



RAHAPESU ANDMEBÜROO

# Pesastatud teenused krüptovara kauplemise platvormidel

Detsember 2025



## Sissejuhatus

Krüptovara\* ja plokiahela tehnoloogia ning nendega seotud tehnoloogiate vastutustundliku arengu ja kasutamise toetamine on Eesti Vabariigi üks olulisi prioriteete. Kuigi krüptovara võib olla innovatsiooni ajend, on seda kuritarvitanud ebaseadusliku tegevusega seotud osapooled, nagu küberkurjategijad ja sanktsioneeritud isikud. Krüptovaraga seotud ebaseadusliku finantstegevuse riskid on seotud ka krüptovarateenuse osutajate, täpsemini krüptovara kauplemise platvormidega, mis tegutsevad *pesastatud teenusepakkujatena* või osutavad *pesastatud teenuseid*. Rahapesu Andmebüroo (edaspidi RAB) avaldab käesoleva analüüsi, et tõsta teadlikkust pesastatud krüptovara kauplemise platvormidest ja sellest, kuidas neid ja nende teenuseid võidakse kuritegelikel eesmärkidel ära kasutada.

Pesastatud krüptovara kauplemise platvormid võivad asjakohaste riskide maandamismeetmete puudumisel kahjustada rahapesu ja terrorismi rahastamise tõkestamise (AML/CFT) kontrollimeetmeid, mis kehtivad laiemas krüptovara ökosüsteemis. Kuna õigusrikkujad kasutavad finantskuritegude toimepanemiseks ja seadustest möödahiilimiseks üha enam krüptovara, on pesastatud krüptovara kauplemise platvormid üha haavatavamad laiemas krüpto ökosüsteemis. Seda nii krüptovara kauplemise platvormidele, kes kohaldavad hoolsusmeetmeid, kui ka finants- ja õiguskaitseasutuste võimele seirata tehinguid ja tuvastada ebaseaduslikke tegevusi.<sup>1</sup> RAB on toonud analüüsis välja ohumärgid, mis aitavad tuvastada ebaseaduslikult tegutsevate isikute omanduses, halduses või kontrolli all olevaid pesastatud krüptovara kauplemise platvorme.

Analüüsi koostamisel konsulteeriti USA Rahandusministeeriumi Finantskuritegude Tõkestamise Võrgustikuga (FinCEN), mis samuti panustas projekti tulemustesse.

## Mis on pesastatud krüptovara kauplemise platvormid / pesastatud teenused?

Krüptovara on vahetatav väärtus, mis võib toimida nagu valuuta, kuid millel ei ole kõiki reaalse valuuta omadusi; näiteks ei ole sellel enamikus riikides seadusliku maksevahendi staatust.<sup>2</sup> Omandiõiguse saab krüptovarale omistada plokiahela kaudu, mis on jaotatud andmebaasi tehnoloogia liik ning mis krüptograafiliselt allkirjastab tehingud ja rühmitab need plokkidesse.<sup>3</sup> Omandiõiguse määramisel seotakse krüptovara tähtnumbrilise identifikaatoriga aadressiga, mis tähistab krüptovara ülekande võimalikku sihtkohta.<sup>4</sup> Sageli kasutatakse krüptovara hoidmiseks või ülekandmiseks „rahakotte”. Rahakott on liides, mis võimaldab krüptovara hoiustada või üle kanda ning luua ja talletada krüptovara omaniku avalikke ja privaatsaid võtmeid. Rahakottide tüübid erinevad kasutatava tehnoloogia, väärtuse hoiustamise koha ja viisi poolest, aga ühtlasi ka selle poolest, kes kontrollib varale juurdepääsu.

\* Eesti õigusloomes ja erialakirjanduses on sageli sünonüümidena kasutatud erinevaid termineid nagu virtuaalvaluuta, virtuaalväering, krüptovaluuta, krüptovara ja digitaalne vara. Selles analüüsis kasutame mõistet krüptovara, mis on kooskõlas värskemate EL-i regulatsioonide ja Eesti õigusloomega. Konkreetsele krüptovara liigile antud nimetus (nt „digitaalvaluuta”, „krüptovaluuta”, „virtuaalvaluuta”, „virtuaalväering”, „digitaalne vara” jne) ei määra iseenesest selle regulatiivset käsitlust. Nähtuste kirjeldamiseks kasutas RAB ka terminoloogiat, mida kasutavad laialdaselt finantseerimisasutused ja krüptovara kauplemise platvormid. See mõisteraamistik on üksnes illustratiivne ega ole käsitletav RAB-i poolt [regulatiivsel eesmärgil] kinnitatuna.

<sup>1</sup> [RAB-i aastaraamat 2022](#) (2023), lk 45.

<sup>2</sup> Krüptovara, millel on valuutaga võrdne väärtus või mis toimib valuuta asendajana – mida nimetatakse konverteeritavaks krüptovaraks – on seega „valuutat asendav väärtus”.

