üldjuhul uus töötõendus iga 10 minuti järel ja juhul kui neid luuakse samaaegselt mitu, võetakse vastu see, mis on keerulisem. Kogu töötõenduse süsteem ja suur loatu süsteem on plokiahela turvalisuse kesksekteks osadeks. Turvalisus on otseselt seotud suure hulga halduritega, kes kontrollivad süsteemi vastavalt konsensusprotsessile, et kindlustada andmete järjepidevus.[8]

Haldurid allkirjastavad plokid digitaalselt ja igale plokile luuakse kaks võtit, mille kaudu seotakse algne saatja antud sisuga. Esimene, avalik võti on sarnane digitaalse allkirjaga, mida ka Eestis laialdaselt kasutatakse – kõigile nähtav ja mille kaudu identifitseeritakse nii digitaalsõnumi saatja, kui saaja. Teine, privaatvõti, on teada ainult kasutajale ja seda kasutatakse tehinguteks ja digitaalsõnumite allkirjastamiseks, nt kui tahetakse kellelegi krüptoraha üle kanda.[9] Et omada ülevaadet oma krüptorahast, seda saata ja vastu võtta, on loodud tarkvara rakendused mida nimetatakse virtuaalseteks rahakottideks ja just neile juurdepääsuks ongi vaja eelmainitud võtmeid.

Virtuaalsete rahakottide pakkujad (*wallet providers*) on ühendused, kes võimaldavad tarkvara rakenduse või muu vahendaja kaudu omada, hoiustada ja üle kanda krüptoraha. Vastavad pakkujad peavad üleval kasutaja krüptoraha bilanssi, mis tavaliselt tähendab krüpteeritud vahenduste ajaloo tõlkimist lihtsalt loetavasse formaati, mis on sarnane pangakonto väljavõttega. Pakkujate eesmärgiks on hõlbustada osalemist virtuaalses krüptoraha süsteemis, võimaldades kasutajatele hõlpsamat vahetuste ja ülekannete tegemist ning kõige selle jaoks ka suuremat turvalisust. Viimase tagamiseks pakuvad nad krüpteerimist, mitmevõtmelist allkirja kaitset, tagavara hoidlat ja nö miksimist (*mixing*), mis tõstab krüptoraha anonüümsust.[10] Rahakottide pakkujaid on erinevaid, peamised on kaks tüüpi, mis erinevad oma kohese kasutuse ja turvalisuse poolest. Esiteks veebi rahakotid, nii-öelda kuumhoidla (*hot storage*), ja ühenduseta rahakotid, nii-öelda külmhoidla (*cold storage*). Vastavaid teenuseid pakutakse arvutitele, mobiiliseadmetele ja pilverakendustele. Pakutavaid rahakoti lahendusi on kolm. Üheks on riistvaraline võimalus, kus pakutakse spetsiifilist riistvaralahendust, et hoida oma

[8] World Bank Group. Distributed Ledger Technology (DLT) and Blockchain, lk 6.
[9] *Ibidem*, lk 8-9.
[10] FATF, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, juuni 2014, lk 8.

krüptograafilisi võtmeid, sellisteks on näiteks Ledger Wallet[11] ja Cryptotag[12]. Seejärel tarkvaralahendus, kus läbi rakenduse pääseb ligi võrgustikule, saab saata ja vastu võtta krüptoraha, näiteks Jaxx[13]. Kolmandaks on nii-öelda järelvaatav pakkuja (*custodian wallet provider*), mis hoiustab kasutaja võtmeid veebis, näiteks Coinbase[14]. Kasutajatel on vabad käed oma rahakotti ka ise ülal pidada, ilma pakkujat kasutamata.

Krüptoraha ülekannete kiirus virtuaalsete rahakottide vahel varieerub ja oleneb ülekande liigist. Nagu ka eelnevalt selgitatud, peab ülekande tegemisel tehingu kinnitama kogu võrgustik enne, kui see lõpuni viiakse. Nii on näiteks Bitcoini süsteemis kokku lepitud standardiks kuus kinnitust, mida ülekanne peab läbima enne, kui seda saab pidada lõpetatuks. Sealjuures mõjutavad ülekande kiirust kaks peamist faktorit – võrgustiku aktiivsus ja ülekannete teenustasud. Mida rohkem tehakse ülekandeid, mida võrgustik peab läbi töötama, seda kauem iga ülekanne aega võtab. Seda sellepärast, et on ainult loetud arv kaevureid, kes iga plokki läbi töötab ja milles on lõpmatu arv ülekandeid, mida saab sinna kaasata. Sellest tulenevalt prioritiseerivad näiteks konkreetselt Bitcoini kaevurid tööd vastavalt sellele, milline on tasu suurus, mida nad kinnitamise eest saavad. Seega, mida kõrgemat tasu kasutaja maksab, seda tõenäolisem on, et kaevur just tema ülekande ette võtab ja see siis kiiremini lõpule saab viidud. Nagu ka enne mainitud, vajab Bitcoini ülekanne kaevandajatelt kuute kinnitust, enne kui see käiku võetakse. Keskmiselt võtab ploki kaevandamine 10 minutit, nii et võib eeldada, et ülekanne võtab aega umbes kuus korda 10 minutit, ehk umbes ühe tunni. Siiski on Bitcoini suur populaarsus põhjustanud aegajalt ka mõningast süsteemi ülekoormust. Juba 2017. aastal võis keskmine ülekandele kuluv aeg varieeruda parematel päevadel 30 minutist kuni 16 tunnini äärmuslikematel aegadel. Bitcoini kogukond on antud küsimuse lahendamise osas lahknenud kaheks. Mõned süsteemi liikmed, eriti need, kes eelistavad Bitcoin Cashi, usuvad, et lahenduseks on suuremad ploki mahud, mis on võimelised hoidma ploki kohta rohkem ülekandeid. Teised aga leiavad, et tuleks kasutada pigem võrgustiku tööd kiirendavaid lahendusi nagu Segregated Witness (SegWit) ja Lightning Network. [15]

Bitcoini on võimalik kaevandada maksimaalselt 21 miljonit ühikut, 2020 aprilli seisuga oli alles jäänud kaevandada 2,6 miljonit ühikut, aprill 2021 seisuga 2,3 miljonit[16], hetkel kaevandatakse

[11] Vaata - https://www.ledger.com/
[12] Vaata - https://cryptotag.io/
[13] Vaata - https://jaxx.io/
[14] Vaata - https://wallet.coinbase.com/
[15] Buchko, S., *How Long do Bitcoin Transactions Take?,* CoinCentral, 2017.
[16] Faggart, A., *What Happens to Bitcoin Miners When all Coins are Mined?*, Bitcoin.com, 2021.

neid päevas umbes 1800. Niisiis on 88% sellest tööst juba tehtud ja usutakse, et juba kaevandatud kogusest umbes 30% on igaveseks kadunud üksnes kaotatud võtmete ja kokku jooksnud kõvaketaste tõttu.[17] Kuigi viimaste aastate liikumist ja praeguste numbrite põhjal arvutusi tehes võiks tunduda, et bitcoinid saavad otsa aastal 2024, arvatakse, et on väheusutav, et viimane bitcoin enne aastat 2140 kaevandatakse. Nimelt seisneb asja keerukus selles, et kaevurite tasu kaevandamise eest vähendatakse iga nelja aasta tagant, kui näiteks algusaastatel oli selleks 50 BTCd, siis aastal 2020 kukkus see number juba 6,25 BTCni. Seetõttu jääb ka kaevureid aina vähemaks ja viimaste bitcoinideni jõudmine võtab kauem aega kui võiks arvata. Võib juhtuda, et kaevandamine jäetakse mingil hetkel hoopis soiku. Seda kõike muidugi juhul, kui Bitcoini protokolli suuri muudatusi ei tehta, mis muujuures võiks lasta ka kaevandamise kogust suurendada.[18]

Bitcoinide tuleviku ja kaevandamise lõpu osas on palju arutelusid. Lõpp on küll lähedal, aga seda vaid teatud mõttes. Näiteks jääb paljude kaevurite motivatsioon Bitcoini plokiahelate valideerimiseks püsima, sest nad saavad ka edaspidi koguda kasutajatelt tehingutasusid, mis ehk ka oluliselt tõusma võivad hakata. Küll aga võib olla palju ka neid, kes oma tulu peamiselt kaevandamisest on kogunud ja kes otsustavad süsteemist välja astuda, kui kaevandamisega tulu teenida võimalik ei ole. Bitcoini süsteemi jaoks tähendaks see tragöödiat, sest selle esmane eesmärk, milleks on detsentraliseeritud plokiahela süsteem, satuks löögi alla, kuna selline süsteem tuginebki keskusest loomise pärast just kaevuritel ja kui neid pole, on see hukule määratud.[19]

Virtuaalvaluuta vahetuse pakkuja on kas isik või ühendus, mis oma majandustegevusena pakub võimalust isikutel oma krüptoraha vahetada päris raha, muude vahendite, teist liiki krüptoraha ja samuti väärismetallide vastu vahendustasu eest. Sellised vahetused aktsepteerivad üldiselt väga laiaulatuslikke erinevaid maksmisviise, sealhulgas sularaha, ülekandeid, krediitkaarte ja erinevaid liike krüptoraha. Isikud kasutavad virtuaalvaluuta vahetusi, et teha sisse- või väljamakseid oma krüptoraha kontodel.[20] Virtuaalvaluuta vahetuspunkti alla käivad ka vastavad sularaha automaadid, mida hetkel on suhteliselt vähe kuid nende number on kasvutrendis. Näiteks Tallinnas on selliseid automaate hetkel 7[21]. Automaatides saab krüptoraha müüa ja osta, automaat saab ka väljastada omanikule ta võtmed, printides need

[17] Buchko, S., *How many bitcoins are left?*, CoinCentral, 2020.
[18] Hayes, A., *What Happens to Bitcoin After All 21 Million Are Mined?*, Investopedia, 28.02.2021.
[19] Buchko, S., *How many bitcoins are left?*, CoinCentral, 2020.
[20] FATF, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, 2014, lk 7.
[21] Vaata - https://coinatmradar.com/

tšekile QR koodina ja samuti saab seal genereerida ka ajutise rahakoti, kui endal ühte parasjagu ei ole.

Kauplemisplatvormid toimivad kui turud – nad ei vaheta krüptoraha nagu valuuta vahetuspunktid, vaid toovad kokku kasutajad, kes seda ise teha saavad. Seal teevad ostjad ja müüjad pakkumisi omavahel.[22] Kauplemisplatvormid ei ole juhitud mõne isiku või majandusettevõtte poolt, vaid tegemist on süsteemiga, mis on juhitud eelprogrammeeritud tarkvara poolt ja kus ei ole ühtegi inimesest vahemeest. Sellepärast on need ka tuntud kui P2P (ingl *peer-to-peer* - partnervõrk) ehk detsentraliseeritud vahetused. Nende platvormide eeliseks on tsenseeritus, soodne hind ja korrektse kasutamise korral turvalisus ning privaatsus. Puudusteks on aga pikemad vahetuse ajad, kasutuskeerukus, madalam likviidsus ja on seetõttu levinud pigem entusiastide seas. Küll aga eelistatavad paljud neid tihti just tänu detsentraliseeritusele, sest keskse organi puudumine raskendab oluliselt valitsuse võimalikku ligipääsu.[23]

Peale esimese krüptoraha Bitcoini tulekut on ajaga lisandunud väga palju erinevaid ja erinevate omadustega alternatiivset krüptoraha, mida nimetatakse altcoin'ideks. Hetkel on turul ligi 9204 erinevat krüptovaluutat, virtuaalvaluutade koguväärtus ulatub üle 1,8 triljoni ja vaid aasta aega tagasi oli see 200 miljard eurot. Turu koguväärtusest 75% kuuluvad hetkel turu liidri positsioonil olevatele krüptovaluutadele (Bitcoin, Ethereum, Binance Coin, WRP ja Tether).[24] Altcoin'e on olemas kahesuguseid, esiteks need, mis kasutavad Bitcoin'ile sarnast protokolli, muutustega aluskoodis, tuntumad näiteks Litecoin ja Dodgecoin. Teised aga vastavat protokolli ei kasuta, vaid on loonud oma plokiahela ja protokolli, näiteks Ethereum ja Ripple.[25] Bitcoin on esmapilgul anonüümne, kuid omab teatud määral siiski jälitusvõimalusi, seega kutsutakse seda pigem pseudo-anonüümseks krüptorahaks. Kasutajad saavad näha ülekannete jada kõikide kontode puhul, kuid mitte miski süsteemis ei vii kokku kontot konkreetse isikuga ja samas saavad nad luua nii palju kontosid kui nad soovivad.[26] Tegelikkuses ei ole süsteem aga õhukindel. Tegelik isik konto taga on võimalik selgeks teha, kui nii-öelda ründajal on ligipääs mitmele haldurile. Samuti siis, kui isik on kuidagi oma päris identiteedi sidunud oma kontoga, seda kas läbi rahakoti pakkujate, vahendusplatvormide või ülekannete. Tegelikkuses on kõik

[22] European Central Bank, *Virtual currency schemes – a further analysis*, 2015, lk 8.
[23] Marshall, A., *P2P Cryptocurrency Exchanges, Explained,* Cointelegraph.com, 07.04.2017.
[24] Vaata - https://coinmarketcap.com/coins/views/all/
[25] Zainuddin, A., *Altcoins vs Tokens: What's the Difference?*, Masterthecrypto.com, 2020.
[26] Grinberg, R., *Bitcoin: An Innovative Alternative Digital Currency*, Hastings Science and Technology Law Journal, 2011, vol 4, 164.

ülekanded ja tehingud Bitcoini süsteemis kõigile nähtavad ja õige isikuni jõudmine on võimalik, kuid tehniliselt keeruline ja ajamahukas.[27] Kõige aktiivsem ja tuntum täielikult anonüümne krüptoraha on Monero (XMR), mis kasutab krüptograafilisi kilpe nii saatja kui vastuvõtja aadresside puhul. Sarnaselt Bitcoinile on seega võimalik teha privaatseid tehinguid. Monero on täielikult asendatav, mis tähendab seda, et osakud on omavahel asendatavad ja neid ei saa panna musta nimekirja juhul kui neid on varem valesti kasutatud, sest neid ei ole võimalik jälitada.[28] Kui Monerol on saatmise privaatsus juba sisseehitatud ja toimiv vaikimisi, siis teine märkimisväärne anonüümne krüptovaluuta süsteem Dash (tuleneb sõnapaarist ingl *digital cash* – digitaalne raha) omab seda funktsiooni valikuna. Dash loodi eesmärgiga parandada Bitcoini kitsaskohti, nagu kiirus, kulud ja juhtimine. Kui varem märgitult võtab Bitcoini tehingute kinnitamine aega umbes 10 minutit, siis Dash teeb selle ära 4 sekundiga. Ka Bitcoini 6 dollarilisele tehingutasuga võrreldes pakub Dash kasutajasõbralikumat lahendust ehk tehingute tegemist alates poolest dollarist, kuigi tihedamate tehingute puhul see tõuseb. Dash töötab kahetasandilisel võrgustikul, kus esimesel astmel on kaevandajad ja teisel juba pisut meisterlikumad tehingutega tegelejad.[29]

Pseudo-anonüümseid krüptorahasid on aga võimalik muuta anonüümsemateks. Üks võimalus on kasutada miksimisteenust (ingl *mixer* – mikser, pesuteenus, trummel), mis jätab mulje nagu oleks ülekanne tehtud mõnelt teiselt aadressilt. Miksimine saadab krüptoraha mitmete ülekande seeriatena, mis teeb krüptoraha seostamise konkreetse tehinguga väga keeruliseks. Teenust pakuvad näiteks Bitcoin Laundry ja Bitmixer.io.[30] On ka välja toodud, et krüptovaluutad on rohkelt kasutuses kelmide seas, ebaseaduslikud tulud võivad olla juba virtuaalvaluutadena aga neid saab ka digitaalselt vahetada. Uued rahapesu puudutavad tehnikad, mis põhinevad krüptovaluutal, hõlmavadki just miksimis- ja vahendusteenuseid.[31] Teine võimalus on kasutada Tor'i, mis on põrandaalune laiali hajutatud süsteem internetis, mis peidab ära tõelise IP aadressi ja sellega kasutaja tegeliku identiteedi, saates tehingu läbi mitmete arvutite üle maailma samal ajal seda krüpteerides. Selle mõju saab veelgi suurendada ka miksimist kasutades.[32] Lisaks saab kasutada ka laiendatud virtuaalset Tumedat rahakotti (*Dark Wallet*), mis on brauseripõhine ja

[27] Van Wirdum, A., *Is Bitcoin Anonymous? A Complete Beginner's Guide*, Bitcoinmagazine.com, 18.11.2015.
[28] Vaata - https://web.getmonero.org/resources/moneropedia/fungibility.html
[29] Vaata - https://en.wikipedia.org/wiki/Dash_(cryptocurrency)
[30] FATF, *Virtual Currencies – Key Definitions and Potential AML/CFT Risk*s, juuni 2014, lk 6.
[31] EU SOCTA 2021 Europol, Serious and Organised Crime Threat Assessment. *A corrupting influence: the infiltration and undermining of europe's economy and society by organised crime*, lk 32.
[32] FATF, 2014, lk 6.

kasutab anonüümsuse tõstmiseks miksimist, detsentraliseeritud kauplemist, tsenseerimata platvorme, börsi platvorme ja informatsiooni musta turgu. [33]

1.1.1. Krüptovaluuta käsitlus maailmas

Järgnevalt toob autor välja erinevate maailmas tunnustatud finantssektori organisatsioonide seisukohad ja hinnangud krüptovaluutale. Seda selleks, et saaks selgema pildi, mil moel krüptovaluutat defineeritakse ning kuidas seda vastavate organisatsioonide poolt hinnatakse, kui uut liiki ja alternatiivset maksevahendit. Krüptovaluuta puhul on tegemist küllatki uudse lahendusega, kuid juba on kõik alltoodud organisatsioonid pidanud vajalikuks endapoolne analüüs või seisukoht välja anda.

1.1.2. Euroopa Keskpank (ECB)

Euroopa Keskpanga (European Central Bank; ECB) 2015 aasta analüüsi[34] kohaselt ei ole virtuaalvaluuta ei majandusliku ega juriidilise definitsiooni järgi ei raha ega valuuta. Euroopa Liidu keskpangad ei tunnista virtuaalvaluutat ega nende süsteeme raha- või valuuta maailma kuuluvaks, nii nagu majanduskirjanduses valuutat tuntakse. Samamoodi ei ole virtuaalvaluuta raha ega valuuta ka juriidilisest vaatepunktist. Majanduskirjanduse järgi on rahal kolm funktsiooni:

a) vahetuse vahend (kasutades seda kauplemises vahendina, et ei peaks kasutama partertehinguid);
b) selle väärtus säilib (raha saab koguda ja hiljem välja võtta);
c) arveldusühik (raha on kui standard, mõõtes kaupade, teenuste, varade ja kohustuste väärtust).

Bitcoinil, kui kõige populaarsemal virtuaalrahal on vahetuse meetodina piiratud võimalused, kuna neid aktsepteeritakse maailmas maksevahendina üldiselt üsna vähe. Teiseks on sellel väga kõrge väärtuse muutlikus, kui tahta neid päris valuuta vastu vahetada. Seega on enamike kaupade ja teenuste puhul krüptoraha kasutu isegi lühiajaliseks väärtuse hoidmiseks, seda enam pikaajalise investeeringuna. Näiteks on Bitcoini väärtus ühe päeva jooksul muutnud ka 40%. Just neil põhjustel ei ole virtuaalvaluuta sobiv arveldusühikuna. Seega ei saa Bitcoini ja sellega sarnaseid virtuaalvaluutasid võtta kui teatud tüüpi raha, kuigi ei saa välistada, et tulevikus võidakse luua stabiilsem virtuaalne valuuta.[35]

[33] FATF, 2014, lk 6.
[34] European Central Bank, *Virtual currency schemes – a further analysis*, 2015, lk 23-25.
[35] *Idem*, lk 23-24.

Õiguslikus mõttes on raha midagi, mida kasutatakse laialdaselt, et tehingute puhul vahetada väärtust. Valuuta mõistet kasutatakse vermitud raha puhul, ehk siis tänapäeval on selleks mündid ja paberraha. Valuutana peetakse silmas ka spetsiaalset rahatüüpi, mida kasutatakse mõnes riigis ametliku rahana ja on seal tunnustatud. Kuna virtuaalvaluutat ei kasutata laialdaselt, ei ole see õiguslikult raha ja kuna sellel puuduvad vermitud versioonid, siis mitte ükski virtuaalvaluuta ei ole selles mõttes valuuta. Eurotsoonis tunnustatakse rahana vaid euro münte ja paberraha, seega õiguslikult peab neid aktsepteerima. Immateriaalne raha pangakontol, panga raha krediidi või tšekkidena eurodes ja elektrooniline raha, ei ole õiguslikud pakkumused aga kuna sellist vormi raha laialdaselt kasutatakse ja aktsepteeritakse, võib euro rahana võtta ka kõiki neid erinevaid eelviidatud vorme. Seda ei saa aga öelda virtuaalvaluuta koha, kuna neid ei aktsepteerita laialdaselt ja neil ei ole ka ühtegi ülaltoodud füüsilist vormi, need ei ole ühegi riigi ametlikuks rahaks, õiguslikult tagatud ega oma pakkumuse võimet, need on midagi muud kui tuntud valuutad. Seega ei ole keegi kohustatud virtuaalvaluutat maksena vastu võtma ja neid saab maksevahendina kasutada vaid vastastikusel kokkuleppel.[36]

Kuna virtuaalvaluuta on oma olemuselt suhteliselt uus, areneb pidevalt ja seda erinevates suundades ning ei oma hetkel suurt kasutust, ei näe Euroopa Keskpank 2015 aasta seisuga vajadust uueks seadusandluseks või hetkel kehtiva Euroopa Liidu seadusandluse laiendamiseks. Peetakse soovitavaks, et mingi ühtlane õiguskindlus saavutatakse, kuidas hetkel kehtivat seadust virtuaalvaluutaga seonduvate aspektidega kohaldada. Peetakse vajalikuks virtuaalvaluutale definitsiooni andmist, seda erinevates kontekstides, kuid antud analüüsi puhul keskenduti virtuaalvaluutale kui maksevahendile ning tulevikus plaanivad täiustada oma 2012 aasta seisukohta. Definitsioon ei tohiks sisaldada sõna „raha“, sest on selge, et virtuaalvaluuta ei oma raha olemust ja neid ei aktsepteerita nii laialdaselt ja sellisel tasemel nagu raha. Välja tuleb jätta 2012 aasta definitsioonist sõna „reguleerimata“, kuna mõned regulatsioonid ja jurisdiktsioonid aktsepteerivad mõnda virtuaalvaluuta aspekti. Samuti jäeti välja „kasutatud ja aktsepteeritud teatud virtuaalses keskkonnas“, et segadust mitte tekitada. Kõike eeltoodut arvesse võttes defineerib Euroopa Keskpank virtuaalvaluuta kui digitaalse väärtuse esinduse, mis ei ole välja antud keskpanga, krediidiasutuse või e-raha institutsiooni poolt, mida mõningatel juhtudel saab kasutada alternatiivselt rahale. Analüüsis on läbivalt kasutatud väljendit virtuaalvaluuta süsteem, et näidata ka seda, et väärtust saab ka üle kanda. [37] ECB ei näe hetkel põhjust ja vajadust laiendada EL õiguslikku raamistikku virtuaalvaluutaga

[36] European Central Bank, 2015, lk 24.
[37] *Idem*, lk 25.

puutuvalt.[38] Samal ajal on ECB president Christine Lagarde väljendanud, et ECB tahaks olla krüptovaluuta lahenduste arengus pigem aktiivses rollis, mitte arenguid kõrvalt vaadata. ECB hindab ülekannete kiirust ja madalat hinda, võimalust aasta läbi iga päev 24 tundi päevas ülekandeid teostada. ECB on mõelnud välja anda ka omaenda digivaluuta ehk keskpanga digitaalvaluuta (central bank digital currency; CBDC), milleks loodi 2019. aastal ka spetsiaalne töögrupp, kes arengutel silma peal hoiab ja uurib CBDC võimalikku tehnilist võimekust ning seda, kuidas oleks võimalik riske minimeerida.[39] 2021. aasta aprillis ütles ECB juhatuse liige Isabel Schnabel, et digitaalse euro loomine ei ole hetke seisuga midagi kindlat ja teha tuleb veel kõvasti eeltööd, kuid isegi kui digitaalne euro peaks välja tulema alles 4-5 aasta pärast, pole see liiga hilja, sest keegi peale ECB ei suuda tagada sellisel tasemel turvalisust ja andmekaitset.[40]

1.1.3. Rahvusvaheline Valuutafond (IMF)

Rahvusvaheline Valuutafond (IMF) on leidnud[41], et virtuaalvaluuta on väärtuse digitaalne esituslaad, mida annavad välja privaatsed arendajad ja nimetavad need oma arveldusühikutena. Virtuaalvaluutat saab omandada, hoida, sellele ligi pääseda ja üle kanda digitaalselt. Seda saab kasutada väga erinevatel puhkudel aga seda vaid siis, kui lepingupooled on sellega nõustunud. Virtuaalvaluuta mõiste katab laiemat valikut „valuutasid“, alates lihtsamatest võlakirjadest, näiteks Interneti või mobiilikupongid ja lennumiilid. Samuti virtuaalvaluutad, mis on tagatud kullaga, sellisel juhul on need tagatud kombinatsioonina tõelise varaga või riigis kehtiva varaga ja väljaandja krediidivõimekusega ning ka krüptorahad nagu näiteks Bitcoin. Virtuaalvaluuta ei ole kindlasti raha ega ka e-raha, sest ei ole tagatud riiklikult tunnustatud rahaga, vaid neil on oma arveldusühik. IMF näeb virtuaalvaluuta puhul palju riske nii kasutajate turvalisusele, finantsilisele terviklikkusele, maksudest kõrvalehoidumise kui ka efektiivse finantsregulatsiooni puhul. Kuid nad ei välista, et tulevikus uute tehnoloogiliste lahenduste ja võimekuse suurenemisega, võib olukord muutuda.

1.1.4. Euroopa Pangandusjärelvalve (EBA)

[38] *Idem*, lk 32.
[39] Lagarde, C., Interview with “Challenges” magazine, 08.01.2020.
[40] Vaata - https://www.ecb.europa.eu/press/inter/date/2021/html/ecb.in210409~c8c348a12c.en.html
[41] IMF Staff Discussion Note, *Virtual Currencies and Beyond: Initial Considerations*, 2016, lk 7, 35.

Euroopa Pangandusjärelvalve (EBA) kasutab oma analüüsides ja ettepanekutes laiemat mõistet krüptovara. EBA[42] defineerib seda sarnaselt ECB'ga, ehk krüptovaraks on vara, mis:

a) põhineb peamiselt krüptograafial ja DLT tehnoloogial, või sarnastel tehnoloogiatel;
b) ei ole välja antud ega tagatud mõne keskse panga või autoriteedi poolt;
c) saab kasutada vahetustasuna ja/või investeerimiseks ja/või kauba, teenuse saamiseks.

EBA leiab, et krüptorahadel on erinevaid omadusi, milledest mõned tulevikus kindlasti muutuvad, kuid kindlasti tuleks reguleerimisel läheneda pidades silmas rohkem krüptoraha sisu kui tüüpi.

1.1.5. Euroopa Väärtpaberiturujärelvalve (ESMA)

Euroopa Väärtpaberiturujärelvalve (ESMA) on koos EBA ja Euroopa Kindlustus- ja Tööandjapensionide Järelevalvega (EIOPA) välja andnud hoiatuse[43] virtuaalvaluutade kohta. Virtuaalvaluuta on selle hoiatuse kohaselt väärtuse digitaalne esindus, mis ei ole välja antud ega garanteerita ühegi panga või avaliku autoriteedi poolt ning tal ei ole õiguslikult sama staatust kui valuutal või rahal. Hoiatus ongi välja antud põhjusel, et vastavad organisatsioonid leiavad, et virtuaalvaluutad on väga riskantsed, tavaliselt ei ole nad tagatud mitte ühegi tõelise varaga ja on Euroopa Liidu õigusega reguleerimata. Seega ei ole kasutajatel mitte mingit õiguslikku kaitset, kui nad peaksid oma raha kaotama. Riskidena toovad nad näiteks välja:

- Virtuaalvaluuta väärtuse äärmiselt suurt volatiilsust. Virtuaalvaluutat ostes peab arvestama sellega, et sa võid kaotada osa või kõik oma raha.
- Kaitse puudumine. Rahapesudirektiiv reguleerib vaid rahakoti pakkujaid ja vahendusplatvorme, aga virtuaalvaluuta ise on EL õigusega reguleerimata. Samamoodi on reguleerimata digitaalsed rahakotid ja vahetuskohad. Kasutajad on ilma kaitseta, mis on aga tagatud, kui kasutada reguleeritud finantsteenuseid, see tähendab, et kasutaja ei ole kaitstud, kui teenusepakkuja läheb pankrotti, seda häkitakse, varad omastatakse või nendest ilma jäämise eest, kui õiguskaitseorganid sekkuvad.
- Ei pruugi olla võimalust pikka aega oma virtuaalvaluutat vahetada tagatisega raha vastu.
- Alati ei ole hind läbipaistev ja kasutaja ei saa sellega ostu- ja müügitehinguid tehes kindel olla, millega võib väärtuses kaotada.
- Süsteemide katkestused, kui ei ole võimalik tehinguid teha ja mille ajal võib väärtuses kaotada.

[42] EBA Report, *Report with advice for the European Commission on crypto-assets*, 09.01.2019, lk 10,11.
[43] ESMA, EBA, EIOPA, *Warning on the risks of Virtual Currencies*, 12.02.2018, lk 1-2.

- Ebasobivus pikaajalisteks investeeringuteks ja pensioni kogumiseks, kuna sellel ei ole püsivat väärtust, selle tulevikku pole teada, samuti ebausaldusväärsus vahetusplatvormide ja rahakoti pakkujate puhul.

1.1.6. Maailma Pank (WB)

Maailma Pank (World Bank; WB) määratleb krüptoraha kui digitaalvaluuta alamhulga, mis tugineb krüptograafilistele tehnikatele, et saavutada poolte üksmeelsus. Digitaalvaluuta on väärtuse digitaalne esindatus, mis on nimetatud oma arveldusühikuna. Erineb e-rahast, mis on digitaalne maksmise mehhanism ja mida esindab tagatud raha.[44] WB on oma ülevaate koostanud eesmärgiga, et uurida ja anda ülevaade DLTst. WB peab võimalikuks tulevikuks panganduses ja finantssektoris kasutada sama plokiahela tehnoloogiat, millel krüptoraha põhineb. Hetkel nad veel selleks soovitust ei anna, kuid nad näevad sellel suurt potentsiaali ja leiavad, et on vaja veel uuringuid teha. Toovad aga välja, et nii Inglise Pank kui Kanada Pank on jõudnud järeldusele, et hetkel on DLT küll ebaküps, kuid selle arenedes plaanivad nad DLT tulevikus kasutusele võtta.[45]

1.1.7. Rahapesuvastane rakkerühm (FATF)

Rahapesuvastane rakkerühm[46] (Financial Action Task Force; FATF) defineerib sarnaselt teistele virtuaalvaluutat, kui väärtuse digitaalset esindust, mida saab digitaalselt vahetada ning omadustelt on see kui vahetusvahend, arveldusühik ja omab väärtust, kuid sellel ei ole pakkumuse väärtust ja seda ei tunnusta ükski riik. Digitaalvaluuta võib olla digitaalne esindus nii virtuaalvaluutale, mis on tagatiseta, kui ka e-rahale, millel on tagatis olemas. FATF soovitab virtuaalvaluutad jaotada omakorda konverteeritavateks ja mitte konverteeritavateks. Esimesed on siis virtuaalvaluutad, millel on reaalsele valuutale vastav väärtus ja seda on võimalik vahetada raha vastu. Sellised valuutad võivad olla nii tsentraliseeritud kui ka mitte. Mitte konverteeritavad on virtuaalvaluutad, mis on omased kindlale virtuaalsele domeenile või maailmale (näiteks *online* mängus *World of Warcraft*) ja neid ei saa tagatud valuuta vastu vahetada. Täpne definitsioon on, et krüptoraha on matemaatikapõhine detsentraliseeritud konverteeritav virtuaalvaluuta, mis on krüptograafiliselt kaitstud.

[44] World Bank Group. Distributed Ledger Technology (DLT) and Blockchain, 2017, IV.
[45] World Bank Group, 2017. Lk 4-9.
[46] FATF, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, juuni 2014, lk 4-5.

Välja toodud organisatsioonid leiavad üheselt, et krüptoraha ei saa samastada traditsioonilise rahaga. Kindlasti on krüptovaluutal olemas omadused, mis sarnanevad raha kui maksevahendiga, kuna sellega saab teatud teenuste ja kaupade eest maksta. Arveldusühikuna on see aga rangelt kasutatav vaid siis, kui mõlemad tehingupooled sellise makseviisi kasutamisega nõustuvad. Probleemiks on aga selle suur volatiilsus, kus tarbija ei saa isegi ühe päeva lõikes kindel olla, milline tema krüptovaluuta väärtus täpselt on. Positiivne on antud lahenduse puhul aga selle kiirus ja madalad kulud, mistõttu uuritakse nii võimalust DLT süsteem pankades kasutusele võtta, kui ka lausa enda digitaalvaluuta välja anda. Pangad annavad endale aru, et maailm muutub ja arengud selles vallas on viimastel aastatel aina kiiremad, ning nad peavad sellega kaasa liikuma. Digitaliseerimise tulekuga seoses ei ole enam ka tegevuse puhul piirid nii selged ja pigem võetakse globaalseid mõõtmeid ja konkurentsis püsimiseks on vaja uuendustega kaasas käia.

1.1.8. Krüptoraha teistes riikides

Autor peab vajalikuks välja tuua ka üldised regulatsioonid ja seisukohad krüptoraha osas, mida on avaldanud erinevad maailma riigid. ECB 2015 analüüsis[47] toodud kokkuvõtte järgi on riigid jaotunud mitme erineva seisukoha vahel. Euroopa riikidest Soome ja Rootsi leiavad, et krüptoraha ei täida valuutale kehtestatud nõudeid ja ei ole seega vaadeldav kui seaduslik valuuta, Rootsi maksustab krüptoraha aga sarnaselt tavapärase vara puhul. Saksamaa on omakorda võtnud hoiaku, et see on arveldusühik ja ei kvalifitseeru finantsinstrumendiks. Väljaspool Euroopat ei pea ka näiteks Malaisia ja Indoneesia krüptoraha seaduslikuks valuutaks. Viimast seisukohta võib pidada kõige levinumaks, kuid samal ajal kaaluvad mõned riigid aina tõsisemalt krüptovaluutaga seonduvate teenusepakkujate tegevuse reguleerimist, litsentseerimist ja jälgimist. Näiteks Rootsis alluvad vahetusplatsvormid järelvalvele juba 2012. aastast. Taanis ja Saksamaal vahetusplatvormid ei vaja volitusi, kuid viimane mõtleb kohaldada neid teiste krüptovaluutaga seotud teenuste puhul. Prantsusmaal käsitletakse platvorme kui makseteenusepakkujaid ja seega peavad omama samu volitusi. Tais, Indoneesias ja Venemaal on krüptovaluuta keelatud ning alates 31.01.2014 keelati ka Hiinas makseteenused Bitcoiniga.

2019 märtsi seisuga on krüptoraha täielikult keelatud kümnes riigis, mõningatel juhtudel just sellepärast, et sobivat regulatsiooni ei ole veel välja töötatud. On ka riigid, kus on finantsasutustel keelatud krüptovaluutas tehinguid teha. Karmim neist on Hiina, kus on keelatud

[47] European Central Bank, 2015, lk 31-32.

ka vahetusplatvormid. Saudi Araabias, Indias ja Hiinas, kus tehingud on keelatud, näitavad aga uuringud, et see ei peata tegelikkuses krüptorahaga kauplemist. Uuringute järgi tehti 2017 aasta algusest kuni 2019 aasta märtsini tehinguid aktiivselt ning ajas kasvavalt.[48] Sellele aitab kindlasti kaasa süsteemi detsentraliseeritus, mis oligi antud süsteemi loomise eesmärk ja millega eemaldati keskse organisatsiooni või riigi mõjuvõim tehingutesse sekkuda. Ja nagu näha, võib riik tegevuse keelata, kuid ei saa seda takistada. Samal ajal on Hiina näidanud välja topeltmoraali, keelates krüptoraha kasutamise kodanike seas, kuid rakendades samal ajal enda finantsasutustes DLT süsteeme.[49] Kodanikud kasutavad vaatamata keelule siiski varjatult Tether'it, mille abil konverteeritakse raha digitaalseks ja sealt juba edasi erinevateks krüptorahadeks. Tether ise väidab end olevat kui stabiilne krüptovaluuta, mille väärtus on alati 1$ ja mida peeti seetõttu justkui krüptovaluuta keskpangaks. Tänaseks on Tether aga oma tegevusse kaasanud ka firmasid, et tagada oma laene, seega ühe mündi väärtus ei ole enam tagatud nii nagu see algselt programmeeritud oli. Tether andis Hiina Rahvavabariigile ette plaani, kuidas ta enda krüptovaluuta toimida võiks.[50] Tänaseks on Hiina RV välja töötanud oma krüptovaluuta ehk digitaalse jüaani, mille eesmärk on asendada osa ringluses olevast rahast ning hetkel on antud juba miljonite dollarite väärtuses krüptoraha testimiseks kolme suurde linna. Sellega seoses on aga tuntud muret, et digitaalne jüaan võib võimaldada omada Hiina RV'l oma kodanike üle suuremat järelevalvet.[51] Hiina riikliku strateegia põhifookusesse asetatud plokiahela tehnoloogia ja suured plaanid on ka algselt krüptovaluutasse väga halvasti suhtunud Venemaa oma suhtumist muutma pannud, kes on samuti nüüd huvitatud uute tehnoloogiate arendamisest. [52]

Uuringute järgi on krüptoraha lubatud ja seaduslik 111 riigis, kõige Bitcoini-sõbralikumate riikide seas on näiteks Eesti, Hongkong, Saksamaa, Suurbritannia. USA ja Kanada tegelevad regulatsiooni väljatöötamisega, et takistada rahapesu ja pettusi. ELi liikmesriikidel on keelatud välja anda enda krüptovaluutat küll aga toetatakse vahetusplatvormide legaliseerimist.[53] Saksamaad peetakse krüptovaluuta osas maksustamise taevaks, sest nemad peavad krüptovaluutat privaatseks rahaks, mitte valuutaks, kohustuseks või osakuks. Selle erisusega

[48] *Countries Where Bitcoin Is Banned or Legal In 2020,* Cryptonews.com.
[49] Magas, J., *Five Countries Where Crypto Regulation Changed the Most in 2019*, Cointelegraph, 2019.
[50] Ossinger, J., *China's Plan for Digital Yuan Imperils Bitcoin's Biggest Markets*, Bloomberg, 2021.
[51] Kharpal, A., *China has given away millions in its digital yuan trials. This is how it works*, CNBC.com, 2021.
[52] Lucian, A., *Will the 'China Blockchain Narrative' Lead the Cryptocurrency Market in 2020?*, BeInCrypto, 2020.
[53] *Countries Where Bitcoin Is Banned or Legal In 2020*, Cryptonews, 2020.

kaasnevad maksustamisel omanikele kasud, mille kohaselt ei pea makse maksma alla 600 euro müükide puhul ning kui ollakse krüptovaluutat enda käes hoidnud vähemalt aasta, kaob maksukohustus täielikult. Niisiis ei kaasne peale aastat mingeid makse, olenemata sellest, mis summa eest lõpuks oma krüptoraha maha müüakse.[54] USA puhul erineb regulatsioon osariigiti ja näiteks Wyomingi osariigis jõustus 2019. aastal seadus, millega jaotati digitaalsed varad kolmeks, millest virtuaalvaluuta on võrdeline tagatud valuutaga ning sellele kohalduvad samad maksustamise ja järelevalve regulatsioonid. Samuti on krüptoraha omamine õiguslikult lubatud ning staatus on samuti sama, mis tagatud valuutal.[55] Venetsueela andis oma riikliku krüptovaluuta „petro" välja veebruaris 2018 aga nähtus[56] juba sama aasta augusti kuus, et seda ei kasutata kui valuutat. Paljud krüptovaluutaga seotud ettevõtjad pidasid petrot lihtsalt pettuseks. On ka öeldud, et petro on kõige halvem investeering üldse, sest see on kasutu, seda saavad osta vaid välismaalased ja kasutada vaid venetsueelalased. Algselt öeldi, et valuuta on tagatud kullaga, kuid täit selgust selles osas ei ole, selleks võib olla ka mõni mineraal. Ka hinna kujunemine ei olnud selge, välja oli öeldud, et üks petro vastab ühele barrelile õlile, hiljem aga selgitati, et selle väärtus võib tuleneda ka turust.

Riigid on aastate jooksul aru saanud, et krüptovaluuta aina areneb ja muutub populaarsemaks. Seega üritatakse uuendustega kaasas käia, vaikselt kogu süsteemi reguleerida ja samal ajal aru saada millised on võimalikud riskid. Riikide puhul kes on krüptovaluutasse karmimalt suhtunud ja selle ka osaliselt keelustanud, võib üldjuhul täheldada ühisnimetajana autoritaarsemat riigivõimu, kes ei soovi oma kontrolli süsteemi üle mingil viisil käest anda. Kuid aina rohkem diskuteeritakse võimaluse üle, et võtta kasutusele riigi- või liidupõhised krüptorahad. Hetkel tundub, et selle võidujooksu võib võita Hiina. Millist mõju see aga maailma krüptoraha turule avaldaks, ei oska hetkel mitte keegi hinnata. Ja kuigi Euroopa Liit on küll keelanud oma liikmesriikidel enda krüptovaluutat välja anda, kaalutakse samal ajal liidupõhise virtuaalvaluuta kasutuselevõttu. Selline samm oleks tegelikult ka mõistetav, kuna liiduüleselt on kasutuses euro ja loogilisem jätk oleks ka ühine virtuaalvaluuta, mis ei ohustaks liidu saavutatud ühtsust ja pakuks kõigile võrdseid võimalusi.

1.1.9. Krüptoraha käsitlus Eestis

[54] De Hoon, I., *Germany: A Surprising Bitcoin Tax Haven*, Nomoretax.eu.
[55] Lucian, A., *Will the 'China Blockchain Narrative' Lead the Cryptocurrency Market in 2020?*, BeInCrypto, 2020.
[56] https://en.wikipedia.org/wiki/Petro_(cryptocurrency)

Rahandusministeerium oma 2016 aasta analüüsis kasutab alusena just eeltoodud Euroopa Keskpanga, FATF ja EBA definitsioone. Analüüsis kasutatakse mõistet virtuaalvääring, mitte virtuaalvaluuta või virtuaalraha, kuna leitakse, et hetkel ei saa sellist liiki virtuaalset esitlusvormi pidada ametlikult käibivaks vääringuks ehk rahaks. Tõdetakse, et Eestis ei ole välja töötatud definitsiooni ja ei ole seadusandluse tasemel määratletud. Läbivalt on toodud näiteid, kuidas täpselt Bitcoini käsitleda, kuid seda saab samastada üldisemalt virtuaalvaluutana, kuna Bitcoin on selle üks liike. Rahandusministeerium käsitleb seega virtuaalvaluutat ennekõige kui lepingulist vääringut. Rahaliseks vääringuks ei saa seda pidada võlaõigusseaduse (VÕS) § 91 lg 1 ja § 93 lg 1 tulenevalt ehk rahalise kohustuse saab täita ka muul viisil kui sularahas aga see peab tasumise ajal olema kehtiv riigis, mille vääringus makse tehakse.[57] Seega peetakse antud analüüsi kohaselt virtuaalvaluutat vaid lepinguliseks vääringuks, mida saab kasutada vaid lepingupoolte kokkuleppel ning seda ei saa kuidagi samastada rahaga.

Rahandusministeerium on välja andnud ka krüptovarade reguleerimise väljatöötamiskavatuse, kus aga pigem keskendutakse token'itele, mis oma olemuselt ja/või funktsioonidelt sarnanevad väärtpaberile. Eelkõige kaasatakse token'ite kaudu investoritelt kapitali erinevate projektide elluviimiseks, leitakse, et neid peaks kohtlema investorkaitse seisukohalt väärtpaberitega sarnastel alustel.[58] Eesmärkideks on riskide maandamine, suurem õigusselgus ja paindlikum regulatsioon, millede täitmiseks nähakse ette teabe avalikustamise kohustus, kutsenõuded ning teha selgeks, millal allub tegevus EL õigusraamistikku. Eeldatakse ja soovitakse ka token'ite laiemat kasutust.[59] Seega peab Rahandusministeerium vajalikuks krüptovaradega seonduva reguleerimist finantssektoris, investorikaitset ning kapitalikaasamisega seotud riske. Aktsepteeritakse krüptovarasid ja nende nii laialdast kasutust, et selle kasutamist peaks tänapäeva ühiskonnas ühtlustama.

Vabariigi Valitsuse tegevusprogrammis 2015-2019 nähti ette virtuaalvaluutade võimaliku tunnustamise ja kasutamise poliitika välja töötamine. Vabariigi Valitsuse tegevusprogrammis 2019-2023 on ettenähtud Eesti kapitaliturru arendamine, mille ühe tegevusena on krüptovarade ja ühisrahastuse reguleerimise vajaduse analüüs. Valitsus on tegevusprogrammide väljatöötamisel pidanud vajalikuks virtuaalvaluutaga seonduvat lähemalt analüüsida võimaliku reguleerimise eeldusena, kuid seda pigem kapitaliturgu silmas pidades.

[57] Rahandusministeerium, *Analüüs virtuaalvääringute võimaliku tunnustamise ja kasutamise poliitika väljatöötamiseks*, 2016, lk 7.
[58] Rahandusministeerium, Krüptovarade reguleerimise väljatöötamiskavatus, november 2019, lk 2-3.
[59] Idem, lk 6.

Eesti Panga hinnangul mõistetakse virtuaalvaluutasid kui digitaalseid varasid, mida teatavatel juhtudel ja tingimustel on võimalik kasutada poolte kokkuleppel maksevahendina ja millel võib olla ka väärtpaberi tunnuseid. Eesti Pank ei pea õigeks kasutada termineid „valuuta“ ja „raha“, kuna krüptovaluuta ei suuda täita majanduslikus mõttes kõiki raha funktsioone ja leiab, et korrektsem kasutada terminit „krüptovara“. Põhjustena tuuakse välja, et krüptovarade väärtus on väga kõikuv, neid ei saa kasutada stabiilse arvestusühikuna, väärtuse hoidjana ega ka tõhusa maksevahendina. Samuti puudub neil raha või valuuta õiguslik staatus ning puudub tagatis, et soetatud krüptovara saab tulevikus konverteerida tagasi tavarahaks. Kuna krüptovaral ei ole õiguslikku staatust, siis ei laiene sellele ka maksevahendite suhtes kehtestatud õigusaktid, mis tähendab, et tarbija on võimalike pettuste korral kaitsetu.[60] Ei välistata üldse seda, et tulevikus leiab krüptovara laialdast kasutust, seda valdkondades ja viisidel, mida hetkel ei suudeta ettegi kujutada. Kindlad ollakse aga selles, et krüptovara ei hakka kunagi asendama raha. Seda just eelkõige põhjusel, et see on nii kõikuva väärtusega ja tavakodaniku jaoks ei ole see atraktiivne. Finantssektor peab krüptovara puhul atraktiivseks hoopis selle tehnoloogiat ehk plokiahelat, mida pangad kaaluvad ka enda süsteemides kasutusele võtta.[61] Virtuaalvaluutade turuväärtus on kiiresti kasvanud, kuid siiski on see veel väike võrreldes ringluses ja pangakontodel oleva tavaraha väärtusega, mis ulatub üle 7,7 triljoni euro.[62]

1.1.10. Eesti Maksu- ja Tolliamet (EMTA)

Eesti Maksu- ja Tolliamet (EMTA) käsitleb virtuaalvaluutat tulumaksuseaduse (TuMS) § 15 lg 1 tähenduses varana, seega peab virtuaalvaluutalt saadud kasu pealt maksma ka makse. Tulumaksuga maksutatav on virtuaalvaluuta ost, müük ja ka vahendamine. Kui sellise tegevusega saadakse tulu, siis tuludeklaratsioonis tuleb see märkida kui muu vara võõrandamine. Seonduvalt virtuaalvaluutaga on võimalik tulu saada ka kaevandamisega, arvuti andmemahu rentimisel ning töötasu saamine virtuaalvaluutas.[63] Kaevandamine ja virtuaalvaluuta vahetamine tavavaluuta vastu ja vastupidi, ei ole käibemaksuga maksutatav. See on ka kooskõlas Euroopa Kohtu otsusega kohtuasjas C-264/14, mis selgitab, et tõlgendades EL direktiivi 2006/112/EÜ virtuaalvaluuta puhul on vastavalt artikli 135 lõikele 1 punktile e käibemaksust vabastatud tehingud, millega vahetatakse virtuaalvaluutat tavavaluuta vastu. [64]

[60] Eesti Pank, Finantsstabiilsuse ülevaade, 1/2018, lk 21-22.
[61] Madis Müller, Krüptovarad – mull või tulevik?, 15.01.2018.
[62] Eesti Pank, Finantsstabiilsuse ülevaade, 1/2018, lk 21.
[63] EMTA, *Eraisiku virtuaalses valuutas/krüptovaluutas saadud tulu maksustamine*, 26.04.2021
[64] Euroopa Kohtu otsus, 22.10.2015, C-264/14, Skatteverket vs David Hedqvist, p 57.

Virtuaalvaluuta, kohtuasjas konkreetselt bitcoin, on Euroopa Kohtu hinnangul kahesuunalise vooga virtuaalvaluuta, millel ei ole muud mõtet, kui kasutada seda maksevahendina ja seda ei saa käsitleda kui materiaalset vara käibemaksu direktiivi mõttes[65], see on lepinguline maksevahend, mida ei saa seda käsitada arvelduskonto, hoiuse, makse ega ülekandena.[66]

1.1.11. Finantsinspektsioon

Finantsinspektsioon selgitab virtuaalraha olemust kui digitaalset raha, mis on välja antud ja kontrollitav IT ettevõtte poolt, seda kasutab kindel virtuaalne kogukond ja sellel ei ole kaubakatet. Finantsinspektsioon on oma kodulehel avaldanud, et virtuaalraha valdkond on reguleerimata ala ja finantsjärelevalve asutused ei tee vastavate skeemide üle järelevalvet. Teenus ei ole seadusega reguleeritud ja seda kontrollib vaid teenusepakkuja, seega leitakse, et kõik riskid kannab virtuaalraha kasutaja. Viidatakse ESMA, EBA ja EIOPA poolt välja antud hoiatustele seoses virtuaalvaluuta suurtele riskidele, millel on ka eelpool viidatud. Finantsinspektsioon soovitab kasutajatel kontrollida enne investeeringu tegemist, kas ettevõttel on olemas tegevusluba ning, kas pakkumine on Finantsinspektsioonis nõuetekohaselt registreeritud. Viidatakse ka tavalistele riskidele seoses investeerimisega üldiselt, ehk siis ettevõtte kõrge läbikukkumise risk ning lubatud kõrge tootlus, mis ei pruugi realiseeruda. Virtuaalvaluutaga seotud riskid on token'i väärtuse spekulatiivsus, selle väärtus võib kõikuda ja pettuse risk anonüümset laadi tehingute puhul, mis on token'itele omane.[67]

27. novembril 2017 jõustus rahapesu ja terrorismi rahastamise tõkestamise seaduse[68] (RahaPTS) uus redaktsioon, millega võeti Eesti õigusesse üle Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2015/849. Euroopa Liidus on võetud sihiks õiglasem, läbipaistvam ja tõhusam maksustamine, millega toetada jätkusuutlikku majanduskasvu ning investeeringuid. Rahapesu ja terrorismi tõkestatakse ka läbi ettevõtluskeskkonna usaldusväärsuse ja läbipaistvuse suurendamise.[69] 10.03.2020 seadusemuudatusega muudeti virtuaalvääringu teenusepakkuja ja rahakotiteenuse pakkuja tegevusloa saamise nõudeid. Seletuskirjas oli ühe mõju sihtrühmana välja toodud teenuse tarbijad. Raske on hinnata palju neid on, kuid eeldatakse, et teenus on muutumas aasta-aastalt populaarsemaks, mida kinnitab Rahapesu Andmebüroo (RAB) statistika tegevusloa taotluste kohta. Tegevusloa nõuete karmistamise ja turule sisenemise

[65] *Idem*, p 24.
[66] *Idem* p 42.
[67] Finantsinspektsioon, *Virtuaalraha (ICO)*, fi.ee, 27.12.2018.
[68] Rahapesu ja terrorismi rahastamise tõkestamise seadus - RT I, 31.12.2019, 20
[69] SE 459, seletuskiri algatamise juurde, lk 4, 6. (XIII koosseis)

lävendi tõstmisega leiti, et teenus muutub tarbijale turvalisemaks. Teenuse osutajate kontrollitud laitmatu maine ja sobivus aitavad vähendada ka kuritegude, näiteks pettuste, toimepanemise riski.[70]

RAB koostas septembris 2020 virtuaalvääringu teenuse pakkujate uuringu.[71] Uuringu vajadust nähti, kuna virtuaalvääringute kasutajate ja teenusepakkujate arv on kasvanud, sellest tulenevalt ka kuriteoriskid. RABile teadaolevalt kasutatakse Eestis krüptovaluutat kriminaaltulu varjamiseks, rahepesuks, pettusteks ja illegaalsete kaupade ostmiseks. 2018-2019 kasvas tegevusluba taotlenud teenuspakkujate arv kiiresti, seda põhjusel, et Eesti oli krüptovaluuta teenusepakkumiste osas avatud, kokku anti lube välja üle 2000. Märts 2020 seisuga olid tegevusload rahakotiteenuse pakkumiseks 869 ettevõttel ja raha vastu vahetamiseks 946 ettevõttel. RahaPTS muudatuse tõttu tühistati palju tegevuslube, kuna ettevõtted ei suutnud enda tegevust seaduste nõuetega kooskõlla viia, mõned ka oma tegevusest loobunud, mis viis selleni, et augustis 2020 oli tegevuslube kokku 611, kuid kontrollide käigus võib see number veel langeda. 2019 aasta seisuga oli teenusepakkujate käive 1,2 miljardit eurot, mis on kaks korda rohkem kui aasta varem. 91% ettevõtetest võimaldasid kaubelda ja hoiustada Bitcoiniga, levinud olid ka Bitcoin Cash, Etherum ja Litecoin. Üldiselt peab RAB teenusepakkujate hooldusmeetmete täitmist puudulikuks. Vaid 6% Eestis tegutsevat virtuaalvääringu teenust pakkuvatest ettevõtetest esitas RABile 2019 aastal teateid, kuid RahaPTS § 49 järgi on kohustus RABi teavitada, kui keeldutakse tehingute tegemisest või ärisuhte loomisest. Puudujääke nähakse ka ettevõtete poolt isikusamasuse tuvastamisel ja ärisuhte seire teostamisel. On selgunud, et aktsepteeritakse isikusamasuse tuvastamise nõutele mitte vastavaid dokumente. Kuna antud teenuste puhul on üldiselt tegemist kaugteenusega, siis peaks kontrollima ka mitut dokumenti, ehk siis näiteks passile lisaks veel ühte lisadokumenti, seda nõuet aga sageli ei täideta. Samuti selgus, et ei kontrollita kliendi riskiprofiili uuesti kuue kuu möödudes, mis on taas hoolsusmeetmete rikkumine. Analüüs näitas, et sageli on ettevõtted Eestis vaid registreeritud aga tegevus ise ja kliendid asuvad mujal. Peamiselt ilmnes Venemaa, Läti ja muude Ida-Euroopa riikide taust, suurimatest teenusepakkujatest vähem kui 5% tegevus oli Eestis. Ka klientidest on vaid umbes 0,15% Eestist. See aga tähendab, et ettevõtete ja teenusekasutajate seas on palju isikuid RahaPTS § 37 lg 4 mõistes suurema geograafilise riskiga riikidest, mis tekitab omakorda järelevalve ja võimalike kriminaalmenetluste osas probleeme. Leitakse ka, et tegevusloaga ettevõtete rohkusega võib kaasneda mainerisk, mida tõstab ka e-

[70] SE 8, seletuskiri I lugemise juurde, lk 9-10. (XIV koosseis)
[71] Rahapesu andmebüroo (RAB 2020), *Virtuaalvääringu teenuse pakkuja uuring*, 22.09.2020.

residentsus, kuna äriregistri andmetel on rohkem kui kolmandikel ettevõtetel seos vähemalt ühe e-residendiga.