<sup>3</sup> Lisateavet plokiahelate kohta vt EU Blockchain Observatory and Forum „[Blockchain for beginners- basic guiding principles](#)” (2024).

<sup>4</sup> FATF, „[Virtual Currencies Key Definitions and Potential AML/CFT Risks](#)” (2014).

Krüptovara kauplemise platvormid on ettevõtted, mis võimaldavad vahetada üht krüptovara teise krüptovara või *fiat*-valuuta vastu tasu eest ja kokkulepitud kursiga. Kuigi selles valdkonnas on mitmesuguseid ärimudeleid, kontrollivad krüptovara kauplemise platvormid sageli korraka paljusid aadresse ja rahakotte ning neil võib olla juurdepääs *fiat*-valuutale otse või mõne teise finantsasutuse kaudu.

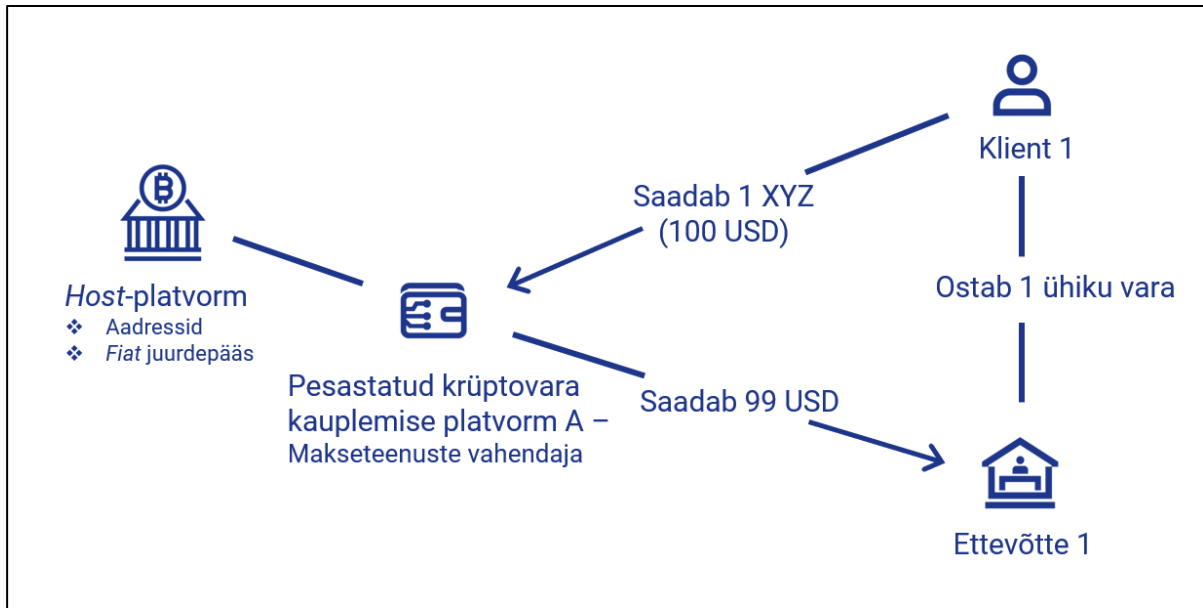
Pesastatud krüptovara kauplemise platvorm on tavaliselt väiksem platvorm<sup>5</sup>, mis pakub oma klientidele teenuseid suuremate krüptovara kauplemise platvormide (tuntud ka kui *hostid* või *host-platvormid*) kontode ja alamkontode kaudu.<sup>6</sup> Sellistel pesastatud krüptovara kauplemise platvormidel võib olla õiguspäraseid ja põhjendatud rakendusi. Näiteks võivad nad kasutada ära suurema krüptovara kauplemise platvormi pakutavat likviidsust, teenuseid ja mugavusi, ning nad võivad kasutada suurema krüptovara kauplemise platvormi aluseks olevat tarkvara, riistvara, plokiahelapõhist (*on-chain*) likviidsust, plokiahelaväliseid (*off-chain*) arveldusi või traditsioonilisi finants- või õiguslikke struktuure. Kuid tegutsemine täielikult või osaliselt teise krüptovara kauplemise platvormi infrastruktuuris, ja mitte iseseisva üksusena, pakub ebaseaduslikele tegutsejatele võimalust luua täiendav kiht enda varjamiseks, mis võib lükata edasi või takistada nii finants- kui ka õiguskaitseasutuste jõupingutusi kahtlaste tegevuste tuvastamisel.<sup>7</sup> Süsteemse haavatavuse tekitab *host*-platvormide suutmatus võtta kasutusele asjakohased reeglid, protseduurid ja kontrollimeetmed, et tuvastada pesastatud tegevust, ning puudused riskipõhiste hoolsuskohustuste rakendamisel pesastatud krüptovara kauplemise platvormide klientide suhtes. Kurjategijad võivad neid haavatavusi ekspluateerida ja kasutada pesastatud krüptovara kauplemise platvormi, millel puuduvad AML/CFT kontrollimeetmed (näiteks kliendi tuvastamise nõuded), et vältida kahtlase tegevuse avastamist ja sellest teatamist.