Eesti kohtupraktikas on virtuaalvaluutat käsitletud vaid ühes lahendis ja seda Riigikohtu halduskolleegiumi poolt 11.02.2016 otsuses. Kaasus põhines virtuaalvaluuta vahetusplatvormi teenuse pakkumisel, kui osteti ja müüdi bitcoine. Kolleegium leidis, et Bitcoin on alternatiivne maksevahend, sellel on rahaline väärtus ja sellega on võimalik täita kohustusi.[72] Bitcoin allub alternatiivse maksevahendina RahaPTS vastavatele sätetele, kuid kohus leidis, et vastavaid sätteid tuleb õigusselguse ja tulevate õigusvaidluste vältimiseks täpsustada.[73]

Eesti professor Ahto Puldas avaldas eestikeelse ülevaate plokiahela tehnoloogiast. Tema ei jaga krüptorahaga seotud entusiasmi ning tema hinnangul ole seni teadlaste seas arusaama, miks palju kiidetud pokiahelaks nimetatud loatut hajusraamatut vaja on. Tema pigem leiab, et oluline on vahet teha teistel sarnastel süsteemidel, millest võib kasu olla. Sellest, kas plokiahelat vaja on, annab ülevaate 2018 uuring. Hajutatud süsteem on selline, kus ei pea mitte kedagi usaldama ehk saabki näitena tuua Bitcoini. Krüptoraha ei kasutata mitu korda ja selleks ongi vajalik hajusraamat, et kontrollida kõigi tegevust ja andmeid, ei olla kindel, et ühte krüptoraha ühikut ei kaustata mitu korda. Buldas toob ka välja, et selline hajutatud süsteem ei saa toimida muidu, kui ei ole sisemist motivaatorit halduritel, miks nad võrgustikust üldse osa võtavad. Selleks on antud juhul klassikaline rahaline motiiv, kuna haldurid teenivad teenustasu. Buldas ei usu, et üksi teine motiiv töötaks. Tema sõnul ei ole ka selge, kas sellist plokiahela tehnoloogiat oleks võimalik mõnes muus süsteemis rakendada ja kas see tehnoloogia ka püsima jääb.[74]

Veel 2018 aastal arvas endine Eesti Panga president ja Euroopa Keskpanga (ECB) nõukogu liige Ardo Hansson, et krüptoraha on üks suur mull, mis varsti taandub. Ta lisas, et; „ Juba paari aasta pärast vaatame tagasi, et miks me sellist muinasjuttu uskusime.“[75] Hetkel on sellest paar aastat möödas ja võib öelda, et taandumise märke pole näha. Loomulikult vahepeal on suuri langusi seoses süsteemi rünnakutega, aga see on ka iga majandussüsteemi normaalne areng, et muudatustele reageeritakse. Üldiselt ikka taastutakse nagu ka 2008 aasta majanduslangusest, mis andis üldse esimesele krüptorahale Bitcoin tõuke.

[72] RKHKo 3-3-1-75-15, p 17.
[73] RKHKo 3-3-1-75-15, p 18, 28.
[74] Lõugas, H., *Professor Buldas: pole selge, kas Bitcoini-plokiahelat üldse vaja on ja kas see püsima jääb*, Geeniusmeedia, 23.02.2018.
[75] Lõvi, S., *Hansson nimetas krüptoraha "täielikuks mõttetuseks", mis peagi välja sureb*, ERR, 07.01.2019

Eesti käsitlus krüptorahast on sarnane teiste riikide omaga ja selgelt ka Euroopa Liiduga, sest oleme liikmesriigiks. Eesti, kui väga digilahendusi pooldav, arendav ja propageeriv riik, suhtub krüptorahasse üldiselt positiivselt ja proovib samamoodi teiste riikidega leida lahendust pigem investeerimise valdkonnas. 2017 aastal hakkas ka levima kuuldus, just kui Eesti annaks välja oma riikliku krüptovaluuta Estcoin.[76] See tekitas palju arvamusi ja segadust, kuni plaanile pani lõpu ECB, kes selle ära keelas. Hetkel on see veel vaid mõte ja alles analüüsi staadiumis, kuid arutletakse ka võimalust kasutada Estcoini e-residentsuse programmis selle ametliku valuutana.

2021 aasta algusest toodi RAB iseseisva asutusena Rahandusministeeriumi valitsemisalasse, seda eesmärgil, et rahapesu vastases võitluses saaks fookust suurendada ja lisaressursse kaasata. Sellisel viisil on RABi tihedam koostöö teiste finantsjärelvalveasutustega, mis annab ka eelisarendajana strateegilise andme- ja riskianalüüsi funktsiooni täitjana parema positsiooni.[77] 18.02.2021 valitsuskabineti istungil otsustati, et rahvusvahelistes rahapesu uurimistes antakse Eesti esindamine Justiitsministeeriumile ja Riigiprokuratuurile, seda just põhjusel, et tegemist on uurimismenetluste ja õigusabialase koostööga.[78] Antud otsused ja struktuurilised muutused näitavad, et Eesti peab rahapesu ja terrorismi vastast võitlust väga oluliseks ning proovib leida kõige mõistlikumad lahendused, et uurimine ja koostöö toimiks ladusalt ning tulemuslikult. Samuti on loodud veebileht cyber.politsei.ee, mille kaudu saab esitada küberkuritegevuse teateid ja samuti antakse nõu, kuidas erinevaid küberkuritegude liike ära tunda ja kuidas end kaitsta.

Prokuratuur hindab küberkuritegudest teavitamise määra suureks, arvatavasti tänu 2020 tehtud suurele ennetus- ja teavitustööle. Probleemiks peetakse ressursipuudust, kuna erinevat liiki küberkuriteod on mahukad ja inimesi uurimisasutustes ei ole piisvalt. Samuti asjaolu, et tegemist on üldiselt kuritegudega, mis ületavad riigi piire, mis vajab rahvusvahelist õigusabi ja väga suurtes mahtudes materjalide läbi töötamist. Selleks ajaks kui tööga kuhugi jõutakse, võivad olla kahtlustatavad juba vahi alt vabastatud ja asunud tõendeid hävitama. Keskkriminaalpolitsei küberkuritegude büroo läbiviidud kontrolli tulemusel selgus, et on olukordi, kus IP-aadressi asumist välisriigis käsitletakse kriminaalmenetlust välistava asjaoluna. Prokuratuur leiab, et tuleb tööd teha, et sellist lähenemist muuta, kuna võimekus

[76] Korjus, K., *We're planning to launch estcoin — and that's only the start*, Medium.com, 19.12.2017
[77] Rahandusministeerium, *Rahapesu andmebürood ootab 2021. aastal ees kiire kasv*, 4.12.2020
[78] Rahandusministeerium, *Rahapesu uurimistes lähevad juhtohjad prokuratuurile*, 18.02.2021.

rahvusvahelisel tasemel uurimisel tegelikult on olemas ja enne otsustusi tuleks koguda täiendavaid tõendeid.[79]

2. Võimalikud riskid

Järgnevalt toob autor välja krüptorahaga seotud riskid ning nõrgad kohad süsteemis, mida kurjategijad ära kasutavad. Et probleemi olemusest, sisust ja ulatusest täpsemalt aimu saada, on välja toodud ka näidetena maailmas aset leidnud rünnakud. Digitaalsed süsteemid on üha rohkem kasutuses, seega liigub läbi nende ka aasta-aastalt rohkem raha, millele kurjategijad püüavad ligi saada ning süsteemi ka enda kasuks ära kasutada.

Rahapesuvastaste ELi õigusnormide tõhusamaks muutmine ja sellest tulenevalt suurenenud finantsalane järelevalve pangandussektoris on muutnud kuritegevussektori poolt kuritegelike tulude liigutamise läbi legaalsete traditsiooniliste pangandussüsteemide aina keerulisemaks. Selle tõttu üritatakse rahapesu suunata pigem sektorite poole, kus alles tekivad kontrollmehhanismid või järelevalve on piiratud. See aga võib kaasa tuua põrandaaluste rahasiirde asutuste, alternatiivsete pangaplatvormide, rahvusvahelise kaubanduse ja anonüümse virtuaalvaluutade kasutamise. Krüptovaluuta kasutamine selles vallas on üha kasvav probleem, kuna ei ole ühist regulatsiooni kehtestamist ja teada, millist anonüümsust sellised teenused pakuvad. [80]

RAB[81] leiab, et virtuaalvaluutaga seotud terrorismi rahastamise riske rahapesu kõrval alahinnatakse. Seda põhjusel, et krüptovaluuta on detsentraliseeritud, neid on kiire ja lihtne kasutada, samal ajal on rahvusvaheline regulatsioon lünklik ja teenusepakkujatelt vajaliku info kätte saamine on õiguskaitseorganitel raskendatud. Ei peeta usutavaks, et terrorismi rahastamisel krüptoraha ei kasutata, kui see on juba laialdaselt kuritegelikus maailmas kasutusel. Kaitsepolitsei ametnik hindas antud intervjuus, et virtuaalvääring on levinud islamiäärmuslaste seas, ISIS kasutas neid oma rahakogumiskampaaniates, samuti kasutasid neid palestiinlased. Ainukeseks raskuseks on nende jaoks krüptovaluuta hinna pidev kõikumine, kui soovitakse seda raha vastu vahetada. Kuid üha enam on tagantjärgi tuvastatud virtuaalvääringuid, mida on kasutatud terrorismi rahastamiseks, seda kas siis relvade ostmiseks

[79] Prokuratuuri aastaraamat 2020
[80] SOCTA 2021, lk 28-29.
[81] RAB 2020.

tumeveebist, kapitali kogumiseks või varade rahvusvaheliseks liigutamiseks. RABile on teenusepakkujate poolt laekunud teateid, kus terrorismiga seotud isikud on soovinud luua ärisuhteid. See näitab selgelt, et terrorismiga seotud inimesed on seotud ka krüptovaluutaga.

Levinud on erinevad krüptokuriteod, kus ei ole subjektiks krüptoraha, vaid näiteks nõutakse rünnaku lõpetamise eest lunaraha krüptorahas. 2017 aastal sai alguse lunavara rünnak nimega WannaCry, mis mõjutas üle maailma ca 300 000 arvuti ning mille kahjud ulatusid erinevatel andmetel sadadest miljonitest miljardite dollariteni. Krüptouss krüpteeris arvutis olevaid failid ning kasutaja ei pääsenud neile enam ligi. Lunarahana nõuti ühelt kasutajalt 300-600 dollarit, kui sooviti, et krüpteering maha võetaks. Rünnak kestis küll vaid neli päeva, aga jõudis selle ajaga see palju kahju teha. USAs esitati süüdistus Põhja-Korea kodanikule P. J. Hyok'ile ja temaga seotud ettevõttele, mida tegelikult kontrollis Põhja-Korea. Nii USA, Suurbritannia kui Austraalia on kinnitanud, et rünnaku taga oli Põhja-Korea.[82] Avaldamata ÜRO raporti kohaselt on Põhja-Korea sellisel viisil kogunud krüptorahas umbes 2 miljardit dollarit.[83] WannaCry jõudis ka Eestisse, aga nakatas vaid kuute arvutit.

Autor märgib, et krüptoraha nõudmine lunarahana on kindlasti põhjustatud selle osalisest anonüümsusest. Hiljem on raske kindlaks teha, kuidas ja kuhu on valuuta täpselt liikunud. Kindlasti ei ole selle selgeks tegemine võimatu, kuid nagu ka eespool mainitud, on enamus krüptorahasid pseudo-anonüümsed ning ülekanded on kõigile avalikud. Kuid selleks, et liikumine plokiahelas kindlaks teha, vajab see vastavaid oskusi ja ressurssi, nii rahalist kui ajalist. Keerulisemaks teeb uurimise kindlasti ka see, kui kasutatakse veel ka erinevaid miksimise teenuseid, mis segavad krüptoraha liikumise jälgi ja muudavad need veelgi anonüümsemaks. Europol leiab, et krüptovaluutade kasutamine ja laialdasem anonüümseks muutmiste tehnikate kasutamine, seal hulgas krüpteerimine, tulevikus aina kasvab.[84]

Korruptsiooni aluseks olevad mehhanismid on ajaga muutunud aga viisid, kuidas tegusid toime pannakse peegeldavad otseselt muutusid ühiskonnas ja tehnoloogias. Näiteks ühe enam on levinud, et just krüptovaluutat kasutatakse korrumpeerunud ametnikele maksmiseks ja seda rahapesu eesmärgil.[85] Arenenud digitaalsete tehnoloogiate laialdane kasutamine ja laiaulatuslik sotsiaalmeedia kasutamine ning krüpteeritud suhtlemise võimalused annavad võimaluse

[82] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[83] Pavlo, W., *Crime And Punishment In The Cryptocurrency World*, Forbes, 25.02.2020.
[84] SOCTA 2021, lk 40.
[85] *Idem*, lk 26.

migrantide smuugeldajatele, et koordineerida oma tegevusi, värvata nii töötajaid, kui ohvreid ja vältida õiguskaitseorganite poolt nende märkamist. Hiljuti on teatatud ka krüptovaluuta kasutamisest salakaubavedajate poolt ja Europoli hinnangul võib seegi lähitulevikus suureneda.[86]

Krüptokaevekaaperdused (*cryptojacking*) on siiani probleem, kuid ei ole hetkel Europoli jaoks prioriteet. Selle haripunkt oli 2018 aastal, kuid langes peale seda põhjusel, et märtsis 2019 suleti kaevesüsteem Coinhive, kus kaevandati krüptoraha Monero, mida oma anonüümsuse tõttu on raskem jälitada.[87] Krüptokaevekaaperduste puhul nakatatakse arvuti viirusega, peale mida kasutatakse arvuti ressursse kas kaevandamiseks või selleks, et varastada krüptoraha teistest digitaalsetest rahakottidest. Antud kaaperdamine on häkkerite seas aina populaarsem, kuna pahavara on kerge arvutitesse paigutada ja ka keeruline avastada ning pigem jääb see märkamatuks. Aina levinum on ka kinnistada pahavara Youtube'i platvormile, kus on kergem leida ohvreid, kes lingile klikiks.[88] Kuigi sellised ründed võivad mõjutada paljusid, on tavaliselt kahjud väikesed ja seetõttu rünnetest teinekord ka ei teatata.[89]

Youtube platvormiga seoses saab tuua hiljutise näite, kus Ripple kaebas kohtusse YouTube'i just põhjusel, et viimane ei suutnud kaitsta tarbijaid krüptovaluuta pettuse eest. Petturid asutasid Youtube platvormi, et esineda Ripple või selle juhina, Brad Garlinhouse'ina, eesmärgiga meelitada vaatajaid saatma neile tuhandete dollarite väärtuses ripple'eid (XRP). Inimestele lubati tagasi saata kokku pea 1 miljoni väärtuses XRP'd, aga seda ei tehtud. Nüüd hageb Ripple, et vastutuse võtaks hoopis YouTube'i, kes peaks oma platvorme rohkem kontrollima ja mitte laskma valekontodel seal tegutseda.[90]

Europol on oma 2019 analüüsis välja toonud, et kui varasemalt olid levinud krüptorünnakud teise maksesüsteemide või tagatud valuuta vastu, siis aastatega on krüptoraha ise sattunud rünnakute sihtmärgiks. Tihti nähakse pahavara ja õngitsemist, mis on suunatud just krüpto-investeerijate ja ettevõtete vastu.[91] Internetis levivate kelmuste puhul tuginetakse üha enam

[86] *Idem*, lk 68.
[87] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2019, lk 54.
[88] Sobers, R., *What Is Cryptojacking? Prevention and Detection Tips*, Varonis.com, 29.01.2021
[89] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2019, lk 54.
[90] Paul, K., *Ripple sues YouTube over cryptocurrency scams*, Reuters, 21.04.2020.
[91] IOCTA 2019, lk 54.

uudsetele investeeringutele, nagu näiteks krüptovaluutad, sellisel kujul on sihtmärgiks võetud tuhanded inimesed Euroopas. [92]

RAB on oma hiljutises uuringus[93] välja toonud üldise trendi Eesti kuritegevuses. Politsei ja Piirivalveameti küberkuritegude uurija tõi oma intervjuus välja, et virtuaalvääringute kasutamine kuritegelikes skeemides on levinud, neid kasutatakse ettevalmistavates etappides ja omavahelises arveldamises. Krüptoraha kasutatakse pea kõigi kuriteo liikide puhul, kuid levinud on kasutatavate taristute või teenuste eest tasumine ja lunarahanõudmine just virtuaalvaluutas. Keskkriminaalpolitsei näeb peamiste riskidena kelmuste, sageli investeerimiskelmuste, ja rahapesu riski. Hetkel on aktuaalsem kelmustega seotud risk, kuna Eestile on tulnud mitmeid õigusabi palveid, kus teenusepakkujad on kelmusi toime pannud. Samuti on õigusabi koostöö kaudu kinnitust leidnud virtuaalvaluutade kasutamine rahapesus. Viru Maakohtu otsuses kriminaalasjas nr 1-19-5363[94] tuvastati virtuaalvääringute kasutamine rahapesuks. RABile antud intervjuus[95] tõi uurija välja, et lihtsamate skeemide puhul pressitakse inimestelt krüptoraha välja, kantakse see teise rahakotti ja seejärel segatakse jälgi. Mahukamate skeemide puhul kaasatakse keegi siseringist, teenusepakkuja töötaja, kes vaatab rahapesu tõkestamise nõuetest mööda. Uurimise teeb keeruliseks just see, et krüptoraha kantakse riikidesse, kus regulatsioonid on nõrgad, vääringute liikumist pole võimalik jälgida ja infot saada. Suurimaks murekohaks tuuaksegi rahvusvaheline koostöö. Virtuaalvääringutega seotud kuriteod on pea kõik rahvusvahelise mõõtmega, mille avastamine ja tõkestamine on keeruline, kui koostöö ei toimi.

RAB leiab[96], et RahaPTS muudatused oli samm õiges suunas, kuid suuri kuriteoriske silmas pidades tuleks teenusepakkujatele kehtivaid nõudeid veelgi karmistada ja panustada lisavahendeid järelevalve sektorisse. Aitaks näiteks aruandluskohustuse sisseviimine, mis annaks parema ülevaate turuosalistest, mis mahus ja millistel turgudel tegutsetakse, see annab omakorda võimaluse riske kaardistada. Teenusepakkujatel peaks olema ka keeld tehinguid kinnitada, kui hoolduskohustust ei suudeta mingil põhjusel täita. Leitakse, et praegune rahapesu tõkestamise regulatsioon ei anna võimalust võidelda teenusepakkujate asjatundmatuse ja pettustega. Tuleb aga kindlasti arvestada ka sellega, et teenusepakkujad ise annavad välja

[92] SOCTA 2021, lk 43.
[93] RAB 2020
[94] Viru Maakohtu 20.11.2019 otsus kriminaalasjas 1-19-5363. https://www.riigiteataja.ee/kohtulahendid/fail.html?id=259824625
[95] RAB 2020
[96] *Ibidem.*

valeinfot ja manipuleerivad tehinguhindadega. RABi arvates oleks võimalike muudatustega seoses loogiline virtuaalvaluutad finantsjärelvalvele allutada.

2.1.1. ICOd ja pettused

Uute kelmuste tüpoloogia on seotud internetis olevate töövahendite ja digitaalsete tehnikatega. Interneti kelmuste liike on palju, need võivad olla, kuid ei ole kindlasti ainult BEC pettused (ingl *Business Email Compromise* – e-postkastide valesti kasutamine), mille sihtrühmaks on ettevõtted ja organisatsioonid, nende sagedus aina kasvab ja muutuvad üha keerukamateks; SIM (kaardi) vahetuse pettus ja *smishing* ehk andmepüük SMSi teel; *online* investeerimispettused, mis üha enam on seotud krüptovaluutaga; andmepüük, mis on jätkuvalt märgatav oht ja oma olemuselt samuti areneb.[97]

Hiljuti sattusid ka Eesti kodanikud õngitsuskirjade ründe alla, kus prooviti Smart-ID ja Mobiili-ID autentimistaotluste saatmise teel saada juurdepääs internetipanka ja kanda seal olevad rahalised vahendid teistele pangakontodele. Mahuka rahvusvahelise politseioperatsiooni tulemusel peeti kinni 3 Rumeenia kodanikku.[98] Riigi Infosüsteemide Ameti andmetel tekitati kahju ligi 40 inimesele ja üle 100 000 euro väärtuses.[99] Hetkel on tuvastatud kannatanuid ka Lätist. Kurjategijate tegevusele saadi jälile tänu sellele, et nii Eesti kui Läti pangad märkisid ära kahtlaseid tehinguid ja seda kokku pea 450 000 euro ulatuses. See aga annab uurijatele aluse arvata, et kogu skeem on palju suurem ja kannatanuid on teistes riikides veel.[100]

Selle aasta 9. veebruaril vahistati 8 inimest mitmete SIM (kaardi) vahetuse pettuste eest, kus ohvriteks olid tuntud inimesed Ameerika Ühendriikidest ja varastatuks peetakse üle 100 miljoni dollari. Varasemalt oli kinni peetud ka üks inimene Maltalt ja üks Belgiast. Rünne ise seisnes selles, et 2020 aasta jooksul olid sihtmärkideks tuhanded inimesed, sealhulgas tuntud sportlased, interneti suunamudijad, muusikud ja nende perekonnad. Kümned kurjategijad töötasid koos, et saada ligipääs kannatanute telefoninumbritele, misjärel nende SIM kaart deaktiveeriti ja number teisaldati kurjategija poolt kontrollitud SIM kaardile. Edasi kasutati

[97] SOCTA 2021, lk 99.
[98] Rattam, E., Küberkuritegevuse ökosüsteem on muutunud teenusepõhiseks. Prokuratuuri aastaraamat 2020.
[99] Liive, R., *Rumeenias tabatud küberpättide ohvriks langes ligi 40 eestlast, kahju üle 100 000 euro*, digi.geenius.ee, 07.04.2021.

[100] *Hook, line and sinker: cybercrime network phishing bank credentials arrested in Romania*, Europol, 29.09.2020.

numbrit selleks, et saada kontroll ohvrite rakenduste või kontode üle nende salasõnade muutmise läbi. See andis võimaluse varastada raha, krüptovaluutat ja isiklikku informatsiooni, samuti seda, mis oli sünkroniseeritud erinevate kontodega. Sealjuures häkiti sotsiaalmeedia kontodesse, mida kasutati ohvrit mängides sisu varastamiseks ja sõnumite saatmiseks. Tavaliselt saab see võimalikuks kasutades ära sideettevõtjaid, lastes neil need vahetused ära teha, kasutades kas ettevõttega seotud isikut või mõnda manipuleerimistehnikat. Aasta aega kestnud Europoli toetusega rahvusvahelises uurimises osalesid Suurbritannia, Ameerika Ühendriigid, Belgia, Malta ja Kanada. Europol soovitab selliste rünnete vältimiseks uuendada pidevalt oma tarkvara, piirata oma isikliku informatsiooni avaldamist internetis, kasutada kahetasandilist autentimist ja kui võimalik, mitte siduda oma telefoninumbrit tundlike kontodega internetis.[101]

Levinud on uut liiki kelmused ehk krüptorahasse või krüptorahaga investeerimiskelmused. Üheks põhjuseks, miks sellist liiki kelmused edukad on, peetakse potentsiaalsete ohvrite tavaliselt mitte nii häid teadmisi sellisest vara liigist.[102] ICO (ing *initial coin offering* – esialgne mündi pakkumus) on detsentraliseeritud raha kaasamise mudel, millega ettevõte otsib võimalust kaasata läbi investorite raha, et luua uus krüptomünt, -rakendus või -teenus. Kui investorid on huvitatud, siis nad saavad osta endale pakkumuse ja vastutasuks saavad krüptovaluuta tokeni, mille ettevõte on välja andnud. Tokenit võib saada kasutada ettevõtte poolt pakutavate teenuste või toodete eest tasumiseks. See saab olla ka kui ettevõtte või projekti osaku esindus.[103] Paralleeliks saab tuua IPO (ingl *Initial Public Offering* – esialgne avalik pakkumus) ehk esmane avalik pakkumine, mil on võimalus esimest korda avalikult ettevõtte aktsiaid osta. Mõlemad on investeerimisinstrumendid konkreetsesse projekti või ettevõttesse. Kuid peamine erinevus on selles, et IPOde puhul saab investeerija kindlasti ettevõtte osaku, kui ICOde puhul on levinumaks krüptorahade väljaandmine. Samuti, IPO puhul on üldiselt tegemist tuntud ja pikaajalise tegevusega ettevõttega. Ettevõte peab IPO korral avaldama ka prospekti, kus investor saab kõik vajaliku info ettevõtte majanduslikust olukorrast ja tuleviku plaanidest, osalistest. Seevastu ICOde puhul ei ole tegemist aktsiaseltsidega, vaid populaarsem on selline investorite kaasamise meetod start-up'ide ehk alles alustatavate uusettevõtete puhul.[104] ICOde välja andmisel peavad ettevõtted esitama *white paper*'i, mis on sisuliselt äriplaan, kus on välja toodud toode, meeskond, projekti eesmärgid ja struktuur. Olemuselt on

[101] *Ten hackers arrested for string of sim-swapping attacks against celebrities*, Europol, 10.02.2021.
[102] IOCTA 2019, lk 54.
[103] https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp
[104] https://cointelegraph.com/ico-101/ico-vs-ipo-key-differences

investeerimine riskantne, sest kunagi ei tea, kuidas ettevõttel minna võib. Ka IPO puhul võib raha kaotada, mis siis, et investeerimise hetkel läks firmal hästi. Start-up'e peetakse üldisemalt veel väga riskantseteks, kuna nad alles alustavad oma tegevusega, samas ei tea kunagi, kas jõutakse pankrotini poole aastaga või on tegemist järgmise Apple Inc'ga. Umbes 86% ICOsid on Ethereumi platvormil.

Alates 2016. aastast on rohkem kui 5000 ICOt kaasanud märkimisväärseid vahendeid, hinnatakse, et need on ületanud juba 50 miljardi piiri. ICOd on muutunud aina populaarsemaks ja saab pidada lausa fenomeniks, sest 2018 aasta esimese üheteist kuu jooksul kaasati rohkem rahalisi vahendeid kui eelneva nelja aasta jooksul kokku. Esimesed ülisuured ICO olid 2018 aasta alguses Telegram, kes kogus 1,7 miljardit dollarit ja Block.one, kes kogus omakorda 4,1 miljardit dollarit.[105] 2019 aasta statistika kohaselt on Eesti ICOde arvu poolest viiendal kohal[106] ja mahu mõttes seitsmendal kohal. Mahu osas juhivad Kaimanisaared, mis omakorda aga tähendab seda, et õiguslik taust on erinev, pidades silmas finantssüsteemi, vastavalt sellele, kust ICO välja antakse.[107]

Kuna ICOd on reguleerimata, on levinud ka pettused. Sellised on projektid, kus ei ole tegelikult mingit kavatsust investeeritud vahenditega projekti eesmärki täita. 2018 aasta uuringu kohaselt leiti, et ligi 80% ICOdest on pettused.[108] Teine samal aastal tehtud uuring leidis samuti, et üle poolte, umbes 55%, puhul oli tegu pettusega. Tuleb aga arvestada sellega, et paljud ICOd kaovad juba 120 päevaga ja mõningaid neist ei ole võimalik enam üles leida, et uuringutesse kaasata.[109] Üks kõige suuremaid ICO pettuseid on olnud Vietnami krüptoraha ettevõtte poolt, kes andsid välja Pincoini tokeni, millega nad kogusid 660 miljonit dollarit umbes 32 000 inimeselt. Investoritele anti alguses vastutasuks raha, hiljem iFan tokeneid. Ja siis vietnamlased kadusid ja neist jäi maha ainult kasutu koduleheküIg, iFan tokenitel polnud väärtust ja investorid olid oma raha kaotanud.[110]

---

[105] Zetzsche, D. A. jt, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators,* Harvard International Law Journal vol 60, nr 2, suvi 2019, lk 268.
[106] *Idem* lk 285.
[107] *Idem* lk 266.
[108] Kim, C., *Report: More Than Three-Quarters of ICOs Were Scams*, CoinDesk, 12.07.2018. https://www.coindesk.com/report-more-than-three-quarters-of-icos-in-2017-were-scams
[109] Palmer, D., *More Than Half of ICOs Fail Within 4 Months, Study Suggests,* CoinDesk, 10.07.2018. https://www.coindesk.com/over-half-of-icos-fail-within-4-months-suggests-us-study
[110] Biggs, J., *Exit scammers run off with $660 million in ICO earnings*, TechCrunch, 13.04.2018. https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/

Kanada lõi võlts ICO lehe selleks, et investoreid harida ohtudest, mis krüptovaluutat ümbritsevad. Veebileht pakkus võimalust investeerida turismi edendamisesse ja keskkonna aktivismi. Lubatakse 85-115% tootlust ja läbi investeeringute toetab ettevõte heategevusorganisatsioone, olemas oli ka YouTube'i video, kus kogu ettevõtmist tutvustati. ICO pakkumusi iseloomustavadki ettevõte kohalik mõju ja sotsiaalne heaolu, kindlasti ka suured teenimise võimalused. Kui veebilehega tutvunud võimalikud investorid olid juba valmis oma raha investeerima ja vastavale nupule vajutasid, suunas see otse lehele, mis ütles, et kogu ettevõtmine on võlts ja selgitas, kuidas ICO pakkumustega seoses punaseid lippe märgata. Kindlasti on ohumärgiks see, kui kinnitatakse, et tulu on garanteeritud ja pole mitte mingit riski. Kelmid kasutavadki ilustatud terminoloogiat ja ebamäärast tehnilist kõnet, et jätta mulje, et võimatu on võimalik. Suureks ohumärgiks on ka see, kui ICO ei too välja partnerite või omanike kontaktinformatsiooni. Vastavatel veebilehtedel on ka pööratult loendavad kellad, mis on mõeldud selleks, et võimalikud investorid tunneks pinget, et nad peavad kiiresti ära otsustama, muidu jäävad suurepärasest võimalusest ilma.[111] See näide ilmestab selgelt, kui suures teadmatuses krüptovaluuta kasutajad teinekord on, kuigi inimesed langevad ka muude kelmuste ohvriteks, on krüptovaluuta kelmuste nagu ka kõigi kuriteo liikide puhul vajalik ennetus- ja teavitustöö.

2019 aastal tehti lõpp Belgias ja Prantsusmaal tegutsevale kuritegelikule organisatsioonile, mis oli üles ehitanud komplektse pettuse skeemi, millega lubati suurt kasu investeerinutega bitcoini, kulda ja teemantidesse. Kahtlustatavad pakkusid oma finantsteenuseid internetiplatvormidel ja samuti seadsid üles riiulifirmasid, mis olid osa nende rahapesuskeemist. Kannatanutele lubati investeeringute pealt kasu 5-35%, peale mida nad teesklesid, et justkui tegeleti investorite rahakottidega ja kutsuti veel raha investeerima. Selleks, et usaldust tugevdada, maksti osadele kannatanutele ka osa intressidest ja kui investorid olid enda poole võidetud, pakuti veel paremaid investeerimisvõimalusi, mis loomulikult vajasid suuremaid rahasummasid. Prantsusmaal olid kannatanuteks teiste hulgas nii suur erafirma, kui ka kohalik omavalitsusasutus. Investeeritud raha paigutati erinevates EL liikmesriikides asuvatele kontodele enne, kui liigutati teistele rahvusvahelistele kontodele. Usutakse, et kelmused tekitasid kokku kahju rohkem kui 6 miljonit eurot. Uurijad leidsid ka arveid mõne miljoni euro väärtuses, mida ei oldud veel jõutud kontodele kanda. Kokku arreteeriti 9 inimest, uurimise

[111] Down M., *The Latest ICO Scam… is Fake?*, Hackermoon 16.03.2019. https://hackernoon.com/the-latest-ico-scam-is-fake-a106b149f099

rakkerühma kuulusid uurijad Belgiast, Iisraelist, Prantsusmaalt, kellel oli ka Europoli tugi.[112] Niivõrd ulatuslikult töötavate kuritegelike organisatsioonide tabamiseks on vaja väga palju ressursse ja rahvusvahelist koostööd, mis antud juhul tõi ka tulemuse.

2.1.2. Digitaalsed rahakotid ja vahetusplatvormid

Krüptorahaga seotud kaotused oli 2019 aasta üheksa kuuga 4,4 miljardit dollarit, 150% sellest, millised olid kaotused varasema terve 2018 aasta peale. See näitab, et ka kurjategijad kohanevad ning otsivad suuremaid ja paremaid tulemusi. Tihti ongi kergem end kaitsta väiksemate rünnakute vastu. Suuremaid ja paremini sihistatud rünnakuid on teinekord raske ette näha ja nendeks ka valmistuda, rünnakud ise on aga kindlasti kurjategijatele tulutoovamad. Aasta-aastalt kuritegude arv kasvab, kuid tihti kuritegusid, mille puhul on kahjud alla 5 miljoni dollari, ei teatata, sest proovitakse keskenduda suurematele ohtudele. Kurjategijad on kannatlikumad ja valmis kulutama rohkem aega, et saada võimalikult suuremat tulu. Üha enam on rohkem kui 100 miljoni dollarilisi varguseid, kuid ka vargad on kavalamad, võttes teinekord raha välja väikeste summade kaupa, mis ei jää sellisel juhul nii palju silma.[113]

Online krüptoraha rahakott on teenus, mis hoiab ja kaitseb kliendi krüptoraha. Krüptovaluuta omamiseks on vaja vaid privaatvõtit ja neid rahakoti teenuse pakkujad hoiavadki. Kui kliendid hoiavad oma krüptoraha *online* rahakotis, siis neil ei ole juurdepääsu oma privaatvõtmetele ja nad peavad lihtsalt usaldama oma rahakotiteenust. Lisaks on olemas ka vahetusplatvormid, kus on võimalik krüptoraha vahetada teise vastu, või siis ka nii-öelda päris raha vastu. Lisaks vahetusteenusele pakuvad platvormid ka rahakoti teenust. Platvormid erinevad vastavalt aktsepteeritud krüptorahadele ja nende teenustasudele.[114] Selleks, et üldse platvormil aktiivne olla, peab klient oma rahakotti samuti samas kohas hoidma. Ka vahetused on võimalikud vaid klientide vahel, kes on samal platvormil. Seega, kuna nad pakuvad mõlemat teenust, siis see on kohaks, kus on kõik olemas, mida investorid või vahetustest huvitatud inimesed otsivad.[115]

---

[112] *Fake investors busted in Belgium and France*, Europol, 29.01.2020. https://www.europol.europa.eu/newsroom/news/fake-investors-busted-in-belgium-and-france
[113] Chavez-Dreyfuss, G., *Cryptocurrency crime surges, losses hit $4.4 billion by end-September: CipherTrace report*, Reuters, 27.11.2019.
[114] Chu, D. *Broker-dealers for virtual currency: regulating cryptocurrency wallets and exchanges*, Columbia Law Review, vol 118:2323, 2018. Lk 2327-2328.
[115] *Idem*. lk 2329.

2013 aastal häkiti väidetavalt ühte kõige turvalisemat *online* rahakotti Inputs.io. Korraldati kaks häkki, millega varastati kokku 4100 BTC, mis olid selle hetke seisuga väärt 1,2 miljonit dollarit. Rünnakuks kasutati vana tehnoloogiaga ohustatud e-kirju, mida ei saanud jälitada ning sisse saadi tänu serveri veale. Vargus toimus lehekülje kuumas ehk *online* rahakotis, mille aktiivsus on vajalik, et teha ülekandeid või väljavõtteid. Kahjuks hoidis aga Inputs.io enamike oma hallatavaid varasid *online* rahakotis. Enamik rahakoti teenuse pakkujaid hoiavad ligi 80% külmades rahakottides ja eks see Inputs.io'le saatuslikuks sai ja seetõttu kahju nii suur oli.[116]

Üks kõige tuntumaid ja suuremaid vahetusplatvormiga seonduv katastroof oli Mt. Gox. Oma tegevuse tipul toimusid umbes 80% Bitconi vahetustest just sellel platvormil. See jõudis aga pankrotini 2014, kui öeldi, et kaotatud on 850 000 bitcoini, mis sellel hetkel olid väärt peaaegu pool miljardit dollarit, ja 28 miljonit dollarit sularaha. Mt. Gox süüdistas kaotuses häkkereid, kes kasutasid ära tarkvara olevat turvaauku, samal ajal öeldes, et leidis 200 000 bitcoini üles. Süüdistus esitati aga Mt. Gox juhile, Mark Karpeles'ile, seda Jaapanis, kuna firma oli Tokyos registreeritud. Süüdistus seisnes vara omastamises ja andmete manipulatsioonis, sest tuli välja, et Karpeles suurendas oma kontot platvormil 1 miljardi dollari võrra ja kandis ettevõtte kontolt, mis hoidis klientide raha, enda nimele 3 miljardit dollarit. Kannatanud aga siiani ootavad oma raha tagasi ja kahjude hüvitamist. Bitcoinile oli selline juhtum suur löök, väärtus langes ja ka üldine krüptoraha maine. Samas juhtis see tähelepanu vahetusplatvormide nõrkadele kohtadele ning saadi aru, et süsteemi peaks kuidagi reguleerima. Just sellel põhjusel oli Jaapan esimene, kes võttis seisukoha, et krüptoraha vahetused peavad olema riiklikul tasemel litsentseeritud. Samuti peavad platvormid oma vahendid hoidma eraldi klientide omadest. [117] See võib olla aga üks hea õppetund kogu krüptoraha süsteemile, et arendajad ja teenuse pakkujad saaks aru, kus on võimalikud turvaaugud ja need elimineerida või vähemalt nende kuritarvitamist tõkestada.

Binance on samuti üks krüptoraha vahetusplatvorm ja 2018 aasta seisuga oli see liigutatavate mahtude suuruselt kõige suurem. Häkkerid kandsid Binance'ilt ära 40 miljoni dollari väärtuses bitcoine. Platvorm ütles, et vargad kasutasid andmepüüki ja viiruseid, et 7000 bitcoini enda valdusesse saada. Nende enda hinnangul oli see 2% nende hoiustatavastest bitcoinidest. Binance ei suutnud ülekannet kuidagi tõkestada aga kohe, kui kanne oli tehtud hakkasid alarmid tööle ning kõik muud kanded peatati. Vahetult peale Binance'i avalikku teadet vargusest, langes

[116] Boase, R., *Hackers steal $1.2 Million of bitcoins from Inputs.io, a supposedly secure wallet service*, coindesk.com, 07.11.2013.
[117] Gibbs, S., *Head of Mt Gox bitcoin exchange on trial for embezzlement and loss of millions*, The Guardian, 11.07.2017.

bitcoini väärtus 3%, nüüdseks on see taastunud.[118] Kuid rahakotte, kuhu bitcoinid kanti, hakati jälgima ning Coinfirm, kes seda tegi, teatas, et kuu aega peale häkki hakati bitcoine uutesse rahakottidesse liigutama. Igasse järgmisesse rahakotti liigutamisega kanti mingi osa veel ühte eraldiseisvasse rahakotti, teinekord on tegemist väikeste summadega. Coinfirmi jaoks oli antud tegevus veidi imelik ja ei osanud sellele konkreetselt selgitust anda. Tegemist võis olla tasude maksmistega häkis kaasategijatele või proovitakse varastatud bitcoine pesta, et need lõpuks välja võtta. Antud rahakotte jälgitakse aga väga hoolsalt ja tagatud valuuta vastu vahetamine on neil kindlasti keeruline.[119] Autor märgib, et hetke seisuga on kõik artiklis välja toodud rahakotid tühjad.[120]

30. detsembril 2020 sattus küberrünnaku alla Eestis resideeruv krüptorahakoti teenus Guarda. Ligipääs saadi häkkides sisse domeenide võõrustamise teenust pakkuvasse GoDaddy'sse, kes pakkus teenust ka siis Guardale. Veidi enne kesköödt tõkestati GoDaddy kaudu Guarda kahekordne autentimine ja domeen suunati hoopis võltsitud sisselogimise vormile. Juba 30 minuti pärast pöördus rahakoti teenus GoDaddy poole, saates kõik dokumendid, et kontod taastada. Vähemalt ettevõtte tegevjuhi Paul Sokolovi sõnul ei olnud GoDaddy väga koostöö aldis ja lahendustele orienteeritud. Guarda on esitanud avalduse Politsei ja Piirivalveametile uurimise alustamiseks. Umbes 9 tunniga suutis teenusepakkuja enda meeskond ligipääsud taastada ja kohe kui oldi kindel, et domeeni kasutamine on taas ohutu, anti sellest sotsiaalmeedia kaudu kõigile oma klientidele ka teada. Guarda saatis kohe kõik dokumendid ja aadressid suurematele vahendusplatvormidele, et saada aadressid, kuhu kelmid raha kandsid, musta nimekirja.[121] 04 jaanuariks oli selgeks tehtud, et suurem osa varastatud virtuaalvaluutast oli kantud Ethereumi rahakotti, sealt Bitcoini ja siis juba teistesse erinevatesse rahakottidesse. Ühikute liikumistel hoitakse silma peal 24/7. Jaanuari algusega oli oma kahjudest teada andnud umbes 100 inimest, kelledest 15% on valmis esitama kollektiivne hagi süüdistusega kelmuses ja varguses, läbi arvutidomeeni võõrustavasse teenusesse sisse häkkimise. Võimalike hagejate arv kasvab pidevalt. Guarda kaalus ka võimalust GoDaddy vastu hagi esitada koos teiste krüpto teenuseid pakkuvate ettevõtetega, sest viga tui nende hinnangul GoDaddy poolt ja mõjutatud olid väga mitmed ettevõtted. Sellest hoolimata on ettevõte valmis oma klientidele vähemalt osa

[118] Shaban, H., *Binance says hackers stole $40 million worth of bitcoin in one transaction*, The Washington Post, 08.05.2019.
[119] Biggs, J., *$6 Million in Stolen Binance Bitcoin Is On the Move Again*, CoinDesk, 13.06.2019.
[120] https://blockchair.com/bitcoin/address/19JPv7roMqfG2PdC42RDxXuT7vbZGT5Asg, https://blockchair.com/bitcoin/address/1JSfJ4WanUHYWF5y84FCDV8QMHLDVr9PE4, https://blockchair.com/bitcoin/address/bc1qcgwn2nv906k3rws803zhxwq3crfgjvnzjejgyq, https://blockchair.com/bitcoin/address/bc1qcgwn2nv906k3rws803zhxwq3crfgjvnzjejgyq
[121] Sokolov, P., *Security Incident on December 20, 2020*, Guarda.com, 02.01.2021.

nende kaotatud summadest hüvitama. Välja on mõeldud erinevaid alternatiive, ühe võimaluse järgi näiteks kõigile makstakse välja kuni 2000$ ulatuses, kui kaotatud oli Bitcoin või krüptovaluuta, alternatiivselt topelt summas Guarda enda tokenite loovutamine kolme aasta jooksul. Ettevõte loobus GoDaddy teenuste kasutamisest, uuendavad ja muudavad oma turvasüsteeme mitmekesisemateks ning samuti otsivad nii-öelda eetilisi häkkereid (ingl *white hat*), kes aitaksid varad üles leida ja samuti infrastruktuuri ja koodi üle vaadata. Guardal on ka plaan välja anda vaevatasu häki eest vastutava isiku kätte saamise eest.[122]

Tänaseks päevaks ei ole antud asjas arenguid teada, Guarda enda blogis midagi rohkem postitanud ei ole, kuigi lubas kliente kursis hoida. Võimalik, et info saadeti otse avalduse esitanud kannatanutele. Kuid samal ajal on ka teada, et selliste kuritegude puhul võtab uurimine palju aega ja vajab ressursside kaasamist. Antud juhtum näitab aga taaskord seda, et isegi rahakoti teenuse pakkuja võib väga aktiivselt tegeleda turvalise teenuse pakkumisega, kuid nõrk lüli võib olla hoopis kuskil mujal, mõne koostööpartneri poolt tehtud vales klikis. Guarda ise tegutseb võib öelda, et väga professionaalselt ja selgelt on valmis oma klientide ja usaldusväärsuse hoidmise nimel osa kahjudest ka enda sissetulekutest ära maksma.

Lisaks on levinud ka varem mainitud miksimisteenused, mis muudavad krüptoraha veel anonüümsemaks. 22.05.2019 oli päev, kui Hollandi Maksu-ja Tolliamet (FIOD) koostöös Europoliga ja Luksemburgi õiguskaitseasutustega surusid maha ühe maailma juhtivad krüptoraha miksimisteenust pakkuva ettevõtte Bestmixer.io. FIOD alustas asja uurimist juba 2018 koostöös interneti turvalisus ja viirusetõrje teenust pakkuva McAfeega, mille tulemusel arestiti 6 serverit Hollandis ja Luksemburgis. Bestmixer.io oli üks suuremaid krüptorahale miksimisteenust pakkuv ettevõte, teenuseid pakkus ta nii Bitcoinile, Bitcoini Cashile ja Litcoinile. Teenusel oli aasta jooksul ringluses vähemalt 200 miljoni dollari väärtuses krüptoraha, mis on umbes 27 000 bitcoini. Teenus garanteeris selle, et kliendid jäävad anonüümseteks. Teenuseid on tegelikult kahte liiki, nii mikserid kui nii-öelda trumblid. Nende tööpõhimõtteks on see, et nad miksivad tuvastatavad või endale märgi külge saanud krüptorahad teistega nii, et originaalallika jäljed hägustuksid. Menetluse tulemusel selgus, et paljud Bestmixer.io krüptorahadel oli kriminaalne taust, mikser ilmselt aitas kriminaalset raha pesta. Hollandi Maksu-ja Tolliamet kogus kokku kõik teenusepakkuja suhtlused viimase aasta

[122] Sokolov, P., *Important Notice On Guarda SAFU***,** Guarda.com, 04.01.2021.

jooksul ja IP aadressid. Kui need on analüüsitud, siis jagatakse neid ka teiste riikide ja Europoliga.[123]

Ehk siis üheks kõige kaitsetumaks kohaks krüptoraha puhul on just vahetusplatvormid ja *online* rahakotid. Platvormid küll pidevalt arendavad programme aga ei suuda kunagi valmis olla kõikideks võimalikeks rünneteks. Tuleb arvestada ka sellega, et iga vahetusplatvormi klientide mass on väga suur ning ei olda lihtsalt võimelised seda kõike haldama. Sellist liiki vargused on ka väga mitmekülgsed ehk ei ole asi ainult turvaaugus. Häkkerid saavad juba vajalikke andmeid rünnaku lõpuleviimiseks andmepüügi ja pahavaraga. Seega peaks iga inimene, kes soovib oma vara kaitsta, teadlikult krüptorahaga ringi käima ja tegema teadlikke otsuseid oma igapäevases tegevuses Internetis.

2.1.3. Jälitamatud

Krüptoraha puhul tekitab ebakindlust kindlasti ka see, et kui see kord kasutaja kontrolli alt väljub, kas siis kantakse teise rahakotti või varastatakse privaatvõti, ei ole seda võimalik enam kuidagi tagasi saada. Ehk siis just samade viidatud häkkide puhul, kui bitcoinid on varastatud ja teise rahakotti kantud, siis on võimalik rahakotti jälgida aga sisu tagasi kanda ei saa. Samuti ei ole võimalik alati kindlaks teha, kes rahakoti taga on. Seda on näha Binance häki puhul, kus rahakotte ja seal toimuvaid liikumisi jälgitakse, kuid kellelegi süüdistust pole esitatud. Üldiselt soovitatakse mitte kasutada *online* rahakotte oma krüptoraha ligipääsuks vajaliku privaatvõtme hoiustamiseks, kuna need on rahakotti pakkujatest kõige kergemini rünnatavad. Pigem kasutada külma rahakotti ehk siis mõnda riistvara lahendust, kus saab oma võtit hoida ja seda kasutada vaid siis, kui on soov ülekandeid teha. Oma võtit niisama mõnel veebilahendusel hoida ei ole mõistlik ega turvaline. Riistvara kõrval on turvalisem lahendus isegi võtme hoidmine paberkandjal. Muidugi on ka näiteks kõvakettal ja paberil omad hävinemise viisid. Maailmas on olnud palju juhtumeid, kus inimesed on ostnud bitcoine ja hiljem enam ei mäleta, kuhu täpselt privaatvõtme panid või on selle ära visanud. Sarnaselt unustas oma rahakoti parooli ära Rain Lõhmus ja ei pääsenud ega pääsegi ostetud ethereumidele ligi, mille väidetav väärtus oli vahepeal suurem kui LHVl.[124] Hetkel on olukord selline, et kui vahetusplatvorm või *online* rahakotihaldur peaks minema pankrotti, seda häkitakse või pannaks õiguskaitseorgani poolt

[123] Europol, Press release: *Multi-million euro cryptocurrency laundering service bestmixer.io taken down*, 22.05.2019.

[124] *Lõhmus teenis krüptorahaga miljoneid, kuid ei saanud sellele ligi*, Äripäev, 13.07.2019

kinni, siis EL õigussüsteem ei anna mingit kaitset vara kaotuse puhul või mingit tagatist, et krüptoraha tagasi saada.

Krüpteerimiste, miksimiste ja tumeveebi (*Dark Net*) kasutamise tõttu ei ole tihti võimalik õiguskaitseorganitel mõistlikult kindlaks teha kurjategija, serverite või kuritegelike infrastruktuuride tegelikke füüsilisi asukohti. See kehtib ka krüptoraha puhul. Raske on kindlaks teha, millise jurisdiktsiooni alla kuritegu kuulub, kes seda uurima peaks ja kuidas tõendeid koguda saab, kas ja kuidas saaks kasutada jälitustegevust või jälgimist. Kuna osa infot hoitakse ka pilvedel, siis võib see kuuluda mitme jurisdiktsiooni alla. Et selliste kuritegude uurimine oleks efektiivsem ja kiirem on vaja parandada riikide ülest ja organisatsioonide vahelist koostööd. Järgmisena peavad Eurojust ja Europol tähtsaks välja töötada rahvusvaheline õiguslik raamistik, et tagada otsene ligipääs andmetele, seal hulgas pilvedel olevale. [125]

Lisaks on maailmas levinud ka rahapesu ja selle teenuse pakkumine krüptovaluutaga. Viimasega tegeles Hispaanias kriminaalne organisatsioon pakkudes suures ulatuses rahapesu teenust teistele kuritegelikele ühendustele. Kriminaalidel olid mitmeid erinevad skeeme, kuidas raha pesta ja raha päritolu varjata. *Modus operandi*'na tuvastati näiteks krüptoraha-automaatide kasutamine ja *smurfing* ehk raha jaotamine paljude erinevate inimeste vahel väikeste summade kaupa, et mitte tõmmata tähelepanu suurtele tehingutele ja sissemaksetele. Organisatsioon ise haldas ühte krüptovaluuta vahendusteenust ja kahte krüptoraha-automaati, et kriminaalse taustaga raha krüptoraha vastu vahetada. *Smurfing*uks kasutati ka mitmeid pangakontosid ja hiljem neid veel kihistati, liigutades raha läbi erinevate pangakontode, mis lõpuks krüptovaluutadeks vahetati. Süüdistus esitati 16 inimesele, arestiti varasid, kanepitaimi ja dokumente aga kõige tähelepanuväärsem on kokku 24 külma- ja kuumarahakoti ning pangakontode külmutamine, kus oli kokku 9 miljonit eurot.[126]

3. Krüptorahaga seotud kuriteod Eesti karistusõiguses

Justiitsministeeriumi Kriminaalpoliitika osakond peab kindlalt tehnoloogiaga seotud kuritegusid tuleviku kuritegudeks. Eesti kuritegevuse 2018 uuringus on välja toodud, et tavakelmuste arv on kahanenud, kuid arvutikelmuste juhtumite arv on pidevalt kasvanud, samal

[125] *Common challenges in combating cybercrime*, joint report, Europol and Eurojust Public Information, juuni 2019.
[126] *Cryptocurrency laundering as a service: members of a criminal organisation arrested in Spain*, Europol, 08.05.2019.

ajal on nende vahekord tasakaalustunud. Prognoositakse ka teiste kuritegude puhul sarnast krüptopuudutust, ehk siis, et vähemalt on osaliselt teod seotud mõne digitaalse lahendusega.[127] See on ka täitesti mõistetav ja eeldatav, sest digitaalsete lahenduste osakaal igapäevaelus pidevalt suureneb ja on muutunud täiest tavaliseks. Autor julgeks hetkel isegi arvata, et arvutikelmuste puhul on teatamiste protsent mõnevõrra väiksem, kui see on tavakelmuste puhul, seega võiks arvata, et toimepandud tegude arv on ka suurem.

Nagu ka varasemalt on töös tähelepanu juhitud, siis krüptokuritegudel on rahvusvaheline mõõde ning rahvusvahelisest koostööst oleneb kuritegude avastamisel, uurimisel ja menetlemisel palju. Näiteks Samoast laekunud petukirjade ja -kõnede algallikani jõudmiseks on vaja toimivat riikidevahelist õigusabi, ent Eestil pole hulga riikidega juriidilist koostööraamistikku.[128] Eesti poolt sõlmitud õigusabi lepingud on toodud Justiitsministeeriumi lehel[129], kuid need, mis on sõlmitud EL liikmesriikidega on nüüd reguleeritud EL Nõukogu määrusega. Õigusabi leping[130] on meil küll ka Venemaaga sõlmitud, kuid kui seda lugeda, siis kriminaalasjades kriminaalmenetluse osa on väga lühike ja sisaldab vaid kahte artiklit. Artiklid 59 ja 60 reguleerivad vaid seda, et kui üks lepingupooltest soovib, et teine pool oma riigis oma kodaniku vastu kriminaalmenetluse alustaks, siis on seda õigus paluda ja toodud on siis ka see, milline vastav palve peab olema. Seega ei ole Eesti ja Venemaa vahel mingeid regulatsioone, mis kohustaks teist poolt menetlusele kaasa aitama või informatsiooni välja andma. Sama moodi on ajamahukas ja keeruline menetleda asju, kus jäljed viivad mõnda Aafrika riiki, nagu ka viimasel ajal levinud petukirjade allikas Nigeeria. Rahvusvaheline koostöö on aga ajakriitiline, kuna digijäljed ja digitõendid võivad kiirelt kaduda. Krüptokuritegevus oma olemuselt on piiriülene, liigub läbi arvutite ja serverite, mis võivad füüsiliselt asuda ükskõik kus, üle maailma. Järelikult on rahvusvahelise koostöö arendamine, kindlasti selline valdkond, millega kõik riigid peaksid üheskoos tegelema, et krüptokuritegevust tõhusamalt ja kiiremini avastada ja ka ennetada.