Joonisel 1 on toodud üks näide pesastatud krüptovara kauplemise platvormi tegevusest. Pesastatud krüptovara teenuse osutaja A tegutseb makseteenuse vahendajana. Pesastatud krüptovara teenuse osutaja A haldab mitmeid krüptovara rahakotiaadresse suure krüptovara kauplemise platvormi ehk *host*-platvormi juures. *Host*-platvorm lubab pesastatud krüptovara teenuse osutajal A vahetada krüptovara *fiat*-valuuta vastu. Näites ostab Klient 1 Ettevõttelt 1 ühiku vara hinnaga 99 dollarit. Klient 1 maksab vara eest ühe XYZ-mündiga, mis on 100 dollari väärtusega krüptovara. Makse sooritamiseks annab Klient 1 XYZ-mündi omandiõiguse üle ühele pesastatud krüptovara teenuse osutaja A aadressidest *host*-platvormile. Pesastatud krüptovara teenuse osutaja A suunab seejärel *host*-platvormi konverteerima XYZ-mündi *fiat*-valuutasse (väärtusega 99 dollarit) ja kandma need 99 dollarit pesastatud krüptovara teenuse osutaja A *fiat*-valuuta kontolt *host*-platvormil Ettevõttele 1. Ülejäänud 1 dollari säilitab pesastatud krüptovara teenuse osutaja A enda kasumina või teenustasuna.

<sup>5</sup> Analüüsis võttis RAB arvesse mitmeid näitajaid, et üldiselt hinnata krüptovara kauplemise platvormi suurust, nagu näiteks kauplemismahtusid, hoitavat vara, klientide arvu ja tehingute väärtuseid. Näiteks: kui krüptovara kauplemise platvorm A teostab päevas 100 000 tehingut ja krüptovara kauplemise platvorm B teostab päevas 25 000 tehingut, hindaks RAB, et platvorm A on suurem kui B.

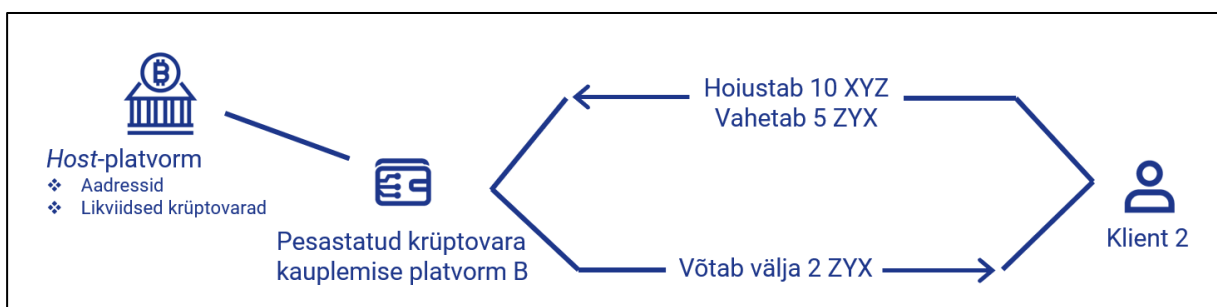
<sup>6</sup> FATF, „[Virtual Assets and Virtual Asset Service Providers, Updated Guidance for a Risk-Based Approach](#)” (2021), lk 53. (seal kirjeldatakse pesastatud teenuseid kui „kontode pakkumist väiksematele krüptovara kauplemise platvormidele, et anda neile juurdepääs likviidsusele ja kauplemispaaridele”).

<sup>7</sup> [RAB-i aastaraamat 2022](#) (2023), lk 45.