Siseministeeriumi juhtimisel tehti krüptokuritegevuse uuring „Küberkuritegude tulevik tehnoloogia arengu valguses“, mille läbiviimiseks paluti tuge Euroopa Komisjonilt ning mis valmis veebruaris 2020. Analüüsiti tuleviku tehnoloogiaid ja kuidas neid on võimalik kasutada, et toime panna küberkuritegusid. Samuti seda, kuidas võivad infotehnoloogilised arengud

[127] Kuritegevus Eestis 2018, kriminaalpoliitika uuringud, Justiitsministeerium, Tallinn 2019. lk 17.
[128] Kuritegevus Eestis 2018, lk 17.
[129] Justiitsministeerium, *Riikide õiguskoostöö lepingud*, 5.09.2014.
[130] Eesti Vabariigi ja Vene Föderatsiooni leping õigusabi ja õigussuhete kohta tsiviil-, perekonna- ja kriminaalasjades - RT II 1993, 16, 27

mõjutada nii kübertehnoloogiast sõltuvaid kuritegusid, kui neid, millele aitavad küberlahendused kaasa. Lõpuks anti soovitusi, kuidas hoida ära seda, et tulevikutehnoloogiaid küberkuritegevuses ära kasutatakse.[131] Konkreetne soovitus oli seadusandlusliku, regulatiivse ja organisatoorse keskkonna ettevalmistamine, et suuta adekvaatselt reageerida ja vastata küberkuritegevusega seotud väljakutsetele, mida tehnoloogia areng kaasa toob. Et seda kõike kohaldada, soovitatakse uurida: kas on vaja õiguslikult või regulatiivselt sekkuda tehnoloogiasse; milline on riikliku küberturvalisuse keskuse tähtsus; edasi arendada Eesti osavõttu ja toetust rahvusvahelises küberkuritegevuse vastases tegevuses ning arendada küberturvalisuse vastupidavust.[132] Antud soovitusi võib pidada universaalseteks ja mõnes mõttes ka enesestmõistetavateks aga need on tõesti suunad kuhu küberkuritegevuse rahvusvahelist olemust arvestades, Eesti liikuma peab.

Krüptoraha süsteemi proovitakse maha rahustada ka karmimate regulatsioonidega. Euroopa Parlamendi ja Nõukogu direktiivi finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamisest muudeti direktiiviga 2018/843 (AMLD5)[133], ning millega muudeti ka varasemaid direktiive. Regulatsioon on karmim virtuaalvääringu teenuse pakkujale kohaldatavate hoolsusmeetmete suhtes, peamiselt virtuaalvaluuta pakkujale ehk vahendusplatvormidele ja rahakoti teenuste pakkujale, kes hoiavad ka oma klientide privaatvõtmeid. Vastava muudatusega peavad teenusepakkujad läbi hoolsusmeetmete rakendamise oma klientide isikud avalikustama ning iga kahtlase tehingu puhul teavitama sellest finantsjärelevalve asutusi. Samas jäävad kättesaamatuks ja anonüümseks ikkagi kasutajad, kes kasutavad riistvara ja tarkvara rahakotte või kasutavad vahetuseks üldse teisi P2P platvorme. Kindlasti jäävad anonüümseteks Monero ja Dashi kasutajad, kuni neil pole põhjust kasutada digitaalseid vahetusplatvorme või järelvaatavaid rahakoti teenuseid.[134]

2018 uuringu järgi oli Eestis registreeritud üksikud virtuaalrahaga toime pandud pettused. Mõnel juhul lubati turule tuua uus krüptoraha, koguti investeeringutena raha, andes vastu uut krüptoraha ja siis lõpetati tegevus ning valuuta ei saanud väärtust, sest seda ei hakatud laiemalt kasutama, ehk siis tegemist oli eelpool selgitatud ICO pettustega. Registreeritud on ka nii-öelda

[131] Bellasio, J. jt, The Future of Cybercrime in Light of Technology Developments, RAND Europe, veebruar 2020, lk 1.
[132] *Idem*, lk 11.
[133] 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. – ELT L156/43.
[134] IOCTA 2019, lk 59.

tavalistele kaardipettustele sarnanevaid skeeme, kus teise isiku virtuaalraha kontolt tehakse ülekanne tuvastamata omanikuga kontole.[135] Siinkohal võib siis tegemist olla kas privaatvõtme enda valdusesse saamisega ja seejärel krüptoraha ülekandmisega, mis võib olla põhjustatud lihtsalt kasutaja lohakusest. Keerukama võimalusena on tegemist häkkimisega rahakotti või vahetusplatvormi. Järgmise, 2019 aasta, uuringu kohaselt ütles Kriminaalpoliitika osakond, et kunagi varem ei ole Eestis registreeritud nii palju küberkuritegusid kui 2018 aastal. Eristatakse arvutikelmusi karistusseadustiku (KarS) § 213 järgi ning arvutiandmete ja -süsteemi kuritegusid KarS §-d 206, 207, 216[1], 217[1] järgi. Viimased on olemuselt ja menetluslikult keerulisemad. Kokku oli 2018 aastal arvutikuritegusid 965, millest 768 olid arvutikelmused.[136] 2020 aasta kriminaalpoliitika uuringus pole välja toodud eraldi krüptovaluutaga seotud kuritegude arvu, sellele enam nii palju tähelepanu ei pöörata. Mainitud on ainult seda, et küber- ja arvutikuritegude osakaal on kasvutempos.[137]

Üks Eesti tuntumaid ja suuremaid krüptorahaga seotud kuritegusid on Dennis Einasto süüasi, mille kohtulik arutamine algas 2019 aasta veebruaris. Süüdistuse järgi sisenes Einasto varastatud kasutajakontodesse ja kandis sealt enda kontole bitcoine, mille teel teenis ta tulu üle kolme miljoni euro. Kriminaaltulu arvutamisel arvestati isiku tegelikku sissetulekut ja bitcoini väärtust kuriteo toimepanemise ajal.[138] Prokuratuur teiste õiguskaitseorganite kaasabil on suutnud tuvastada 28 417,95 euro päritolu, kui tegelikult peetakse kuritegelikuks tuluks 3 245 788,31 eurot. Vaatamata Europoli ja FBI abile, ei ole suudetud tuvastada ülejäänud tulu päritolu. Üheks süüdistuspunktiks on arvutikuriteo ettevalmistamises KarS § 216[1] lg 1 järgi, mis seisnes selles, et Einasto valdas oma elukohas talle kuuluvas arvutis, vähemalt viit erinevat, temale mitte kuuluvat krüptoraha ja veebimajandusega seotud andmebaasi koos neis sisalduvate kasutajatunnuste ja paroolidega, eesmärgiga panna toime arvutikuritegusid. Lisaks esitati süüdistus 96 episoodis arvutikelmuses KarS § 213 lg 2 p 1 järgi ning 118 episoodis arvutisüsteemile ebaseaduslikult juurdepääsu hankimises KarS § 217 lg 1 p 1 järgi. Lisaks ka veel arvutikuriteo ettevalmistamises KarS § 216[1] lg 1 järgi ning rahapesus, mis on toime pandud grupis ning suures ulatuses KarS § 394 lg 2 p 1,3 järgi. Esimesel kohtuistungil heideti riiklikule süüdistajale ette seda, et kõiki kannatanuid pole suudetud tuvastada, tuvastada on suudetud viis kannatanut ja suurem osa on prokuratuuri hinnangul tuvastamatud, kuid siiski tuleks nad kannatanutena kaasata. Kaitsjad aga leidsid, et isegi Europoli ja FBIga tehtud koostöö pole

[135] Justiitsministeerium, *Kuritegevus Eestis 2018*, kriminaalpoliitika.ee, Tallinn 2019, lk 20.
[136] Justiitsministeerium, *Kuritegevus Eestis 2019*, kriminaalpoliitika.ee, Tallinn 2020, küberkuriteod.
[137] Justiitsministeerium, *Kuritegevus Eestis 2020*, kriminaalpoliitika.ee, Tallinn 2021.
[138] Arula, E., *Krüptoraha varastamises süüdistatav mees astus kohtu ette*, Tartu Postimees, 12.02.19

piisav, prokuratuur ei pingutanud piisavalt ja peaks olema võimalik jälgida sarnaselt kõigi teiste veebitoimingutega. [139]

Kahjuks ei ole autoril kättesaadav konkreetne süüdistusakt, aga kui veidi analüüsida süüdistuse teksti, mida autor loodab on ajakirjanik sõna-sõnalt prokuröri kõnest kirja pannud, siis saab teha järeldusi, milliseid tehnoloogilisi võimalusi Einasto väidetavalt kasutas. Kasutatud on sõna krüptoraha, mis võib mõnevõrra segadust tekitada, kuid samas viidatud bitcoinile, siis võib kindel olla, et tegemist oli krüptoraha bitcoiniga. Teine väljend on veebimajandusega seotud andmebaas, mille puhul on arvatavasti silmas peetud, kas rahakoti teenust või vahendusplatvormi. Mõlemad tegutsevad majandustegevuses ja *online*'is, samuti haldavad mõlemad andmeid ehk rahakotte koos kasutajatunnuste ja privaatvõtmetega. Seega hetkel ei saa autor kindel olla, millisest andmebaasist pärit andmete valdamises süüdistus on esitatud. Arvestades ka kõike, mida autor on töös plokiahela tehnoloogia osas välja toonud ja kuidas see toimib, siis julgeks arvata, et kaitsja väide, et raha liikumine Einasto arvutisse peaks olema jälgitav samamoodi, kui Delfi kommentaariumi kommentaarid, ei ole lihtsalt mitte mingil moel võrreldav. Plokiahela süsteem on küll teoreetiliselt avalik ja liikumised on nähtavad piisava võimekuse korral, kuid kasutajaid ja kontosid liikumiste taga niisama lihtsalt ei näe. Tartu Maakohus kuulutas 12.08.2020 kohtuotsusega Dennis Einasto kõigis prokuratuuri poolt esitatud süüdistuspunktides süüdi ja mõistis talle kogumis karistuseks 4 aastat, 5 kuud ja 26 päeva vangistust. Hetkel ei ole maakohtu otsus jõustunud ja see on edasi kaevata ringkonnakohtusse.

3.1.1. Karistusõiguslik regulatsioon

Õigusriikliku karistusõiguse ülesanne demokraatlikus riigis on ühiskonna kui inimeste sotsiaalse kooselu aluste kaitse. Selle ülesande esimene aspekt on kaitsta inimeste õigushüvesid, milleks on – sotsiaalse kooselu alused, ühiskondlikud põhiväärtused, näiteks elu, tervis, omand ja vabadus. Sellised õigused eksisteerivad vastavalt ühiskondlikule lepingule, kokkuleppele. Samuti on karistusõiguse ülesanne tagada õiguskorra, ehk sotsiaalsete normide osa, mida kaitsevad õigusnormid, terviklikus ja puutumatus.[140]

[139] Kalev, M., Eesti geniaalseim kuritegu? Kolm miljonit eurot tulu, aga kannatanuid justkui polegi, Eesti Ekspress, 12.03.2019.
[140] Sootak, J., Karistusõiguse alused, Juura, Tallinn 2003. Lk 18.

Järgnevalt analüüsib autor seda, kas Eestis on karistusõiguslikult krüptoraha puhul selle kasutajad kaitstud võimalike õiguslike riivete puhul.

3.1.2. Mis on krüptoraha karistusõiguslikult?

Krüptoraha puhul kasutatakse väga palju erinevaid väljendeid ja nimetusi. Sõnaühendi teine pool on, kas raha, vara, arveldusühik või valuuta. Samas on paljud pangad ja riigid üheselt leidnud, et rahaks ega valuutaks krüptoraha nimetada ei saa, sest sellel puuduvad majandusteaduslikult vastavad omadused. Nad ei eita, et on rahaga sarnaseid jooni ehk saab teenuse või kauba eest tasuda ning sellel on olemas mingi väärtus. Probleemiks on nende käsitluse järgi see, et väärtus on pidevas muutumises. Õiguslikus mõttes ei sobi see raha definitsiooniga, sest krüptoraha ei ole nii laialdaselt kasutuses kui nii-öelda tavaline raha, turuosa võrreldes ringluses oleva tavarahaga on marginaalne. Samuti ei ole krüptorahale vastavat füüsilist ja käega katsutavat vastet nagu näiteks on eurol. Samal ajal on aga täiesti aktsepteeritav pangakontol olev raha ja krediit, mida ei peeta õiguslikult pakkumuseks, kuid samuti selliseid nii-öelda raha virtuaalseid vorme on tunnustatud, sest kogu ühiskond seda teeb.

Autor aga leiab, et krüptorahale meie karistusõiguses ja ühiskonnas üldiselt koha leidmiseks, peaksime me keskenduma mitte sellele, kust see tuleb ja mille jaoks seda kasutatakse, vaid sellele, mis see ise on, tema olemusele. Oli ju algselt krüptoraha luues eesmärk leida midagi alternatiivset nii-öelda tavalisele rahale, jättes alles selle mõõdetava väärtuse, aga samal ajal muutes selle iseseisvaks riigist ja tõstes ülekannete kiirust.

Seadusandja on pidanud vajalikuks reguleerida krüptorahaga seonduvat vastavalt RahaPTSle. Seaduse pealkiri kasutab juba sõna „rahapesu“ ehk algselt oli mõeldud kui klassikalise rahaga seotud kuritegevuse reguleerimiseks. RahaPTS § 1 lg 1 järgi on seaduse eesmärk on ettevõtluskeskkonna usaldusväärsust ja läbipaistvust suurendades tõkestada Eesti Vabariigi rahandussüsteemi ning majandusruumi kasutamist rahapesuks ja terrorismi rahastamiseks. Seega ei peagi vaatama seadust nii kitsalt kui raha vaid pigem silmas pidama rahandussüsteemi ja majandusruumi. Krüptoraha oma kasutusalalt on kindlasti üks majandussüsteemi osa ja selle osakaal aina kasvab. Viimase redaktsiooniga (AMLD5) on kaotatud krüptorahale antud selgitus kui alternatiivne maksevahend ning eelistatakse virtuaalväärinud mõistet. Muudatusega on lisatud ka RahaPTS § 2 lg 10 järgi virtuaalvääringu teenuse pakkujad kui isikud, kelle suhtes seadust kohaldatakse. Samal ajal on see RahaPTS § 2 lg 5 kohaselt justkui samastatav finantsasutusega, kuna kohalduvad samad sätted. Üheks finantsasutuse alaliigiks vastava

seaduse kohaselt on ka valuutavahetused. Krüptorahal on seega palju erinevaid omadusi, mis sobivad paljude erinevate käsitluste korral kattuvate omaduste poolest.

Samamoodi on hiljuti ka reguleeritud täpsemalt, kas ja kuidas peaksid olema krüptorahad maksustatud. TuMS § 15 lg 1 mõttes on maksustatav vara. Omadusena on varale toodud, et ta peab olema võõrandatav ja samal ajal ka varaliselt hinnatav. Krüptoraha seda ka kindlasti on. Seega ka varaga ehk siinkohal krüptorahaga seotud tegevused, võõrandamise ja vahetamised, on tulumaksuga maksustatavad, kui sellest saadakse kasu, TuMS § 37 lg 1 järgi. Seega on krüptovara vähemalt TuMS definitsiooni järgi kui vara. Seadusandja on näinud, et krüptorahaga seotud osalistele kasu toovad tegevused on tõusuteel ja juba piisavalt igapäevased, et need ka seadusega reguleerida. Maksustamise osas peab olema regulatsioon ühtne ja on mõeldamatu, et oleks mingi vahend, millega saab tekkida kasu aga see maksustatav ei ole. Sellisel juhul muutuks see kiirelt aina populaarsemaks, kui sellel piisav kindlus muidugi on, ja nii-öelda sööks teised vara liigid lihtsalt välja, kuna tõenäoliselt oleks see liik soodsamas olukorras teiste ees.

Kas aga krüptoraha mahub oma olemuselt karistusõiguslikult vara mõistesse? Vara all mõistetakse inimese kõikide tema asjade ja õiguste, varaühikute kogumit, millel on rahaline väärtus. Varaühiku iseloomustavaks omaduseks on see, et neid on üldiselt võimalik teistele isikutele raha vastu võõrandada. Kaitstakse varaühikuid mitte ainult vahetu väärtuse, vaid ka tegevusvabaduse pärast, et inimene saaks oma varaühikuid kasutada, tal oleks selleks vabadus.[141] Krüptorahal on olemas tema rahaline väärtus ja seda saab vahetada tagatud valuuta vastu vahetusplatvormidel.

Kui vaadata varavastaste süütegude süstematiseerimist õigushüve alusel, on eristatav see, kas kaitstaval õigushüvel on rahaline väärtus. Seega jagatakse süüteod toimepanduks kas õigushüve vastu, mille väärtus ei ole oluline või rahalise vaatusega õigushüve vastu. Esimesel juhul kaitstakse omandit, mis on asjaõigusseaduse (AÕS)[142] § 68 järgi täielik võim asja üle.[143] Krüptoraha puhul saaks rääkida omandist siis, kui on olemas privaatvõti. Ilma selleta ei pääse inimene oma krüptorahale kuidagi ligi ning ei saa sellega mingeid käsutusi teha. Võib järeldada, et privaatvõti on see, mis justkui omandi loob. Selleks, et mingit õigushüve rikkuda, näiteks läbi varguse, peab see olema reaalselt midagi, mida on võimalik rikkuda.

[141] Kairjak, M., Sootak, J., Varavastased süüteod, 4. väljaanne, Juura, Tallinn 2017. Lk 16.
[142] Asjaõigusseadus - RT I, 22.02.2019, 11.
[143] Varavastased süüteod, 2017. Lk 17

3.1.3. Süüteod omandi vastu

Küll aga tekib küsimus, kas krüptoraha on „asi“. Asi on füüsiline ehk kehaline ese, midagi sellist, mida saab käega katsuda ja nii ka ära võtta, hõivata. Kuna aga krüptoraha iseenesest ei ole käega katsutav, vaid asub virtuaalses rahakotis, pole võimalik seda käeliselt ära võtta. Seega ei ole krüptoraha asi tsiviilõiguse üldosa seaduse (TsüS)[144] § 49 tähenduses, mis eeldab, et asi on kehaline. Eesti kohtupraktika[145] kohaselt saab tuua antud juhul paralleeli pangakaardil oleva rahaga, kus tegemist on arvelduskonto omaniku varalise nõudega panga vastu arvelduskontol näidatud ulatuses. Krüptoraha puhul oleks siis omaniku nõue rahakoti teenuse pakkuja vastu. Nõue iseenesest ei saa olla omaniku valduses, kuna valdus on tegelik võim asja üle, seega on rahakoti teenusepakkujal tegelik võim.

Võib tekkida küsimus olukorras, kus privaatvõti ei ole rahakotis hoiustatud, vaid asub näiteks mälupulgal. Privaatvõtme väärtus kui selline on immateriaalne, see on andmete jada. Antud töös on pikalt analüüsitud, et krüptoraha kontole ei pääse kuidagi ligi ilma privaatvõtmeta, seda ei saa kuskilt tuletada ning kontole ei ole juurdepääsu ka teenuse pakkujal. Tulles tagasi TsüS § 49 juurde, siis kui privaatvõti on mälupulgal, või ka näiteks paberil, on tegemist kehalise esemega, mida saab hõivata ja selle enda valdusesse saamisel on ainuvaldus ka krüptorahale, millele selle privaatvõtmega juurde pääseb.

Arvutiprogramm ei ole asi. Küll aga peetakse asjaks disketti või muud programmikandjat.[146] Arvutiprogramm on arvutile arusaadetavate käskude kogum. Eristatakse süsteemiprogramme, mis peavad tagama operatsioonisüsteemi töö, ja rakendusprogramme, mis on mõeldud kasutajale arvutis asjade tegemiseks, näiteks tekstitöötlus.[147] Privaatvõti ei ole arvutiprogramm antud definitsiooni mõttes. Ta ei paku ega anna arvutile mingeid käske, vaid avab juurdepääsu krüptorahale. Kirjanduses on jõutud aga ka seisukohale, et arvutitarkvara sisaldumine disketil või kõvakettal on programmi, kui asja vältimatu eksistentsivorm.[148] Privaatvõti küll ei ole arvutitarkvara, aga üldiselt on see esindatud digitaalsel kujul, krüpteeritud numbrijadana. Siit saab tõmmata ka paralleeli, et juhul kui võti on digitaalsel kujul ja see ei ole paberile trükituna, saab seda antud arvamuse kohaselt ka kindlasti asjaks lugeda.

[144] Tsiviilõiguse üldosa seadus - RT I, 06.12.2018, 3.
[145] RKKK 3-1-1-83-07, p 14.
[146] Varavastased süüteod, 2017. Lk 25.
[147] https://et.wikipedia.org/wiki/Arvutiprogramm
[148] Varavastased süüteod, 2017. Lk 25.

Asi karistusõiguse mõttes tähendab liikuvat asja ehk vallasasja, mida saab füüsiliselt ära võtta ja ära viia.[149] Kui rääkida privaatvõtmest, kui välisel andmekandjal või paberil olevat võtit, siis on ka antud kriteerium täidetud. Seda saab liigutada ja endale võtta, ära viia. Seega autor järeldab, et privaatvõti, kui see ei asu andmesüsteemis, vaid mõnel välisel andmekandjal või paberi peal, on asi, mille vastased teod on kvalifitseeritavad kui süütegu omandi vastu. Ehk siis on võimalik toime panna vargust, röövimist ja omastamist.

Tsiviilõiguslikult kuulub asi isikule olenemata selles, milline on selle asja rahaline või muu majanduslik väärtus. Sellise määratluse on üle võtnud ka karistusõigus. Vargusega on tegemist mistahes asja hõivamise puhul ja asja väärtust tuleb arvestada üksnes siis kui asja olemus on selle väärtusega väljendatav.[150] Seda näiteks juhul kui tuleb kindlaks teha, kas vargus on toime pandud vähe väärtusliku asja vastu või mitte, sellest oleneb süüteo kvalifikatsioon. Rahaline väärtus tuleb siis tuvastada vaid juhul, kui see on süüteokoosseisu asjaolu, millel on karistusõiguslik tähendus.[151] Väheväärtuslik on asi, mille väärtus on väiksem kui 20 miinimumpäevamäära[152] aga kui väärtus selgelt seda ületab, siis ei ole vaja menetluses kindlaks teha, kui palju see täpselt on.

Privaatvõtme varguse puhul võib muidugi tekkida mõningaid probleeme. Asja väärtust hinnatakse rahaliselt kannatanule tekitatud tegeliku kahju varastatud kauba müügihinna alusel.[153] Varastatu väärtus tuvastatakse summas, mis võimaldab kahju hüvitamise või kannatanul endal soetada samaväärne asi.[154] Kui kõigepealt võtta privaatvõtme väärtus, kui krüptoraha väärtus, millele ta juurdepääsu omab, siis saab loogiliselt järeldada, et väärtus sõltub teo toimepanemise ajal vastava krüptoraha väärtusest. Hetke väärtust ei ole raske kindlaks teha, tuleb vaid vaadata krüptoraha nii-öelda börse ja saab täpselt igal ajahetkel, isegi kellaajaliselt, väärtuse kindlaks teha. Küsimus tekib aga hoopis sellest, kas ja kuidas süüteo toimepanija teadis privaatvõtmele vastava krüptoraha väärtust ning kas ta pidi seda teadma ja eeldama. Teadmiseks võib pidada olukorda, kus isik on kas otse privaatvõtme omanikult või ka mõne kolmanda allika kaudu teada saanud just selle konkreetse privaatvõtme juurde kuuluva krüptoraha väärtuse. Sellisel juhul peaks isik ka vastavalt ka vastutama. Kui aga süüteo toimepanija ei teadnud täpset väärtust, vaid lihtsalt teadis, et mingile hulgale krüptorahale selle

[149] *Idem*. lk 26.
[150] *Idem.* lk 31.
[151] *Ibidem*
[152] RKKK 3-1-1-117-13, p 8.
[153] Varavastased süüteod, 2017, lk 33.
[154] RK 3-1-1-14-00

võtmega juurde pääseb ning võib olla ka kuuldes uudistest, kui väärtuslikud krüptorahad olla võivad, loota suurele kasule. Kasu võib osutuda väga suureks, kuid ka väga väikeseks. Mõlema näite puhul on aga probleemiks reaalse väärtuse menetluslikult tõestamine. Riigikohus on öelnud, et varastatu varalise väärtuse küsimusest ei saa mööda minna, see näitab kuriteoga tekitatud kahju suurust, seega ka kuriteo raskust ning süü suurust.[155] Kui aga privaatvõti on varastatud ja seda ei suudeta kuidagi tagasi saada, on krüptoraha väärtust võimatu tõendada. Tegelik omanik enam oma kontole juurde ei pääse ning menetluslikult ei ole väärtust võimalik tõsikindlalt selgeks teha. Sellisel juhul vastutaks kurjategija vaid võtme andja väärtuse järgi, ehk kui on tegemist kõvaketta või külma laoga, siis vastavalt selle turuhinnale. Krüptoraha tegelikku väärtust on autori hinnangul võimalik tõendada esimese toodud näite puhul, kui kurjategija sai väidetavast krüptoraha väärtusest otse omanikult või mõnest teisest allikast teada. Muidugi tuleb leida mitmeid usaldusväärseid allikaid, mis aga ei puutu konkreetselt koosseisu ja on pigem menetluslik küsimus, kuidas täpselt varastatud krüptovaluuta väärtust tõendada. On naiivne arvata, et kuriteo toimepanija uurijatele ise privaatvõtme üle annaks, sest sellest talle mingit võimalikku kasu ei oleks. Võimalus on vaid privaatvõti leida isiku valdusest mõnel füüsilisel kujul või arvutis salvestatuna.

Omand AÕS § 68 lg 1 järgi on isiku täielik õiguslik võim asja üle ja omanikul on õigus asja kasutada, käsutada ja vallata. Krüptoraha puhul saab täieliku võimu vaid juhul, kui sinu omandis on privaatvõti. Mingil muul viisil krüptoraha käsutada ega kasutada ei ole võimalik. Võõra valduse rikkumise all mõeldakse senise valduse ja tegeliku asjavalitsemise võimu kõrvaldamist tema tahte vastaselt või ilma tema tahteta.[156] Krüptoraha olemuselt ei ole siin autori hinnangul mingit erisust või küsimuse kohta varavastase koosseisu puhul. Omandi vastu suunatud süütegude korral, nii varguse, röövimise kui omastamise puhul, leiab autor, et krüptoraha puhul on võimalik koosseis täita, kui süüteo objektiks on privaatvõti mõnel materiaalsel kujul.

3.1.4. Süüteod vara vastu tervikuna

Kelmuse ja väljapressimise koosseisu puhul on teo objektiks vara. Juriidiline vara mõiste näeb selles konkreetsete varaosade suhtes õiguslikult täpselt fikseeritud õiguste ja kohustuste kogumit. Majanduslik lähenemine lähtub TsüS §-st 66, mille järgi on vara isikule kuuluvate rahaliselt hinnatavate õiguste ja kohustuste kogum. Vara võivad moodustada näiteks rahalise

[155] RKKK 3-1-1-60-01, p 9.1.
[156] Varavastased süüteod, 2017, lk 55.

väärtusega asjad, konkreetse varalised õigused, samuti eeldatav või saadaolev varaline kasu, näiteks väärtpaberitelt.[157] Krüptorahal on rahaline väärtus olemas. See on küll ajas muutuv ja väga kõikuv, kuid seda on konkreetses ajahetkes võimalik kindlaks teha. Majandusliku varamõiste kohaselt on kõik võimalikud varad kelmuse või väljapressimise eest karistusõiguslikult kaitstud. Majandusliku varamõiste alla ei lähe vaid vara, millel pole rahalist väärtust.[158] Krüptorahal on see aga kindlasti olemas ja seega kvalifitseerub nende nõuete järgi vara alla. Eeltoodud loetelu järgi saab krüptoraha väärtuseks pidada eeldavat või saadaolevat varalist kasu, mida võib saada krüptoraha kasutamisest, müügist või vahetusest tulenevast kasust.

KarS § 211 järgi on investeerimiskelmus investeeringu saamine üldsusele või kindlaksmääratud isikute ringile suunatud teabes olulistes asjaoludes valeandmetes esitamises või oluliste asjaolude esitamata jätmise teel. Kaitstavaks õigushüveks on vara ja eelmises punktis on ka jõutud järeldusele, et krüptovaluuta seda karisusõiguslikus mõttes on. Ühe koosseisuteona on valeandmete esitamine, mis on täidetud, kui olulised asjaolud ei vasta tõele, on objektiivses vastuolus reaalsusega või eelduseid tegelikkuses ei eksisteeri. Valeandmed on ka finantsprognoosis esitatud järeldused aga seda mitte selles osas, kas need tulevikus täituvad või mitte, vaid, et kas esitatus on ebaõigeid faktiväiteid.[159] ICO pettuseid puudutavas osas on toodud näiteid, kuidas viimasel ajal on levinud pettused, kus investorite kaasamise eesmärgil esitatakse tõele mitte vastavaid *white paper*'eid, seda äriühingute poolt, mis ei plaanigi oma token'eid või krüptovaluutat välja anda, kuid selle tegevuse jaoks raha küsivad. Investeering ise on pikaajalise kasu samaise eesmärgil tehtav rahaline ülekanne, mis võib seisneda rahalises ülekandes osakute omandamiseks või laenu andmises. Koosseis kohaldub kõikidel juhtudel, kui investeeringu saamise vastutasuks kantakse üle mingi rahaliselt hinnatav õigus. Koosseis on täidetud kui investor on teostanud rahapaigutuse.[160] Seega on kindlasti antud objektiivne koosseis täidetud, kui investeeritakse näiteks krüptovaluuta teenusega alustavasse ettevõttesse pangaülekandega eurodes. Kuna investeeringul peab olema mingi rahaliselt hinnatav õigus ja krüptovaluutal on rahaline väärtus, siis ka sellise investeeringu tegemisel pettuse ohvriks langemise korral kvalifitseerub tegu antud paragrahvi alla. Koosseisu kohaldamise puhul on ka tähtis vorm, kuidas võimalikust investeeringu võimalusest teavitati. Ehk siis vajalik on üldsusele või kindlaksmääratud isikute ringile suunatud teave, mitte vaid ühele inimesele ja

[157] Sootak, J., Pikamäe, P., Karistusseadustik, kommenteeritud väljaanne, 5. trükk, Juura, 2021, lk 694.
[158] *Ibidem.*
[159] Sootak, J., Pikamäe, P., Karistusseadustik, komm vlj, 5. Tallinn: Juura 2021, lk 704, p 4.1.
[160] *Idem*, lk 706, p 7.1.

avaldatud peab olema ka piisavalt teavet pakkumistingimuste kohta, et investor saaks teha otsustuse, kas osakuid osta või märkida.[161] ICO pettuste puhul tehakse üldiselt investeerimisvõimalus teatavaks kodulehel, millest teavitatakse krüptovaluutast huvitatud gruppe Internetis. Sarnaselt prospektiga IPOde puhul, on tavaliselt *white paper*'is olemas piisavalt andmeid, et antud koosseisu täita. Üldiselt lubatakse väga suuri kasumeid intresside näol, lisaks tavaliselt asutatava teenusepakkuja/ettevõtte token'eid. Kui aga ükski nendest lubadustest lõpuks ei täitu ja seda põhjusel, et ettevõtet ei looda ja seda polnud isegi plaanis ning kelmid investeeringuteks saadud rahaga kaovad, on koosseis täidetud.

3.1.5. Arvutisüsteemidega seotud süüteod

Arvutikuritegevusevastase konventsiooni, tuntud ka kui Budapesti konventsioon, definitsiooni kohaselt on arvutisüsteemiks andmeid programmi järgi automaatselt töötlev seade või omavahel ühendatud seadmed.[162] Rõhk siis sellel, et tegemist peab olema seadmetega. Omavahel ühendatud seadmete puhul juhindutakse arusaamast, et mitu kehalist eset toimivad ühe funktsionaalse üksusena. Näiteks lauaarvuti koos oma emaplaadi, kõvakettaga ja lisaseadmeteks on klaviatuur, hiir ja printer.[163] Käesoleva töö puhul saaksime rääkida arvutisüsteemist kui kellegi arvutist, kus tal on midagi krüptovaluutaga seonduvat salvestatud. Plokiahel ja DLT süsteem ise, kui selline, on küll serveritega tagatud ja töötavad serverite üleselt, kuid nad ei ole reaalselt ühes või mitmes omavahel seotud arvutisüsteemis karistusõiguslikus tähenduses.

Konventsiooni definitsiooni järgi on andmeteks töötlemiseks sobivas vormis esitatud teave või programm, mille abil arvutisüsteem toimib.[164] EL Parlamendi ja nõukogu direktiivi 2013/40EL kohaselt on arvutiandmed faktide, teabe või mõistete esitamine infosüsteemis töötlemiseks sobivas vormis, sealhulgas programm, mille abil saab infosüsteemi panna ülesannet täitma.[165] Seega ei ole silmas peetud vaid programmi ja teavet, mille abil arvutisüsteem toimib, vaid ka teavet, mille abil saab panna infosüsteemi ülesandeid täitma. Viimase alla käibki just krüptovaluutat toetav plokiahel. See ei ole programm kui selline, vaid andmestruktuuri eriliik, mis salvestab ja jagab andmeid üle andmebaasi, omamata selget asukohta ja koopiaid hoitakse

[161] *Idem*, lk 706, p 6.2.
[162] Arvutikuritegevusvastane konventsioon, art 1a. - RT II 2003, 9, 32.
[163] Sootak, J., Pikamäe, P., Karistusseadustik. Komm vlj 5. Tallinn: Juura 2021, lk 674, p 9.
[164] Arvutikuritegevusvastane konventsioon, art 1a. - RT II, 2003, 9, 32.
[165] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2013/40, 12.08.2013, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK. - ELT L 218/8, Art 2 pb.

ühises võrgus. Arvutiandmed kui sellised, võivad paikneda nii arvutisüsteemis kui ka sellest väljaspool.[166] Plokiahelad ja kübervaluuta ise just arvutisüsteemist väljaspool asuvadki, seega karistusõiguslikult on need käsitletavad arvutiandmetena.

KarS § 206 lg 1 järgi on karistatav arvutiandmetesse sekkumine ehk arvutisüsteemis olevate andmete ebaseaduslik muutmine, kustutamine, rikkumine ja sulustamine. Koosseisuobjektideks on arvutisüsteem ja arvutiandmed. Arvutisüsteemi mõiste puhul on keskseks andmete automaattöötlus, mis töötab põhimõttel, et andmed sisestatakse seadmesse, mingi käsuna, näiteks nupule või nuppude kombinatsioonile vajutamisega. Seejärel need töödeldakse ja lõpuks väljastatakse mingi väljundina, kas siis näiteks heli, pildi või välja prinditud paberina.[167] Sellise mõiste alla käivad ka igasugused erinevad kodumasinad ja –lahendused, mitte ainult selgelt arvutid või nutitelefonid ja tahvelarvutid. Seaduse kommentaarides on küll viidatud kriitikale[168] seoses laia määratlusega ja võimalikule ülekriminaliseerimisele. Autor aga tooks välja, et viimane muudatus antud sättes on jõustunud 2015 aastal, kui aga tänapäeval on üha rohkem uudiseid ja juhtumeid sellest, kuidas koduseadmetesse sisse häkitakse, eriti neisse, millel on ka kaamera olemas. Pigem on antud juhul seadusandlus mõnevõrra ajast ees olnud. Näitena saab tuua beebikaamerad.[169] Teise koosseisutunnusena nähakse ette arvutiandmeid, mille definitsiooni on eespool lahti kirjutatud. Arvutiandmed peavad olema ka sobivas vormis, mida lihtsustatult saab pidada lihtsalt vormiks, mida arvuti suudab vahetult töödelda.[170] Autor leiab, et krüptoraha enda süsteem ja selle toimimiseks vajalikud osad, ei kuulu KarS § 206 lg 1 koosseisu alla. Plokiahel on küll süsteem, kuid seda ei saa pidada arvutisüsteemiks antud koosseisu puhul ja karistusõiguslikus mõttes, sest plokiahela toimimisel ei teki konkreetset väljundit. Plokiahel küll kasutab arvuti võimekust ja ressursse, et uusi tehinguid ja plokke kinnitada aga selle tulemusel ei ole ühtegi silmaga nähtavat väljastatud andmekogumit või andmeid, nagu seda on näiteks televiisori või printeri puhul. On leitud, et sätet ei ole võimalik kohaldada, kui andmed asuvad kuskil mujal, nii öelda pilves või internetiserveris, mingi teenusepakkuja juures ja neile hangitakse juurdepääs mõne arvutisüsteemi abil.[171] Krüptovaluuta ei asu mõnes arvutis, vaid just teenusepakkuja juures, tavaliselt rahakoti teenusepakkuja juures, ja füüsiliselt seda arvutist nö välja võtta ei saa, ilma,

[166] Sootak, J., Pikamäe, P., Karistusseadustik. Komm vlj 5. Tallinn: Juura 2021, lk 675, p 14.
[167] *Idem*, lk 674, p 8
[168] *Ibidem*
[169] Chuck, E., Abbruzzese, J., *'I'm in your baby's room': Nest cam hacks show risk of internet-connected devices*, NBC News, 21.12.2018.
[170] Sootak, J., Pikamäe, P., Karistusseadustik. Komm. vlj, 5. Tallinn: Juura 2021, lk 677.
[171] Sootak, J., Pikamäe, P., Karistusseadustik. Komm. vlj, 5. Tallinn: Juura 2021, p 32, Lk 682.

et tavavaluutaks konverteerida. Samamoodi privaatvõti ei ole arvutisüsteem, vaid see võimaldab plokiahelale ligipääsu ilma, et midagi ise konkreetselt suudaks töödelda. Privaatvõti võimaldab juurdepääsu krüptovaluutale arvutisüsteemi, ehk siis konkreetse internetivõrgus oleva seadme abil. Samas on leitud, et selline regulatsioon, kus andmed peavad paiknema arvutisüsteemis, eksib konvensiooni art 4 vastu, mille eesmärk on karistada kõigi arvutiandmete vastu toimepandud tegude eest.[172]

On toodud ka välja näide, et kui telefon hävitatakse, andmed kustutatakse lõplikult, tekib ideaalkogum KarS § 203-ga (asja rikkumine või hävitamine). Sätte kohaldamine ei ole võimalik, kui andmed asuvad internetis asuva teenusepakkuja juures või internetiserveris.[173] Seega ei ole säte kohaldatav krüptovaluuta osas, sellisel juhul saab rääkida mõnes muust koosseisust. Küll aga on võimalik oma privaatvõtit hoiustada telefonis. Telefoni lõhkumise või hävitamise tagajärjel on privaatvõti igaveseks kadunud ja selle tagajärjel ka ligipääs krüptovaluutale. Seadustiku kommentaar küll ütleb, et arvutisüsteemi väärtus ei ületa tavaliselt 4000 eurot[174], kuid on teada, et krüptoraha väärtus on tihtilugu suur aga seda muidugi mitte kõigi seda omavate isikute puhul. Sellisel juhul oleks täidetud KarS § 203 muud eeldused koosseisu täitmiseks.

Küll aga saaks KarS § 206 kohaldada juhul kui toime on pandud arvutikelmus (KarS § 213), isik peaks vastutama lisaks ka käesoleva sätte järgi. Näitena on toodud küll panga kontoseisu muutmisega seoses, kui keegi siseneb teise isiku kontole internetipanga kaudu ja teeb tehinguid, mille tagajärjel kontoseis muutub.[175] Siinkohal saab tuua selge paralleeli virtuaalsesse rahakotti sisenemise ja sealt krüptoraha mujale kandmisega. Leitakse viis teise nii öelda krüptovaluuta kontole sisse saamiseks ja seda eesmärgil seal leiduvad rahalise väärtusega mündid teise rahakotti kanda, millega kannatanu kontoseis muutub. Üldjuhul ei saa krüptovaluuta puhul rääkida sarnaselt kontoseisu muutmisega väikese intensiivsusega muudatusest, suuremal hulgal juhtudel on tegemist ikkagi rahalist väärtust omavate vahenditega, mis on ka kasutaja jaoks olulised.

KarS § 207 järgi on reguleeritud arvutisüsteemi toimimise takistamine. Kaitstav õigushüve on õigustatud huvi arvutisüsteemi tõrgeteta toimimise suhtes.[176] Sellise välja toodud õigushüve

[172] *Idem*, p 14, lk 676.
[173] *Idem*, p 32, lk 682.
[174] *Ibidem.*
[175] *Ibidem.*
[176] RKKK 3-1-1-94-14, p 205.

puhul võiks koosseisu sobida vahetusplatvormide toimimine. Kasutajad eeldavad ja soovivad, et vahetusplatvorm töötaks ilma tõrgeteta ja nad saaks katkestuseta platvormi kasutada. Seda näiteks juhul, kui keegi häkiks süsteemi ja meelega blokeeriks kõik võimalikud plokiahela kinnitamised või lõikab ära plokkide vahelise ahela. Sarnaselt KarS § 206'ga ei kuulu sellised ründed antud koosseisu alla põhjusel, et plokiahelat ei saa pidada arvutisüsteemiks. Ründed krüptorahaga seotult on pigem sooviga kasu saada, mitte ainult segadust ja paanikat külvata, kuigi on ka selliseid häkkereid. KarS § 207 lg 1 võiks kohalduda antud teema kontekstis näiteks krüptovaluuta kaevandustes olevatele serveritele tehtava ründe puhul. Seda sellel ajal kui kaevandamisega tegeletakse ja seda tegevust mõne pahavara abil kuidagi takistatakse, tööd häiritakse. Samamoodi teise arvutisüsteemi, serveritesse, pahavara abil tungimine eesmärgiga kasutada seal olevat võimekust selleks, et krüptovaluutat ise kaevandada. Seda on hiljuti juhtunud Microsofti omanduses olevas ettevõttes[177] ja viidatud on ka sellele, et veel 2020 aastal Eesti IT-taristu vastase ründe käigus kasutati riigi vahendeid krüptoraha kaevandamiseks.[178] Koosseisu täitmiseks peaks kindlasti ka arvutisüsteem olema nii häiritud, et seda on tunda. Kindlasti mõne võimsama süsteemi puhul ei panda teinekord tähelegi, et keegi nende süsteemis midagi toimetab ja see tuleb välja alles hiljem elektriarvel.

KarS § 213 järgi on arvutikelmus teisele isikule varalise kahju tekitamise eest arvutiprogrammi või andmete ebaseadusliku sisestamise, muutmise, kustutamise, rikkumise, sulustamise või muul viisil andmetöötlusprotsessi ebaseadusliku sekkumise teel varalise kasu saamise eesmärgil. Krüptoraha süsteemide puhul on autor juba eelnevalt analüüsinud, et krüptoraha on karistusõiguslikus mõttes kui vara ja sellel on rahaline väärtus olemas. Koosseisuteoks on ebaseaduslik sekkumine andmetöötlusprotsessi, mis peab omakorda mõjutama andmetöötlusprotsessi tulemust. Teo piiritlemise küsimus tekib juhul, kui mitte ainult toimepanija ei sekku andmetöötlusprotsessi, vaid ka asjasse puutuv kolmas isik kontrollib andmetöötlusega seonduvat.[179] Krüptorahaga seonduvate võimalike koosseisude puhul selline asjaolu aga antud analüüsi puhul tähtsust ei oma, sest keskendutakse krüptoraha ja sellega seotud plokiahela omadustele. See, kas ka keegi puudutatud kolmas isik on eksimusse viidud sisuliselt asja ei muuda. Krüptoraha puhul on selle varale vastavus tuvastatud, seega on võimalik koosseis objektiivsest poolest nii arvutikelmus, kui ka kelmus.

[177] Young, C., *Cybercriminals Hacked GitHub's Servers for Crypto Mining,* Interesting Engineering, 05.04.2021.
[178] Rattam, E. *Küberkuritegevuse ökosüsteem on muutunud teenusepõhiseks,* Prokuratuuri aastaraamat 2020.
[179] *Ibidem.*

Asjakohane on arvutikelmuse puhul paralleel pangaautomaadist raha väljavõtmisega. Kui automaadist raha välja võtta soovitakse, peab sisestama PIN-koodi. Antud koosseisu mõttes on andmete sisestamisega tegemist siis, kui leiab aset andmete kohalik ehk vahetu lisamine arvutisüsteemi.[180] Kui isik ise ja otse automaadis PIN-koodi sisestab, saab seda pidada andmete sisestamiseks koosseisu mõttes. Selleks, et tuvastada, kas andmete sisestamine on ka arvutisüsteemiga seotud peab see algne sisestamine toimuma kuidagi ühtses arvutisüsteemis. Ühe lähenemise järgi moodustab pangaautomaat panga serverite ühtse süsteemi, seega kui sisestada PIN-kood automaadis, võetakse läbi selle ühendust töötleva serveriga. Kui seda käsitlust aga eitada ja öelda, et need ei ole ühtne süsteem, siis leitakse ikkagi, et tegemist on andmete sisestamisega. Seda põhjusel, et õigustatud isik lõppsüsteemi ehk pangaserveri ja sisestatud PIN-koodi tagajärjel andmeid saatev pangaautomaadi puhul on üks ja sama isik ehk pank.[181] Plokiahela süsteemi puhul on vaja krüptoraha väljavõtmiseks või suunamiseks kasutada mõnda vahendusplatvormi või P2P lahendust. Selleks aga, et sinna juurde pääseda ja reaalselt ka krüptorahaga midagi teha saaks on vaja privaatvõtit, mis pangaautomaadi analoogia puhul on siis justkui PIN-kood. Krüptoraha käsutamiseks piisab vahetusplatvormile sisselogimisest, et kõik vajalikud kanded ja vahetused ära teha. Privaatvõti küll ei pruugi olla vastaval platvormil, vaid hoopis kuskil pilves või mõne riistvara lahenduse peal, kuid selleks, et kandeid teha, on vaja privaatvõti sisestada vastavasse platvormi. Seega on tegemist ühtse arvutisüsteemiga, kus sisestamine toimub ja mis käsud vastu võtab ja vastavalt ka kanded teeb.

Koosseisu puhul on elemendina välja toodud ka andmete edastamine aga näitena pangaautomaadi puhul on tegemist sellega siis, kui kasutatakse teise panga pangakaarti, kui see, mis panga oma on kasutatav automaat. Samas on märgitud, et sisestamise ja edastamise eristamisel ei ole praktilist tähendust, kuid edastamise all on mõeldud muul viisil andmetöötlusprotsessi ebaseaduslikku sekkumist paragrahvis.[182] Krüptoraha puhul autor siin võimalikke elulisi alternatiive ei näe. Kuna kui juba ühele vahetusplatvormile minna, tuleb kõik tegevused seal teha, ka teised osapooled leida, kellega valuutavahetusi teha või kellele müüa. Tehingud ei ole plokiahela lahenduste puhul võimalikud üle platvormide.

Kui pangakaarti kasutab selleks mitteõigustatud isik omavoliliselt peetakse arvutikelmuse koosseis täidetuks.[183] Sarnaselt krüptorahaga saab rääkida privaatvõtme omavolilisest

[180] Sootak, J., Pikamäe, P., Karistusseadustik. Komm. vlj, 5. Tallinn: Juura 2021, lk 710-711.
[181] *Idem*, lk 710.
[182] *Idem*. lk 711.
[183] *Ibidem*.

kasutamisest. Omavoliline on kasutamine igal juhul, kui tegelik omanik ei ole selleks nõusolekut andnud või kui omanik on nõusoleku kasutamiseks antud, kuid väiksemas ulatuses, kui seda kasutaja teeb. Vastavalt asjaoludele on koosseisu mõttes suhteliselt kerge kindlaks teha, kas omanik on nõusoleku andnud või mitte. Krüptoraha seisukohta võib aga kindlalt öelda, et kui virtuaalrahakotti või vahetusplatvormi sisse häkitakse, mille tulemusel saadakse enda valdusesse kasutajate privaatvõtmeid, ei ole olemas omaniku nõusolekut. Häkkerid juba oma olemuselt on isikud, kes vastavaid teadmisi kasutades otsivad süsteemis viga, mille kaudu mõnda süsteemi sisse tungida, et kahju tekitada ja/või endale kasu saada. Isikutel, kes üritavad süsteemi sisse tungida vigu otsides, ei saa olla seaduslikku õigust vastavale varale. Teine viis kuidas nad juurdepääsu saavad, on andmepüük ja pahavara kasutamine, mis on samuti oma olemuselt inimeste nii-öelda õnge püüdmine, mille tulemusel saavad häkkerid juurdepääsud andmetele, millele nad muidu ei oleks juurde saanud, kasutades ära inimeste lihtsameelsust ja teadmatust. Kõik süsteemi sisse murdmised on pahaloomulised ja tavaliselt ikka ilma omaniku nõusolekut. Vahetusplatvorm ei tee vahet, kas privaatvõtme on sisestanud krüptoraha tegelik omanik või keegi võõras, identifitseeritaksegi end platvormil võtmega ning eeldatakse, et see, kes seda kasutab, on ka reaalne omanik.

Eraldi on ka välja toodud, et eelpool analüüsitud pangaautomaadist raha väljavõtmise põhimõtted kohalduvad ka Interneti-tehingute korral.[184] Siinkohal saab vahetusplatvormi samastada pangakontoga, sest platvormil on võimalik hoida oma krüptoraha ja sellega kandeid, tehinguid teha. Vahetusplatvorm muudab plokiahelal põhineva informatsiooni kergemini loetavamaks, mis ka sarnaneb pangakonto väljavõttega. Kelmusega on tegemist olukorras, kui makse või kande tegija väidab nii-öelda müüjale, et ta on selleks õigustatud isik. Vahetusplatvormid isikusamasust ja omandiõigust kuidagi ei kontrolli, seda kinnitab nende jaoks privaatvõtme olemasolu. Seega ka antud juhul on koosseis sobiv krüptorahaga seotud olukordade puhul.

Ebaseaduslik sekkumine peab viima muudatusteni andmetöötlusprotsessi tulemustes. Vastavat viidet ei ole küll seaduse tekstis sees, kuid sellegipoolest on vajalik, et antud tunnus oleks koosseisu osana täidetud, et lugeda tegevust arvutikelmuseks.[185] Privaatvõtit kasutades mingitki varakäsutust krüptorahaga tehes toimuvad muudatused plokiahelas ja neid muutusi võib pidada väga ulatuslikuks. Kui keegi soovib varakäsutusena krüptoraha kanda, siis selleks on vaja mitmete haldurite kinnitust, mille tulemusel luuakse uus plokk, mis ahelale liidetakse. Selleks,

[184] *Idem*, lk 714.
[185] *Idem*, lk 714.

et plokk kinnitada, on vaja paljude haldurite pool teha tööd ja see vajab ressursse. Kui plokk on juba kinnitatud, siis tagasi seda enam pöörata ei saa. Ligipääs krüptoraha olemuse kohaselt on ainult ühel inimesel, see on tema valduses läbi privaatvõtme. Plokiahel on avalik, seega kõik näevad, et krüptovaluuta on selle inimese oma, tunnustavad ja kinnitavad tema tegevused.

Analüüsitava sätte puhul on ka vajalik, et tekiks varaline kahju.[186] Kuna on selge, et krüptorahal on rahaliselt mõõdetav väärtus, siis on ka selge, et kui krüptoraha kellegi valdusest tema nõusolekuta väljub, tekib ka varaline kahju. Rahaliselt on väärtuslikud kõik võimalikud asjad ja väljundid, mida inimesed on valmis ostma ja/või müüma. Krüptoraha atraktiivsuses küsimust ei ole, kuna selle turg ja maht aina suureneb ning kasutamine muutub populaarsemaks.

Häkkerite olemuse ja süsteemi murdmisega on tegelikult ka juba täidetud koosseisu subjektiivne koosseis. Üldiselt toimuvad rünnakud platvormide ja digitaalsete rahakottide vastu ikka ja ainuüksi rahalise kasu eesmärgil. Üksikutel juhtudel on võimalik, et häkker on palgatud, et testida ja kontrollida süsteemi turvalisust kuid on vähe tõenäoline, et sellisel juhul mindaks klientide varade ja rahakottide kallale. Arvutikelmuse koosseisu täitmiseks on krüptoraha süsteemi olemust silmas pidades kõik eeldused olemas.

KarS § 216[1] järgi on arvutikuriteo ettevalmistamine seadme või arvutiprogrammi, mis on loodud või kohandatud eelkõige KarS §-de 206, 207, 213, 217 sätestatud kuritegude toimepanemiseks, või kaitsevahendi, mille abil on võimalik hankida juurdepääs arvutisüsteemile või muul viisil kättesaadavaks kattesaadavaks tegemine, et panna ise või võimaldada kolmandal isikul panna toime KarS §-de 206, 207, 213, 217 sätestatud kuritegu. Sätte kohaldamise põhjuseks oli häkkerite seadmete suurenev populaarsus ja kättesaadavus mustal turul. Koosseisu objektideks on füüsilised seadmed ja arvutiprogrammid, viimase all on silmas peetud viiruseid, usse, nuhkvara, pahavara ning kaitsevahendid, mille puhul on mõeldud andmepüügi (*phishing*) tulemusel saadud salasõnade välja uurimine ja kogumine.[187] Seadmete ja arvutiprogrammide puhul ei ole seoses krüptoraha olemusega midagi teistsugust või konkreetselt seostatavat antud koosseisu mõttes. Andmepüük on aga ka krüptoraha privaatvõtmete enda kätte saamiseks populaarne viis ning üha laialdasemalt kasutatav. Seega antud koosseisu alla läheks konkreetselt privaatvõtme omamine, kui see on saadud andmepüügi tulemusel.

[186] *Idem*, lk 715.
[187] *Idem*, p3. lk 725-726.

KarS § 217 ehk nn häkkimiskoosseisu järgi on karistatav arvutisüsteemile ebaseaduslikult juurdepääsu hankimine kaitsevahendi kõrvaldamise või vältimise teel. Kaitstavaks õigushüveks on isiku õigustatud huvi hoida arvutisüsteemis olevaid andmeid saladuses, samuti isiku huvi arvutisüsteemi puutumatuse ja kättesaadavuse vastu. Seetõttu peetakse antud paragrahvi arvutikuritegevuse normistikus kesksel kohal olevaks.[188] Teoobjektiks on taaskord arvutisüsteem, mis tähendab, et säte ei kaitse arvutiandmeid, mis on väljaspool arvutisüsteeme ehk riistvaral või pilvel, Internetis olevaid. Nagu ka eespool on juba analüüsitud, plokiahel arvutisüsteemi mõiste alla ei kuulu, seega ei saa sinna ka sisse häkkida selle koosseisu mõttes. Seega krüptovaluutaga seotult saab antud koosseisu puhul rääkida näiteks kellegi seadmetesse sisse häkkimisest, selleks tulemüürist läbi tungimise teel või mingil moel salasõna kindlaks tegemisel, ning seejärel arvutisüsteemist saada kätte vajalikud andmed isiku krüptoraha hoidvasse rahakotti sisse saamiseks.

3.1.6. Võimalikud eesmärgid

Krüptovaluuta on karistusõiguses veel suhteliselt uudne kontseptsioon ja hetkel on tegemist pigem küsimus selles, kas see juba praegustesse koosseisudesse sobitud, mitte nii palju sellel, kas peaks sätteid krüptovaluutale vastavalt kohandama. EL ei näe veel põhjust olemasoleva seadusandluse laiendamiseks, pigem soovitakse õiguskindlust virtuaalvaluutaga seonduva kohaldamisel ja selle defineerimisel. Samal ajal leitakse riikides viise kuidas krüptovaluuta pealt saadavat tulu ikkagi maksustada. Tekkib põhjendatud küsimus, et kui krüptovaluutadega tehtavate tehingute ja sealt saadava tulu saamine on maksustatud, kas ei peaks ka maksumaksjate õigushüved olema sama moodi kaitstud ning seadusandja ka selle kaitsmiseks vajalikke samme võtma? Krüptovaluuta loomisel oli peamiseks fookuseks küll detsentraliseeritus ja eraldatus riigivõimust, kuid mingil määral need tänapäeva maailmas ikkagi seotud on ja neid kokkupuute alasid peaks ka reguleerima.