**Joonis 1. Näide pesastatud krüptovara kauplemise platvormi tegevusest**

Joonisel 2 on toodud veel üks näide pesastatud krüptovara kauplemise platvormi tegevusest. Skeemil on pesastatud krüptovara kauplemise platvorm B vahetusteenuse osutaja, millel on suure krüptovara kauplemise platvormi ehk *host-platvormi* juures avatud mitmeid krüptovara aadresse. *Host-platvorm* hoiab erinevaid krüptovarasid likviidsete reservidena, sealhulgas XYZ-münti ja ZYX-münti. Klient 2 teeb mitu tehingut krüptovaraga: hoiustab kümme XYZ-münti, vahetab need viie ZYX-mündi vastu ja võtab seejärel kaks ZYX-münti välja. Kliendi 2 jaoks tundub, et kõik need tehingud toimuvad pesastatud krüptovara kauplemise platvormi B rakendusliidese kaudu (nt rakendus Kliendi 2 telefonis). Tegelikult teeb pesastatud krüptovara kauplemise platvorm B samad tehingud *Host-platvormiga*. Nii näiteks, kui Klient 2 hoiustab 10 XYZ-münti, määrab pesastatud krüptovara kauplemise platvorm B müntide omandiõiguse ühele oma aadressidest, mida haldab *host-platvorm*. Kui Klient 2 vahetab 10 XYZ-münti viie ZYX-mündi vastu, teeb pesastatud krüptovara kauplemise platvorm B sama vahetuse *host-platvormiga*. *Host-platvorm* tuvastab, et tehingu teostab pesastatud krüptovara kauplemise platvorm B, kuid samal ajal puuduvad tal tunne oma klienti (*know your customer* - KYC) andmed ja tõhusad seirevõimalused Kliendi 2 suhtes.



**Joonis 2. Näide pesastatud krüptovara kauplemise platvormi tegevusest**

Oluline on märkida, et kuigi eespool toodud näited kirjeldavad lihtsustatud pesastatud teenuse osutamist, võivad pesastatud teenused olla ka oluliselt keerulisemad ja hõlmata mitmeastmelisi pesastatud teenuseid, sealhulgas tehingu mõlemal poolel.

Pesastatud krüptovara kauplemise platvormide kasutamine on funktsionaalselt sarnane krediitiasutuste korrespondentpanganduse teenuste või korrespondentkontode

kasutamiseks. Korrespondentpanganduses kaasab üks krediitiasutus (*vastuvõttev või respondentasutus*<sup>8</sup>) eraldiseisva krediitiasutuse (*korrespondent- või teenuseosutaja asutuse*), et sooritada piiriüleseid tehinguid või makseid või osutada teatavaid pangateenuseid, tavaliselt teises riigis. Nii nagu pesastatud krüptovara kauplemise platvormide puhul, on ka korrespondentpangandusteenused seaduslikud, kui vastuvõttev asutus ise ei paku samasuguseid pangateenuseid – nagu rahvusvahelised pangaülekanded, tšekkide arveldamine ja maksmine või välisvaluutas arveldamine –, kuid korrespondentasutus neid pakub. Nagu pesastatud krüptovara kauplemise teenused, võivad ka korrespondentpanganduse teenused vähendada finantsasutuste ja õiguskaitseasutuste võimet tuvastada ebaseaduslike rahaliste vahendite liikumist.<sup>9</sup> Seetõttu on Financial Action Task Force (FATF) soovitanud kehtestada mitmeid täiendavaid õiguslikke nõudeid korrespondentpangandussuhetele ja selgitanud 2019. aasta juhistes, et korrespondentpangandussuhete ennetusmeetmed võivad olla kohaldatavad ka pesastatud suhetele.<sup>10</sup>

## Analüüs

RAB vaatas üle enda valduses oleva finantsteabe pesastatud krüptovarateenuse osutajate kohta ja valis edasiseks analüüsiks välja 12 pesastatud krüptovara kauplemise platvormi. Analüüsiti ka plokiahelasiseseid (*on-chain*) ja -väliseid (*off-chain*) tehinguid,<sup>11</sup> kolmandate osapoolte plokiahela analüüsitarkvara<sup>12</sup> ja avalikke allikaid (OSINT).<sup>13</sup> RAB jälitas rohkem kui üheksat miljonit andmepunkti ja seiras tehinguid, mis liikusid tehingu algatajalt saajani pesastatud krüptovarateenuse osutajate kaudu. Lisaks võrdles RAB krüptovara kauplemise platvormide teadaolevate omanike, ettevõtete struktuuride ja litsentside kohta avalikult teadaolevaid andmeid infoga, mida erinevad osapooled on RAB-ile esitanud.

## Tähelepanekud ja tüpoloogiad

RAB täheldas, et kuigi tuvastatud pesastatud krüptovara kauplemise platvormid kasutasid pesastatud teenuste osutamiseks erinevaid mudeleid ja neil oli erinev kliendibaas, oli neil ühiseid struktuurilisi jooni, mis varjasid nende klientide tehingute tegelikku olemust ja eesmärki. RAB-i hinnangul võimaldasid pesastatud krüptovara kauplemise platvormid liigutada ebaseaduslikust tegevusest saadud rahalisi vahendeid. Mittetäielik loetelu näidetest:

- ❖ Mitmed krüptovara kauplemise platvormid löid keerulisi omandistruktuure või

<sup>8</sup> Vastuvõttev pank on mis tahes pank, mille jaoks teine pank loob, haldab, administreerib või juhib korrespondentkontosuheteid. Vt Bank for International Settlements, Correspondent Banking, „[2.1 Concept of correspondent banking](#)“ (2016).