Antud tööd analüüsides näeb, et plokiahela tehnoloogia ei mahu hästi kuhugi, kuna tegemist on arvutiandmetega, mis ei ole konkreetse arvutisüsteemiga seotud. Plokiahela ja DLT tehnoloogia peal asub aga kogu krüptovaluuta süsteemi toimimine ja mingit kaitset see rünnakute eest vajaks. Neil on sarnasusi pangasüsteemide ja serverisüsteemidega, kuid hetkel need karistusõiguslikult kaitstud pole.

[188] *Idem*, p2, lk 728.

Krüptovaluuta kasutajal on teoreetiliselt võimalik oma vara kaitsta, kuna krüptovaluuta defineeritakse kui vara, millel on väärtus ja samamoodi saab kaitsta oma arvutiandmetesse tungimise ja privaatvõtme ehk krüptorahale juurdepääsu rikkumise puhul. Küll aga kui juba privaatvõti on ühe isiku omanduses ei saa tehtavaid tehinguid plokiahela tehnoloogiat silmas pidades tagasi pöörata. Autor ei arva, et kuritegude uurimise ja avastamine oleks kerge protsess aga küberkuritegude ja kindlasti ka krüptovaluutat puudutavate kuritegude puhul on see veel keerulisem. Tuleb arvestada tehnoloogilisi arenguid, nende nüansse ja kogu halli ala, mida krüptovaluuta oma pseudo-anonüümsuse ja võimalike jälgede peitmisega omab.

Töös toodud näidete puhul oli tihtilugu näha, et kui ründed toimusid mõne teenusepakkuja vastu, siis pöörduti küll õiguskaitseorganite poole aga ise oldi väga aktiivsed jälgede ajamiseks ja kindlaks tegemisel, kes ja kuidas nende andmetele ja varadele juurde pääses. Selles vallas peetakse turvalisust äärmiselt oluliseks nii enda kaitseks kui ka klientide usalduse võitmiseks, et oma tegevusega edukalt areneda ja raha teenimiseks. Tuleb tõdeda, et küberruumis aktiivselt toimetavatel ja seal tegutsevatel teenusepakkujatel ning osalistel on tihtilugu suuremad teadmised ja võimekused, et krüptovaluutaga toimuval ja suurtest andmemahtudest ülevaadet saada. Seetõttu on kindlasti väga tähtsad head suhted kõigi küberruumi osalistega, kellel on andmetele juurdepääs. Ka Guarda juhtumi puhul võtsid nad ise teiste teenusepakkujatega ühendust, et varastatud krüptoraha musta nimekirja panna. See aga eeldab mingit usaldust ja teise poole valmidust ja tahtmist üldse mingit kaasabi osutada. Selle suunas peaks liikuma ka riiklikud ja rahvusvahelised õiguskaitse- ja uurimisorganid, et tagada uurimiste efektiivsus ja nende tulemused.

Kindlasti ei saa mööda vaadata rahvusvahelisest mõõtmest. Küberruum ei tunne riigi piire ja seal toimuv on piirideülene. See muudab aga ka kuritegude tõkestamise, avastamise ja uurimise ka palju mahukamaks ning keerulisemaks. Sellest tulenevalt on eriti antud valdkonnas väga vajalik rahvusvaheline koostöö riikide ja organisatsioonide vahel, et tagada parem võitlus kuritegevusega. Koostöö tõhustamiseks ja selle kaasa aitamiseks on vajalik ka rahvusvahelise seadusandluse ühtlustamine, seda nii karistusõiguslikult inimeste õiguste kaitseks kui ka selle eelduseks olevalt krüptovaluutasse puutuvate omaduste arusaamist, nende lahti seletamist ja õiguskaitse normidesse sisse viimist. Selleks on vaja Eestil leida viise võimendada koostööd nii riigi siseselt kui rahvusvaheliselt, et suuta efektiivselt võidelda ohtudega, mida tehnoloogia areng tulevikus võib tuua. Sama moodi peaks Eesti üle vaatama oma ressursside paigutuse ning võttes arvesse küberruumis toimuva ja tulevikku vaadates selle pigem aktuaalsemaks ja aktiivsemaks muutumise, muuta riigi valmisolek sellest tulenevate ohtude ja õigushüvede

rikkumise vastu võitlemisel võimekamaks. Ka prokuratuur on välja toonud, et ressursi puudus on peamine, mis on küberkuritegude uurimisel takistuseks, mis tähendab, et uurimiste puhul on vältimatud otsuste tegemine, et milliseid tegusid on aega ja võimalus uurida, ning milliseid mitte. Selleks oleks vaja täpsemalt uurida ja analüüsida, kus ja millest on kõige suuremad puudujäägid ning sellest tulenevalt proovida need vajaka jäämised tuleviku perspektiivis kõrvaldada.

Kokkuvõte

Viimase 12 aastaga, alates loomisest, on krüptovaluuta populaarsus ja kasutajate arv kasvanud märkimisväärselt. Töö kirjutamise hetkel on loodud üle 9000 krüptovaluuta ja *token*'i, millede koguväärtus ületab 1,6 triljonit eurot ning nende suurus kasvab ajas pidevalt. Seoses krüptovaluuta väärtuse pideva kõikumise ja viimasel ajal suurte tõusudega, tunneb krüptorahasse investeerimise vastu huvi üha enam inimesi. Seetõttu on kasutuses mitmeid pettusi ja skeeme, kuidas võimalikelt huvilistelt nende raha või krüptovaluuta kätte saada. Samuti tunneb krüptovaluuta anonüümsuse tõttu selle kasutamise vastu huvi kuritegevusega seotud organisatsioonid, kuna kriminaalse tulu jälgi on sel viisil kergem peita ja ka oma igapäeva tegevuses ei torka vahendite liigutamised õiguskaitseorganitele nii selgelt silma. Kuna krüptovaluuta turg pidevalt kasvab, on vajadus ka tegeleda osaliste ja kasutajate õiguste kaitsega. Keerulisemaks teeb selle Internetile omaselt rahvusvaheline mastaap, sest sel juhul on rikkumisi raskem tuvastada ja uurida.

Uurimiseesmärgiks on magistritöös analüüsida krüptovaluuta sobituvust Eesti karistusõiguslikku süsteemi arvestades selle uudsust, kiiret arengut, selle mitte kvalifitseerumist tunnustatud raha tüübina ja rahvusvahelise üldise regulatsiooni puudumist aga samal ajal soovi selle poole liikuda. Käesoleva töö eesmärgiks on uurida ja leida vastus järgmistele probleemküsimustele:

- Kas arvestades krüptovaluuta eriomadusi on võimalike rünnete puhul omaniku õigused Eestis karistusõiguslikult kaitstud?
- Kas karistusõiguslik regulatsioon krüptovaluutadega seonduvalt on Eestis piisav ja kas tuleviku perspektiive silmas pidades suudetakse käia krüptovaluuta arenguga kaasas?

Tulenevalt autori teadmistest Eesti karistusõigusest ja krüptovaluutast püstitati magistritöö hüpoteesiks, et Eesti karistusõigus ei hõlma kõiki krüptovaluutadega seonduvate kuritegude kvalifitseerimiseks vajalikke koosseise, et oleks tagatud kuritegudega kahjustatud isikute õiguste kaitse.

Magistritöö esimeses peatükis avatakse krüptovaluuta ja plokiahela toimimise süsteeme selleks, et paremini nende toimimismehhanisme ja nüansse mõista. Tuuakse välja, kuidas toimib vastastikusel kokkuleppel ja usaldusel põhinev plokiahel ning miks on inimesed valmis sinna panustama. Selgitatakse süsteemi detsentariseerituse olemust ja miks anonüümsust väga

tähtsaks peetakse aga kuidas tegelikult on võimalik ülekandeid jälgida ja võimalusi ning oskusi omades siiski omaniku identiteet selgeks teha. Kui soovitakse krüptoraha päritolu varjata on võimalus kasutada ka erinevaid miksimisteenuseid. Süsteemi vaieldamatult tähtsateks osaks on ka vahetusplatvormid ja rahakotiteenuse pakkujad, millede toimimise põhimõte ja neid tagavad lahendused on lahti seletatud. Rahakoti teenusepakkujad hõlbustavad ülekannete ja vahetuste tegemist, turvalisuse tagamiseks pakuvad nad krüpteerimist ning mitmevõtmelist kaitset. Vahetusplatvormide puhul on tegemist süsteemiga, kus ei ole ühtegi vahemeest ja detsentraliseeritusse tõttu ongi need eelistatud. Selleks, et krüptovaluutaga seonduvat ja selle mõju hinnata ning kokkuvõttes ka võimalikke regulatsioone kohaldada on vajalik, et kõik krüptovaluutat puudutavad asjaolud ja lahendused oleksid mõistetavad.

Kuna krüptovaluuta on muutunud ajas aina populaarsemaks, soovitakse seda ikkagi küberruumist väljas pool maailma pankade ja finantsasutuste poolt defineerida. Selleks, et teada, kas ja kuhu võiks maailm krüptovaluutaga seonduvalt liikuda on vaja ülevaadet, kuhu on esimese kümnendiga jõutud. Majanduslikus mõttes ei peeta krüptovaluutat rahaks, sest tal puuduvad selleks raha kolm põhilist funktsiooni ja puuduseks on just selle väärtuse kiire muutumine ajas ja selle mitte aktsepteerimine üldise maksevahendina. Ka juriidiliselt ei ole see raha, kuna puudub füüsiline vorm ja laialdane levik. Samal ajal töös viidatud institutsioonid, sh ECB ja WB, hindavad aga väga plokiahelda võimekust ja selle poolt pakutavaid lahendusi ning ECB isegi kaalub digitaalsevaluuta kasutusvõttu tulevikus. See näitab, et kuigi krüptovaluuta ümber on palju kahtlusi ja ebakindlust, nähakse sellel palju positiivseid omadusi, mis aitaksid kaasa tuleviku finantssektori toimimisele.

Maailma riigid on krüptovaluuta levikule reageerinud erinevalt. On riike, kus on see keelatud ja levinuim on seisukoht, et krüptovaluuta ei ole seaduslik vaaluta. Seaduslik on see aga rohkem kui 111 riigis ning mõningad neist on alustanud krüptovaluuta õigusliku reguleerimisega, eelkõige rahapesu tõkestamiseks. Samuti on alustatud krüptovaluuta pealt teenitava tulu maksustamisega ja teenuseid pakkuvate platvormidele käibemaksu kohustuse seadmisest, samal ajal on Saksamaa tekitanud krüptovaluutaga tegelemiseks maksustamise osas kasutajatele soodsad võimalused. Kõik see, mis maailmas krüptovaluuta reguleerimisega soovitakse teha ilmestab selgelt, et saadakse aru, et krüptoraha ei ole kuhugi kadumas ja selle aktiivsemale kasutamisele peab reageerima. Jääb mulje, et justkui mõned riigid kardaksid seda puutuda ja ei ole suutnud endale selle toimimise põhimõtteid selgeks teha. Muidugi võib olla ka vastupidi, et just on aru saadud kui palju võimalusi see maailma tasandil annab ning kardetakse kontrolli ja võimu käest anda. Samal ajal teised riigid proovivad plokiahela

tehnoloogiat ja DLTd enda kasuks pöörata seda finantssektori arendamise jaoks. On ka arusaadav, et kuna küberruum on raskesti hoomatav ja selle võimalused pidevalt arenevad on vaja kõigepealt midagi reguleerides kõikvõimalikud riskid selgeks teha ja valmis olla tulevikus tekkivateks probleemideks. Viimast ei saa kunagi tagada aga valmisolek selleks peaks olema.

Eesti käsitluse järgi on krüptovaluuta lepinguline vääring, mida ei saa samastada rahaga ja on kasutatav vaid lepingupoolte kokkuleppel. Töös tuuakse välja, kuidas seni on krüptoraha reguleeritud ja tulevikku vaatavalt hinnatud, seda Rahandusministeeriumi väljatöötamiskavatsuses, Eesti Panga ja EMTA poolt. Üldiselt peetakse silmas kapitalituru arengut ja finantssektorit ning peetud vajalikuks ka virtuaalvaluuta pealt saadud kasu maksustamine. RAB tegi uuringu virtuaalvääringu teenuse pakkujate osas, kuna pidas vajalikuks hinnata võimalikke kuriteo riske. Uuringus leiti, et tänu RahaPTS muudatustele on teenusepakkujate turgu suudetud korrastada, paljudelt on tegevusload ära võetud ja alles jäänutelt nõutakse oma tegevuse seadusega kooskõlla viimist. Kuid sellegi poolest on näha, et hoolsusmeetmete rikkumine ettevõtete poolt on laialdane ja sellele aitab kaasa tegevuse kaugteenuse iseloom. Hetkel peetakse Eestis tähtsaks rahapesu vastast võitlust. Seda on välja toonud nii prokuratuur kui RAB. Ressursside ja teadmiste suunamine terrorismi ja rahapesu tõkestamisele on kindlasti vajalik samm ning on viimane aeg seda teha. Jääb justkui mulje, et krüptovaluuta kasutamise elavnedes prooviti reguleerida just finantsilist poolt jättes märkamata, et krüptovaluuta kui maksevahendi kasutamisel on palju halli ala, mida saavad ära kasutada kurjategijad. Eesti küll liigub oma struktuurimuudatustega küberkuritegevuse vastase võitluse võimekuse tõstmise suunas, kuid need kindlasti ei suuda veel oma ressursside osas sammu pidada küberruumi võimekuse ja kurjategijate arenguga.

Autor pidas vajalikuks tuua välja ka riskid, mis krüptovaluutaga kaasnevad. Kuna tegemist on maksevahendina kasutatava lahendusega, millega kaasneb üldiselt ka anonüümsus, on tegemist kurjategijate jaoks väga atraktiivse vahendiga. Üheks probleemiks on rahapesu, millele on tähelepanu juhtinud ka RAB, kellele on teenusepakkujate poolt tulnud teateid, mis viitavad selgelt klientide seotusele terrorismiga. Krüptoraha kasutatakse ka terrorismiga tegelevate organisatsioonide poolt oma tegevuseks vajalike vahendite soetamiseks. Lunavara rünnakute puhul on mõjutatud isikuid ja asutusi sellise rünnaku olemuse tõttu üldiselt palju ja nende puhul nõutakse lunaraha krüptovaluutas. Ka korruptsioonis on üha enam kasutusele võetud altkäemaksu ja meelehea edasi andmist krüptorahana ja ikka eesmärgil jääda ametivõimudele märkamatuks.

Üheks viimasel ajal levinud kuriteo liigiks on kelmused krüptovaluutaga, millele on tähelepanu juhtinud ka Keskkriminaalpolitsei. Internetis levivate kelmuste liike on palju, nende sagedus kasvab ja muutuvad üha keerukamateks. Eraldi on peatutud ka ICO pettustel, mille eesmärk on võimaliku investeerimisvõimaluse pakkumisega krüptovaluutasse petta inimestelt välja rahalisi vahendeid. Kuna küprovaluuta on aina populaarsem ja on jätnud uudistes mulje kui hea ja kerge viis raha teenimiseks, siis tihti tunduvad sellised pakkumised inimeste jaoks väga ahvatlevad. Töös on välja toodud mitmeid ICO pettuste skeeme, mis ilmestava selgelt kui ulatuslikud sellised skeemid on, kui suurt kahju tekitatakse ja kuidas need riigi piire ei tunne. Just selliste omaduste tõttu on vastavaid kuritegusid raske avastada, uurida ja menetleda, vaja on ulatuslikke ressursse ning head rahvusvahelist koostööd. ICOd ise on ka täiesti reguleerimata. Märkimata ei saa jätta ka vajadust inimesi teavitada selliste pettuste olemasolust, kuna üldiselt satuvad selliste pettuste ohvriks inimesed, kes ei oska ega tea pakutava investeeringu kohta piisavalt uurida, et olla kindel, et investeeringul on vähemalt mingigi teenimisvõimalus.

Pidevate rünnete alla satuvad ka vahetusplatvormid, kuna seal asuvad paljude krüptorahade ligipääsuks vajalikud privaatvõtmed, hoiustatakse krüptovaluutat. Tekitatud kahju on viimaste aastatega kasvanud mitmekordselt ja aastate lõigetes räägitakse miljarditest dollaritest. Rünnakuid viiakse üldiselt läbi häkkidena kasutades turvaauke, andmepüüki ja viiruseid. Samas ei ole harvad ka juhused, kui varad kannavad ära vahetusplatvormi enda haldajad ja omanikud, kellel on klientide krüptovaluutadele kergem ligipääs. Kõik toodud näited ilmestavad selgelt seda, et krüptorahade kasutajad soovivad küll anonüümsust ja ei taha, et pangad või riik teaksid nende varade asukohta ja suurust, kuid selline reguleerimata ja kokkuleppe peale üles ehitatud süsteemis saadakse aga tihti petta või varad varastatakse. Kuritegevuseks annab kübermaailm head võimalused tegutseda märkamatult, kuid nö tavainimesele on kaotused tihtilugu suured. Nii õiguskaitseorganid kui teenusepakkujad ise tegelevad sellega, et varastatud krüptoraha jälgida, kuhu see jõuab ja kes rünnaku taga on, kuid tavaliselt suudetakse piisavalt oma jälgi peita rahakottide vahel liikumisega ja miksimisteenuste kasutamisega.

Töö järgmine peatükk keskendub sellele, kas krüptovaluutaga tegelevate isikute õigused on Eesti karistusõiguses kaitstud ning kuidas seda erinevate seaduste mõttes reguleeritakse. RahaPTS järgi kohaldatakse seadust virtuaalvääringu teenuse pakkujatele ja neile kohalduvad sarnased sätted finantsasutusega, seega on neil käsitluse kohaselt kattuvaid omadusi. Kuna virtuaalvääring on võõrandatav ja varaliselt hinnatav on sellest saadav tulu tulumaksuga maksustatav ja seda peetakse TuMS järgi varaks. Virtuaalvaluutale annab juurdepääsu privaatvõti, mida hoiustatakse erinevatel viisidel, kas pilves näiteks rahakoti teenuse pakkuja

juures või füüsiliselt mõnel andmekandjal. Privaatvõtmele juurdepääsu saamisel või selle hävitamisel on oluline hinnata ka selle väärtust, mida saab teha kontrollides sellele vastava krüptoraha hetke vastavast tunnustatud valuutale. Samuti on oluline kindlaks teha, kas omandi rikkuja oli teadlik vahendite väärtusest, millele valduse rikkumisele ta juurde pääses. Kui väärtusest teadlik ei oldud, vastutatakse vaid privaatvõtme enda väärtuse eest, kui on tegemist näiteks kõvaketta või juba väga hävituskindlaks tehtud külmlaoga võtme jaoks.

Levinud on ICOdega seotud pettused, kus huvitatud investoritele esitatakse *white paper*'i peal valeandmeid ja nad viiakse eksimusse lubades tulevikus suuri tulusid krüptovaluutaga tegeleva ettevõtte tegevusest. Eesti karistusõiguses on selline tegevus kaetud KarS § 211 koosseisuga, kuna investeering tehakse vara näol, kas tunnustatud valuuta või krüptoraha ülekandmise teel ja teabes esitatakse valesid asjaolusid. Krüptovaluutaga on tihedalt seotud kindlasti ka arvutisüsteemid ja arvutiandmed. Tähtis ongi vahet teha, et arvutisüsteemi osad on arvutid kui kehalised esemed koos oma lisaseadmetega. Plokiahel ja DLT saab käsitleda ikkagi arvutiandmetena. Mõlemat definitsiooni tuleb tähele panna koosseisude hindamisel. KarS § 206 lg 1 kohaselt on karistatav arvutiandmetesse sekkumine aga seda arvutisüsteemis olevate andmete vastu. Kuna aga plokiahel ei asu üheski arvutisüsteemis vaid kasutab ainult arvutisüsteemide ressursse ja konkreetselt mõnega neist seotud ei ole siis antud koosseis krüptovaluutale ei kohaldu. KarS § 206 saaks rääkida vaid nt telefoni, kui arvutiseadme, salvestatud andmete rikkumise puhul, kus võib olla virtuaalvaluutaga seotud või neile juurdepääsu lubavaid andmeid. Samas juhul kui on toime pandud arvutikelmus, vastutatakse ka antud koosseisu järgi, juhul kui sisenetakse virtuaalsesse rahakotti ja kantakse krüptoraha mõnda teise rahakotti. Arvutisüsteemi toimimise takistamisest KarS § 207 mõttes saaksime rääkida vaid siis, kui soovitakse kasutada mõne arvutisüsteemi ja seal olevate serverite võimsust selleks, et krüptoraha kaevandada. Süsteemi toimimise takistamine peab kindlasti olema tunnetatav, mida aga teinekord võimsamate serverisüsteemide puhul tunda ei ole ja nõuda saaks vaid suurenenud elektriarve tasumist, mida on kaevandamisega seotult kindlasti märgata.

Arvutikelmuse KarS § 213 koosseisu on samuti võimalik krüptovaluuta puhul kohaldada, kui tekitatakse varalist kahju. Paralleeli saab tuua pangaautomaadist raha välja võtmisega, kus PIN koodi substitutsiooniks on privaatvõti. Krüptorahale pääseb ligi vahetusplatvormil kasutades selleks privaatvõtit ja kuna kõik vara käsutused toimuvad ühe platvormi siseselt saab ka antud koosseisu kohaldada. Üldiselt saadakse privaatvõtmele ligipääs kas häkkides, mõnda pahavara kasutades või andmepüügiga ja sellised süsteemi sisse murdmised või inimeste lihtsameelsuse ära kasutamised on pahatahtlikud ja sellisel juhul saab kindel olla, et vara omanik ei ole andnud

sellele juurdepääsuks oma luba. Samuti saab krüptovaluutaga tehtavaid vahetusi samastada pangakonto ülekannetega, mis antud koosseisu alla samuti käib. Sarnaselt pangaga toimub sellises juhul muudatus andmesüsteemis ehk plokiahelas, tagasi aga neid kandeid pöörata võimalik enam ei ole, erinevalt pangaülekannete puhul, kus raha jälitamise puhul on see teoreetiliselt võimalik. KarS § 216[1] on võimalik kohaldada juhtudel, kui *phishing*'uga saadakse juurdepääs privaatvõtmele. Häkkimiskoosseis KarS § 217 on võimalik kohaldada vaid arvutisüsteemi puhul, seega ka ainult seadmetesse juurdepääsu saamise puhul ning plokiahel selle alla ei kuulu ja mõeldav on vaid kaitsevahenditest läbitungimise teel kellegi koodide, privaatvõtmele juurde pääsu saamine.

Analüüsi tulemusel võib öelda, et magistritöö püstitatud hüpotees leidis tõendamist ehk kõiki krüptovaluuta eriomadusi silmas pidades, ei ole seadusandja hetkel kõiki võimalikke õigushüvesid suutnud kaitsta. Küptovaluuta on küll enamikel juhtudel kaitstud kui vara seoses selle rahaliselt mõõdetava väärtusega, seda nii pettuste toimepanemisel kui pangakontoga sarnaselt virtuaalsest rahakotist krüptoraha ära kandmise puhul, kui on saadud juurdepääs privaatvõtmele ja selle abil on vahetused tehtud. Hetkel on veel kaitsmata plokiahel ja sealt toime pandavad ründed, millede kahjud võivad ulatuda miljonitesse eurodesse. Seda just põhjusel, et plokiahelat ei saa defineerida arvutisüsteemina, kuna ei ole konkreetselt ühenduses serveritega ning sellest tulevad ka probleemid plokiahela vastaste rünnete defineerimisel. Eestis oleks õiguslikuks arenguks vaja analüüsida kübermaailma ja krüptoraha olemust tulevikku vaadates, selleks, et suurendada arusaama ja valmisolekut võimalike õigushüvede kahjustamisega võitlemiseks. Analüüsi tulemusel saaks võimalikud kitsaskohad likvideerida. Kindlasti on selleks vajalik rahuvaheline koostöö, seda nii Euroopa Liidu kui maailma mastaabis, ja kursis olek globaalselt toimuvate arengute ja muudatustega, et leida Eesti jaoks kõige õigem lahendus.

Cryptocurrency in criminal law

Abstract

Satoshi Nakamoto created Bitcoin in 2009 and after that there has been a rapid development in the cryptocurrency world. The growing popularity of cryptocurrency is old news and more people every day find their way to this complex world of new possibilities. So many altcoins have been created and the market cap of cryptos is growing every day. As the value and popularity grows so does the risks that is opposes. Cryptocurrency's technology is not fully regulated outside the cyberspace.

Purpose of this thesis is to analyse cryptocurrency's suitability in Estonian criminal law system regarding its novelty, rapid development, its non-qualification as a currency and absence of efficient international regulation, but at the same time having a desire to move in this direction. In this thesis author tries to find answers to following legal questions:

- Regarding the special features and characteristics of cryptocurrencies are the rights of the owners protected enough in the Estonian criminal law?
- Is the regulation in criminal law sufficient enough as to cryptocurrency, if not, what are the areas that need development?

Conclusions in this paper will line an overview how and in what way cryptocurrency is regulated in the world and more specifically in Estonia and weather the means to fight against crime are efficient enough. The global view is needed as to the nature of internationality cryptocurrencies.

In the first chapter of the thesis it is explained how cryptocurrency works and what are the technological mechanism behind it. Cryptocurrency is based on blockchain, what uses encrypted and mathematical algorithms, with the purpose to be unreadable for third parties. Anonymity and deserialization were the main purpose to create cryptocurrency. Blockchain itself is based on the consensus mechanism, that if is accepted by all the nodes and by confirming each block the synchronisation and security of the chain is ensured. Blockchain is a data structure that is used in some distributed ledgers which stores and transmits data in blocks that are all connected by a digital chain. Cryptocurrency is stored in digital wallets, that have a purpose to make transactions and exchanges easier. Crypto is moved through exchange

platforms, that are almost like markets but do not have a middle man and that is the reason why they are decentralized and more private. You can trace all the transactions made in the blockchain, but to do so, it is needed to have high level technical knowledge and enough time. If the users want to improve their anonymity and hide their traces a mixing service can be used for money laundering that makes it more difficult to find the source where that exact coin is from.

Cryptocurrency is relatively new technological phenomena, but internationally it has been tried to define what it is both in the financial and legal systems. The financial sector, included FAFT, IMF and banks all over the world, for example ECB, WB, are trying to define what cryptocurrency is. It I found that in the economical definition cryptocurrency cannot be defined as money because it is lacking the functions that are needed for a fiat money. It means that it has limited ways to be used in transactions and it is not accepted everywhere. Also because of the high volatility of the currency it is not considered as legitimate currency and its value is not a constant. In a legal definition it does not fit under the meaning of money, because it is not so widely acknowledged and it has no physical form, both characteristics needed for fiat money. All that creates uncertainty and confusion, because it does not fit in the known systems in our world. It is usually defined as an alternative may of payment that can be used is both parties have agreed on that. At the same time banks have not excluded an option take a use of the DLT technology that blockchain is based on and maybe even develop its own digital currency. But also, it is agreed that cryptocurrencies have a lot of risks that include its volatility, uncertainty of the systems, not having enough regulations and being without certain value.

Many countries have understood over the years that virtual currency is evolving and becoming more popular and thus wanting to be innovative and have a part of the possible success they are trying to find possibilities to regulate its system and evaluate the possible risks. Countries who have been stricter about it and at least partially banned the use of cryptocurrency have usually more authoritarian power that does not wish to give up or lessen their control over the system in any way. However, the opportunity to introduce their own or union-based virtual currency is been discussed more and more seriously. At the moment it seems that the first one to introduce its own cryptocurrency might be China and its possible impact on the world's market cannot be known at the moment. And although the European Union has prohibited Member States to issue their own virtual currency at the same time the introduction of a unitary virtual currency under discussion.