<sup>9</sup> FATF „[Guidance on correspondent banking services](#)“ (2016), lk 9.

(„piiriüleseid korrespondentpangandussuheteid peetakse olemuselt riskantsemaks kui riigisiseseid korrespondentkliendisuheteid“).

<sup>10</sup> Vt üldiselt FATF, soovitus 10 ja 13 (2012–2023), „[International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation](#)“; FATF, „[Updated Guidance for a Risk-based Approach to Virtual Assets and VASPs](#)“ (2019).

<sup>11</sup> Plokiahelasisesed (*on-chain*) tehingud hõlmavad krüptovara otseülekandeid osapoolte vahel, kus need tehingud avalikult plokiahelas registreeritakse. Need tehingud kinnitatakse võrgustiku poolt konsensusmehhanismi kaudu, tagades plokiahela võrgustiku terviklikkuse ja turvalisuse. Seevastu plokiahelavälised (*off-chain*) tehingud on väärtuse ülekanded, mida vahendab kolmas osapool tagatisena või muude meetodite abil. Sellest hoolimata kajastuvad plokiahelavälised tehingud lõppkokkuvõttes plokiahelas lõppsaldo kujul.

<sup>12</sup> Kolmanda osapoole plokiahela analüüsitarkvara on abivahend, mis seostab andmeid plokiahelast ning muudest allikatest, et aidata tuvastada kõrvalekaldeid, võimalikke riske ja potentsiaalset ebaseaduslikku või kuritegelikku tegevust.

<sup>13</sup> Avalike allikate analüüs (OSINT) võib toetada näiteks riiklikku julgeolekut, õiguskaitset tegevust ja ärilisi otsuseid. OSINT uurib avalikke (avatud allikatest pärit) andmeid, mis on algselt kogutud ja avaldatud ühel eesmärgil, ning uuskasutab neid teisel eesmärgil, et tuua selgust varjatud nüanssidele. Vt European Union, European data, „[What is OSINT: Open-source intelligence?](#)“ (mai 2022).

rakendasid keerukaid tegevuspraktikaid, et varjata või hägustada: (i) jurisdiktsioone, kus nad tegutsesid; (ii) teenuste osutamiseks kasutatud juriidilisi isikuid; (iii) seda, kas ja millises jurisdiktsioonis olid nad litsentseeritud; ning (iv) osutatud teenuste liiki ja ulatust.

- ❖ Mitmed krüptovara kauplemise platvormid tegutsesid mitmeastmelise pesastamise kaudu, st väiksem pesastatud krüptovara kauplemise platvorm viis tehinguid läbi suurema pesastatud krüptovara kauplemise platvormi enne, kui tehing jõudis lõppsaajani. RAB ei suutnud tuvastada muud ärilist eesmärki, kui rahaliste vahendite päritolu tahtlikku varjamist.
- ❖ Mõnikord registreerisid väiksemad pesastatud krüptovara kauplemise platvormid end suurema platvormi juures jaekliendi või eraisikuna, mitte eraldiseisva juriidilise isikuna. See võib raskendada korrespondentteenust pakkuval krüptovara kauplemise platvormil rahapesu ja terrorismi rahastamise riskide hindamist. Põhjuseks on see, et pesastatud krüptovara kauplemise platvormi kavandatud tegevuse tegelikku olemust ei avalikustata. Samuti ei avalikustata klientide poolt pesastatud teenuses hoiustatavate rahaliste vahendite eeldatavat mahtu ja allikat ega esitata teavet ka muude riskide kohta, mis on seotud pesastatud krüptovara kauplemise platvormide tegutsemisega nende platvormil.
- ❖ Selle asemel, et teostada *oma äritegevust* täies mahus oma platvormi kaudu, näis, et mõned suuremad krüptovara kauplemise platvormid kasutasid korrespondentasutustes avatud pesastatud teenuseid. Selle tulemusel tuvastati, et plokiahelas omistati tehinguid ebatäpselt ehk korrespondentteenust pakkuvale *host*-platvormile, mitte tehingutes osalenud krüptovara kauplemise platvormile, mis tarbis pesastatud teenuseid.
- ❖ Mitmel krüptovara kauplemise platvormil, sealhulgas väiksematel pesastatud krüptovara kauplemise platvormidel ja suurematel *host*-platvormidel, ei paistnud olevat asjakohaseid AML/CFT-poliitikaid, -protseduure ja -kontrolle, et seirata nende taristu kaudu teostatavaid tehinguid. Ühtlasi ei paistnud, et nad oleksid rakendanud piisavat hoolsuskohustust oma klientide suhtes. Teatud juhtudel olid AML/CFT-poliitikad avaldatud küll nende platvormide veebilehel, kuid OSINT-andmed näitasid, et neid poliitikaid alati ei järgitud.
- ❖ Mõned *host*-platvormid osutasid kaudseid pesastatud teenuseid reguleerimata krüptovara kauplemise platvormidele, sealhulgas nendele, kes olid oma tegevusloa kaotanud rahapesu ja terrorismi rahastamise tõkestamise kohustuste rikkumise tõttu. See võib viidata ärisuhete, seehulgas respondentsuhete, puudulikule seirele.

## Näidisjuhtumid

RAB tuvastas andmetes mitu murettekitavat suundumust, mis näitasid, et mitu pesastatud krüptovara kauplemise platvormi olid seotud ka Venemaa ebaseadusliku finantstegevusega. Alltoodud näidisjuhtumid illustreerivad vaid mõningaid RAB-i poolt avastatud murettekitavaid toiminguid. Sealhulgas näitlikustavad nad *white-label* ja pesastatud krüptovara kauplemise platvormide arvu üldist kasvu jurisdiktsioonides, kus tegutsevad Venemaa või tema mõju all olevad krüptovara kauplemise platvormid ja muud teadaolevad pahatahtlikud üksused. Avalikud aruanded ja avalikest allikatest saadud teave kinnitasid, et pärast 2022. aastal alanud Venemaa täiemahulist sissetungi Ukrainasse, eriti pärast mobilisatsioonijärgset rändelainet Venemaalt välja, kasvas mitmetes teistes riikides Venemaal tegutsevate krüptovara kauplemise platvormide kioskite ja kullerite arv, kus sai vahetada krüptovara sularahaks või vastupidi.

### Näidisjuhtum nr 1

Pesastatud krüptovara kauplemise platvorm 1 (NX1) oli Kasahstanis registreeritud krüptovarateenuse osutaja, millel olid kontorid Kasahstanis, Kõrgõzstanis, Venemaal ja Ukrainas. NX1 vahetas krüptovara, kuid aktsepteeris ka pangatehinguid fiat-valuutas (USA dollarid, Kasahstani tenged, Venemaa rublad ja Kõrgõzstani somid). NX1 osutas klientidele oma veebisaidil teenuseid ja suhtles klientidega sotsiaalmeedias ja mitmes foorumis, mis olid peamiselt venekeelsed. Enamik Kasahstani panku aktsepteeris NX1 tehinguid, samuti tegid seda mitmed pangad ja makseteenuste pakkujad teistes jurisdiktsioonides. Analüüs näitab, et enamik NX1 rahakotiaadressidest kuulus klastrisse<sup>14</sup>, mis oli seotud suurema krüptovara kauplemise platvormiga (EX1). See suurem platvorm oli omakorda pesastatud teise krüptovara kauplemise platvormi (EX2) juures.<sup>15</sup> EX2 osutas osa krüptovarateenustest omakorda läbi respondentsuhete mitme suurema ja globaalselt tuntud krüptovara kauplemise platvormi juures. Enne lõppsihtkohta jõudmist läbisid selle struktuuri tõttu paljud NX1 klientide tehingud mitu kihti. Seepärast varjasid paljud neist tehingutest tegelikku algatajat ja saajat, kui neil puudus nähtav seaduslik äriiline eesmärk.

### Näidisjuhtum nr 2

Pesastatud krüptovara kauplemise platvorm 2 (NX2) oli Ukrainas asuv krüptovarateenuse osutaja. Hoolimata sellest, et NX2 tegutses krüptovara kauplemise platvormina, oli ta host-platvormi EX3 kliendina registreeritud kui eraisik. NX2 oli minimaalse veebijäljega ja OSINT-teave ei viidanud sellele, et ta oleks osutanud krüptovarateenuseid. Samas näitas tehingute analüüs plokiahelas, et NX2 kaudu toimuva kauplemistegevuse maht ja liik viitas isikliku kasutamise asemel ärilisele kasutamisele. Näiteks tegi NX2 tuhandeid tehinguid suure hulga vastaspooltega. Üldiselt oli iga tehingu keskmine väärtus madal, kuid tehingute kogumaht ulatus kümnetesse miljonitesse dollaritesse. Plokiahela analüüs viitas NX2 tehingute seosele mitmete hasartmänguplatvormide, teiste krüptovarateenuse osutajate ja maksevahendajatega.