In Estonia it has been stated there is not a definition for cryptocurrency and it is defined as a tender to pay for some commodities and it is not regulated by law. There are some ways to regulate the crypto as to the tax law by taxing all the profits that are made in the exchange or selling of cryptos. Estonian Bank has a firm belief that cryptocurrency will never replace the fiat money but they do not exclude the fact that in the future virtual currency will have a major effect. The market cap of cryptos have been growing fast, as to 1,4 trillion euros, but it is only a small portion of fiat money in circulation, that is more than 7,7 trillion euros.

Estonians Financial Intelligence unit that is fighting against money laundering, had made a analysis in 2020 regarding virtual currency service providers that showed the number of providers have risen significantly in the recent years and it is known that cryptocurrencies are used to hide criminal profits, money laundering, to commit frauds and to but illegal goods. After a recent legislative amendment that have tightened the issuing of activity licences. It was seen that so many service providers did not compel to basic anti-money laundering and person identification regulations. Even though some people in the financial industry firmly believe that crypto is just a bug bubble that will soon explode, the analysis states, that even today it is still popular and with that more risks are relevant. There has been made some structural changes to be more efficient in detecting and preventing cybercrime in general. Estonian Procecuter's Offices finds that the main issue is the lack of resources and the global scale of the crimes, that makes it even more difficult to investigate.

The author brings out the risks associated with cryptocurrency and weaknesses in the system that the criminals use. To get an idea of the nature, content, and extent of the problem, some attacks in the world have also been outlined as examples. As digital systems are increasingly in use it is no surprise that also criminals are trying to use the system to their benefit.

EU legislation regarding anti-money laundering has become more efficient and consequently increased financial supervision in the banking sector which has made moving criminal revenues through legal traditional banking systems more complicated. As a result, money laundering is been directed to sectors that haven't yet developed that strict control mechanisms or where supervision is limited. This however leads to the need and creation of underground cash transfer agencies, alternative bank platforms and anonymous virtual currencies. The use of cryptocurrency in this case is an increasing problem, as there is no common regulation to find out what kind of anonymity such services are offering regarding crime.

Estonian Financial Intelligence Unit (RAB) believes that the risks of virtual currency connected to terrorism financing are underestimated compared to money laundering. The rapid growth in the use of virtual currencies and the number of service providers in the past years has also enhanced the risks of criminality in the field. The information gathered by RAB indicates that virtual currencies are exploited also in Estonia for hiding criminal income and for money laundering as well as for committing fraud and for buying illegal goods and services. This is because the cryptocurrency system is decentralized, they are quick and easy to use, while international regulation is incomplete, and receiving the information needed from service providers is difficult for law enforcement agencies. It is not considered to be credible that cryptocurrency is not used for financing terrorism if it is already widely used in the criminal world. According to the Estonian Internal Security Service, virtual currencies are more and more widespread among Islamic extremists who use them for organizing money-raising campaigns, sharing anonymous wallet addresses through social media or communication applications. Such campaigns are used today too, among others to support the armed groupings or the families of foreign combatants who live in refugee camps. The only things that hinder the very widespread exploitation of virtual currencies for terrorist financing are the great fluctuation of the exchange rate of the cryptocurrency and limited possibilities to exchange it for money. RAB has also received messages from the service providers where the persons involved in terrorism have wanted to establish business relations. This clearly shows that people involved in terrorism are also associated with cryptocurrency.

There are different crimes that are not subject to cryptocurrency, but, for example, require the ransom in cryptocurrency. In 2017, the ransomware attack was started with the name Wannacry, which affected about 300,000 computers around the world and whose losses amounted to hundreds of millions to billions of dollars. Cryptoworm encrypted data on the computer and the user couldn't access them anymore. As a ransom for encryption, there was a demand for a payment in the Bitcoin cryptocurrency. Wannacry also reached Estonia, but only the six computers were infected. Apparently behind the attack was a North Korean citizen and a company controlled by the state.

The author notes that demand for cryptocurrency as ransom is certainly caused by its partial anonymity as it is difficult to determine its source, but it is not impossible. Even though most cryptocurrencies are pseudo-anonymous and the transfers are public, in order to track the transfers in the blockchain it needs appropriate skills and resources. The investigation is made more complicated using mixing services that interfere with the traces of cryptocurrency

movements and make them more anonymous. Europol considers that the use of encrypted currencies and extensive use of anonymous modification techniques, including encryption, will grow in the future.

However, the mechanisms underlying corruption have changed the way in which the acts are reflected directly in society and technology. For example, one more widespread use of it is that cryptocurrency is used to pay corrupt officials for money laundering purposes. The widespread use of developed digital technologies and extensive use of social media and the possibilities of encrypted communication can provide an opportunity for migrants to coordinate their activities, recruit both workers, and victims and avoid the law enforcement agencies. Recently there have been reports indicating the use of cryptocurrency also by smugglers.

Cryptojacking is still a problem but not a priority for Europol. In the case of cryptojacking, the computer is infected with a virus, after which computer resources are used for mining or to steal the cryptocurrency from other digital wallets. Said hijacking is more popular among hackers, as malware is easy to place and complicated to discover and remains rather unnoticed. It is also increasingly common to embed the malware on the YouTube platform, where it is easy to find victims to click on the link. Although such attacks may affect many, the losses are usually small and therefore not reported.

With regard to the YouTube platform, there is a recent case where Ripple sued Youtube over cryptocurrency scams just because the latter failed to protect consumers from cryptocurrency "giveaway" scams that use fake social media profiles to dupe victims into sending money. Scammers on YouTube have been impersonating Ripple and its chief executive, Brad Garlinghouse, to bait viewers into sending them thousands of dollars worth of XRP, a cryptocurrency championed by Ripple. People were promised to get in return up to 1 million dollars worth of XRPs, but it never happened.

In its recent study, RAB has brought out a general trend in Estonian crime that the use of virtual currencies in criminal schemes are widespread, they are used in preparatory stages and for interconnection. The cryptocurrency is used for all sorts of crime, but it is common to pay for infrastructures or services used and the ransom is in virtual currency. Estonia has received a number of legal advice requests where service providers have committed scams. Also, the use of virtual currencies in money laundering has been confirmed through legal cooperation. Viru

County Court judgment in Criminal Matter No 1-19-5363 was detected the use of virtual currencies in money laundering.

Ministry of Justice in Estonia belies that cybercrime and crime relating to technology are certainly the crime of the future. The global scale of the crimes needs better international relations, that Estonia in general has with EU states, but is lacking with Russia and is very difficult to execute in Africa where a lot of phishing schemes are originated. European Commission helped with a research as to what Estonia should be doing going forward and it was fount that the three main suggestions was prepare legislative, regulative organisational environment to adequately respond to cybercrime. Also, to build cybercrime capacity in light of the technological development, for example having a nation-wide awareness programme, strengthen higher education and research on emerging technologies and to explore the need of professional development. As well to ensure that there is sufficient technological expertise, skills and to identify were investments are needed in Estonian law enforcement and justice systems.

Then in the thesis it was analysed what kind on offences regarding cryptocurrencies are penalised in Estonian Penal Code and how are the owner rights protected. As the virtual currency has a monetary value it defines as a asset it classifies in some damages against property. It is important to understand the difference in computer systems and data and how it fulfils the requirements with cybercrime. Computer system is a computer and other connected hardware that are connecter, so for example a laptop and a mouse, printer etc, but also some kind of server. Computer data is something that is in the computer system and cannot be outside of it, for example on a hard-drive, USB stick or on a cloud or in the Internet. Therefor Penal Code § 206 - interference with computer data would be acceptable only when the interfered data is in a computer system, and an example can be a mobile phone that hold some sort of connection or private key to cryptocurrencies. Penal Code § 207 - hindering of functioning of computer systems would apply when if some kind on computer system is used for mine cryptocurrencies and by that the computer system is interfered or the functioning is hindered.

Both computer related frauds and investment frauds are compatible. Investment frauds as to the Penal Code § 211 are popular with the initial coin offerings, aka ICO, when receipt of an investment through, that usually contains investment to some sort of service provided for cryptocurrency, and presenting of false information among the essential information addressed to the public or specified group of persons or failure to submit essential information. That kind

on fraud schemes have been more and more frequent because people see cryptocurrencies as a quick way to gain some income. Computer fraud as to Penal Code § 213, qualifies when the private key is used in a similar way as a PIN code of bankcard and then all the assets will be moved or withdrawn. Penal Code § 216^1 preparation of computer-related crime can be used when a criminal gets a hold of the private key via phishing. Ant the classical hacking classification is in the Penal Code § 217 that criminalizes obtaining access to computer systems illegally. It can be used only when computer systems are used, their defence mechanisms are removed, for example a firewall or codes, and then got the hold of someone's private key. Blockchain does not qualify as it is a data system.

In conclusion it can be said that the author's hypothesis was proved. The current criminal law and Penal Code in Estonia does not provide enough protection when legal rights that are connected to cryptocurrencies, are violated. In most cases cryptocurrency is protected as property, because its worth can be measured in money. These cases would be fraud schemes and also similarly to thefts from bank accounts that can be equivalent to cryptocurrency theft from virtual wallet providers. It is prerequisited that the perpretator have got a hold of the private key in some way and made the transfers. At this stage crimes related to blockchain are still not protected, where the attacs are become more frequent and the damages are up to millions of euros. The reason it is still unprotected is the definition of blockchain and it is not a computersystem, because it has no real connection to the servers and is located in the Internet, on a could.

In Estonia it is needed to analyse cyberspace and the nature of cryptocurrencies looking forward, so it can build a common understanding and preparedness to fight against possible attacks and undermining of the law. With an effective and comprehensive analysis possible weaknesses and shortcoming can be removed. It definitely needs more efficient international cooperation, globally and also in the European Union, to be aware of international developments and changes and to find the best solution for Estonia.

KASUTATUD ALLIKAD

Kasutatud kirjandus

1. Arula, E., *Krüptoraha varastamises süüdistatav mees astus kohtu ette*, Tartu Postimees, 12.02.19. https://tartu.postimees.ee/6520846/kruptoraha-varastamises-suudistatav-mees-astus-kohtu-ette?_ga=2.164374137.774328925.1587985276-450726865.1587135184
2. Bellasio, J. jt, *The Future of Cybercrime in Light of Technology Developments*, RAND Europe, 2020. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA137-1/RAND_RRA137-1.pdf
3. Biggs, J., *$6 Million in Stolen Binance Bitcoin Is On the Move Again*, CoinDesk, 13.06.2019. https://www.coindesk.com/the-stolen-binance-btc-is-on-the-move-again
4. Biggs, J., *Exit scammers run off with $660 million in ICO earnings*, TechCrunch, 13.04.2018. https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/
5. Boase, R., *Hackers steal $1.2 Million of bitcoins from Inputs.io, a supposedly secure wallet service*, CoinDesk, 07.11.2013. https://www.coindesk.com/hackers-steal-bitcoins-inputs-io-wallet-service
6. Buchko, S., *How Long do Bitcoin Transactions Take?*, CoinCentral, 12.12.2017. https://coincentral.com/how-long-do-bitcoin-transfers-take/
7. Buchko, S., *How many bitcoins are left?*, CoinCentral, 30.04.2020. https://coincentral.com/how-many-bitcoins-are-left/
8. Chavez-Dreyfuss, G., *Cryptocurrency crime surges, losses hit $4.4 billion by end-September: CipherTrace report*, Reuters, 27.11.2019. https://www.reuters.com/article/us-crypto-currencies-crime/cryptocurrency-crime-surges-losses-hit-44-billion-by-end-september-ciphertrace-report-idUSKBN1Y11WH
9. Chu, D., *Broker-dealers for virtual currency: regulating cryptocurrency wallets and exchanges*, Columbia Law Review, vol 118:2323, 2018. https://columbialawreview.org/wp-content/uploads/2018/12/Chu-BROKER-DEALERS_FOR_VIRTUAL_CURRENCY_REGULATING_CRYPTOCURRENCY_WALLETS_AND_EXCHANGES.pdf

10. Chuck, E., Abbruzzese, J., *'I'm in your baby's room': Nest cam hacks show risk of internet-connected devices*, NBC News, 21.12.2018. https://www.nbcnews.com/tech/tech-news/i-m-your-baby-s-room-nest-cam-hacks-show-n950876
11. Cointelegraph, *ICO Vs IPO: Key Differences*. https://cointelegraph.com/ico-101/ico-vs-ipo-key-differences
12. *Countries Where Bitcoin Is Banned or Legal In 2020*, Cryptonews. https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm
13. Cybernetica, *Krüptograafiliste algoritmide elutsükli uuring 2017*, versioon 2.0, Riigi Infosüsteemi amet, 09.02.2018. https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf
14. De Hoon, I., *Germany: A Surprising Bitcoin Tax Haven*, nomoretax.eu. https://nomoretax.eu/bitcoin-tax-haven-germany
15. Down M., *The Latest ICO Scam… is Fake?*, Hackermoon 16.03.2019. https://hackernoon.com/the-latest-ico-scam-is-fake-a106b149f099
16. EBA, *Report with advice for the European Commission on crypto-assets*, 09.01.2019. https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1
17. Eesti Pank, *Finantsstabiilsuse ülevaade*, 1/2018. https://www.eestipank.ee/publikatsioon/finantsstabiilsuse-ulevaade/2018/finantsstabiilsuse-ulevaade-12018
18. EMTA, *Eraisiku virtuaalses valuutas/krüptovaluutas saadud tulu maksustamine*, 26.04.2021 https://www.emta.ee/et/eraklient/tulu-deklareerimine/muu-tulu/eraisiku-virtuaalses-valuutaskruptovaluutas-saadud-tulu
19. ESMA, EBA, EIOPA, *Warning. ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies*, 12.02.2018. https://www.esma.europa.eu/press-news/esma-news/esas-warn-consumers-risks-in-buying-virtual-currencies
20. European Central Bank, *Virtual currency schemes – a further analysis*, 02.2015. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
21. Europol and Eurojust, joint report: *Common challenges in combating cybercrime*, 06.2019. https://www.europol.europa.eu/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf

22. Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2019. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
23. Europol, press release: *Cryptocurrency laundering as a service: members of a criminal organisation arrested in Spain*, 08.05.2019. https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain
24. Europol, press release: *Fake investors busted in Belgium and France*, 29.01.2020. https://www.europol.europa.eu/newsroom/news/fake-investors-busted-in-belgium-and-france
25. Europol, press release: *Hook, line and sinker: cybercrime network phishing bank credentials arrested in Romania*, 29.09.2020. https://www.europol.europa.eu/newsroom/news/hook-line-and-sinker-cybercrime-network-phishing-bank-credentials-arrested-in-romania
26. Europol, Press release: *Multi-million euro cryptocurrency laundering service bestmixer.io taken down*, 22.05.2019. https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down
27. Europol, press release: *Ten hackers arrested for string of sim-swapping attacks against celebrities*, 10.02.2021. https://www.europol.europa.eu/newsroom/news/ten-hackers-arrested-for-string-of-sim-swapping-attacks-against-celebrities
28. Europol, Serious and Organised Crime Threat Assessment. *A corrupting influence: the infiltration and undermining of europe's economy and society by organised crime*, EU SOCTA 2021. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment
29. Faggart, A., *What Happens to Bitcoin Miners When all Coins are Mined?*, Bitcoin.com, 15.08.2015. https://news.bitcoin.com/what-happens-bitcoin-miners-all-coins-mined/
30. Financial Action Task Force, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, 06.2014. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf
31. Finantsinspektsioon, *Virtuaalraha (ICO)*, 27.12.2018. https://www.fi.ee/et/finantsinspektsioon/finantsinnovatsioon/virtuaalraha-ico

32. Frankenfield, J., *Initial Coin Offering (ICO)*, Investopedia, 3.11.2020. https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp
33. Gibbs, S., *Head of Mt Gox bitcoin exchange on trial for embezzlement and loss of millions*, The Guardian, 11.07.2017. https://www.theguardian.com/technology/2017/jul/11/gox-bitcoin-exchange-mark-karpeles-on-trial-japan-embezzlement-loss-of-millions
34. Grinberg, R., *Bitcoin: An Innovative Alternative Digital Currency*, Hastings Science and Technology Law Journal, 2011, vol 4. https://sites.cs.ucsb.edu/~rich/class/cs293b-cloud/papers/bitcoin.legal.pdf
35. Hayes, A., *What Happens to Bitcoin After All 21 Million Are Mined?*, Investopedia, 28.02.2021. https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/#citation-2 https://harvardmagazine.com/2000/01/code-is-law-html
36. IMF, Staff Discussion Note: *Virtual Currencies and Beyond: Initial Considerations*, 20.06.2016. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Virtual-Currencies-and-Beyond-Initial-Considerations-43618
37. Justiitsministeerium, *Kuritegevus Eestis 2018*, kriminaalpoliitika.ee, Tallinn 2019. https://www.kriminaalpoliitika.ee/et/kuritegevus-eestis-2018
38. Justiitsministeerium, *Kuritegevus Eestis 2019*, kriminaalpoliitika.ee, Tallinn 2020. https://www.kriminaalpoliitika.ee/kuritegevuse-statistika/kuberkuriteod.html
39. Justiitsministeerium, *Kuritegevus Eestis 2020*, kriminaalpoliitika.ee, Tallinn 2021. https://www.kriminaalpoliitika.ee/kuritegevus2020/kuberkuriteod
40. Justiitsministeerium, *Riikide õiguskoostöö lepingud*, 5.09.2014. https://www.just.ee/et/eesmargid-tegevused/rahvusvaheline-oiguskoostoo/riikide-oiguskoostoo-lepingud
41. Kairjak, M., Sootak, J., Varavastased süüteod, 4. väljaanne, Juura, Tallinn 2017.
42. Kalev, M., *Eesti geniaalseim kuritegu? Kolm miljonit eurot tulu, aga kannatanuid justkui polegi*, Eesti Ekspress, 12.03.2019. https://ekspress.delfi.ee/kuum/eesti-geniaalseim-kuritegu-kolm-miljonit-eurot-tulu-aga-kannatanuid-justkui-polegi?id=85575889 (tasuline artikkel)
43. Kharpal, A., *China has given away millions in its digital yuan trials. This is how it works*, CNBC.com, 04.03.2021. https://www.cnbc.com/2021/03/05/chinas-digital-yuan-what-is-it-and-how-does-it-work.html

44. Kim, C., *Report: More Than Three-Quarters of ICOs Were Scams*, CoinDesk, 12.07.2018. https://www.coindesk.com/report-more-than-three-quarters-of-icos-in-2017-were-scams
45. Korjus, K., *We're planning to launch estcoin — and that's only the start*, Medium.com, 19.12.2017. https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790
46. Lagarde, C., Interview with "Challenges" magazine, 08.01.2020. https://www.ecb.europa.eu/press/inter/date/2020/html/ecb.in200108~f3ba434000.en.html
47. Lessig, E., *Code Is Law. On Liberty in Cyberspace*, Harvard Magazine 01/2020.
48. Liive, R., *Rumeenias tabatud küberpättide ohvriks langes ligi 40 eestlast, kahju üle 100 000 euro*, digi.geenius.ee, 07.04.2021. https://digi.geenius.ee/rubriik/uudis/rumeenias-tabatud-kuberpattide-ohvriks-langes-ligi-40-eestlast-kahju-ule-100-000-euro/
49. Lucian, A., *Will the 'China Blockchain Narrative' Lead the Cryptocurrency Market in 2020?*, BeInCrypto, 17.04.2020. https://beincrypto.com/will-the-china-blockchain-narrative-lead-the-cryptocurrency-market-in-2020/
50. Lõugas, H., *Professor Buldas: pole selge, kas Bitcoini-plokiahelat üldse vaja on ja kas see püsima jääb*, geeniusmeedia, 23.02.2018. https://digi.geenius.ee/rubriik/uudis/professor-buldas-pole-selge-kas-plokiahelat-uldse-vaja-ja-kas-see-pusima-jaab/
51. Lõvi, S. /ERR, *Hansson nimetas krüptoraha "täielikuks mõttetuseks", mis peagi välja sureb*, 07.01.2019 https://www.err.ee/892935/hansson-nimetas-kruptoraha-taielikuks-mottetuseks-mis-peagi-valja-sureb
52. Magas, J., *Five Countries Where Crypto Regulation Changed the Most in 2019*, Cointelegraph, 29.12.2019. https://cointelegraph.com/news/five-countries-where-crypto-regulation-changed-the-most-in-2019
53. Marshall, A., *P2P Cryptocurrency Exchanges, Explained*, 07.04.2017. https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained
54. Mäe, I., Mandel, M., *Lõhmus teenis krüptorahaga miljoneid, kuid ei saanud sellele ligi*, Äripäev, 13.07.2019 https://www.aripaev.ee/uudised/2019/07/13/lohmus-teenis-kruptorahaga-miljoneid-kuid-ei-saanud-sellele-ligi

55. Müller, M., *Krüptovarad – mull või tulevik?*, Eesti Pank, 15.01.2018. https://www.eestipank.ee/blogi/kruptovarad-mull-voi-tulevik
56. Ossinger, J., *China's Plan for Digital Yuan Imperils Bitcoin's Biggest Markets*, Bloomberg, 6.03.2021. https://www.bloomberg.com/news/articles/2021-03-05/china-s-plan-for-digital-yuan-imperils-bitcoin-s-biggest-markets
57. Palmer, D., *More Than Half of ICOs Fail Within 4 Months, Study Suggests*, CoinDesk, 10.07.2018. https://www.coindesk.com/over-half-of-icos-fail-within-4-months-suggests-us-study
58. Paul, K., *Ripple sues YouTube over cryptocurrency scams*, Reuters, 21.04.2020. https://www.reuters.com/article/google-lawsuit-fraud/ripple-sues-youtube-over-cryptocurrency-scams-idUSL5N2C93E8
59. Pavlo, W., *Crime And Punishment In The Cryptocurrency World*, Forbes, 25.02.2020 https://www.forbes.com/sites/walterpavlo/2020/02/25/crime-and-punishment-in-the-cryptocurrency-world/#6b2359dd48fe
60. Rahandusministeerium, *Analüüs virtuaalvääringute võimaliku tunnustamise ja kasutamise poliitika väljatöötamiseks*, 2017. https://www.rahandusministeerium.ee/et/system/files_force/document_files/2016-vv_virtuaalvaaringute_analuus-22-07.pdf?download=1
61. Rahandusministeerium, *Krüptovarade reguleerimise väljatöötamiskavatus*, november 2019. https://www.rahandusministeerium.ee/sites/default/files/news-related-files/kruptovarade_reguleerimise_vtk.pdf
62. Rahandusministeerium, *Rahapesu andmebürood ootab 2021. aastal ees kiire kasv*, 4.12.2020. https://www.rahandusministeerium.ee/et/uudised/rahapesu-andmeburood-ootab-2021-aastal-ees-kiire-kasv
63. Rahandusministeerium, *Rahapesu uurimistes lähevad juhtohjad prokuratuurile*, 18.02.2021. https://www.rahandusministeerium.ee/et/uudised/rahapesu-uurimistes-lahevad-juhtohjad-prokuratuurile
64. Rahapesu andmebüroo, *Virtuaalväärингu teenuse pakkuja uuring*, 22.09.2020. https://www.fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvringu-tee
65. Rattam, E., *Küberkuritegevuse ökosüsteem on muutunud teenusepõhiseks*. Prokuratuuri aastaraamat 2020. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2020/kuberkuritegevuse-okosusteem-muutunud-teenusepohiseks

66. Redman, J., *Triple-Entry Bookkeeping: How Satoshi Nakamoto Solved the Byzantine Generals' Problem*, Bitcoin.com, 2.02.2020. https://news.bitcoin.com/triple-entry-bookkeeping-how-satoshi-nakamoto-solved-the-byzantine-generals-problem/
67. Riigikogu. Arvutikuritegevusvastane konventsioon, 23.11.2001. https://www.riigiteataja.ee/akt/550359
68. Schnabel, I., Interview with Der Spiegel, ECB, 9.04.2021 https://www.ecb.europa.eu/press/inter/date/2021/html/ecb.in210409~c8c348a12c.en.html
69. Shaban, H., *Binance says hackers stole $40 million worth of bitcoin in one transaction*, The Washington Post, 8.05.2019. https://www.washingtonpost.com/technology/2019/05/08/binance-says-hackers-stole-million-worth-bitcoin-one-transaction/
70. Sobers, R., *What Is Cryptojacking? Prevention and Detection Tips*, 29.01.2021. https://www.varonis.com/blog/cryptojacking/
71. Sokolov, P., *Important Notice On Guarda SAFU*, Guarda.com, 04.01.2021. https://guarda.com/blog/important-notice-on-guarda-safu/
72. Sokolov, P., *Security Incident on December 20, 2020*, Guarda,com, 02.01.2021. https://guarda.com/blog/security-incident-on-december-30-2020/
73. Sootak, J., Karistusõiguse alused, Tallinn: Juura 2003.
74. Sootak, J., Pikamäe, P., Karistusseadustik. Komm vlj, 5. vlj. Tallinn: Juura 2021.
75. Zainuddin, A., *Altcoins vs Tokens: What's the Difference?*, Master The Crypto, 2020. https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/
76. Zetzsche, D. A. jt, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, Harvard International Law Journal, vol 60, nr 2, 2019. https://harvardilj.org/wp-content/uploads/sites/15/3_ICO_60.2.pdf
77. Van Wirdum, A., *Is Bitcoin Anonymous? A Complete Beginner's Guide*, Bitcoin Magazine, 18.11.2015. https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283
78. World Bank Group. *Distributed Ledger Technology (DLT) and Blockchain*, 2017. http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf
79. Young, C., *Cybercriminals Hacked GitHub's Servers for Crypto Mining*, Interesting Engineering, 05.04.2021. https://interestingengineering.com/cybercriminals-hacked-githubs-servers-for-crypto-mining

Kasutatud kohtupraktika

1. Euroopa Kohtu otsus, 22.10.2015, C-264/14, Skatteverket vs David Hedqvist.
2. RKHKo 3-3-1-75-15
3. RKKK 3-1-1-117-13
4. RKKK 3-1-1-14-00
5. RKKK 3-1-1-60-01
6. RKKK 3-1-1-83-07
7. RKKK 3-1-1-94-14
8. Viru Maakohtu 20.11.2019 otsus kriminaalasjas 1-19-5363. https://www.riigiteataja.ee/kohtulahendid/fail.html?id=259824625

Kasutatud õigusaktid

1. Arvutikuritegevusvastane konventsioon, art 1a. - RT II, 2003, 9, 32. https://www.riigiteataja.ee/akt/550359
2. Asjaõigusseadus. - RT I, 22.02.2019.
3. Eesti Vabariigi ja Vene Föderatsiooni leping õigusabi ja õigussuhete kohta tsiviil-, perekonna- ja kriminaalasjades. - RT II, 26.01.1993.
4. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2013/40, 12.08.2013, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK. - ELT L 218/8. https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32013L0040&qid=1619289068742&from=EN
5. 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. – ELT L156/43. https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32018L0843
6. Karistusseadustik – RT I, 03.03.2021, 3.
7. Rahapesu ja terrorismi rahastamise tõkestamise seadus - RT I, 14.04.2021, 6
8. Tsiviilõiguse üldosa seadus – RT I, 22.03.2021, 8.
9. Tulumaksuseadus – RT I, 26.03.2021, 2.

10. Võlaõigusseadus – RT I, 04.01.2021, 19.

Kasutatud muud allikad:

1. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
2. https://et.wikipedia.org/wiki/Arvutiprogramm
3. SE 459, seletuskiri algatamise juurde, lk 4, 6. (XIII koosseis)
4. SE 8, seletuskiri I lugemise juurde, lk 9-10. (XIV koosseis)
5. Rahapesu andmebüroo (RAB 2020), Virtuaalvääringu teenuse pakkuja uuring, 22.09.2020.