### Näidisjuhtum nr 3

Pesastatud krüptovara kauplemise platvorm 3 (NX3) oli krüptovarateenuse osutaja, kes pakkus oma klientidele krüptovara sularahaks ja vastupidi vahetamise OTC teenuseid<sup>16</sup>. NX3 tegevuskohad asusid Venemaal, kuid ta väitis, et asub Tšehhis. NX3 kasutas klientidega suhtlemiseks sotsiaalmeediat ja reklaamis avalikult oma äärmiselt tagasihoidlikke KYC-(tunne oma klienti) hoolsusmeetmeid. NX3 pesastas oma tegevuse, avades oma kasutajakontod suuremate krüptovara kauplemise platvormide (sh esimese juhtuminäite EX2) juures, et kaubelda oma klientide nimel. RAB-i analüüs näitab, et mõned rahakotiaadressid olid otseselt kuritegevusega seotud ning NX3 teostas tehinguid Venemaa

<sup>14</sup> Termin „klaster” viitab plokiahela analüüsis omavahel seotud või grupeeritud tegevusele või käitumisele. Klaster võib tähendada osapoolte rühma, kes teevad tehinguid koos, kelle tegevusmustrid kattuvad, keda seostatakse avalike allikate või analüütilise teabe kaudu või kes on muul viisil omavahel ühendatud.

<sup>15</sup> EX2 tuvastas hoolsusmeetmete rakendamise käigus valesi, et NX1 puhul on tegemist jaekliendist üksikisikuga, mitte krüptovara kauplemise platvormiga, kuigi EX2 valduses olevast teabest nähtus, et NX1 tegutses krüptovarateenuse osutajana.

<sup>16</sup> Krüptovara käest-kätte kauplemine (*over the counter* – OTC) on protsess, mille käigus kaks osapoolt ostavad ja müüvad krüptovara otse üksteiselt. OTC-teenused tagavad krüptovara ökosüsteemis likviidsuse, võimaldades krüptovara üksikasutajatel teha suuri tehinguid krüptovarade vahel või krüptovarast fiat-valuutasse, leevendades samal ajal hinnakõikumisi.

pankadega. Lisaks toimisid mõned rahakotiaadressid transiitkontodena, kuhu laekus ja kust viivimatult kanti edasi identne summa krüptovara.

#### Case Study #4

Pesastatud krüptovara kauplemise platvorm 4 (NX4) oli Leedus asuv veebis tegutsev krüptovarateenuse osutaja, millel oli oma veebileht. NX4 pakkus oma klientidele võimalust vahetada fiat-valuutat krüptovaraks ja vastupidi Venemaal asuvates pankades. Samuti võimaldas see tema klientidel osta krüptovara krediitkaardiga, sealhulgas rahvusvaheliselt tegutsevate suurte finantsasutuste kaudu. NX4 lubas oma klientidele kiiret tehingute töötlemist (kahe tunni jooksul). Analüüs näitas, et NX4 osutas pesastatud teenuseid teistele krüptovara kauplemise platvormidele, mis olid tuntud kahtlaste tehingute töötlemise poolest, ning lisaks sellele näitas plokiahel otseseid tehinguid tumeveebi turgudega. RAB-i kogus täiendavat teavet, mis näitas, et NX4 rahapesu ja terrorismi rahastamise tõkestamise poliitika ei vastanud tema äritegevuse riskiprofiilile. Ilmnes, et NX4 varjas tahtlikult oma tegelikke andmeid ning jättis mainimata oma asukohariigi, kus ta oli registreeritud või litsentseeritud krüptovarateenuste osutamiseks. RAB-i analüüs näitas, et vaid pooleteise tegevusaasta jooksul oli NX4 töödeldud krüptovara väärtuses üle 6,5 miljoni USA dollari.

## Pesastatud teenuste tunnused ja ohumärgid

Analüüsi käigus tuvastas RAB mitmeid ohumärke, mis olid seotud ebaseaduslike pesastatud krüptovara kauplemise platvormidega. Regulatsioone järgivatel krüptovarateenuse osutajatel ja finantsasutustel võivad need ohumärgid raskendada KYC-protseduuride rakendamist oma klientide suhtes, kelmuseohvritel oma õiguste kaitsmist või tarbijaõiguste kasutamist, järelevalveasutustel tõhusa järelevalve teostamist krüptovarateenuste osutajate üle ning õiguskaitseasutustel uurimiste läbiviimist. Kuna ükski eraldiseisev ohumärk ei viita tingimata ebaseaduslikule või kahtlasele tegevusele, peaksid krüptovarateenuse osutajad ja finantsasutused arvestama kõigi seonduvate faktide ja asjaoludega enne konkreetse tehingu kahtlaseks määramist.

### Juriidilise isiku omandisuhetega seotud ohumärgid

Ohumärgid, mis viitavad pesastatud krüptovara kauplemise platvormile või krüptovarateenuse osutajale, mis on kuritegeliku taustaga isikute omanduses, halduses või kontrolli all:

- ❖ *Omandisuhted või finantssidemeid riikliku taustaga isikute (PEP) või kuritegeliku taustaga isikutega.*
- ❖ *Katsed eraldada ühe äriüksuse erinevad osad õigusliku või finantsilise vastutuse tõttu.*
- ❖ *Õiguslikud või nõuetele vastavust käsitlevad dokumendid on ebamäärased või suunavad kirjavahetuse „seaduslikule esindajale” või muule volitatud kolmandale isikule.*
- ❖ *Ettevõtte andmete varjamine kasutades sealhulgas varifirmasid, nominaalosanikke, registreeritud esindajaid ning mass- ja virtuaaladresse tegevuskoha aadressina.*
- ❖ *Ühel ettevõttel on mitmed kasutajakontod sama krüptovarateenuse osutaja juures ning neil on suured oma kontode vahelised ja välised tehingumahud.*

## Erinevate (asukoha)riikidega seonduvad ohumärgid

Ohumärgid, mis viitavad püüdlustele vältida tugeva järelevalve või õiguskaitsesega jurisdiktsioone:

- ❖ *Tegutsemine riikides või territooriumitel, mida loetakse kõrgema riskiga piirkondadeks. Näiteks piirkonnad, kus puudub krüptovarateenuse osutajatega seonduv regulatsioon.*
- ❖ *Ärimudelid, mis on loodud range finantsjärelevalvega klientide või riikide ja territooriumite vältimiseks.*
- ❖ *Tsentraalselt mitte hallatava (non-hosted) taristu või selle majutusteenuse kasutamine riikides või territooriumitel, mida loetakse kõrgema riskiga piirkondadeks, või kõrgema riskiga hostimisteenuste kasutamine.*
- ❖ *Ettevõtte asukoha-, registreerimis- ja litsentseerimisriigi varjamine teenuse kasutustingimustes, veebilehel, rakenduses ja sotsiaalmeedias.*
- ❖ *Sage registreerimis- ja litsentseerimisriigi muutmine. Seejuures on võimalik, et proovitakse vältida litsentseerimist või otsitakse leebema järelevalvega piirkonda.*

## Riskijuhtimisega seonduvad ohumärgid

Pesastatud teenuse puudulikele riskijuhtimise protseduurireeglitele ja kontrollidele viitavad ohumärgid hõlmavad muu hulgas:

- ❖ *Krüptovara kauplemise platvorm ei pruugi tuvastada, et klient kasutab oma kontot ärieesmärkidel. Samuti võib klient tegutseda krüptovara kauplemise valdkonnas ilma nõutud tegevusloata.*
- ❖ *„Kopeeri ja kleebi” tüüpi riskijuhtimise mudeli ja protseduurireeglite dokumendid, mis võivad viidata „white label”<sup>17</sup> teenusepakkujatele või sellistele krüptovara kauplemise platvormidele, mis ei kohalda piisavaid hoolsusmeetmeid.*
- ❖ *Krüptovara kauplemise platvormil puuduvad AML/CFT-hoolsusmeetmeid kirjeldavad dokumendid.*
- ❖ *Reklaamid, mis rõhutavad nõrku või olematuid KYC-kontrolle ja kliendiandmete talletamist.*

## Plokiahela ja teenustega seotud ohumärgid

Ohumärgid, mis viitavad sellele, et krüptovara kauplemise platvorm võib vahendada ebaseaduslikke tehinguid:

- ❖ *Pakub arveldusmehhanisme, mis kasutavad suures koguses sularaha, kinkekaarte või muid esitajapõhiseid varasid.*
- ❖ *Pakub arveldamist kõrgema riskiga finantsasutuste kaudu, mis on seotud sanktsioneeritud riikide, territooriumite, finantsasutuste ja isikutega. Need finantsasutused võivad olla riikides või territooriumitel, kus krüptovara kauplemise platvorm väidab end mitte tegutsevat.*
- ❖ *Pakub või aktsepteerib fiat-valuutat riikides ja piirkondades, mida loetakse kõrgema riskiga territooriumiteks, või sellistes riikides ja piirkondades, mida krüptovara kauplemise platvorm väidab mitte teenindavat.*
- ❖ *Võtab vastu või teostab tehinguid plokiahelas olevate kõrge riskiga isikutega, näiteks aadressidega, mis on seotud lunavara, tumeveebi turgude, sanktsioneeritud isikute või terrorismi rahastamisega.*

---

<sup>17</sup> *White label* virtuaalvaluuta vahetus viitab varasemalt loodud rakendusele või kauplemisplatvormile, mida platvormi operaator saab soetada karbitootena ja kohandada, et käivitada enda krüptovara kauplemise teenus. Need karbitootedeks loodud ja põgusalt kohandatavad rakendused ja platvormid on sisuliselt valmis krüptovara kauplemise platvormid, mille võivad isikud osta selle asemel, et arendada ise välja oma krüptovara kauplemise rakendus või platvorm.

- ❖ *Võimaldab või teostab kiirkorras või suure väärtusega transiitülekandeid (st pakub transiit- ehk läbivoolukontosid).*
- ❖ *Ainult ühe vastaspoolega toimuvad tehingud võivad viidata sellele, et pesastatud krüptovara kauplemise platvorm toimib ebaseadusliku rahakogumise kanalina või rahamuula teenusena.*